AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00334	8/29/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
LIONRA TECHNOLOGIES LIMITED	PALO ALTO NETWORKS, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,685,436	3/23/2010	Lionra Technologies Limited
2	8,566,612	10/22/2013	Lionra Technologies Limited
3	7,921,323	4/5/2011	Lionra Technologies Limited
4			
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Print Save As... Reset

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-00322	8/19/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
LIONRA TECHNOLOGIES LIMITED	FORTINET, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,302,708	11/27/2007	Lionra Technologies Limited
2	7,685,436	3/23/2010	Lionra Technologies Limited
3	7,921,323	4/5/2011	Lionra Technologies Limited
4	8,566,612	10/22/2013	Lionra Technologies Limited
5			

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Print Save As... Reset

AO 120 (Rev. 08/10)

TO:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:22-cv-305	8/8/2022	Eastern District of Texas

PLAINTIFF	DEFENDANT
LIONRA TECHNOLOGIES LIMITED	CISCO SYSTEMS, INC.

	PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1	7,916,630	3/29/2011	Lionra Technologies Limited
2	8,566,612	10/22/2013	Lionra Technologies Limited
3	7,921,323	4/5/2011	Lionra Technologies Limited
4	7,302,708	11/27/2007	Lionra Technologies Limited
5	7,685,436	3/23/2010	Lionra Technologies Limited

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director **Copy 3—Upon termination of action, mail this copy to Director**
Copy 2—Upon filing document adding patent(s), mail this copy to Director **Copy 4—Case file copy**

Print Save As... Reset

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	REQUEST ID
10/903,785	7685436	2436	16387

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 140558 on 04/25/2016 via Private PAIR in view of the certification copied below that authorized the change.

- Correspondence Address

The address for Customer Number 140558 is:
140558
Davidson, Berquist, Jackson & Gowdey LLP
Harris Corporation
8300 Greensboro Drive
Suite 500
McLean, VA 22102

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Kimani Clark/
Name:	Kimani Clark
Registration Number:	45969

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	REQUEST ID
10/903,785	7685436	2436	16387

PAIR Correspondence Address/Fee Address Change

The following fields have been changed to Customer Number 140558 on 04/25/2016 via Private PAIR in view of the certification copied below that authorized the change.

- Maintenance Fee Address

The address for Customer Number 140558 is:
140558
Davidson, Berquist, Jackson & Gowdey LLP
Harris Corporation
8300 Greensboro Drive
Suite 500
McLean, VA 22102

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

An attorney or Agent of Record registered to practice before the Patent and Trademark Office who has been given power of attorney in this application

Signature:	/Kimani Clark/
Name:	Kimani Clark
Registration Number:	45969

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/903,785	03/23/2010	7685436	2551-0032	4954

42624 7590 03/03/2010

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 830 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

John M. Davis, Brentwood, TN;
Richard J. Takahashi, Phoenix, AZ;

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 4954

SERIAL NUMBER	FILING OR 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/903,785	07/30/2004 RULE	713	2436	2551-0032

APPLICANTS

John M. Davis, Brentwood, TN;
Richard J. Takahashi, Phoenix, AZ;

**** CONTINUING DATA ***************************

This appln claims benefit of 60/507,976 10/02/2003

**** FOREIGN APPLICATIONS *********************

IF REQUIRED, FOREIGN FILING LICENSE GRANTED
** 10/04/2004

Foreign Priority claimed	STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
☐ yes ☐ no	TN	10	29	4
35 USC 119 (a-d) conditions met ☐ yes ☐ no ☐ Met after Allowance				
Verified and Acknowledged _____ Examiner's Signature Initials				

ADDRESS
42624

TITLE

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

FILING FEE RECEIVED		
874	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

42624 7590 11/03/2009

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/903,785	07/30/2004	John M. Davis	2551-0032	4954

TITLE OF INVENTION: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	02/03/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRAORE, FATOUMATA	2436	713-192000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 Davidson Berquist
2 Jackson & Gowdey, LLP
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: ITT Manufacturing Enterprises, Inc.
(B) RESIDENCE: (CITY and STATE OR COUNTRY): Wilmington, DE

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☒ Issue Fee
☒ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 501860 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
☒ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date February 1, 2010

Typed or printed name Kimani Clark Registration No. 45,969

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	10903785
Filing Date:	30-Jul-2004
Title of Invention:	SYSTEM AND METHOD FOR A SECURE I/O INTERFACE
First Named Inventor/Applicant Name:	John M. Davis
Filer:	Kimani Clark
Attorney Docket Number:	2551-0032

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1510	1510
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**1810**

Electronic Acknowledgement Receipt

EFS ID:	6919823
Application Number:	10903785
International Application Number:	
Confirmation Number:	4954
Title of Invention:	SYSTEM AND METHOD FOR A SECURE I/O INTERFACE
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Kimani Clark
Filer Authorized By:	
Attorney Docket Number:	2551-0032
Receipt Date:	01-FEB-2010
Filing Date:	30-JUL-2004
Time Stamp:	13:51:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1810
RAM confirmation Number	137
Deposit Account	501860
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.11

1	Issue Fee Payment (PTO-85B)	Issue_Fee_Transmittal_2551-0032_12-1-10.pdf	262811 5d12b80385b522753db0509422ca608cf5d6fb67	no	1
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	31831 5284d4cbb5f39082435db7f3c5e9a56ad15bc5a1	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	294642		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

42624 7590 11/03/2009

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 11/03/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/903,785	07/30/2004	John M. Davis	2551-0032	4954

TITLE OF INVENTION: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	02/03/2010

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.13

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

42624 7590 11/03/2009

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/903,785	07/30/2004	John M. Davis	2551-0032	4954

TITLE OF INVENTION: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$755	$300	$0	$1055	02/03/2010

EXAMINER	ART UNIT	CLASS-SUBCLASS
TRAORE, FATOUMATA	2436	713-192000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/903,785	07/30/2004	John M. Davis	2551-0032	4954

42624 7590 11/03/2009

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2436	

DATE MAILED: 11/03/2009

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 454 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 454 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.15

Notice of Allowability	Application No.	Applicant(s)	
	10/903,785	DAVIS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *communications filed on 10/06/2009 and telephonic interview on 10/29/2009*.

2. ☒ The allowed claim(s) is/are *1-3, 5, 7-9, 11, 12, 14-22, 30-33*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.16

Examiner-Initiated Interview Summary	Application No.	Applicant(s)	
	10/903,785	DAVIS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

All Participants:

(1) *FATOUMATA TRAORE*.

(2) *KIMANI CLARK, Reg. No. 45,969*.

Status of Application: _____

(3) _____.

(4) _____.

Date of Interview: *29 October 2009*

Time: *3:00PM*

Type of Interview:
☒ Telephonic
☐ Video Conference
☐ Personal (Copy given to: ☐ Applicant ☐ Applicant's representative)

Exhibit Shown or Demonstrated: ☐ Yes ☐ No
If Yes, provide a brief description: .

Part I.

Rejection(s) discussed:
N/A

Claims discussed:
Claims 1, 6, 14

Prior art documents discussed:
N/A

Part II.

SUBSTANCE OF INTERVIEW DESCRIBING THE GENERAL NATURE OF WHAT WAS DISCUSSED:
The examiner contacted Applicant's representative, Kimani Clark (Reg. No. 45,969), to get authorization to amend claims 1 and 14 and to cancell claims 6 and 34 in order to put the appfication in condition of allowance

Part III.

☐ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview directly resulted in the allowance of the application. The examiner will provide a written summary of the substance of the interview in the Notice of Allowability.
☐ It is not necessary for applicant to provide a separate record of the substance of the interview, since the interview did not result in resolution of all issues. A brief summary by the examiner appears in Part II above.

(Applicant/Applicant's Representative Signature – if appropriate)

DETAILED ACTION

1. This is in response to the amendment filed October 6, 2009. Claims 1, 5 and 14 have been amended. Claims 4, 10, 13, 23-29 have been cancelled. Claims 1-3, 5-9, 11-12, 14-22 and 30-34 are pending and have been considered below.

Response to Arguments

2. Applicant's arguments filed 04/27/2009 with respect to the prior art rejection of the claims have been fully considered and they are persuasive.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Kimani Clark Reg. No. 45,969 on 10/29/2009.

The application has been amended as follows:

Amend Claims 1, 5 and 14:

1. (Currently Amended) A security processor to process incoming packets and outgoing packets, the security processor comprising:

a switching system to send the outgoing packets and receive the incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a

plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming packets and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

5. (Amended) The security processor of claim [[4]] 1 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

14. (Currently Amended) A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing packets and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming packets and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming and outgoing packets are provided

with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core;

a cryptographic core, coupled to the packet engine and receiving the incoming packets from the switching system via the packet engine and communicating the outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

Cancel claims 6 and 34

Allowance

4. Claims 1-3, 5, 7-9, 11, 12, 14-22 and 30-33 are allowed.

Examiner's Statement of Reason for allowance

5. The following is an examiner's statement of reasons for allowance:

Narad et al (US 6,157,955) is relates to a general-purpose programmable packet-processing platform for accelerating network infrastructure applications which have been structured so as to separate the stages of classification and action. Network packet classification, execution of actions upon those packets, management of buffer flow, encryption services, and management of

Network Interface Controllers are accelerated through the use of a multiplicity of specialized modules. A language interface is defined for specifying both stateless and stateful classification of packets and to associate actions with classification results in order to efficiently utilize these specialized modules..

Wu et al (US 7,493,659) is directed to intrusion detection and analysis system and method are disclosed. The system includes a data-monitoring device comprising a capture engine operable to capture data passing through the network and configured to monitor network traffic, decode protocols, and analyze received data. The system further includes an intrusion detection device comprising a detection engine operable to perform intrusion detection on data provided by the data-monitoring device. Application program interfaces are provided and configured to allow the intrusion detection device access to applications of the data-monitoring device to perform intrusion detection. The system also includes memory for storing reference network information used by the intrusion detection device to determine if an intrusion has occurred.

Savarda et al (US 2003/0196091) is directed to a packet is processing by encapsulating the packet with a packet-object header if the packet does not have a packet-object header. The encapsulated packet is processed based on information contained in the packet-object header using a plurality of transform modules that are coupled to each other in a series or pipeline configuration. The plurality of transform modules process the encapsulated packet independent of each other.

6. The prior art of record taken alone or in combination do not teach or render obvious the limitations as recited in independent claims 1 and 14. The cited references, whether alone or in combination fail to disclose or suggest the following limitation : *" a packet engine, coupled to*

the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines, and wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines an egress path within the security processor upon exit from a corresponding cryptographic core; a cryptographic core, coupled to the packet engine and receiving incoming packets from the switching system via the packet engine and communicating outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core; a signature database; and an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database"

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to FATOUMATA TRAORE whose telephone number is (571)270-1685. The examiner can normally be reached on Monday- Friday (every other Friday off) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Thursday October 29, 2009.

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	**Art Unit**
	FATOUMATA TRAORE	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/25/2007	04/04/2008	10/20/2008	07/16/2009	10/29/2009				
1	1	✓	✓	✓	✓	=				
2	2	✓	✓	✓	✓	=				
3	3	✓	✓	✓	✓	=				
	4	✓	✓	✓	O	-				
9	5	✓	✓	✓	✓	=				
	6	✓	✓	✓	O	-				
4	7	✓	✓	✓	✓	=				
5	8	✓	✓	✓	✓	=				
6	9	✓	✓	✓	✓	=				
	10	✓	✓	✓	-	-				
7	11	✓	✓	✓	✓	=				
8	12	✓	✓	✓	✓	=				
	13	✓	-	✓	-	-				
13	14	✓	✓	✓	✓	=				
14	15	✓	✓	✓	✓	=				
15	16	✓	✓	✓	✓	=				
16	17	✓	✓	✓	✓	=				
17	18	✓	✓	✓	✓	=				
18	19	✓	✓	✓	✓	=				
19	20	✓	✓	✓	✓	=				
20	21	✓	✓	✓	✓	=				
21	22	✓	✓	✓	✓	=				
	23	✓	✓	✓	✓	-				
	24	✓	✓	✓	✓	-				
	25	✓	✓	✓	✓	-				
	26	✓	-	-	-	-				
	27	✓	-	-	-	-				
	28	✓	-	-	-	-				
	29	✓	-	-	-	-				
10	30			✓	✓	=				
11	31			✓	✓	=				
12	32				✓	=				
22	33				✓	=				
	34				✓	-				

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.24

OK TO ENTER: /F.T./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:		Confirmation No.:	4954
DAVIS, John M., et al		Attorney Docket:	2551-0032
Appl. S.N.:	10/903,785	Group Art Unit:	2436
Filing Date:	July 30, 2004	Examiner:	TRAORE, Fatoumata
Title:	**SYSTEM AND METHOD FOR A SECURE I/O INTERFACE**	Date:	August 28, 2009

AMENDMENT AFTER FINAL

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Final Office Action mailed July 20, 2009, Applicants request that the application be amended as follows:

Amendments to the claims are reflected in the listing of the claims which begins on page 2; and

Remarks begin on page 7.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	4	"20040177262".pn. "6643451".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 13:39
L2	3099	(switch$3 control$4) same packet same (classificat$3 classif$3 group$3 caterorizat$3 caterogisat$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 13:44
L3	4651	713/153.ccls. 713/160.ccls. 713/192.ccls. 713/193.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 13:44
L5	16	2 and 3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 13:45
L6	103	(processor microprocess $3) same packet same (classificat$3 classif$4) same (select$3 enabl $3 switch$3) same (cryptographic encrypt $3 encod$3 steganography mask$3 obsficat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 14:09
L7	1	6 AND 3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 14:17
L8	6	"6157955".pn. "7493659".pn. "20030196081".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/29 14:53

S1	16	packet with classificat $3 with polic$3 with (cryptograph$3 or crypto or encrypt$3 or decrypt)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/19 12:41
S2	1942	packet and classificat $3 and polic$3 and (cryptograph$3 or crypto or encrypt$3 or decrypt) and (switch$3 or rout$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 13:50
S3	13	(packet and classificat $3 and polic$3 and (cryptograph$3 or crypto or encrypt$3 or decrypt) and (switch$3 or rout$3)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 13:51
S4	0	(packet same classificat $3 same polic$3 same (cryptograph$3 or crypto or encrypt$3 or decrypt) same (switch $3 or rout$3)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 14:02
S5	30	(packet same classificat $3 same polic$3 same (cryptograph$3 or crypto or encrypt$3 or decrypt) same (switch $3 or rout$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 14:02
S6	132	(packet same classificat $3 same polic$3 same (cryptograph$3 or crypto or encrypt$3 or decrypt$ or securit$3) same (switch$3 or rout $3 or buffer or input or port))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 14:12
S7	201	("5764645").PN. OR ("6157955").URPN.	US-PGPUB; USPAT; USOCR	ADJ	ON	2008/10/20 16:21
S8	12	S2 and S7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 16:22
S9	6	"6983366".pn. or "20040010545".pn. or "20030014627".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 17:18

S10	0	packet adj engine near9 switch$3 adj system near9 (cryptographic encrypt $3 encod$3 steganography) near9 intrusion adj detect$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/06/03 08:52
S11	0	packet adj engine near9 switch$3 adj system near9 (cryptographic encrypt $3 encod$3 steganography) near9 intrusion adj detect$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:52
S12	0	packet near9 (classificat $3 classif$4) near9 switch$3 near9 (cryptographic encrypt $3 encod$3 steganography) near9 intrusion adj detect$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:53
S13	0	packet near9 (classificat $3 classif$4) near9 switch$3 near9 (cryptographic encrypt $3 encod$3 steganography) near9 intrusion	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:54
S14	2	packet near9 (classificat $3 classif$4) near9 switch$3 near9 (cryptographic encrypt $3 encod$3 steganography)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:54
S15	40	processor same packet same (classificat$3 classif$4) same switch $3 same (cryptographic encrypt $3 encod$3 steganography)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:57
S16	52	security near4 processor same intrusion adj detect$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 10:50

S17	9	secur$3 adj processor near9(traffic near4 flow span$4 manag$3 intrusion near3 dtect $3) near6 packet	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:08
S18	317	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:46
S19	0	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet near9 signature near9 (match $3 compar$3 identif$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:47
S20	0	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet near9 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:48
S21	2	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet near9 (cryptographc encrypt $3 encipher$3 encod $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:49
S22	2	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet near9 (cryptographic encrypt $3 encipher$3 encod $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:49
S23	184	713/192.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 14:02

S24	96099	packet and switch$3 and (cryptographic encrypt$3 encipher$3 encod$3 intrusion near3 detect$3 traffic near3(flow analyz$3 spann$3 manag$3) polic$3 signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 14:05
S25	31	S23 and S24	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 14:06
S27	0	hash near9 intrusion near S11 detection near6 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/06/03 17:21
S28	0	hash near9 intrusion near2 detection near6 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/06/03 17:21
S29	0	hash near9 intrusion adj detection near6 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 17:22
S30	244261	hash$3 near9 intrusion adj detectionand signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 17:22
S31	0	hash$3 near9 intrusion adj detectionand and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 17:22
S32	6	hash$3 near9 intrusion adj detection and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 17:22

S33	0	security near6 processor and packet near4 (engine unit classif$4 classificat$3) and (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/07/16 16:14
S34	0	packet near4 (engine unit classif$4 classificat $3) same (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/07/16 16:15
S35	220	packet near4 (engine unit classif$4 classificat $3) same (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/16 16:15
S36	131	security near6 processor and packet near4 (engine unit classif$4 classificat$3) and (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/16 16:15
S37	30	security near6 processor same packet near4 (engine unit classif$4 classificat$3) and (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/16 16:15
S38	41	security near6 processor and packet near4 (engine unit classif$4 classificat$3) same(intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/16 16:25
S54	4639	713/153.ccls. 713/160. ccls. 713/192.ccls. 713/193.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/23 16:36

S55	254	(switch$3 control$4 select$3 chang$3 swap $4 exchang$3) near5 (system device module program component) same Packet near5 (engine device component system) same (classif$4 classificat$3 categorizat $3 categorisat$3 categoriz$3 group$3 sort$3) same (crypto cryptograph$3 encrypt $3 encod$3 decrypt$3 scrambl$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/23 16:45
S56	5	S54 and S55	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/23 16:47
S59	42	((swich$3 control$4) same packet same (classificat$3 classif$3 group$3 caterorizat$3 caterogisat$3) same (cryptograph$3 encrypt $3 decrypt$3)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/23 16:50
S60	24920	(switch$3 control$4) same packet same (classificat$3 classif$3 group$3 caterorizat$3 caterogisat$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/23 16:59
S61	4	((switch$3 control$4) same packet same (classificat$3 classif$3 group$3 caterorizat$3 caterogisat$3)).ab. and S54	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/10/23 17:00

10/29/2009 4:33:13 PM
C:\Documents and Settings\ftraore\My Documents\EAST\Workspaces\10903785_securelOinterfaceafterRCE.wsp

Issue Classification

Application/Control No.	Applicant(s)/Patent Under Reexamination
10903785	DAVIS ET AL.
Examiner	**Art Unit**
FATOUMATA TRAORE	2436

ORIGINAL		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
713	192	H 0 4 L 29 / 06 (2006.01.01)	
		G 0 6 F 9 / 02 (2006.01.01)	
		G 0 6 F 12 / 14 (2006.01.01)	

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
713	153	160	193		

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	16	17	22	33										
2	2	17	18		34										
3	3	18	19												
	4	19	20												
9	5	20	21												
	6	21	22												
4	7		23												
5	8		24												
6	9		25												
	10		26												
7	11		27												
8	12		28												
	13		29												
13	14	10	30												
14	15	11	31												
15	16	12	32												

/FATOUMATA TRAORE/ Examiner.Art Unit 2436	10/30/2009	**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	22	
/NASSER G MOAZZAMI/ Supervisory Patent Examiner.Art Unit 2436	10/29/2009	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	14	2

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	**Art Unit**
	Traore, Fatoumata	2436

SEARCHED			
Class	**Subclass**	**Date**	**Examiner**
713	189, 160, 151, 153, 168 limited text search	07/25/2007	FT

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
EAST searchattached	07/24/2007	FT
EAST Search performed	04/03/2008	FT
EAST search performed	10/19/2008	FT
EAST search performed and consulted with TRUONG THANHNGA B	07/16/2009	FT
EAST seach performed	08/24/2009	FT

INTERFERENCE SEARCH			
Class	**Subclass**	**Date**	**Examiner**
713	153, 160, 192, 193 limited text search	10/24/2009	FT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:		Confirmation No.:	4954
DAVIS, John M., et al		Attorney Docket:	2551-0032
Appl. S.N.:	10/903,785	Group Art Unit:	2436
Filing Date:	July 30, 2004	Examiner:	TRAORE, Fatoumata
Title:	**SYSTEM AND METHOD FOR A SECURE I/O INTERFACE**	Date:	August 28, 2009

AMENDMENT AFTER FINAL

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Final Office Action mailed July 20, 2009, Applicants request that the application be amended as follows:

Amendments to the claims are reflected in the listing of the claims which begins on page 2; and

Remarks begin on page 7.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A security processor to process incoming and outgoing packets, the security processor comprising:

a switching system to send and receive packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines;

a cryptographic core, coupled to the packet engine and receiving incoming packets from the switching system via the packet engine and communicating outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

2. (Original) The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

3. (Original) The security processor of claim 1 further comprising:

a local data bus coupled to the switching system; and

a modulo engine coupled to the local data bus.

4. (Canceled)

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.36

5. (Amended) The security processor of claim [[4]] 1 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

6. (Amended) The security processor of claim [[4]] 1 wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the corresponding one of the plurality of cryptographic cores.

7. (Original) The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

8. (Original) The security processor of claim 7 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

9. (Original) The security processor of claim 7 further comprising a key management engine coupled to the local data bus.

10. (Canceled).

11. (Original) The security processor of claim 7 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

12. (Original) The security processor of claim 11 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

13. (Canceled).

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.37

14. (Currently Amended) A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system, wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines;

a cryptographic core, coupled to the packet engine and receiving incoming packets from the switching system via the packet engine and communicating outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

15. (Original) The security processing system of claim 14 further comprising a modulo engine coupled to the local data bus.

16. (Original) The security processing system of claim 15 further comprising a key management engine coupled to the local data bus.

17. (Original) The security processing system of claim 14 wherein the memory and the security processor are within the same cryptographic boundary.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.38

18. (Original) The security processing system of claim 14 wherein the security processor is formed on a single chip.

19. (Original) The security processing system of claim 14 further comprising:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

20. (Original) The security processing system of claim 19 wherein the translator performs steganographic translation of the received data.

21. (Original) The security processing system of claim 19 wherein the translator performs encryption translation of the received data.

22. (Original) The security processing system of claim 14 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

23-29. (Canceled)

30. (Previously Presented) The security processor of claim 1 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.

31. (Previously Presented) The security processor of claim 1 wherein the packet engine is further operable to remove an IP header from the incoming packets.

32. (Previously Presented) The security processor of claim 1, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.39

33. (Previously Presented) The security processing system of claim 14, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

34. (Previously Presented) The security processor of claim 23, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.40

REMARKS

Claims 1-3, 5-9, 11-12, 14-25 and 30-33 are pending in the application. Applicants thank the Examiner for the indication of allowance of claims 4 and 6 (Office Action dated July 20, 2009, p. 12). In response, Applicants have amended claims 1 and 14 to include the indicated allowable limitations of claim 4. Applicants have canceled claims 4, 23-25 and 34 without prejudice, and amended claims 5 and 6 to depend from claim 1 (which now includes the limitations of claim 4) instead of claim 4. Pending claims 2-3, 5-9, 11-12, 15-22 and 30-33 depend from claims 1 and 14 which include the indicated allowable limitations of claim 4, and as such, those claims are also allowable. Accordingly, the application should be in condition for allowance, and Applicants respectfully request the timely issuance of a Notice of Allowance.

CHARGE STATEMENT: Deposit Account No. 501860, order no. **2551-0032**.
The Commissioner is hereby authorized to charge any fee specifically authorized herein (including the one-month extension of time), or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.
This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER



Respectfully submitted,

By: 

Kimani Clark
Registration No.: 45,969

Davidson Berquist Jackson & Gowdey LLP
Phone: 703.894.6400
Fax: 703.894.6430

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.41

Electronic Acknowledgement Receipt

EFS ID:	6207519
Application Number:	10903785
International Application Number:	
Confirmation Number:	4954
Title of Invention:	System and method for a secure I/O interface
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Kimani Clark
Filer Authorized By:	
Attorney Docket Number:	2551-0032
Receipt Date:	06-OCT-2009
Filing Date:	30-JUL-2004
Time Stamp:	11:03:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment After Final	Amendment_After_Final_2551-0032_10-6-09.pdf	20942 164d1c7ff43bd9e553af9c6823e25425c2edd31f	no	1

Warnings:	
Information:	

2	Claims	AF_Claims_2551-0032_10-6-09.pdf	195084 3423732e3c3844d3f2facadfc4fc5caf63a3ea75	no	5
Warnings:					
Information:					
3	Applicant Arguments/Remarks Made in an Amendment	AF_Remarks_2551-0032_10-6-09.pdf	51198 5c21d66b9dde23aa5312f31a5fbf461c912c9b5b	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	267224		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/903,785	07/30/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 10/06/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 24	Minus	** 29	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 2	Minus	***4	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/JACQULYN L. WILLIAMS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/903,785	07/30/2004	John M. Davis	2551-0032	4954

42624 7590 07/20/2009

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
07/20/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/903,785	DAVIS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11,12,14-25 and 30-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9, 11, 12, 14-25, 30-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed April 27 2009. Claims 1, 14, 23 have been amended. Claims 10, 13, and 26-29 have been cancelled. Claims 32-34 have been added. Claims 1-9, 11, 12, 14-25 and 30-34 are pending and have been considered below.

Response to Arguments

2. Applicant's arguments filed 04/27/2009 have been fully considered but they are not persuasive. Applicant amended claims 1, 14 and 25 to add the limitations of cancelled 10 in combination with newly added limitations. In response to applicant's argument that "In fact, signatures are not discussed in the ~955 patent at all. Thus, the independent claims and all the dependent claims are not anticipated by the ~955 patent, and the Office Action has not alleged that the limitations missing from the ~955 patent are taught by any of the secondary references". The examiner submits that in intrusion detection system a signature is generated by hashing information about a packet such as header information or the plain text packet (see column 14, lines 20-67). In response to applicant argument about the newly added limitations, the examiner submits the limitation are taught by the newly find prior art Wu et al US 7,493,659.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a. A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 5, 10, 14-17, 23-25 and 30-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al (US 6,157,955) in view of Wu et al (US 7493,659).

Claims 1 and 14: Narad et al discloses a security processor to process incoming and outgoing packets, the security processor comprising:

i. A switching system to send and receive packets (*Fig. 2, items 104 106*);

ii. A packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packet sent by the packet engine to the switching system (*each Ethernet MAC receives packets into buffers addressed by buffer points obtained from a producer-consumer ring and then passes the buffer (that is, passes the buffer pointer) to a classification Engine for processing, and from there to the Policy Processor)(column 6, line 55 to column 7, line 6, line 63 to column 8, line 20; Fig.2)*;

iii. A cryptographic core, coupled to the packet engine and receiving incoming packets from the switching system via the packet engine and communicating outgoings packets to the switching system via the packet engine to provide encryption and decryption processing for packet received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core *(alternatively the action code 108 may choose to send the packet to the attached cryptographic processor (Crypto) 246 for encryption, decryption compression, decompression, security key*

management, parsing of IPSEC headers, or other associated functions) (column 8, line 67 to column 9, line 25);

iv. a signature database (*hash table*)(column 14, lines 20-67); and

v. an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database

vi. A local data bus coupled to the switching system (Fig. 2); and

(1) Memory coupled to the local data bus (Fig. 2).

Narad et al do not explicitly discloses an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database. However, Wu et al discloses a network intrusion detection and analysis processor which further discloses an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database (*column 2, lines 28-46; column 5, line 43 to column 5, line* 3).Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Narad et al such as to couple the intrusion detection system between the cryptographic core and the packet engine. On would have been motivated to do so in order to accurately detect various intrusions hidden in high-speed network traffic as taught by Wu et al (column 2, lines 5-10).

Claim 2: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further disclose that the packet engine is

further operable to handle security context management processing for the incoming and outgoing packets (column 9, lines 1-55)

Claims 3 and 15: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claims 1 and 14 above, and Narad et al further disclose that the security processor comprises:

i. A local data bus coupled to the switching system (Fig. 2); and

ii. A modulo engine coupled to the local data bus (Fig. 2., item 110)

Claim 5: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claim 4 above, and Narad et al further discloses that the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines *(column 7, lines 63 to column 9, lines 65)*

Claims 10: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claim 1 above, and Narad et al further discloses an intrusion (filtering/blocking) *detection system coupled between the cryptographic core and the packet engine (column 4, lines 40-50*)

Claim 16: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claim 15 above, and further disclose a key management engine coupled to the local data bus (column 7, lines 1-5).

Claims 7, 17 and 18: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claims 3 and 14 above, and Narad et al further disclose that the memory and the security processor are within the same cryptographic boundary (Fig.2).

Claim 23: Narad et al and Wu et al disclose an Internet security processor comprising:

i. A first interface to couple to the trusted network and to the un-trusted network(Fig. 2);

ii. A second interface to couple to a host processor(Fig. 2);

a switching system operable to selectively couple to the first interface or the second interface(Fig. 2);

iii. A local data bus, coupled to the switching system (Fig.2, Fig.3);

iv. a .switching system operable to selectively couple to the first interface or the second interface;

v. A plurality of packet engines coupled to the switching system to handle classification processing for incoming packet received by the plurality of packet engines from the switching system and outgoing packet sent by the plurality of packet engines to the switching system(*column 6, line 55 to column 7, line 6, line 63 to column 8, line 20; Fig.2*);

vi. a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packet received from and sent to the plurality of packet engines, wherein the plurality of

packet engines are interposed between the switching system and the plurality of cryptographic cores (*column 8, line 67 to column 9, line 25*); and

vii. A control processor, coupled to the local data bus, to control data packet flow within the security processor system (Fig.2, Fig.3).

Claim 24: Narad et al and Wu et al disclose an Internet security processor as in claim 23 above, and Narad et al further discloses that the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the un-trusted network (column 13 lines 25-58).

Claim 25: Narad et al discloses an Internet security processor as in claim 24 above, and Narad et al further discloses that the security processor implements data packet security and authentication functions to support the secure communication channel (column 13, lines 25-58).

Claim 30: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claims1 above, and Narad et al further disclose wherein the packet engine is further operable to add at least one of an IP header or MAC address to the outgoing packets (column 20, lines 50-67)

Claim 31: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claims 1 and 14 above, and further disclose wherein the packet engine is further operable to remove at least one of an IP header from the incoming packets (column 20, lines 50-67).

Claims 32, 33 and 34: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claims 14 and 23 above, and Wu et al `further discloses wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet (column 5, lines 43-67).

5. Claims 8, 9, 11, 12, 19, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al (US 6,157,955) in view of Wu et al (US 7493,659) in further view of Savarda et al (US 2003/0196081).

Claim 8: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, while neither of then explicitly disclose a control processor coupled to the local data bus, for exception handling of the incoming and outgoing packets. However, Savarda et al further discloses a control processor coupled to the local data bus, for exception handling of the incoming and outgoing packets (The packet inspection/outbound policy module 108 may be configured with multiplexing circuitry to integrate the outbound and inbound packet streams into a single stream for pipeline processing in the packet co-processor 100. In addition, the packet inspection/outbound policy module 108 may be further configured to inspect packet-objects to ensure their integrity) (paragraph [0031]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to handle exception of incoming and outgoing packets in Narad et al's disclosure. On would have been motivated to do so in order to maintain system integrity.

Claim 9: Narad et al, Wu et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and Narad et al further discloses that a key management engine coupled to the local data bus (*column 7, lines 1-5*).

Claim 11: Narad et al, Wu et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and Narad et al further discloses that the security processor handles substantially all security processing for the incoming and outgoing packets (column 7, line 62 to column 9, line 65).

Claim 12: Narad et al, Wu et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 11 above, and Narad et al further discloses that the security processor further handles substantially all network processing for the incoming and outgoing packets (*column7, line 62 to column 9, line 65).*

Claim 19: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claim 14 above, and Narad et al further discloses a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface (Fig. 2), but does not explicitly discloses a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory. However, Savarda et al discloses a system fro processing a packet object using multiple pipelined processing modules, which further discloses a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory (the SAD contains parameter information about each SA. Such parameters may include the security protocol algorithms and keys for Authentication Header (AH) or Encapsulating Security Payload (ESP) security protocols,

sequence numbers, protocol mode, and SA lifetime. For outbound packets, the SPD is consulted to determine if IPSec processing is required and/or if other processing or discarding of the packet is to be performed. If IPSec is required, then the outbound SAD is searched for an existing SA that matches the packet profile) (paragraphs [0004], [0009], [0024], and [0026]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator in Narad et al disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 21 Narad et al, Wu et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 19 above, and Savarda et al further discloses that the translator performs encryption translation of the received data (the cryptographic chip may perform the encryption, decryption, and/or authentication transforms as required. After completion of the cryptographic operations, the system processor may further process the packet to finish any remaining IPSec transforms) (paragraphs [0007], 0026] and Fig.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt received data in Narad et al disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 22: Narad et al and Wu et al disclose a distributed processing in a cryptographic acceleration chip as in claim 14 above, but does not explicitly discloses a step of executing a boot code or a step authenticating the code. However, Savarda et al discloses

a system for processing a packet object using multiple pipelined processing modules, which further discloses

> Execute boot code to load firmware for execution by the
>
> security processor (One approach is based primarily on software. For example, dedicated software modules may be developed for execution on a workstation to implement the IP packet manipulations, encryption, and authentication operations associated with the IPSec protocol) (paragraphs [0006], [007], [0019]); and
>
> Authenticate the boot code using a mechanism internal to the 10 security processor prior to operation of the security processor (This approach, however, may be limited in its performance as the system processor performs many or all of the functions. Encryption, decryption, and/or authentication are typically processor intensive) (paragraphs [0006], [007], [0019]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to execute and encrypt the code in Narad et al's disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

6. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al (US 6,157,955) in view of Wu et al (US 7493,659) and Savarda et al (US 2003/0196081) as applied to claim 19 above, in further view of Carr et al (US 6788800).

Claim 20: Narad et al, Wu et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 19 above, while neither of them explicitly

discloses a translator performing steganographic translation of the received data. However, Carr et al discloses an authentication object using embedded data, which further discloses a step of performing steganographic translation of the received data (it also steganographically embeds security data into product) (column 1, lines 38-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combine system Narad et al, Wu et al and Savarda et al such as to perform steganographic translation. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Allowable Subject Matter

7. Claims 4 and 6 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes,

which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Friday, July 17, 2009.

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 10/903,785	Applicant(s)/Patent Under Reexamination DAVIS ET AL.	
	Examiner FATOUMATA TRAORE	Art Unit 2436	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,493,659	02-2009	Wu et al.	726/26
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	**Art Unit**
	Traore, Fatoumata	2436

SEARCHED

Class	Subclass	Date	Examiner
713	189, 160, 151, 153, 168 limited text search	07/25/2007	FT

SEARCH NOTES

Search Notes	Date	Examiner
EAST searchattached	07/24/2007	FT
EAST Search performed	04/03/2008	FT
EAST search performed	10/19/2008	FT
EAST search performed and consulted with TRUONG THANHNGA B	07/16/2009	FT

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	**Art Unit**
	Traore, Fatoumata	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/25/2007	04/04/2008	10/20/2008	07/16/2009					
	1	✓	✓	✓	✓					
	2	✓	✓	✓	✓					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	O					
	5	✓	✓	✓	✓					
	6	✓	✓	✓	O					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	✓	✓	✓					
	10	✓	✓	✓	-					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	-	✓	-					
	14	✓	✓	✓	✓					
	15	✓	✓	✓	✓					
	16	✓	✓	✓	✓					
	17	✓	✓	✓	✓					
	18	✓	✓	✓	✓					
	19	✓	✓	✓	✓					
	20	✓	✓	✓	✓					
	21	✓	✓	✓	✓					
	22	✓	✓	✓	✓					
	23	✓	✓	✓	✓					
	24	✓	✓	✓	✓					
	25	✓	✓	✓	✓					
	26	✓	-	-	-					
	27	✓	-	-	-					
	28	✓	-	-	-					
	29	✓	-	-	-					
	30			✓	✓					
	31			✓	✓					
	32				✓					
	33				✓					
	34				✓					

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L16	0	security near6 processor and packet near4 (engine unit classif$4 classificat$3) and (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/07/16 16:14
L17	0	packet near4 (engine unit classif$4 classificat $3) same (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/07/16 16:15
L18	220	packet near4 (engine unit classif$4 classificat $3) same (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/16 16:15
L19	131	security near6 processor and packet near4 (engine unit classif$4 classificat$3) and (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/16 16:15
L20	30	security near6 processor same packet near4 (engine unit classif$4 classificat$3) and (intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/16 16:15
L21	41	security near6 processor and packet near4 (engine unit classif$4 classificat$3) same(intrusion near4 detect$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/07/16 16:25
S1	16	packet with classificat $3 with polic$3 with (cryptograph$3 or crypto or encrypt$3 or decrypt)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/19 12:41

S2	1942	packet and classificat $3 and polic$3 and (cryptograph$3 or crypto or encrypt$3 or decrypt) and (switch$3 or rout$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 13:50
S3	13	(packet and classificat $3 and polic$3 and (cryptograph$3 or crypto or encrypt$3 or decrypt) and (switch$3 or rout$3)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 13:51
S4	0	(packet same classificat $3 same polic$3 same (cryptograph$3 or crypto or encrypt$3 or decrypt) same (switch $3 or rout$3)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 14:02
S5	30	(packet same classificat $3 same polic$3 same (cryptograph$3 or crypto or encrypt$3 or decrypt) same (switch $3 or rout$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 14:02
S6	132	(packet same classificat $3 same polic$3 same (cryptograph$3 or crypto or encrypt$3 or decrypt$ or securit$3) same (switch$3 or rout $3 or buffer or input or port))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 14:12
S7	201	("5764645").PN. OR ("6157955").URPN.	US-PGPUB; USPAT; USOCR	ADJ	ON	2008/10/20 16:21
S8	12	S2 and S7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 16:22
S9	6	"6983366".pn. or "20040010545".pn. or "20030014627".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 17:18

S10	0	packet adj engine near9 switch$3 adj system near9 (cryptographic encrypt $3 encod$3 steganography) near9 intrusion adj detect$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/06/03 08:52
S11	0	packet adj engine near9 switch$3 adj system near9 (cryptographic encrypt $3 encod$3 steganography) near9 intrusion adj detect$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:52
S12	0	packet near9 (classificat $3 classif$4) near9 switch$3 near9 (cryptographic encrypt $3 encod$3 steganography) near9 intrusion adj detect$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:53
S13	0	packet near9 (classificat $3 classif$4) near9 switch$3 near9 (cryptographic encrypt $3 encod$3 steganography) near9 intrusion	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:54
S14	2	packet near9 (classificat $3 classif$4) near9 switch$3 near9 (cryptographic encrypt $3 encod$3 steganography)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:54
S15	40	processor same packet same (classificat$3 classif$4) same switch $3 same (cryptographic encrypt $3 encod$3 steganography)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 08:57
S16	52	security near4 processor same intrusion adj detect$3	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 10:50

S17	9	secur$3 adj processor near9(traffic near4 flow span$4 manag$3 intrusion near3 dtect $3) near6 packet	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:08
S18	317	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:46
S19	0	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet near9 signature near9 (match $3 compar$3 identif$4)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:47
S20	0	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet near9 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:48
S21	2	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet near9 (cryptographc encrypt $3 encipher$3 encod $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:49
S22	2	switch$3 near4 system near9 (traffic near4 flow span$4 manag$3 intrusion near3 detect $3) near6 packet near9 (cryptographic encrypt $3 encipher$3 encod $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 13:49
S23	184	713/192.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 14:02

S24	96099	packet and switch$3 and (cryptographic encrypt$3 encipher$3 encod$3 intrusion near3 detect$3 traffic near3(flow analyz$3 spann$3 manag$3) polic$3 signature)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 14:05
S25	31	S23 and S24	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 14:06
S26	2	"7424744".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/06/03 17:16
S27	0	hash near9 intrusion near S11 detection near6 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/06/03 17:21
S28	0	hash near9 intrusion near2 detection near6 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2009/06/03 17:21
S29	0	hash near9 intrusion adj detection near6 signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 17:22
S30	244261	hash$3 near9 intrusion adj detectionand signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 17:22
S31	0	hash$3 near9 intrusion adj detectionand and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 17:22

S32	6	hash$3 near9 intrusion adj detection and signature	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2009/06/03 17:22

7/16/2009 6:03:57 PM
C:\Documents and Settings\ftraore\My Documents\EAST\Workspaces\10903785_securelOinterfaceafterRCE.wsp

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:	Confirmation No.: 4954
DAVIS, John M., et al	Attorney Docket: 2551-0032
Appl. S.N.: 10/903,785	Group Art Unit: 2136
Filing Date: July 30, 2004	Examiner: TRAORE, Fatoumata
Title: **SYSTEM AND METHOD FOR A SECURE I/O INTERFACE**	Date: April 27, 2009

RESPONSE

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action mailed October 27, 2009, Applicants request a three-month extension of time to file this response and request that the application be amended as follows:

Amendments to the specification begin on page 2;

Amendments to the claims are reflected in the listing of the claims which begins on page 3; and

Remarks begin on page 9.

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph beginning on page 15, line 27, with the following rewritten paragraph:

Packet engines 228 may each be interposed between ~~coupled to~~ a cryptographic core 232 and the switching system 208 as shown in Figure 2. Packet engines 228 may each comprise microprocessors customized for packet operations such as, for example, packet processing and classification. Examples of packet engines suitable for use with the present invention are described in detail in U.S. patent application Ser. No. 09/880,701 (entitled "METHOD AND SYSTEM FOR HIGH-SPEED PROCESSING IPSEC SECURITY PROTOCOL PACKETS" filed by Lee P. Noehring et al. on Jun. 13, 2001), which is incorporated by reference herein. Each packet engine 228 may, for example, process packets needing initial NAT processing and firewall table entry setup, process packets corresponding to existing NAT and firewall tables, and process IPSec packets.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.69

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A security processor to process incoming and outgoing packets, the security processor comprising:

a switching system to send and receive packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system; [[and]]

a cryptographic core, coupled to the packet engine and receiving incoming packets from the switching system via the packet engine and communicating outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database.

2. (Original) The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

3. (Original) The security processor of claim 1 further comprising:

a local data bus coupled to the switching system; and

a modulo engine coupled to the local data bus.

4. (Original) The security processor of claim 1 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.70

5. (Original) The security processor of claim 4 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

6. (Original) The security processor of claim 4 wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the corresponding one of the plurality of cryptographic cores.

7. (Original) The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

8. (Original) The security processor of claim 7 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

9. (Original) The security processor of claim 7 further comprising a key management engine coupled to the local data bus.

10. (Canceled)

11. (Original) The security processor of claim 7 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

12. (Original) The security processor of claim 11 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

13. (Cancelled)

14. (Currently Amended) A security processing system comprising:

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.71

(a) a security processor comprising:

a switching system to send outgoing and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

a cryptographic core, coupled to the packet engine and receiving incoming packets from the switching system via the packet engine and communicating outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core;

a signature database; and

an intrusion detection system coupled between the cryptographic core and the packet engine and responsive to at least one packet matching a signature stored in the signature database; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

15. (Original) The security processing system of claim 14 further comprising a modulo engine coupled to the local data bus.

16. (Original) The security processing system of claim 15 further comprising a key management engine coupled to the local data bus.

17. (Original) The security processing system of claim 14 wherein the memory and the security processor are within the same cryptographic boundary.

18. (Original) The security processing system of claim 14 wherein the security processor is formed on a single chip.

19. (Original) The security processing system of claim 14 further comprising:

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.72

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

20. (Original) The security processing system of claim 19 wherein the translator performs steganographic translation of the received data.

21. (Original) The security processing system of claim 19 wherein the translator performs encryption translation of the received data.

22. (Original) The security processing system of claim 14 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

23. (Currently Amended) A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

a first interface to couple to the trusted network and to the un-trusted network;

a second interface to couple to a host processor;

a switching system operable to selectively couple to the first interface or the second interface;

a local data bus, coupled to the switching system;

a plurality of packet engines coupled to the switching system to handle classification processing for incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system;

a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from and sent to the plurality of packet

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.73

engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores;

a signature database;

an intrusion detection system coupled between the plurality of cryptographic cores and the plurality of packets engine and responsive to at least one packet matching a signature stored in the signature database and

a control processor, coupled to the local data bus, to control data packet flow within the security processor.

24. (Original) The security processor of claim 23 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the untrusted network.

25. (Original) The security processor of claim 24 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

26.-29. (Cancelled)

30. (Previously Presented) The security processor of claim 1 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.

31. (Previously Presented) The security processor of claim 1 wherein the packet engine is further operable to remove an IP header from the incoming packets.

32. (New) The security processor of claim 1, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

33. (New) The security processing system of claim 14, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.74

34. (New) The security processor of claim 23, wherein the at least one packet matching the signature stored in the signature database comprises a plain text packet.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.75

REMARKS

Favorable reconsideration of this application, in view of the present amendment and in light of the following discussion, is respectfully requested. After entry of this amendment, claims 1-9, 11, 12, 14-25 and 30-34 will be pending in this application.

Claims 1, 14 and 23 have been amended herewith. Claim 10 has been canceled herewith and its subject matter incorporated into the independent claims. Thus, the changes are supported by the originally filed drawings and specification (including original claim 10), and the changes do not introduce any new matter. Furthermore, the addition of claims 32-34 is supported starting at the last paragraph of page 30 of the specification and by Figure 3.

In the outstanding Office Action, the specification was objected to as not including antecedent basis for a portion of the independent claims. The specification has been updated to include the "interposed" language in light of the objection to the specification. This change is supported by the originally filed specification. For example, Figure 2 illustrates packet engines 228 interposed between the switching system 104 and cryptographic cores 232.

In addition, the previously pending claims were rejected under 35 U.S.C. 102/103 as being anticipated by or rendered obvious by U.S. Patent No. 6,157,955 (hereinafter "the '955 patent"), either alone or in combination with at least one other reference. Those rejections, however, have been rendered moot by the amendments to the independent claims. Each of the independent claims now recites "a signature database" and "an intrusion detection system ... responsive to at least one packet matching a signature stored in the signature database." Such a positively recited limitation is not taught by the applied references.

In light of the inclusion of the subject matter of claim 10 into the independent claims, the previous rejection of claim 10 will be discussed hereafter. The outstanding Office Action asserts that the '955 patent "discloses an intrusion filtering/blocking) detection system coupled between the cryptographic core and the packet engine." The Office Action cites col. 4, lines 40-50, of the '955 patent in support of this assertion. However, that section describes a programming language generally and does not describe the claimed "intrusion detection system ... responsive to at least one packet matching a signature stored in the signature database." In fact, signatures are not discussed in the '955 patent at all. Thus, the independent claims and all the dependent claims are

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.76

not anticipated by the '955 patent, and the Office Action has not alleged that the limitations missing from the '955 patent are taught by any of the secondary references.

Consequently, all pending claims of this application should be patentable over the applied references of record. An early and favorable action to that effect is respectfully requested.

CHARGE STATEMENT: Deposit Account No. 501860, order no. **2551-0032.**
The Commissioner is hereby authorized to charge any fee specifically authorized herein (including the one-month extension of time), or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.
This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER
42624

Respectfully submitted,

By: _____

Michael R. Casey, Ph.D.
Registration No.: 40,294

Davidson Berquist Jackson & Gowdey LLP
Phone: 703.894.6400
Fax: 703.894.6430

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.77

Electronic Patent Application Fee Transmittal

Application Number:	10903785
Filing Date:	30-Jul-2004
Title of Invention:	System and method for a secure I/O interface
First Named Inventor/Applicant Name:	John M. Davis
Filer:	Michael Raymond Casey
Attorney Docket Number:	2551-0032

Filed as Large Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with $0 paid	1253	1	1110	1110

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**1110**

Electronic Acknowledgement Receipt

EFS ID:	5223172
Application Number:	10903785
International Application Number:	
Confirmation Number:	4954
Title of Invention:	System and method for a secure I/O interface
First Named Inventor/Applicant Name:	John M. Davis
Customer Number:	42624
Filer:	Michael Raymond Casey
Filer Authorized By:	
Attorney Docket Number:	2551-0032
Receipt Date:	27-APR-2009
Filing Date:	30-JUL-2004
Time Stamp:	14:09:45
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1110
RAM confirmation Number	376
Deposit Account	501860
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	10903785_cover.pdf	23182 04e337b0f1c4556706c2094089cafb64f68c8e12	no	1
Warnings:					
Information:					
2	Specification	10903785_spec.pdf	29974 f0f2725abb8e826e0c4c7eb454d1b0e3067f70b6	no	1
Warnings:					
Information:					
3	Claims	10903785_claims.pdf	237985 ecf4e21e5b5055269c1c52bb1c6305bad5a52831	no	6
Warnings:					
Information:					
4	Applicant Arguments/Remarks Made in an Amendment	10903785_remarks.pdf	145926 3e0b5af8f5fa9e1a39f0374ea470ad86ce570227	no	2
Warnings:					
Information:					
5	Fee Worksheet (PTO-875)	fee-info.pdf	29948 d648eb92b765f9e6f94e041109f0465dad895d7b	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	467015		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☒ To be Mailed
10/903,785	07/30/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 04/27/2009	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 28	Minus	** 29	= 0	X $26 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***4	= 0	X $110 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/NICHELE PETERSON/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/903,785	07/30/2004	John M. Davis	2551-0032	4954

42624 7590 10/27/2008

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
10/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/903,785	DAVIS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25,30 and 31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25, 30-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 11, 2008 has been entered. Claims 1, 14 and 23 have been amended. Claims 13 and 26-29 have been cancelled. Claims 31 and 32 have been added. Claims 1-12, 14-25 and 30-31 are pending and have been considered below.

Response to Arguments

2. Applicant's arguments with respect to claims 1-12, 14-25, 30 and 31 have been considered but are moot in view of the new ground(s) of rejection.

Specification

3. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d) (1) and MPEP § 608.01(o). Correction of the following is required: Claims 1, 14 and 23 recite the limitation of “wherein the packet engine is interposed between the switching system and the cryptographic core”.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-6, 10, 14-17, 23-25, 30 and 31 are rejected under 35 U.S.C. 102(b) as being anticipated by Narad et al (US 6,157,955).

Claims 1 and 14: Narad et al discloses a security processor to process incoming and outgoing packets, the security processor comprising:

i. A switching system to send and receive packets (*Fig. 2, items 104 106*);

ii. A packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packet sent by the packet engine to the switching system (*each Ethernet MAC receives packets into buffers addressed by buffer points obtained from a producer-consumer ring and then passes the buffer (that is, passes the buffer pointer) to a classification Engine for processing, and from there to the Policy Processor)(column 6, line 55 to column 7, line 6, line 63 to column 8, line 20; Fig.2)*;

iii. A cryptographic core, coupled to the packet engine and receiving incoming packets from the switching system via the packet engine and

communicating outgoings packets to the switching system via the packet engine to provide encryption and decryption processing for packet received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core *(alternatively the action code 108 may choose to send the packet to the attached cryptographic processor (Crypto) 246 for encryption, decryption compression, decompression, security key management, parsing of IPSEC headers, or other associated functions) (column 8, line 67 to column 9, line 25*);

iv. A local data bus coupled to the switching system (Fig. 2); and

(1) Memory coupled to the local data bus (Fig. 2).

Claim 2: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses that the packet engine is further operable to handle security context management processing for the incoming and outgoing packets (column 9, lines 1-55)

Claims 3 and 15: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claims 1 and 14 above, and further discloses that the security processor comprises:

i. A local data bus coupled to the switching system (Fig. 2); and

ii. A modulo engine coupled to the local data bus (Fig. 2., item 110)

Claim 4: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses the packet engine is

one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines (Fig. 3, items 208, 238, 212,242).

Claim 5: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claim 4 above, and further discloses that the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines *(column 7, lines 63 to column 9, lines 65)*

Claim 6: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claim 4 above, and further discloses the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the 5 corresponding one of the plurality of cryptographic cores (*column 9, lines 16-27)*

Claims 10: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses an intrusion (filtering/blocking) *detection system coupled between the cryptographic core and the packet engine (column 4, lines 40-50*)

Claim 16: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claim 15 above, and further discloses a key management engine coupled to the local data bus (column 7, lines 1-5).

Claims 7, 17 and 18: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claims 3 and 14 above, and further discloses that the memory and the security processor are within the same cryptographic boundary (Fig.2).

Claim 23: Narad et al discloses an Internet security processor comprising:

i. A first interface to couple to the trusted network and to the un-trusted network(Fig. 2);

ii. A second interface to couple to a host processor(Fig. 2);

a switching system operable to selectively couple to the first interface or the second interface(Fig. 2);

iii. A local data bus, coupled to the switching system (Fig.2, Fig.3);

iv. a .switching system operable to selectively couple to the first interface or the second interface;

v. A plurality of packet engines coupled to the switching system to handle classification processing for incoming packet received by the plurality of packet engines from the switching system and outgoing packet sent by the plurality of packet engines to the switching system(*column 6, line 55 to column 7, line 6, line 63 to column 8, line 20; Fig.2*);

vi. a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packet received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores (*column 8, line 67 to column 9, line 25*); and

vii. A control processor, coupled to the local data bus, to control data packet flow within the security processor system (Fig.2, Fig.3).

Claim 24: Narad et al discloses an Internet security processor as in claim 23 above, and Narad et al further discloses that the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the un-trusted network (column 13 lines 25-58).

Claim 25: Narad et al discloses an Internet security processor as in claim 24 above, and Narad et al further discloses that the security processor implements data packet security and authentication functions to support the secure communication channel (column 13, lines 25-58).

Claim 30: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claims1 above, and further discloses wherein the packet engine is further operable to add at least one of an IP header or MAC address to the outgoing packets (column 20, lines 50-67)

Claim 31: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claims 1 and 14 above, and further discloses wherein the packet engine is further operable to remove at least one of an IP header from the incoming packets (column 20, lines 50-67).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a. A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 8, 9, 11, 12, 19, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al (US 6,157,955).in view of **Savarda et al** (US 2003/0196081).

Claim 8: Narad et al and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and **Savarda et al** further discloses a control processor coupled to the local data bus, for exception handling of the incoming and outgoing packets (The packet inspection/outbound policy module 108 may be configured with multiplexing circuitry to integrate the outbound and inbound packet streams into a single stream for pipeline processing in the packet co-processor 100. In addition, the packet inspection/outbound policy module 108 may be further configured to inspect packet-objects to ensure their integrity) (paragraph [0031]). Therefore, it would

have been obvious to one having ordinary skill in the art at the time the invention was made to handle exception of incoming and outgoing packets in Narad et al's disclosure. On would have been motivated to do so in order to maintain system integrity.

Claim 9: Narad et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and Narad et al further discloses that a key management engine coupled to the local data bus (*column 7, lines 1-5*).

Claim 11: Narad et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and Narad et al further discloses that the security processor handles substantially all security processing for the incoming and outgoing packets (column 7, line 62 to column 9, line 65).

Claim 12: Narad et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 11 above, and Narad et al further discloses that the security processor further handles substantially all network processing for the incoming and outgoing packets (*column7, line 62 to column 9, line 65).*

Claim 19: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, and Narad et al further discloses a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface (Fig. 2), but does not explicitly discloses a translator coupled to the memory interface to perform translation of

data received by the memory interface from the memory. However, Savarda et al discloses a system fro processing a packet object using multiple pipelined processing modules, which further discloses a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory (the SAD contains parameter information about each SA. Such parameters may include the security protocol algorithms and keys for Authentication Header (AH) or Encapsulating Security Payload (ESP) security protocols, sequence numbers, protocol mode, and SA lifetime. For outbound packets, the SPD is consulted to determine if IPSec processing is required and/or if other processing or discarding of the packet is to be performed. If IPSec is required, then the outbound SAD is searched for an existing SA that matches the packet profile) (paragraphs [0004], [0009], [0024], and [0026]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator in Narad et al disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 21 Narad et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 19 above, and Savarda et al further discloses that the translator performs encryption translation of the received data (the cryptographic chip may perform the encryption, decryption, and/or authentication transforms as required. After completion of the cryptographic operations, the system processor may further process the packet to finish any

remaining IPSec transforms) (paragraphs [0007], 0026] and Fig.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt received data in Narad et al disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 22: Narad et al discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, but does not explicitly discloses a step of executing a boot code or a step authenticating the code. However, Savarda et al discloses a system for processing a packet object using multiple pipelined processing modules, which further discloses

i. Execute boot code to load firmware for execution by the security processor (One approach is based primarily on software. For example, dedicated software modules may be developed for execution on a workstation to implement the IP packet manipulations, encryption, and authentication operations associated with the IPSec protocol) (paragraphs [0006], [007], [0019]); and

ii. Authenticate the boot code using a mechanism internal to the 10 security processor prior to operation of the security processor (This approach, however, may be limited in its performance as the system processor performs many or all of the functions. Encryption, decryption, and/or authentication are typically processor intensive) (paragraphs [0006], [007], [0019]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to execute and encrypt the code in Narad et al's disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

8. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Narad et al (US 6,157,955). in view of Savarda et al (US 2003/0196081) as applied to claim 19 above, in further view of Carr et al (US 6788800).

Claim 20: Narad et al and Savarda et al disclose a distributed processing in a cryptographic acceleration chip as in claim 19 above, while neither of them explicitly discloses a translator performing steganographic translation of the received data. However, Carr et al discloses an authentication object using embedded data, which further discloses a step of performing steganographic translation of the received data (it also steganographically embeds security data into product) (column 1, lines 38-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combine system Narad et al and Savarda et al such as to perform steganographic translation. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT,

Tuesday, October 21, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Notice of References Cited	Application/Control No. 10/903,785	Applicant(s)/Patent Under Reexamination DAVIS ET AL.	
	Examiner FATOUMATA TRAORE	Art Unit 2436	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,157,955	12-2000	Narad et al.	709/228
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	**Art Unit**
	Traore, Fatoumata	2436

SEARCHED			
Class	**Subclass**	**Date**	**Examiner**
713	189, 160, 151, 153, 168 limited text search	07/25/2007	FT

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
EAST searchattached	07/24/2007	FT
EAST Search performed	04/03/2008	FT
EAST search performed	10/19/2008	FT

INTERFERENCE SEARCH			
Class	**Subclass**	**Date**	**Examiner**

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.99

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	Art Unit
	Traore, Fatoumata	2436

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/25/2007	04/04/2008	10/20/2008						
	1	✓	✓	✓						
	2	✓	✓	✓						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	✓						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	-	✓						
	14	✓	✓	✓						
	15	✓	✓	✓						
	16	✓	✓	✓						
	17	✓	✓	✓						
	18	✓	✓	✓						
	19	✓	✓	✓						
	20	✓	✓	✓						
	21	✓	✓	✓						
	22	✓	✓	✓						
	23	✓	✓	✓						
	24	✓	✓	✓						
	25	✓	✓	✓						
	26	✓	-	-						
	27	✓	-	-						
	28	✓	-	-						
	29	✓	-	-						
	30			✓						
	31			✓						

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.100

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	16	packet with classificat $3 with polic$3 with (cryptograph$3 or crypto or encrypt$3 or decrypt)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/19 12:41
S2	1942	packet and classificat $3 and polic$3 and (cryptograph$3 or crypto or encrypt$3 or decrypt) and (switch $3 or rout$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 13:50
S3	13	(packet and classificat $3 and polic$3 and (cryptograph$3 or crypto or encrypt$3 or decrypt) and (switch $3 or rout$3)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 13:51
S4	0	(packet same classificat $3 same polic$3 same (cryptograph$3 or crypto or encrypt$3 or decrypt) same (switch $3 or rout$3)).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 14:02
S5	30	(packet same classificat $3 same polic$3 same (cryptograph$3 or crypto or encrypt$3 or decrypt) same (switch $3 or rout$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 14:02
S6	132	(packet same classificat $3 same polic$3 same (cryptograph$3 or crypto or encrypt$3 or decrypt$ or securit$3) same (switch$3 or rout $3 or buffer or input or port))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 14:12
S7	201	("5764645").PN. OR ("6157955").URPN.	US-PGPUB; USPAT; USOCR	ADJ	ON	2008/10/20 16:21

S8	12	S2 and S7	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 16:22
S9	6	"6983366".pn. or "20040010545".pn. or "20030014627".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/10/20 17:18

10/21/2008 10:58:15 AM

Best Available Copy

RECEIVED
CENTRAL FAX CENTER

AUG 11 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:
DAVIS, John M., et al
Appl. S.N.: 10/903,785
Filing Date: July 30, 2004
Title: **SYSTEM AND METHOD FOR A SECURE I/O INTERFACE**

Confirmation No.: 4954
Attorney Docket: 2551-0032
Group Art Unit: 2136
Examiner: TRAORE, Fatoumata
Date: August 11, 2008

Mail Stop RCE
Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

REQUEST FOR CONTINUED EXAMINATION (RCE)

This is a request for continued examination (RCE) under 37 CFR 1.114 of the above-identified application. Please continue the examination of this application.

Prerequisites
• This application was filed on/after June 8, 1995, is not abandoned, and no court action has been filed, or if filed, it has been terminated.
• An issue fee has not been paid (unless a petition under Rule 313(c)(2) is also being filed – see item 4 below).
• Prosecution has been closed as defined in Rule 114(b).
• Reply to any outstanding action and Rule 17(e) fee must be enclosed.

This application is entitled under Rule 114 to withdrawal of any outstanding finality or of any allowance plus a new action by the Examiner. Consideration on the merits of each submission (e.g., IDS, Amendment, new arguments, new evidence, but not appeal/reply briefs themselves) filed herewith or before the new action is respectfully requested.

Please consider the following before the next Official Action:

1. Submission required under 37 CFR 1.114:			
a.	☐	**Previously submitted**. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked. Please ☐ enter ☐ do not enter the Amendment filed	
	i.	☐	Consider the arguments in the appeal brief filed and/or reply brief filed
	ii.	☐	Other:
b.	☒	**Enclosed**	

Continued on next page . . .

Request for Continued Examination (RCE) of Application No. 10/630,559

RECEIVED
CENTRAL FAX CENTER
AUG 11 2008

	i.	☒	Amendment / Reply	ii.	☐	Information Disclosure Statement

2. Miscellaneous:

a.	☐	Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)
b.	☐	Other:

3. After payment of issue fee:

	☐	The issue fee has been paid, but this RCE is based on Rule 313(c)(2). See enclosed petition.
		☐ IDS Letter ☐ Cited Appln(s) ☐ Foreign Search Report/OA ☐ PTO-1449 ☐ Cited Documents

4. Fees (The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.):

a.	☒		The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Deposit Account No. 501860, order no. **2551-0032**. I have enclosed a duplicate copy of this sheet.
b.	☐		Check number _____ in the amount of _____ enclosed
	i.	☒	RCE fee required under 37 CFR 1.17(e)
	ii.	☒	Extension of time fee (37 CFR 1.136 and 1.17) [Petition for Extension of Time is hereby made.]

CHARGE STATEMENT: Deposit Account No. 501860, order no. **2551-0032.**

The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER

42624

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor, Arlington, VA 22203
Main: (703) 894-6400 • FAX: (703) 894-6430

Respectfully submitted,

By: _____

Michael R. Casey, Ph.D.
Registration No. **40,294**

PAGE 5/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Best Available Copy

RECEIVED
CENTRAL FAX CENTER

AUG 11 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:	Confirmation No.: 4954
DAVIS, John M., et al	Attorney Docket: 2551-0032
Appl. S.N.: 10/903,785	Group Art Unit: 2136
Filing Date: July 30, 2004	Examiner: TRAORE, Fatoumata
Title: **SYSTEM AND METHOD FOR A SECURE I/O INTERFACE**	Date: August 11, 2008

RESPONSE

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action mailed April 9, 2008, having extended the due date to August 11, 2008, and having granted the Request for Continued Examination filed herewith, please amend the application as follows:

Amendments to the claims are reflected in the listing of the claims which begins on page 2; and

Remarks begin on page 7.

08/12/2008 HMARZI1 00000025 501860 10903785
02 FC:1251 120.00 DA

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.105

Best Available Copy

Appln. of: DAVIS, John M.
Serial No.: 10/903,785
Filed: July 30, 2004

RECEIVED
CENTRAL FAX CENTER
AUG 11 2008

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A security processor to process incoming and outgoing packets, the security processor comprising:

a switching system to send and receive packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system; and

a cryptographic core, coupled to the packet engine and ~~communicating~~ receiving incoming ~~and outgoing~~ packets [[to]] from the switching system via the packet engine and communicating outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core.

2. (Original) The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

3. (Original) The security processor of claim 1 further comprising:

a local data bus coupled to the switching system; and

a modulo engine coupled to the local data bus.

4. (Original) The security processor of claim 1 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

5. (Original) The security processor of claim 4 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all

PAGE 7/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.106

Best Available Copy

of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

6. (Original) The security processor of claim 4 wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the corresponding one of the plurality of cryptographic cores.

7. (Original) The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

8. (Original) The security processor of claim 7 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

9. (Original) The security processor of claim 7 further comprising a key management engine coupled to the local data bus.

10. (Original) The security processor of claim 1 further comprising an intrusion detection system coupled between the cryptographic core and the packet engine.

11. (Original) The security processor of claim 7 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

12. (Original) The security processor of claim 11 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

13. (Cancelled)

14. (Currently Amended) A security processing system comprising:

(a) a security processor comprising:

PAGE 8/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.107

Best Available Copy

a switching system to send outgoing and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming packets received by the packet engine from the switching system and the outgoing packets sent by the packet engine to the switching system;

a cryptographic core, coupled to the packet engine and ~~communicating~~ receiving incoming ~~and outgoing~~ packets [[to]] from the switching system via the packet engine and communicating outgoing packets to the switching system via the packet engine, to provide encryption and decryption processing for packets received from and sent to the packet engine, wherein the packet engine is interposed between the switching system and the cryptographic core; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

15. (Original) The security processing system of claim 14 further comprising a modulo engine coupled to the local data bus.

16. (Original) The security processing system of claim 15 further comprising a key management engine coupled to the local data bus.

17. (Original) The security processing system of claim 14 wherein the memory and the security processor are within the same cryptographic boundary.

18. (Original) The security processing system of claim 14 wherein the security processor is formed on a single chip.

19. (Original) The security processing system of claim 14 further comprising:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

PAGE 9/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.108

Best Available Copy

20. (Original) The security processing system of claim 19 wherein the translator performs steganographic translation of the received data.

21. (Original) The security processing system of claim 19 wherein the translator performs encryption translation of the received data.

22. (Original) The security processing system of claim 14 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

23. (Currently Amended) A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

a first interface to couple to the trusted network and to the un-trusted network;

a second interface to couple to a host processor;

a switching system operable to selectively couple to the first interface or the second interface;

a local data bus, coupled to the switching system;

a plurality of packet engines coupled to the switching system to handle classification processing for [[the]] incoming packets received by the plurality of packet engines from the switching system and outgoing packets sent by the plurality of packet engines to the switching system;

a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from and sent to the plurality of packet engines, wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores; and

a control processor, coupled to the local data bus, to control data packet flow within the security processor.

PAGE 10/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.109

Best Available Copy

24. (Original) The security processor of claim 23 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the untrusted network.

25. (Original) The security processor of claim 24 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

26.-29. (Cancelled)

30. (New) The security processor of claim 1 wherein the packet engine is further operable to add at least one of an IP header or a MAC address to the outgoing packets.

31. (New) The security processor of claim 1 wherein the packet engine is further operable to remove an IP header from the incoming packets.

PAGE 11/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.110

Best Available Copy

Appln. of: DAVIS, John M.
Serial No.: 10/903,785
Filed: July 30, 2004

REMARKS

Favorable reconsideration of this application, in view of the present amendment and in light of the following discussion, is respectfully requested. After entry of this amendment, claims 1-12, 14-25, 30 and 31 will be pending.

Claims 1, 14 and 23 have been amended herewith. The changes are supported by the originally filed specification and drawings and do not introduce any new matter. For example, Figure 2 illustrates packet engines 228 interposed between the switching system 104 and cryptographic cores 232. Furthermore, the addition of claims 30 and 31 are supported by the last two paragraphs of page 16 of the specification and the last paragraph of page 17 of the specification.

Claims 1-6, 10 and 14-18 stood rejected as being anticipated by Krishna et al. (U.S. Patent Publication No. 2003/0014627 (hereinafter "the '627 publication")). Independent claims 1 and 14 have been amended herewith, rendering moot the rejection of the earlier pending claims 1-6, 10 and 14-18. In order to accentuate the difference already discussed with respect to the '627 publication, claims 1 and 14 have been further amended to recite that "the packet engine is ***interposed between*** the switching system and the cryptographic core." This feature is not found in the '627 publication, in combination with the other elements of claims 1 and 14. Instead, the '627 publication shows a packet distributor 206 (which the Office Action alleges corresponds to the claimed switching system) interposed between a packet classifier 304 and crypto/authentication units 316 (which the Office Action alleges correspond to the claimed packet engine and cryptographic cores, respectively).

The Office Action appears to admit that the claimed configuration is not taught given that the Office Action does not deny the earlier remarks about the '627 publication not teaching the previously discussed configuration. Instead, the Office Action merely alleged that the discussed distinction was not, in its opinion, found in the previously pending claims. Since the claimed subject matter has not been alleged to be present in the '627 publication, the rejection of claims 1-6, 10 and 14-18 should be withdrawn.

Furthermore, it is respectfully noted that the Office Action has failed to establish a prima facie case of anticipation for claim 4 as well. Claim 4 recites that "the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the

PAGE 12/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.111

Best Available Copy

security processor transit one of the plurality of packet engines." The Office Action does not provide any support for its assertion that the '627 publication "discloses the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines." In its assertion that claim 1 teaches a packet engine, the Office Action identified the packet classifier 304 and does not provide any indication that multiple such packet classifiers 304 are disclosed in the '627 publication. The Office Action adds that "the architecture enables parallel processing of packets through a plurality of cryptography engines, for example four and includes a classification engine to efficiently process encryption/decryption of data packets (paragraph [0024], [0027])." This, however, ignores that the claim recites plural packet engines, not plural cryptographic cores. Thus, the Office Action has not provided any evidence to support the rejection of claim 4. As a result, claim 5, which depends from claim 4, is also patentable over the '627 publication.

In addition, new claims 30 and 31 are separately patentable over the '627 publication as the Office Action has not provided any evidence that the packet classifier 304 of the '627 publication "add[s] at least one of an IP header or a MAC address to the outgoing packets" or "remove[s] an IP header from the incoming packets."

Claims 7-9, 11, 12, 18, 19, 21 and 22 depend from claim 1 or claim 14. Those claims are patentable for at least the reasons set forth above for the patentability of claims 1 and 14.

Claims 23-25 stand rejected under 35 U.S.C. 103 as being unpatentable over Ke et al. (U.S. Patent No. 7,095,716 (hereinafter "the '716 patent")) in view of the '627 publication. Similar to the arguments discussed above with respect to the rejection of claims 1 and 14, neither the '716 patent nor the '627 publication teach the claimed "plurality of packet engines" and the claimed "plurality of cryptographic cores ... wherein the plurality of packet engines are interposed between the switching system and the plurality of cryptographic cores" to perform the recited functions. As such, those claims are patentable over the applied combination of references, and the outstanding rejection should be withdrawn.

PAGE 13/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.112

Best Available Copy

Appln. of: DAVIS, John M.
Serial No.: 10/903,785
Filed: July 30, 2004

All pending claims of this application, therefore, should be patentable over the applied references of record. An early and favorable action to that effect is respectfully requested.

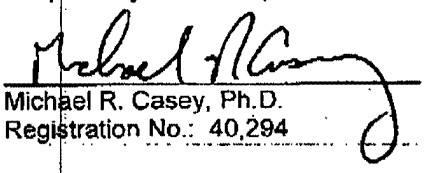
CHARGE STATEMENT: Deposit Account No. 501860, order no. 2551-0032.

The Commissioner is hereby authorized to charge any fee specifically authorized herein (including the one-month extension of time), or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER
42624

Respectfully submitted,

By: 

Michael R. Casey, Ph.D.
Registration No.: 40,294

Davidson Berquist Jackson & Gowdey LLP
Phone: 703.894.6400
Fax: 703.894.6430

PAGE 14/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.113

Best Available Copy

FACSIMILE TRANSMISSION

RECEIVED
CENTRAL FAX CENTER
AUG 11 2008

To: United States Patent and Trademark Office

Facsimile No.: (571) 273-8300

From: Davidson Berquist Jackson & Gowdey, LLP

No. of Pages (including this page): 14

IF YOU DO NOT RECEIVE CLEARLY ALL PAGES, PLEASE CONTACT US IMMEDIATELY BY TELEPHONE AT (703) 894-6400.

USPTO: PLEASE ACKNOWLEDGE CLEAR RECEIPT OF ALL PAGES INDICATED ABOVE BY FAXING THIS PAGE BACK TO (703) 894-6430

In re Patent Application of:		Atty. Docket No.:	2551-0032
	DAVIS, John M. et al.	Confirmation No.:	4954
Appln. No.:	10/903,785	Group Art Unit:	2136
Filed:	July 30, 2004	Examiner:	TRAORE, Fatoumata
Title:	SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Date:	August 11, 2008

Name(s) of paper(s) being transmitted:

- Reply Transmittal Cover Sheet
- Response
- Request for Continued Examination

CERTIFICATE OF FACSIMILE TRANSMISSION				
I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office at the above facsimile number on the date shown below.				
Name:	Michael R. Casey	Signature:	Date:	08/11/2008

CUSTOMER NUMBER

42624

DAVIDSON BERQUIST JACKSON & GOWDEY, LLP
4300 WILSON BLVD., 7TH FLOOR, ARLINGTON, VA 22203
703.894.6400 (main) • 703.894.6430 (Fax)

PAGE 1/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Best Available Copy

RECEIVED
CENTRAL FAX CENTER
AUG 11 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:		Atty. Docket No.:	2551-0032
DAVIS, John M. et al.		Confirmation No.:	4954
Appln. No.:	10/903,785	Group Art Unit:	2136
Filed:	July 30, 2004	Examiner:	TRAORE, Fatoumata
Title:	SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Date:	August 11, 2008

REPLY/AMENDMENT/LETTER TRANSMITTAL COVER SHEET

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a reply/amendment/letter in the above-identified application and includes the attachments hereto. The signature below is treated as the signature to the attachments in the absence of a signature thereto.

FEE REQUIREMENTS

	Claims remaining after amendment		*Highest number previously Paid For*		*Present Extra*	*Rate: Large/Small Entity*	
1. *Total*	26	minus	29	*	= 0	X $50 / $ 25 =	$0
			* If this number is less than 20, enter "20"				
2. *Independent Claims*	3	minus		**	= 0	X $210 / $105 =	$0
			** If this number is less than 3, enter "3"				
3. If amendment enters multiple dependent claim(s) into this application for first time (leave this line blank if this is an reissue application)						$370 / $185 =	$0
4. **Original due date:** July 9, 2008							
				Check time period and enter appropriate fee			
5. **Petition is hereby made** to extend the original due date to cover the date this response is filed for which the requisite fee is:				☒ 1 month ☐ 2 months. ☐ 3 months ☐ 4 months ☐ 5 months.		$120 / $60 $460 / $230 $1050 / $525 $ 1640/ $820 $2230 / $1115	$120
6. ☐ Attached is a Petition/Fee under Rule No.						$	$
7. Other Fee for Request for Continued Examination							$810
8. **Total Fee Enclosed:**							$930

08/12/2008 HMARZI1 00000025 501860 10903785
01 FC:1801 810.00 DA

This is a 2 page form, continued on next page . . .

Best Available Copy

RECEIVED
CENTRAL FAX CENTER
AUG 11 2008

In re Patent Application of: DAVIS, John M. et al.
Appln. No.: 10/903,785

TRANSMITTAL COVER SHEET, PAGE 2
Attorney Docket No. 2551-0032
Confirmation Number: 4954

9. ☒ Please charge the total fee on line 8 above to our deposit account below under the stated order number.

CHARGE STATEMENT: Deposit Account No. 501860, order no. (client-matter no.) **2551-0032.**

The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER
42624

Respectfully submitted,

By: _____
Michael R. Casey
Registration No.: 40,294

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203
Main: (703) 894-6400 • FAX: (703) 894-6430

PAGE 3/14 * RCVD AT 8/11/2008 4:22:59 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/10 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):02-56

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.116

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/903,785	07/30/2004	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
FOR	NUMBER FILED	NUMBER EXTRA					
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 08/11/2008	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 26	Minus	** 29	= 0	X $25 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 3	Minus	***4	= 0	X $105 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/KIM WATSON SAUNDERS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/903,785	07/30/2004	John M. Davis	2551-0032	4954

42624 7590 04/09/2008

DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/903,785	DAVIS ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12 and 14-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12 and 14-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment file on January 31, 2008. Claims 1, 14 and 23 have been amended; Claims 13 and 26-29 have been cancelled; Claims 1-12 and 14-25 are pending and have been considered below.

Claim Objections

2. Claim 13 was objected to under 37 CFR1.75 as being a substantial duplicate of claim 10. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k). the objection has been withdrawn in view to the cancellation of claim.

Response to Arguments

3. Applicant's arguments filed January 31, 2008 have been fully considered but they are not persuasive.

Applicant argued that “those claims all recite that the cryptographic core is coupled to the packet engine a feature that is not found in Krishna. Applicant notes that Fig. 2 of the present application the packet proceed in the following order: switching system 208, packet engine 228 and cryptographic core 232. As the communication path goes, the packet engine is between the switching system, and the cryptographic core. Thus, independent claims 1 and 14 recite "a packet engine, coupled to the switching system,,

and "a cryptographic core, coupled to the packet engine". The examiner respectfully disagrees and submits that Krishna et al discloses ***a packet engine, coupled to the switching system***(see Fig. 3, item 302(as the switching engine) 306 and 312 (as the packet engine) and further discloses ***a cryptographic core*** (Fig.3 item 316) ***is coupled to the packet engine*** (see Fig 3, item 304, 306). Which meet the limitation of amended claims 1 and 14? the preamble of he claims recites the limitation of "the security processor comprising" which is an open ended claim.

Applicant argued that "Applicant respectfully notes that the same cannot be said for Krishna, where the packets are communicate from the crypto/auth 316 directly to the distributor 306 and not "via" the packet classifier 304". It is noted that the claim does not recite the above feature. The examiner respectfully disagrees with applicant's characterization of the prior art references and the claimed invention. For what's recited in the claim as presented ***Krishna et al*** discloses the above limitation(Fig. 3).

Applicant argued that "Also specifically with respect to claim 6, applicant draws the Examiner's attention to the fact that the cited references in the office action do not mention, the claimed "tags". In reply the examiner submits that ***Krishna et al*** discloses the claimed tag (The result of packet classification is a classification tag. This structure holds IPSec security association data and per-flow statistics)(paragraphs [0068],[0074], [0075]).

Applicant argued that "Like Krishna, Ke does not describe the plurality of packet engines handling the classification processing being in line between a switch and the

crypto cores. The examiner respectfully disagrees and submits as discussed above this feature is disclosed by ***Krishna et al*** (see Fig.3).

To the extent that the response to the applicant's arguments, may have mentioned new portions of the prior art references which were not used in the prior office action, this does not constitute new a new ground of rejection. It is clear that the prior art reference is of record and has been considered entirely by applicant. See In re Borer, 363 F.2d 455, 458 n.2, 150 USPQ 441, 4441 n.2 (CCPA 1966) and In re Bush, 296 F.2d 491,496, 131 USPQ 263,267 (CCPA 1961).

The mere fact that additional portions of the same reference may have been mentioned or relied upon does not constitute new ground of rejection. In re Meinhardt, 392, F.2d 273,280, 157 USPQ 270,275 (CCPA 1968).

In light of the above, the claims remain rejected and this office action made final

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-6, 10, 14-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Krishna et al (US 2003/0014627).

Claim 1: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip comprising:

i. A switching system to send and receive packets (Fig. 3 items 302, 306, 318 and paragraphs [0010]-[0012]);

ii. A packet engine, coupled to the switching system, to handle classification

processing for the incoming and outgoing packets (Fig. 3 item 304 and paragraphs [0010]-[0012]); and

iii. A cryptographic core, coupled to the packet engine and communicating incoming and outgoing packets to the switch via the packet engine, to provide encryption and decryption processing for packets received from the packet engine(Fig. 3 item 316 and paragraphs [0010]-[0012]).

Claim 2: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses that the packet engine is further operable to handle security context management processing for the incoming and outgoing packets (According to this configuration, packets are received from the LAN or WAN and go directly through the cryptography acceleration chip and are processed as they are received from or are about to be sent out on the WAN, providing automatic security processing for IP packets)

(paragraphs [0029], [0038]).

Claim 3: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses that the security processor comprises:

iv. A local data bus coupled to the switching system (As shown in FIG. 1A, the cryptography acceleration chip 102 may be part of an otherwise standard network line card 103 which includes a WAN interface 112 that connects the processing system 100 to a WAN, such as the Internet, and manages in-bound and out-bound packets) (paragraphs [0027], [0030], [0037]); and

v. A modulo engine coupled to the local data bus (The chip 102 on the card 103 may be connected to a system bus 104 via a standard system interface 106. The system bus 104 may be, for example, as standard PCI bus, or it may be a high speed system switching matrix, as are well known to those of skill in the art. The processing system 100 includes a processing unit 114, which may be one or more processing units, and a system memory unit 116) (paragraphs [0027], [0030], [0037]).

Claim 4: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses the packet engine is one of a plurality of packet engines and substantially all of the incoming and

outgoing packets to the security processor transit one of the plurality of packet engines (the architecture enables parallel processing of packets through a plurality of cryptography engines, for example four, and includes a classification engine configured to efficiently process encryption/decryption of data packets) (paragraph [0024], [000027]).

Claim 5: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 4 above, and further discloses that the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines (the architecture enables parallel processing of packets through a plurality of cryptography engines and includes a classification engine configured to efficiently process encryption/decryption of data packets) (paragraphs [0010], [0024], [0042], [0052])

Claim 6: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 4 above, and further discloses the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the 5 corresponding one of the plurality of cryptographic

cores (Thus it would be desirable to have a cryptography accelerator chip architecture that is capable of implementing the IPSec specification (or any other cryptography standard), at much faster rates than are achievable with current chip designs) (paragraphs [0009], [0038], [0060]).

Claims 10: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses an intrusion (filtering/blocking) detection system coupled between the cryptographic core and the packet engine (the classifier includes four different modes that allow all IPSec selector matching operations to be supported, as well as general purpose packet matching for packet filtering purposes, for fragment re-assembly purposes, and for site blocking purposes) (paragraphs [0040], [0041], [0052], [0058]);

Claim 14: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip comprising:

i. A switching system to send and receive packets(Fig. 3 items 302, 306, 318 and paragraphs [0010]-[0012]);

ii. A packet engine, coupled to the switching system, to handle classification processing for the incoming and outgoing packets(Fig. 3 item 304 and paragraphs [0010]-[0012]); and

iii. A cryptographic core, coupled to the packet engine and communicating incoming and outgoing packets to the switch via the

packet engine, to provide encryption and decryption processing for packets received from the packet engine(Fig. 3 item 316 and paragraphs [0010]-[0012]); and

iv. A local data bus coupled to the switching system (As shown in FIG. 1A, the cryptography acceleration chip 102 may be part of an otherwise standard network line card 103 which includes a WAN interface 112 that connects the processing system 100 to a WAN, such as the Internet, and manages in-bound and out-bound packets) (paragraphs [0027], [0030], [0037]);

v. A memory coupled to the local data bus (paragraphs [0026], [0027], [0038].

Claim 15: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, and further discloses a modulo engine coupled to the local data bus (The chip 102 on the card 103 may be connected to a system bus 104 via a standard system interface 106. The system bus 104 may be, for example, as standard PCI bus, or it may be a high speed system switching matrix, as are well known to those of skill in the art. The processing system 100 includes a processing unit 114, which may be one or more processing units, and a system memory unit 116) (paragraphs [0027], [0030], [0037]).

Claim 16: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 15 above, and further discloses a key management engine coupled to the local data bus (paragraphs [0011], [0012], [0038], [0056]).

Claim 17: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, and further discloses that the memory and the security processor are within the same cryptographic boundary (Fig.2 items 204, 212, 214).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 7-9, 11, 12, 18, 19, 21 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Krishna et al** (US 2003/0014627) in view of **Savarda et al** (US 2003/0196081).

Claims 7, 18: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claims 3 and 14 above, but does not explicitly discloses that the cryptographic core, and the modulo engine are formed on a single chip.

However, **Savarda et al** discloses a system fro processing a packet object using multiple pipelined processing modules, which further discloses cryptographic core, and the modulo engine in a single chip (Fig.1 and paragraph [0024]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the cryptographic core and the modulo engine on a single chip in **Krishna et al**'s disclosure. On would have been motivated to do so in order to increase the performance and to lower cost associate with the fabrication.

Claim 8: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and **Savarda et al** further discloses a control processor coupled to the local data bus, for exception handling of the incoming and outgoing packets (The packet inspection/outbound policy module 108 may be configured with multiplexing circuitry to integrate the outbound and inbound packet streams into a single stream for pipeline processing in the packet co-processor 100. In addition, the packet inspection/outbound policy module 108 may be further configured to inspect packet-objects to ensure their integrity) (paragraph [0031]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to handle exception of incoming and outgoing packets in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity.

Claim 9: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and **Krishna et al** further discloses that a key management engine coupled to the local data bus (paragraphs [0011], [0012], [0038], [0056]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to couple the key management engine to the local data bus in **Krishna et al**'s disclosure. On would have been motivated to do so in order to increase system performance.

Claim 11: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and **Krishna et al** further discloses that the security processor handles substantially all security processing for the incoming and outgoing packets (The IPSec cryptography protocol specifies two levels of lookup: Policy (Security Policy Database (SPD) lookup) and Security Association (Security Association Database (SAD) lookup) (paragraphs [0029], [0039], [0056]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to handle security processing in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 12: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 11 above, and **Krishna et al** further discloses that the security processor further handles substantially all network processing for the incoming and outgoing packets (According to this configuration, packets are received from the LAN or WAN and go directly through the cryptography acceleration chip and are processed as they are received from or are about to be sent out on the WAN, providing automatic security processing for IP packets) (paragraphs [0029], [0039], [0056]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to handle security processing in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 19: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, and **Krishna et al** further discloses a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface (Fig. 1A), but does not explicitly discloses a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory. However, **Savarda et al** discloses a system fro processing a packet object using multiple pipelined processing modules, which further discloses a translator coupled to the memory interface to perform translation of data received by the memory interface from the

memory (the SAD contains parameter information about each SA. Such parameters may include the security protocol algorithms and keys for Authentication Header (AH) or Encapsulating Security Payload (ESP) security protocols, sequence numbers, protocol mode, and SA lifetime. For outbound packets, the SPD is consulted to determine if IPSec processing is required and/or if other processing or discarding of the packet is to be performed. If IPSec is required, then the outbound SAD is searched for an existing SA that matches the packet profile) (paragraphs [0004], [0009], [0024], [0026]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 21 **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 19 above, and **Savarda et al** further discloses that the translator performs encryption translation of the received data (the cryptographic chip may perform the encryption, decryption, and/or authentication transforms as required. After completion of the cryptographic operations, the system processor may further process the packet to finish any remaining IPSec transforms) (paragraphs [0007], 0026] and Fig.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt received data in **Krishna et al**'s disclosure. On

would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 22: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, but does not explicitly discloses a step of executing a boot code or a step authenticating the code. However, **Savarda et al** discloses a system fro processing a packet object using multiple pipelined processing modules, which further discloses

vi. Execute boot code to load firmware for execution by the security processor (One approach is based primarily on software. For example, dedicated software modules may be developed for execution on a workstation to implement the IP packet manipulations, encryption, and authentication operations associated with the IPSec protocol)(paragraphs [0006], [007], [0019]); and

vii. Authenticate the boot code using a mechanism internal to the 10 security processor prior to operation of the security processor (This approach, however, may be limited in its performance as the system processor performs many or all of the functions. Encryption, decryption, and/or authentication are typically processor intensive)(paragraphs [0006], [007], [0019]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to execute and encrypt the code in **Krishna et**

al's disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

8. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Krishna et al** (US 2003/0014627) in view of **Savarda et al** (US 2003/0196081) as applied to claim 19 above, in further view of **Carr et al** (US 6788800).

Claim 20: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 19 above, while neither of them explicitly discloses a translator performing steganographic translation of the received data. However, **Carr et al** discloses an authentication object using embedded data, which further discloses a step of performing steganographic translation of the received data (it also steganographically embeds security data into product) (column 1, lines 38-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combine system **Krishna et al** and **Savarda et al** such as to perform steganographic translation. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

9. Claim 23-25 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Ke et al** (US 7095716) in view of **Krishna et al** (US 2003/0014627) .

Claim 23: **Ke et al** discloses an Internet security processor comprising:

viii. A first interface to couple to the trusted network and to the un-trusted network(fig. 2);

ix. A second interface to couple to a host processor(Fig. 2);

a switching system operable to selectively couple to the first interface or the second interface(Fig. 2);

x. A local data bus, coupled to the switching system (column 4, lines 28-39 and Fig.2, Fig.3);

xi. A plurality of packet engines coupled to the switching system to handle classification processing for the incoming and outgoing packet(column 4, lines 28-39; column 6, lines 37-62 and Fig.2, Fig.3);

xii. a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packet received from the packet engine (column 4, lines 28-39 and Fig.2, Fig.3); and

xiii. A control processor, coupled to the local data bus, to control data packet flow within the security processor system (column 4, lines 28-39 and Fig.2, Fig.3).

but does not explicitly discloses that a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption

and decryption processing for packet received from the packet engine. However, **Krishna et al**'s a security processor, which further discloses a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packet received from the packet engine (Fig. 3 item 316 and paragraphs [0010]-[0012]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to couple the crypto core to the packet engine via switching system in **Ke et al**'s disclosure. On would have been motivated to do so in order to increase the performance and to lower cost associate with the fabrication.

Claim 24: **Ke et al** and **Krishna et al** disclose an Internet security processor as in claim 23 above, and **Ke et al** further discloses that the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the un-trusted network The one or more processing boards can process the received data packets by performing one or more of: policy enforcement, virtual private network traffic encryption and decryption, key negotiation, firewall protection, network address translation, tunnel encapsulation and de-capsulation, and hot backup between processing boards) (column 2 lines 25-58, column 10 lines 46-51, abstract and Fig.6B).

Claim 25: **Ke et al** and **Krishna et al** disclose an Internet security processor as in claim 24 above, and **Ke et al** further discloses that the security processor implements data packet security and authentication functions to support the secure communication channel (After the packet passes the inspection provided by the stateful inspection engine (645) (e.g., the packet is authenticated)(column 11, lines 17-24).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

b. Huynh et al (US 6983366) Packet processor.

c. Pandya (US (2004/0010545) Data processing system using internet protocos and RDMA.

11. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Friday, April 4, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	Art Unit
	Traore, Fatoumata	2136

SEARCHED			
Class	Subclass	Date	Examiner
713	189, 160, 151, 153, 168 limited text search	07/25/2007	FT

SEARCH NOTES		
Search Notes	Date	Examiner
EAST searchattached	07/24/2007	FT
EAST Search performed	04/03/2008	FT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.139

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	Art Unit
	Traore, Fatoumata	2136

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/25/2007	04/04/2008							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	-							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							
	21	✓	✓							
	22	✓	✓							
	23	✓	✓							
	24	✓	✓							
	25	✓	✓							
	26	✓	-							
	27	✓	-							
	28	✓	-							
	29	✓	-							

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.140

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	31272	(processor or microprocessor or device or computer) same (send$3 or transfer$3 or receiv $3) same (packet or data or file or message) same (cryptograph$3 or encrypt$3 or encipher $3 or decrypt$3 or decipher$3 or scrambl $3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:42
S2	2362	(processor or microprocessor or device or computer) same (send$3 or transfer$3 or receiv $3) same (packet or data or file or message) same (cryptograph$3 or encrypt$3 or encipher $3 or decrypt$3 or decipher$3 or scrambl $3)same (bus)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:42
S3	17568	S1 and (packet or data or file or message) same (classificat$3 or classif$3 or categori$7 or group$3 or arrang $5 or sort$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:48
S4	17568	S1 and ((packet or data or file or message) same (classificat$3 or classif $3 or categori$7 or group$3 or arrang$5 or sort$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:35
S5	1537	S2 and ((packet or data or file or message) same (classificat$3 or classif $3 or categori$7 or group$3 or arrang$5 or sort$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:49

S6	3731	S4 and (security same management)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:50
S7	451	S6 and ((incom$3 or outg$3)same packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:51
S8	0	S7 and (packet near engine same bus same cryptogra$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:52
S9	28	S7 and (packet near engine)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:04
S10	2303	process$3 same as (packet or data or frame or datagram$2 or file or messag$3 or mail) same (cryptograph$43 or encrypt$3 or encipher $3 or cipher$3 or scramble$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:23
S11	1813	713/189	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:23
S12	121	S10 and S11	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:24
S13	76	S12 and bus	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:24

S14	1364	S10 and ((packet or data or file or message) same (classificat$3 or classif $3 or categori$7 or group$3 or arrang$5 or sort$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:35
S15	661	713/160	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:35
S16	27	S15 and S14	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:44
S17	4613	713/151 or 713/153 or 713/168	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:44
S18	131	S14 and S17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:44
S19	98	US-4423287-$.DID. OR US-5784459-$. DID. OR US-4885789-$.DID. OR US-5619657-$.DID. OR US-5822431-$.DID. OR US-5884277-$. DID. OR US-6092202-$.DID. OR US-6115819-$.DID. OR US-6199113-$.DID. OR US-6247129-$. DID. OR US-4386234-$.DID. OR US-4755940-$.DID. OR US-4864615-$.DID. OR US-4864616-$. DID. OR US-4870681-$.DID. OR US-4901348-$.DID. OR US-4910773-$.DID. OR US-4933971-$.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:54

		DID. OR US-4956862-$.DID. OR US-4965568-$.DID. OR US-4985919-$.DID. OR US-4997288-$.DID. OR US-5008936-$.DID. OR US-5012515-$.DID. OR US-5016277-$.DID. OR US-5022076-$.DID. OR US-5032979-$.DID. OR US-5201000-$.DID. OR US-5235641-$.DID. OR US-5241594-$.DID. OR US-5261070-$.DID. OR US-5268962-$.DID. OR US-5301231-$.DID. OR US-5359660-$.DID. OR US-5416842-$.DID. OR US-5436857-$.DID. OR US-5506393-$.DID. OR US-5553280-$.DID. OR US-5588060-$.DID. OR US-5590196-$.DID. OR US-5596718-$.DID. OR US-5633933-$.DID. OR US-5657388-$.DID. OR US-5675771-$.DID. OR US-5684950-$.DID. OR US-5724274-$.DID. OR US-5742845-$.DID. OR US-5774879-$.DID. OR US-5778071-$.DID. OR US-5781724-$.DID.				
S20	5	S19 and S10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:54

S21	16	US-20020108059-$.DID. OR US-5892899-$.DID. OR US-6049876-$.DID. OR US-6101255-$.DID. OR US-20020066014-$.DID. OR US-5432950-$.DID. OR US-5940628-$.DID. OR US-5737760-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:14
S22	2	"20030196081".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:15
S23	121	S11 and S10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:15
S24	121	S23 and S10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:16
S25	1	S22 and S10	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:16
S26	6	"20030196081".pn. or "20040123121".pn. or "7095716".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 14:18
S27	1	steganographic translation	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 14:19
S28	942	steganographic	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 14:19

S29	25	S28 and S17	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 14:19
S30	1257	(switch$3 or io or input or output) and packet and cryptograph $3.clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/04/03 12:48
S31	184	((switch$3 or io or input or output) and packet and cryptograph $3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/04/03 12:48
S32	2	"7095716".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2008/04/03 15:19

4/4/2008 9:29:11 AM
C:\Documents and Settings\ftraore\My Documents\EAST\Workspaces\10903785_securelOinterface.wsp

RECEIVED
CENTRAL FAX CENTER
JAN 31 2008

FACSIMILE TRANSMISSION

To: United States Patent and Trademark Office

Facsimile No.: (571) 273-8300

From: Davidson Berquist Jackson & Gowdey, LLP

No. of Pages (including this page): 13

IF YOU DO NOT RECEIVE CLEARLY ALL PAGES, PLEASE CONTACT US IMMEDIATELY BY TELEPHONE AT (703) 894-6400.

USPTO: PLEASE ACKNOWLEDGE CLEAR RECEIPT OF ALL PAGES INDICATED ABOVE BY FAXING THIS PAGE BACK TO (703) 894-6430

In re Patent Application of:		Atty. Docket No.:	2551-0032
	DAVIS, John M. et al.	Confirmation No.:	4954
Appln. No.:	10/903,785	Group Art Unit:	2136
Filed:	July 30, 2004	Examiner:	TRAORE, Fatoumata
Title:	SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Date:	January 31, 2008

Name(s) of paper(s) being transmitted:

- Reply Transmittal Cover Sheet
- Response

CERTIFICATE OF FACSIMILE TRANSMISSION				
I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office at the above facsimile number on the date shown below.				
Name:	J. Scott Davidson	Signature:	Date:	1/31/2008

CUSTOMER NUMBER
42624

DAVIDSON BERQUIST JACKSON & GOWDEY, LLP
4300 WILSON BLVD., 7TH FLOOR, ARLINGTON, VA 22203
703.894.6400 (main) • 703.894.6430 (Fax)

PAGE 1/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

RECEIVED
CENTRAL FAX CENTER
JAN 31 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:		Atty. Docket No.:	2551-0032
	DAVIS, John M. et al.	Confirmation No.:	4954
Appln. No.:	10/903,785	Group Art Unit:	2136
Filed:	July 30, 2004	Examiner:	TRAORE, Fatoumata
Title:	SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Date:	January 30, 2008

REPLY/AMENDMENT/LETTER TRANSMITTAL COVER SHEET

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a reply/amendment/letter in the above-identified application and includes the attachments hereto. The signature below is treated as the signature to the attachments in the absence of a signature thereto.

FEE REQUIREMENTS

	Claims remaining after amendment		*Highest number previously Paid For*		*Present Extra*	*Rate: Large/Small Entity*	
1. *Total*	24	minus	29	*	= 0	X $50 / $ 25 =	$0
			* If this number is less than 20, enter "20"				
2. *Independent Claims*	3	minus		**	= 0	X $210 / $105 =	$0
			** If this number is less than 3, enter "3"				
3. If amendment enters multiple dependent claim(s) into this application for first time (leave this line blank if this is an reissue application)						$370 / $185 =	$0
4. **Original due date:** October 31, 2007							
				Check time period and enter appropriate fee			
5. **Petition is hereby made** to extend the original due date to cover the date this response is filed for which the requisite fee is:				☐ 1 month ☐ 2 months. ☒ 3 months ☐ 4 months ☐ 5 months.		$120 / $60 $460 / $230 $1050 / $525 $ 1640/ $820 $2230 / $1115	$1050
6. ☐ Attached is a Petition/Fee under Rule No.						$	$
7. Other Fee for							$
8. **Total Fee Enclosed:**							$1050

02/01/2008 PCHOMP 00000016 501860 10903785

01 FC:1253 1050.00 DA

This is a 2 page form, continued on next page . . .

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.148

RECEIVED
CENTRAL FAX CENTER
JAN 31 2008

In re Patent Application of: DAVIS, John M. et al.
Appln. No.: 10/903,785

TRANSMITTAL COVER SHEET, PAGE 2
Attorney Docket No. 2551-0032
Confirmation Number: 4954

9. ☒ Please charge the total fee on line 8 above to our deposit account below under the stated order number.

CHARGE STATEMENT: Deposit Account No. 501860, order no. (client-matter no.) **2551-0032.**

The Commissioner is hereby authorized to charge any fee specifically authorized hereafter, or any missing or insufficient fee(s) filed, or asserted to be filed, or which should have been filed herewith or concerning any paper filed hereafter, and which may be required under Rules 16-18 (missing or insufficiencies only) now or hereafter relative to this application and the resulting Official Document under Rule 20, or credit any overpayment, to our Accounting/ Order Nos. shown above, for which purpose a duplicate copy of this sheet is attached.

This CHARGE STATEMENT does not authorize charge of the issue fee until/unless an issue fee transmittal sheet is filed.

CUSTOMER NUMBER
42624

Respectfully submitted,

By: _____
J. Scott Davidson
Registration No.: 33,489

Davidson Berquist Jackson & Gowdey LLP
4300 Wilson Blvd., 7th Floor, Arlington, Virginia 22203
Main: (703) 894-6400 • FAX: (703) 894-6430

PAGE 3/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.149

RECEIVED
CENTRAL FAX CENTER
JAN 31 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of:	Confirmation No.: 4954
DAVIS, John M., et al	Attorney Docket: 2551-0032
Appl. S.N.: 10/903,785	Group Art Unit: 2136
Filing Date: July 30, 2004	Examiner: TRAORE, Fatoumata
Title: **SYSTEM AND METHOD FOR A SECURE I/O INTERFACE**	Date: January 31, 2008

RESPONSE

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action July 31, 2007, please amend the application as follows:

Amendments to the specification begin on page 2.

Amendments to the claims are reflected in the listing of the claims which begins on page 5.

Remarks begin on page 9.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.150

Appln. of: DAVIS, John M.
Serial No.: 10/903,785
Filed: July 30, 2004

RECEIVED
CENTRAL FAX CENTER
JAN 31 2008

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph on page 7, beginning on line 12, with the following rewritten paragraph:

"IP data packets are received from and transmitted to external network 120 and internal network 116 over interfaces 114 and 118. In other embodiments, security processing system 102 may include a number of additional interfaces to internal or external networks. Security processor 104 performs, for example, routing of data packets from external network 120 to appropriate destinations in internal network 116 and handles IPSec processing for both inbound and outbound data packets. Security processor 104 preferably handles all network and security processing functions for the data packets to provide the most secure I/O interface. However, in alternative embodiments, certain selected networking and/or security functions may be handled by other processors such as, for example, host processor 130. Examples of network and security processing systems and methods, and related communications interfaces and protocols, suitable for implementation in and with security processing system 102 are described in U.S. patent application Ser. No. 09/880,701 (entitled "METHOD AND SYSTEM FOR HIGH-SPEED PROCESSING IPSEC SECURITY PROTOCOL PACKETS" filed by Lee P. Noehring et al. on Jun. 13, 2001, which is now U.S. Patent No. 7,194,766, issued on March 20, 2007) and Ser. No. 10/160,330 (entitled "SYSTEM AND METHOD FOR MANAGING SECURITY PACKET PROCESSING" filed by Lee P. Noehring et al. on May 30, 2002), which applications are incorporated by reference herein."

Please replace the paragraph on page 12, beginning on line 1, with the following rewritten paragraph:

"Switching system 208 may provide a flexible I/O system that allows packet processing engines or packet engines 228 to communicate high-speed data with several different types of interfaces including, for example, streaming interface 200 and direct memory access (DMA) interface 204. A non-limiting example of a switching system and method that are suitable for use with the present invention is described in U.S. patent application

PAGE 5/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.151

Ser. No. 10/172,814 (entitled FLEXIBLE I/O INTERFACE AND METHOD FOR PROVIDING A COMMON INTERFACE TO A PROCESSING CORE, filed by Swaroop Adusumilli et al. on Jun. 12, 2002, which is now U.S. Patent No. 7,072,996, issued on July 4, 2006), which is hereby incorporated by reference. Alternatively, switching system 208 may be implemented using conventional switches. Switching system 208 may provide a common bus interface to packet engines 228."

Please replace the paragraph on page 15, beginning on line 27, with the following rewritten paragraph:

"Packet engines 228 may each be coupled to a cryptographic core 232. Packet engines 228 may each comprise microprocessors customized for packet operations such as, for example, packet processing and classification. Examples of packet engines suitable for use with the present invention are described in detail in U.S. patent application Ser. No. 09/880,701 (entitled "METHOD AND SYSTEM FOR HIGH-SPEED PROCESSING IPSEC SECURITY PROTOCOL PACKETS" filed by Lee P. Noehring et al. on Jun. 13, 2001, which is now U.S. Patent No. 7,194,766, issued on March 20, 2007), which is incorporated by reference herein. Each packet engine 228 may, for example, process packets needing initial NAT processing and firewall table entry setup, process packets corresponding to existing NAT and firewall tables, and process IPSec packets."

Please replace the paragraph on page 18, beginning on line 11, with the following rewritten paragraph:

"Cryptographic cores 232 may provide security processing to perform, for example, IPSec and/or SSL processing. Each cryptographic core 232 may provide high-speed fixed function encryption and authentication hash processing for packet data. Each cryptographic core 232 may receive instructions and key address information affixed to a packet for applying appropriate transforms. Examples of cryptographic cores 232 suitable for use with the present invention are described in the following U.S. patent applications, all of which are incorporated herein by reference: Ser. No. 10/144,004 (entitled "SINGLE-PASS CRYPTOGRAPHIC PROCESSOR AND METHOD" filed by Satish N.

PAGE 6/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.152

Anand et al. on May 13, 2002, which is now U.S. Patent No. 7,266,703, issued on September 4, 2007); Ser. No. 10/144,332 (entitled "SECURITY ASSOCIATION DATA CACHE AND STRUCTURE" filed by Satish N. Anand et al. on May 13, 2002); Ser. No. 10/144,195 (entitled "APPARATUS AND METHOD FOR A HASH PROCESSING SYSTEM USING MULTIPLE HASH STORAGE AREAS" filed by Satish N. Anand on May 13, 2002, which is now U.S. Patent No. 7,213,148, issued on May 1, 2007); and Ser. No. 10/144,197 (entitled "APPARATUS AND METHOD FOR A HASH PROCESSING SYSTEM USING INTEGRATED MESSAGE DIGEST AND SECURE HASH ARCHITECTURES" filed by Satish N. Anand on May 13, 2002)."

PAGE 7/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.153

Appln. of: DAVIS, John M.
Serial No.: 10/903,785
Filed: July 30, 2004

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A security processor to process incoming and outgoing packets, the security processor comprising:

a switching system to send and receive packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming and outgoing packets; and

a cryptographic core, coupled to the packet engine and communicating incoming and outgoing packets to the switch via the packet engine, to provide encryption and decryption processing for packets received from the packet engine.

2. (Original) The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

3. (Original) The security processor of claim 1 further comprising:

a local data bus coupled to the switching system; and

a modulo engine coupled to the local data bus.

4. (Original) The security processor of claim 1 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

5. (Original) The security processor of claim 4 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

PAGE 8/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.154

6. (Original) The security processor of claim 4 wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the corresponding one of the plurality of cryptographic cores.

7. (Original) The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

8. (Original) The security processor of claim 7 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

9. (Original) The security processor of claim 7 further comprising a key management engine coupled to the local data bus.

10. (Original) The security processor of claim 1 further comprising an intrusion detection system coupled between the cryptographic core and the packet engine.

11. (Original) The security processor of claim 7 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

12. (Original) The security processor of claim 11 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

13. (Cancelled)

14. (Currently Amended) A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming and outgoing packets;

PAGE 9/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.155

a cryptographic core, coupled to the packet engine and communicating incoming and outgoing packets to the switch via the packet engine, to provide encryption and decryption processing for packets received from the packet engine; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

15. (Original) The security processing system of claim 14 further comprising a modulo engine coupled to the local data bus.

16. (Original) The security processing system of claim 15 further comprising a key management engine coupled to the local data bus.

17. (Original) The security processing system of claim 14 wherein the memory and the security processor are within the same cryptographic boundary.

18. (Original) The security processing system of claim 14 wherein the security processor is formed on a single chip.

19. (Original) The security processing system of claim 14 further comprising:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

20. (Original) The security processing system of claim 19 wherein the translator performs steganographic translation of the received data.

21. (Original) The security processing system of claim 19 wherein the translator performs encryption translation of the received data.

PAGE 10/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.156

22. (Original) The security processing system of claim 14 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

23. (Currently Amended) A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

a first interface to couple to the trusted network and to the un-trusted network;

a second interface to couple to a host processor;

a switching system operable to selectively couple to the first interface or the second interface;

a local data bus, coupled to the switching system;

a plurality of packet engines coupled to the switching system to handle classification processing for the incoming and outgoing packets;

a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from the packet engine; and

a control processor, coupled to the local data bus, to control data packet flow within the security processor.

24. (Original) The security processor of claim 23 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the untrusted network.

25. (Original) The security processor of claim 24 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

26.-29. (Cancelled)

PAGE 11/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.157

Appln. of: DAVIS, John M.
Serial No.: 10/903,785
Filed: July 30, 2004

RECEIVED
CENTRAL FAX CENTER
JAN 31 2008

REMARKS

This responds to the office action of July 31, 2007. After entry of this amendment, claims 1-12 and 14-25 are pending.

Claim 13 stood rejected under 37 CFR 1.75. That claim is now cancelled.

Claims 1-6, 10 and 13-18 stood rejected as being anticipated by Krishna et al. Those claims are amended and applicant traverses the rejection even as to the original claims. Those claims all recite that the cryptographic core is coupled to the packet engine, a feature that is not found in Krishna. Applicant notes that in Figure 2 of the present application the packets proceed in the following order: switching system 208, packet engine 228 and cryptographic core 232. As the communication path goes, the packet engine is between the switching system and the cryptographic core. Thus, independent claims 1 and 14 recite "a packet engine, coupled to the switching system" and "a cryptographic core, coupled to the packet engine." In contrast, the element ("Fig. 3 item 304") identified by the Office Action as corresponding to the claimed packet engine is coupled to the switching system in Krishna but not the cryptographic core identified by the Office Action ("Fig 3 item 316").

To make the distinction that is already in the claims (as described above) even more clear, the applicant has amended claims 1 and 14 to provide that the cryptographic core coupled to the packet engine is "communicating incoming and outgoing packets to the switch via the packet engine." Applicant respectfully notes that the same cannot be said for Krishna, where the packets are communicated from the crypto/auth 316 directly to the distributor 306 and not "via" the packet classifier 304.

Also, specifically with respect to claim 6, applicant draws the Examiner's attention to the fact that the cited references in the office action do not mention the claimed "tags" and do not seem to suggest such. It would appear that claim 6 is allowable over Krishna for the additional reason that the claimed tags are not disclosed therein.

Reconsideration and allowance is requested.

Claims 23-25 stand rejected over Ke et al. Like Krishna, Ke fails to show:

> "a plurality of packet engines coupled to the switching system to handle classification processing for the incoming and outgoing packets;

PAGE 12/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.158

> a plurality of cryptographic cores each coupled to one of the plurality of packet engines to communicate with the switching system via the plurality of packet engines and to provide encryption and decryption processing for packets received from the packet engine,"

as now recited in those claims. Like Krishna, Ke does not describe the plurality of packet engines handling the classification processing being in-line between a switch and the crypto cores. Even assuming (solely for the sake of argument) that Ke is performing the packet handling described in the claim, Ke's packet processing (for example, packet pre-processing logic 330 of Figure 3) is separated from the processors 370, 375, 380 by the switch 355. Thus, the processors 370, 375 and 380 are communicating directly with the switch—not via the packet logic as the rejected claims require.

Claims 7-9, 11, 12, 18, 19, 21, and 22 stand rejected over Krishna in view of Savarda. Savarda is not relied upon, nor does it disclose the packet engines handling packet classification between a switch and cryptographic processors, as described above with respect to the underlying base claims. Consequently, these dependent claims are also allowable for the same reasons described with respect to the base claims.

Reconsideration and allowance is requested.

CUSTOMER NUMBER
42624

Respectfully submitted,

By: _____
J. Scott Davidson
Registration No.: 33,489

Davidson Berquist Jackson & Gowdey LLP
Phone: 703.894.6400
Fax: 703.894.6430

PAGE 13/13 * RCVD AT 1/31/2008 5:25:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-4/8 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):04-26

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.159

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
10/903,785	07/30/2004	

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY ☒ RATE ($)	SMALL ENTITY ☒ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 01/31/2008	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 24	Minus	** 29	= 0	X $25 =	0	OR	X $ =	
Independent (37 CFR 1.16(h))	* 4	Minus	***4	= 0	X $105 =	0	OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/FELICIA R. FARMER/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
10/903,785	07/30/2004	John M. Davis	2551-0032

CONFIRMATION NO. 4954

42624
DAVIDSON BERQUIST JACKSON & GOWDEY LLP
4300 WILSON BLVD., 7TH FLOOR
ARLINGTON, VA 22203

POA ACCEPTANCE LETTER

OC000000026769365

Date Mailed: 11/20/2007

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/08/2007.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/rmohamed/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.161

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
10/903,785	07/30/2004	John M. Davis	4224-25 US (044.0003)

CONFIRMATION NO. 4954

29906
INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, STE. 325
SCOTTSDALE, AZ 85251

POWER OF ATTORNEY NOTICE

OC000000026769282

Date Mailed: 11/20/2007

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 11/08/2007.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/rmohamed/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.162

Best Available Copy

RECEIVED
CENTRAL FAX CENTER
NOV 0 8 2007

FACSIMILE TRANSMISSION

To: United States Patent and Trademark Office

Facsimile No.: (571) 273-8300

From: Davidson Berquist Jackson & Gowdey, LLP

No. of Pages (including this page): 3

IF YOU DO NOT RECEIVE CLEARLY ALL PAGES, PLEASE CONTACT US IMMEDIATELY BY TELEPHONE AT (703) 894-6400.

USPTO: PLEASE ACKNOWLEDGE CLEAR RECEIPT OF ALL PAGES INDICATED ABOVE BY FAXING THIS PAGE BACK TO (703) 894-6430

In re Patent Application of:	Attorney Docket No.: 2551-0032
DAVIS, John et al.	Group Art Unit: 2136
Application Serial No. 10/903,785	Confirmation No.: 4954
Filing date: July 30, 2004	Examiner: Traore, Fatoumata
Title: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	Date: November 8, 2007

Name(s) of paper(s) being transmitted:

- Executed General Power of Attorney
- Statement Under 37 CFR 3.73(B)

CERTIFICATE OF FACSIMILE TRANSMISSION				
I hereby certify that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office at the above facsimile number on the date shown below.				
Name:	Sarah Lanning	Signature: Sarah Lanning	Date:	11/08/2007

CUSTOMER NUMBER

42624

DAVIDSON BERQUIST JACKSON & GOWDEY, LLP
4300 WILSON BLVD., 7TH FLOOR, ARLINGTON, VA 22203
703.894.6400 (main) • 703.894.6430 (Fax)

PAGE 1/3 * RCVD AT 11/8/2007 3:04:54 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/2 * DNIS:2738300 * CSID:7038946430 * DURATION (mm-ss):01-40

Best Available Copy

RECEIVED
CENTRAL FAX CENTER
NOV 08 2007

STATEMENT UNDER 37 CFR 3.73(B)

Applicant / Patent Owner: DAVIS, John et al. Docket No. 2551-0032

Application No. / Patent No. 10/903,785 Filed / Issued Date: July 30, 2004

Entitled: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Assignee: ITT MANUFACTURING ENTERPRISES, INC. A Corporation
(Name of assignee) (Type of Assignee: corporation, partnership, university, government agency, etc.)

States that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest. (The extent (by percentage) of its ownership interest is %)

in the patent application / patent identified above by virtue of either:

A. ☐ An assignment from the inventor(s) of the patent application / patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel , Frame , or for which a copy thereof is attached.

OR

B. ☒ A chain of title from the inventor(s), of the patent application / patent identified above, to the current assignee shown below:

1.	From: Inventors To: Corrent Corporation The document was recorded in the United States Patent and Trademark Office at Reel 015256 Frame 0889, or for which a copy thereof is attached.
2.	From: Corrent Corporation To: ITT Manufacturing Enterprises, Inc. The document was recorded in the United States Patent and Trademark Office at Reel 020056 Frame 0483, or for which a copy thereof is attached.
3.	From: _____ To: _____ The document was recorded in the United States Patent and Trademark Office at Reel _____ Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.

☐ Copies of assignments or other documents in the chain of title are attached.

As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[Note: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Signature — November 8, 2007 Date

J. Scott Davidson — 703-894-6401

Printed or Typed Name — Telephone Number

Attorney, Registration No. 33,489

Title: _____

Best Available Copy

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

POWER OF ATTORNEY, CORRESPONDENCE ADDRESS AND REVOCATION OF PRIOR POWERS

RECEIVED
CENTRAL FAX CENTER
NOV 0 8 2007

Hon. Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Revocation: I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

Power of Attorney: I hereby appoint the practitioners associated with customer number **42624**, individually and collectively, as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

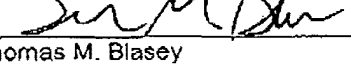
I authorize Davidson Berquist Jackson & Gowdey, LLP to delete names/numbers of persons no longer with the Firm and to act and rely on instructions from and communicate directly with the entity who first sent this case to them and by whom I hereby declare that I have consented after full disclosure to be represented unless/until I instruct Davidson Berquist Jackson & Gowdey, LLP in writing to the contrary.

Correspondence Address: Please recognize or change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to the address associated with Customer Number **42624**.

Assignee Name and Address:

ITT MANUFACTURING ENTERPRISES, INC.
1105 North Market Street, Suite 1217
Wilmington, DE 19801

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record The individual whose signature and title is supplied below is authorized to act on behalf of the assignee			
Signature		Date	11/5/07
Name	Thomas M. Blasey	Telephone	703-790-6314
Title	Assistant Secretary		

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/903,785	07/30/2004	John M. Davis	4224-25 US (044.0003)	4954

29906 7590 07/31/2007

INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, STE. 325
SCOTTSDALE, AZ 85251

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
07/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/903,785	DAVIS ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *30 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 July 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.167

DETAILED ACTION

1. This action is in response of the original filing of July 30th 2004. Claims 1-29 are pending and have been considered below.

Claim Objections

2. Claim 13 is objected to under 37 CFR 1.75 as being a substantial duplicate of claim 10. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Specification

3. The listing of references in the specification is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609.04(a) states, "the list may not be incorporated into the specification but must be submitted in a separate paper." Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered. Applicant is required to update the status of the cited applications number (see pages 7, 12, 16 and 18).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-6, 10, 13-17are rejected under 35 U.S.C. 102(e) as being anticipated by Krishna et al (US 2003/0014627).

Claim 1: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip comprising:

i. A switching system to send and receive packets (Fig. 3 items 302, 306, 318 and paragraphs [0010]-[0012]);

ii. A packet engine, coupled to the switching system, to handle classification

processing for the incoming and outgoing packets (Fig. 3 item 304 and paragraphs [0010]-[0012]); and

iii. A cryptographic core, coupled to the packet engine, to provide encryption and

decryption processing for packets received from the packet engine(Fig. 3 item 316 and paragraphs [0010]-[0012]).

Claim 2: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses that the packet engine is further operable to handle security context management processing for the incoming and outgoing packets (According to this configuration, packets are received from the LAN or WAN and go directly through the cryptography acceleration chip and are processed as they are received from or are about to be sent out on the WAN, providing automatic security processing for IP packets) (paragraphs [0029], [0038]).

Claim 3: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses that the security processor comprises:

iv. A local data bus coupled to the switching system (As shown in FIG. 1A, the cryptography acceleration chip 102 may be part of an otherwise standard network line card 103 which includes a WAN interface 112 that connects the processing system 100 to a WAN, such as the Internet, and manages in-bound and out-bound packets) (paragraphs [0027], [0030], [0037]); and

v. A modulo engine coupled to the local data bus (The chip 102 on the card 103 may be connected to a system bus 104 via a standard system interface 106. The system bus 104 may be, for example, as standard PCI

bus, or it may be a high speed system switching matrix, as are well known to those of skill in the art. The processing system 100 includes a processing unit 114, which may be one or more processing units, and a system memory unit 116) (paragraphs [0027], [0030], [0037]).

Claim 4: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines (he architecture enables parallel processing of packets through a plurality of cryptography engines, for example four, and includes a classification engine configured to efficiently process encryption/decryption of data packets) (paragraph [0024], [000027]).

Claim 5: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 4 above, and further discloses that the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines (the architecture enables parallel processing of packets through a plurality of cryptography engines and includes a classification engine configured

to efficiently process encryption/decryption of data packets) (paragraphs [0010], [0024], [0042], [0052])

Claim 6: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 4 above, and further discloses the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the 5 corresponding one of the plurality of cryptographic cores (Thus it would be desirable to have a cryptography accelerator chip architecture that is capable of implementing the IPSec specification (or any other cryptography standard), at much faster rates than are achievable with current chip designs) (paragraphs [0009], [0038], [0060]).

Claims 10, 13: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 1 above, and further discloses an intrusion (filtering/blocking) detection system coupled between the cryptographic core and the packet engine (the classifier includes four different modes that allow all IPSec selector matching operations to be supported, as well as general purpose packet matching for packet filtering purposes, for fragment re-assembly purposes, and for site blocking purposes) (paragraphs [0040], [0041], [0052], [0058]);

Claim 14: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip comprising:

vi. A switching system to send and receive packets(Fig. 3 items 302, 306, 318 and paragraphs [0010]-[0012]);

vii. A packet engine, coupled to the switching system, to handle classification

processing for the incoming and outgoing packets(Fig. 3 item 304 and paragraphs [0010]-[0012]); and

viii. A cryptographic core, coupled to the packet engine, to provide encryption and

decryption processing for packets received from the packet engine(Fig. 3 item 316 and paragraphs [0010]-[0012]); and

ix. A local data bus coupled to the switching system (As shown in FIG. 1A, the cryptography acceleration chip 102 may be part of an otherwise standard network line card 103 which includes a WAN interface 112 that connects the processing system 100 to a WAN, such as the Internet, and manages in-bound and out-bound packets) (paragraphs [0027], [0030], [0037]);

x. A memory coupled to the local data bus (paragraphs [0026], [0027], [0038].

Claim 15: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, and further discloses a modulo engine coupled to the local data bus (The chip 102 on the card 103 may be connected to a system bus 104 via a standard system interface 106. The system bus 104 may be, for example, as standard PCI bus, or it may be a high speed system switching matrix, as are well known to those of skill in the art. The processing system 100 includes a processing unit 114, which may be one or more processing units, and a system memory unit 116) (paragraphs [0027], [0030], [0037]).

Claim 16: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 15 above, and further discloses a key management engine coupled to the local data bus (paragraphs [0011], [0012], [0038], [0056]).

Claim 17: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, and further discloses that the memory and the security processor are within the same cryptographic boundary (Fig.2 items 204, 212, 214).

6. Claims 23-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Ke et al (US 7095716).

Claim 23: **Ke et al** discloses an Internet security processor comprising:

xi. A first interface to couple to the trusted network and to the un-trusted network;

xii. A second interface to couple to a host processor;

a switching system operable to selectively couple to the first interface or the

second interface;

xiii. A local data bus, coupled to the switching system (column 4, lines 28-39 and Fig.2, Fig.3);

xiv. A plurality of packet engines coupled to the switching system system (column 4, lines 28-39 and Fig.2, Fig.3);

xv. a plurality of cryptographic cores each coupled to one of the plurality of packet

engines system (column 4, lines 28-39 and Fig.2, Fig.3); and

xvi. A control processor, coupled to the local data bus, to control data packet flow

within the security processor system (column 4, lines 28-39 and Fig.2, Fig.3).

Claim 24: **Ke et al** discloses an Internet security processor as in claim 23 above, and further discloses that the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel

with another computing device in the un-trusted network The one or more processing boards can process the received data packets by performing one or more of: policy enforcement, virtual private network traffic encryption and decryption, key negotiation, firewall protection, network address translation, tunnel encapsulation and de-capsulation, and hot backup between processing boards) (column 2 lines 25-58, column 10 lines 46-51, abstract and Fig.6B).

Claim 25: **Ke et al** discloses an Internet security processor as in claim 24 above, and further discloses that the security processor implements data packet security and authentication functions to support the secure communication channel (After the packet passes the inspection provided by the stateful inspection engine (645) (e.g., the packet is authenticated)(column 11, lines 17-24).

Claim 26: **Ke et al** discloses an Internet security processor comprising:
A trusted network (column 4, lines 28-39 and Fig.2, 3); and
A secure interface coupled to the trusted network to carry all incoming and outgoing communications of the trusted network, wherein the secure interface comprises a security processor to handle substantially all security processing for the incoming and outgoing communications (column 4, lines 28-39 and Fig. 3, 4).

Claim 27: **Ke et al** discloses an Internet security processor as in claim 26 above, and further discloses that the security processor performs substantially all

network processing for data packet communications traveling to and from the trusted network (column 4 line 28 to column 5 line 65, and Fig. 2, 3, 4).

Claim 28: **Ke et al** discloses an Internet security processor as in claim 27 above, and further discloses the secure interface handles substantially all security processing for the incoming and outgoing communications (column 4 line 28 to column 5 line 65, and Fig. 2, 3, 4).

Claim 29: **Ke et al** discloses an Internet security processor as in claim 28 above, and further discloses that the information security processing comprises IPSec processing

(column 4 line 28 to column 5 line 65, and Fig. 2, 3, 4).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 7-9, 11, 12, 18, 19, 21, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Krishna et al** (US 2003/0014627) in view of **Savarda et al** (US 2003/0196081).

Claims 7, 18: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claims 3 and 14 above, but does not explicitly discloses that the

cryptographic core, and the modulo engine are formed on a single chip. However, **Savarda et al** discloses a system fro processing a packet object using multiple pipelined processing modules, which further discloses cryptographic core, and the modulo engine in a single chip (Fig.1 and paragraph [0024]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include the cryptographic core and the modulo engine on a single chip in **Krishna et al**'s disclosure. On would have been motivated to do so in order to increase the performance and to lower cost associate with the fabrication.

Claim 8: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and **Savarda et al** further discloses a control processor coupled to the local data bus, for exception handling of the incoming and outgoing packets (The packet inspection/outbound policy module 108 may be configured with multiplexing circuitry to integrate the outbound and inbound packet streams into a single stream for pipeline processing in the packet co-processor 100. In addition, the packet inspection/outbound policy module 108 may be further configured to inspect packet-objects to ensure their integrity) (paragraph [0031]). Therefore, it would

have been obvious to one having ordinary skill in the art at the time the invention was made to handle exception of incoming and outgoing packets in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity.

Claim 9: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and **Krishna et al** further discloses that a key management engine coupled to the local data bus (paragraphs [0011], [0012], [0038], [0056]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to couple the key management engine to the local data bus in **Krishna et al**'s disclosure. On would have been motivated to do so in order to increase system performance.

Claim 11: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 7 above, and **Krishna et al** further discloses that the security processor handles substantially all security processing for the incoming and outgoing packets (The IPSec cryptography protocol specifies two levels of lookup: Policy (Security Policy Database (SPD) lookup) and Security Association (Security Association Database (SAD) lookup) (paragraphs [0029], [0039], [0056]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to handle

security processing in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 12: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 11 above, and **Krishna et al** further discloses that the security processor further handles substantially all network processing for the incoming and outgoing packets (According to this configuration, packets are received from the LAN or WAN and go directly through the cryptography acceleration chip and are processed as they are received from or are about to be sent out on the WAN, providing automatic security processing for IP packets) (paragraphs [0029], [0039], [0056]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to handle security processing in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 19: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, and **Krishna et al** further discloses a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface (Fig. 1A), but does not explicitly discloses a translator coupled to the memory interface to perform translation of

data received by the memory interface from the memory. However, **Savarda et al** discloses a system fro processing a packet object using multiple pipelined processing modules, which further discloses a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory (the SAD contains parameter information about each SA. Such parameters may include the security protocol algorithms and keys for Authentication Header (AH) or Encapsulating Security Payload (ESP) security protocols, sequence numbers, protocol mode, and SA lifetime. For outbound packets, the SPD is consulted to determine if IPSec processing is required and/or if other processing or discarding of the packet is to be performed. If IPSec is required, then the outbound SAD is searched for an existing SA that matches the packet profile) (paragraphs [0004], [0009], [0024], [0026]). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a translator in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 21 **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 19 above, and **Savarda et al** further discloses that the translator performs encryption translation of the received data (the cryptographic chip may perform the encryption, decryption, and/or authentication transforms as required. After completion of the cryptographic

operations, the system processor may further process the packet to finish any remaining IPSec transforms) (paragraphs [0007], 0026] and Fig.6). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt received data in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Claim 22: **Krishna et al** discloses a distributed processing in a cryptographic acceleration chip as in claim 14 above, but does not explicitly discloses a step of executing a boot code or a step authenticating the code. However, **Savarda et al** discloses a system fro processing a packet object using multiple pipelined processing modules, which further discloses

xvii. Execute boot code to load firmware for execution by the security processor (One approach is based primarily on software. For example, dedicated software modules may be developed for execution on a workstation to implement the IP packet manipulations, encryption, and authentication operations associated with the IPSec protocol)(paragraphs [0006], [007], [0019]); and

xviii. Authenticate the boot code using a mechanism internal to the 10 security processor prior to operation of the security processor (This approach, however, may be limited in its performance as the system processor performs many or all of the functions. Encryption, decryption,

and/or authentication are typically processor intensive)(paragraphs [0006], [007], [0019]).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to execute and encrypt the code in **Krishna et al**'s disclosure. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

9. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Krishna et al** (US 2003/0014627) in view of **Savarda et al** (US 2003/0196081) as applied to claim 19 above, in further view of **Carr et al** (US 6788800).

Claim 20: **Krishna et al** and **Savarda et al** disclose a distributed processing in a cryptographic acceleration chip as in claim 19 above, while neither of them explicitly discloses a translator performing steganographic translation of the received data. However, **Carr et al** discloses an authentication object using embedded data, which further discloses a step of performing steganographic translation of the received data (it also steganographically embeds security data into product) (column 1, lines 38-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combine system **Krishna et al** and **Savarda et al** such as to perform steganographic translation. On would have been motivated to do so in order to maintain system integrity by not allowing unauthorized access to the system.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

b. Huynh et al (US 6983366) Packet processor.

c. Pandya (US (2004/0010545) Data processing system using internet protocos and RDMA.

d.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Wednesday July 25th 2007

Nassar G. Moazzami
Supervisory Patent Examiner
7/26/07

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OIPE JC
DEC 10 2004
PATENT & TRADEMARK OFFICE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	10/903,785
Filing Date	July 30, 2004
First Named Inventor	John M. DAVIS
Art Unit	2135
Examiner Name	Unknown
Attorney Docket Number	4224-25 US (044.0003)

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number: Number - Kind Code[2] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/F.T./		US-2002/0066014 A1	05/30/2002	Dworkin et al.	
/F.T./		US-2002/0108059 A1	08/08/2002	Canion et al.	
/F.T./		US-5,432,950	07/11/1995	Sibigtroth	
/F.T./		US-5,737,760	04/07/1998	Grimmer, Jr. et al.	
/F.T./		US-5,892,899	04/06/1999	Aucsmith et al.	
/F.T./		US-5,940,626	08/17/1999	Sollars	
/F.T./		US-6,041,122	03/21/2000	Graunke et al.	
/F.T./		US-6,049,876	04/11/2000	Moughanni et al.	
/F.T./		US-6,101,255	08/08/2000	Harrison et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] – Number[4] – Kind Code[5] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature	/Fatoumata Traore/	Date Considered	07/25/2007

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation in not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and selection option 2.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 | 3

Complete if Known	
Application Number	10/903,785
Filing Date	July 30, 2004
First Named Inventor	John M. DAVIS
Art Unit	2135
Examiner Name	Unknown
Attorney Docket Number	4224-25 US (044.0003)

Examiner Initials*	Cite No.[1]	NON PATENT LITERATURE DOCUMENTS Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/F.T./		MOTOROLA, Digital DNA, Technical Summary, MPC184TS/D, Rev. 1, 6/2002, MPC 184 Security Processor	
/F.T./		Intel® IXP2400 Network Processor: Flexible, High-Performance Solution for Access and Edge Applications, pp. 1-7.	
/F.T./		Intel® Addressing Next-Generation CPE Challenges, The Role of the Intel® XScale™ Technology-based Intel® IXP425 Network Processor in CPE, Intel® Internet Exchange Architecture, February 2002, pp. 1-8.	
/F.T./		Delivering the Next Generation of Broadband Services over the Last Mile, Introducing a New Multi-Service Processor Architecture™, Brecis Communications, March, 2001, pp. 1-8.	
/F.T./		C-PORT™ A Motorola Company, C-5™ Network Processor Data Sheet, Supporting C-5 Network Processor Version DO, January 21, 2002 - Preliminary Version, pp. 1-96.	
/F.T./		DONALD L. EVANS, PHILLIP J. BOND, ARDEN L. BEMENT, Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, May 25, 2001 pp. i-viii, 1-61.	
/F.T./		PATRICK CROWLEY, MARK A. FRANKLIN, HALDUN HADIMIOGLU, PETER Z. ONUFRYK, Network Processor Design Issues and Practices, Volume 1, Chapter 2, pp. 12-13, 148-154, 172-175; Chapter 9, pp. 192-218; Chapter 10, 220-248; and Chapter 12, 250-275, Morgan Kaufmann Publishers, 2003, San Francisco, California.	
/F.T./		Corrent's Families of Security Processors [retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com>.	
/F.T./		Comm Week. Startups take next step at NPU confab [online]. Robert Keenan [retrieved on 6/23/03]. Retrieved from Internet: <URL:www.eet.com>.	
/F.T./		Corrent. The Security Processing Company. Corrent Introduces Industry's First Complete Security Processor Securing Next Generation Internet Transactions Today [online]. May 6, 2002, Las Vegas, NV [retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/press15.phtml>.	
/F.T./		Corrent. The Security Processing Company. Socket Armor™ CR7020 SSL Security Processor [online]. [Retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/products_socket.phtml>.	
/F.T./		Corrent. The Security Processing Company. Packet Armor™ CR7120 IPsec Security Processor [online]. [Retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/products_packet.phtml>.	
/F.T./		Corrent. The Security Processing Company. Corrent Takes Industry Lead With Delivery Of Single-Chip Gigabit Speed Internet Security Processors [online]. December 10, 2001, Tempe, AZ [Retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/press8.phtml>.	
/F.T./		Corrent. The Security Processing Company. Corrent Offers Gigabit-rate VPN/SSL Performance With a Cost-Effective Enterprise and Server PCI Card Solution [online]. December 2, 2002, Tempe, AZ [Retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/press20.phtml>.	
/F.T./		Corrent. The Security Processing Company. Breakthrough Security Performance At Unparalleled Price Point From Check Point And Corrent [online]. March 24, 2003, Redwood City, CA and Tempe, AZ [Retrieved on 4/4/03]. Retrieved from Internet: <URL:www.corrent.com/press24.phtml>.	
/F.T./		Intel® IXP425 Network Processor Family [online]. 2002 [Retrieved on 9/10/02]. Retrieved from Internet: <URL:www.intel.com/design/network/products/npfamily/ixp425.htm>.	
/F.T./		EETimes. Developers Must Balance NPU Programmability and Performance Issues [online] August 5, 2002. (Retrieved on 9/10/02). Retrieved from Internet: <URL:www.eetimes.com/in_focus/embedded_systems/OEG20020802S0032>.	
/F.T./		TechWeb. Algorithm Hides Data Inside Unaltered Images [online] Colin Johnson, June 23, 1999 [Retrieved on 9/16/02]. Retrieved from Internet: <URL:www.techweb.com/wire/story/TWB19990623S0001>.	
/F.T./		Electronic Engineering Times, Headline: Broadcom [online] March 4, 2002 [Retrieved on 9/6/02]. Retrieved from Internet: <URL:www.eetimes.com>.	

Examiner Signature	/Fatoumata Traore/	Date Considered	07/25/2007

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation in not in conformance and not considered. Include copy of this form with next communication to applicant.
[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.
This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO_9199 (1-800-786-9199) and selection option 2.

PTO/SB/08b (08-03)
Approved for use through 08/30/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 3 of 3

Complete If Known	
Application Number	10/903,785
Filing Date	July 30, 2004
First Named Inventor	John M. DAVIS
Art Unit	2135
Examiner Name	Unknown
Attorney Docket Number	4224-25 US (044.0003)

Examiner Initials*	Cite No.[1]	NON PATENT LITERATURE DOCUMENTS Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/F.T./		Electronic Engineering Times, Headline: Security chip speeds SSL/TLS record processing [online] July 8, 2002 [Retrieved on 9/6/02]. Retrieved from Internet: <URL:www.Broadcom.com>.	
/F.T./		Motorola. MPC184: Security Processor [online] [Retrieved on 9/10/02]. Retrieved from Internet: <URL:www//e-www.motorola.com/webapp/sps/…/prod_summary.jsp?code=MPC184&nodeId=01M9732135977 2>.	

Examiner Signature	/Fatoumata Traore/	Date Considered	07/25/2007

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation in not in conformance and not considered. Include copy of this form with next communication to applicant.
[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.
This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO_9199 (1-800-786-9199) and selection option 2.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.187

Notice of References Cited	Application/Control No. 10/903,785	Applicant(s)/Patent Under Reexamination DAVIS ET AL.	
	Examiner Fatoumata Traore	Art Unit 2136	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0014627	01-2003	Krishna et al.	713/153
*	B	US-7,095,716	08-2006	Ke et al.	370/230
*	C	US-2003/0196081	10-2003	Savarda et al.	713/153
*	D	US-6,788,800	09-2004	Carr et al.	382/100
*	E	US-2004/0010545	01-2004	Pandya, Ashish A.	709/203
*	F	US-6,983,366	01-2006	Huynh et al.	713/168
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	Art Unit
	Traore, Fatoumata	2136

SEARCHED

Class	Subclass	Date	Examiner
713	189, 160, 151, 153, 168	07/25/2007	FT

SEARCH NOTES

Search Notes	Date	Examiner
EAST attached	07/24/2007	FT

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.189

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10903785	DAVIS ET AL.
	Examiner	Art Unit
	Traore, Fatoumata	2136

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/25/2007								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.190

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 4954

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/903,785	07/30/2004 RULE	713	2136	4224-25 US (044.0003)

APPLICANTS

John M. Davis, Brentwood, TN;
Richard J. Takahashi, Phoenix, AZ;

**** CONTINUING DATA ***************************

This appln claims benefit of 60/507,976 10/02/2003

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY ****

10/04/2004

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /FATOUMATA TRAORE/ Examiner's Signature	☐ Met after Allowance FT Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		TN	10	29	4

ADDRESS

INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, STE. 325
SCOTTSDALE, AZ 85251
UNITED STATES

TITLE

System and method for a secure I/O interface

FILING FEE RECEIVED		
574	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2303	process$3 same as (packet or data or frame or datagram$2 or file or messag$3 or mail) same (cryptograph$43 or encrypt$3 or encipher$3 or cipher$3 or scramble$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:23
L2	1813	713/189	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:23
L3	121	1 and 2	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:24
L4	76	3 and bus	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:24
L5	1364	1 and ((packet or data or file or message) same (classificat$3 or classif$3 or categori$7 or group$3 or arrang$5 or sort$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:35
L6	661	713/160	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:35
L7	27	6 and 5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:44

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.192

EAST Search History

L8	4613	713/151 or 713/153 or 713/168	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:44
L9	131	5 and 8	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:44

Cisco Systems, Inc. v. Innra Technologies Ltd.
EX-1002 p.193

EAST Search History

L10	98	US-4423287-$.DID. OR US-5784459-$.DID. OR US-4885789-$.DID. OR US-5619657-$.DID. OR US-5822431-$.DID. OR US-5884277-$.DID. OR US-6092202-$.DID. OR US-6115819-$.DID. OR US-6199113-$.DID. OR US-6247129-$.DID. OR US-4386234-$.DID. OR US-4755940-$.DID. OR US-4864615-$.DID. OR US-4864616-$.DID. OR US-4870681-$.DID. OR US-4901348-$.DID. OR US-4910773-$.DID. OR US-4933971-$.DID. OR US-4956862-$.DID. OR US-4965568-$.DID. OR US-4985919-$.DID. OR US-4997288-$.DID. OR US-5008936-$.DID. OR US-5012515-$.DID. OR US-5016277-$.DID. OR US-5022076-$.DID. OR US-5032979-$.DID. OR US-5201000-$.DID. OR US-5235641-$.DID. OR US-5241594-$.DID. OR US-5261070-$.DID. OR US-5268962-$.DID. OR US-5301231-$.DID. OR US-5359660-$.DID. OR US-5416842-$.DID. OR US-5436857-$.DID. OR US-5506393-$.DID. OR US-5553280-$.DID. OR US-5588060-$.DID. OR US-5590196-$.DID. OR US-5596718-$.DID. OR US-5633933-$.DID. OR US-5657388-$.DID. OR US-5675771-$.DID. OR US-5684950-$.DID. OR US-5724274-$.DID. OR US-5742845-$.DID. OR US-5774879-$.DID. OR US-5778071-$.DID. OR US-5781724-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:54

Cisco Systems, Inc. v. Lianra Technologies Ltd.
EX-1002 p.194

EAST Search History

L11	5	10 and 1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:54
L12	16	US-20020108059-$.DID. OR US-5892899-$.DID. OR US-6049876-$.DID. OR US-6101255-$.DID. OR US-20020066014-$.DID. OR US-5432950-$.DID. OR US-5940628-$.DID. OR US-5737760-$.DID.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:14
L13	2	"20030196081".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:15
L14	121	2 and 1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:15
L15	121	14 and 1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:16
L16	1	13 and 1	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 09:16
S1	31272	(processor or microprocessor or device or computer) same (send$3 or transfer$3 or receiv$3) same (packet or data or file or message) same (cryptograph$3 or encrypt$3 or encipher$3 or decrypt$3 or decipher$3 or scrambl$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:42

Cisco Systems v. Lianra Technologies Ltd.
EX-1002 p.195

EAST Search History

S2	2362	(processor or microprocessor or device or computer) same (send$3 or transfer$3 or receiv$3) same (packet or data or file or message) same (cryptograph$3 or encrypt$3 or encipher$3 or decrypt$3 or decipher$3 or scrambl$3)same (bus)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:42
S3	17568	S1 and (packet or data or file or message) same (classificat$3 or classif$3 or categori$7 or group$3 or arrang$5 or sort$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:48
S4	17568	S1 and ((packet or data or file or message) same (classificat$3 or classif$3 or categori$7 or group$3 or arrang$5 or sort$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:35
S5	1537	S2 and ((packet or data or file or message) same (classificat$3 or classif$3 or categori$7 or group$3 or arrang$5 or sort$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:49
S6	3731	S4 and (security same management)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:50
S7	451	S6 and ((incom$3 or outg$3)same packet)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:51
S8	0	S7 and (packet near engine same bus same cryptogra$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/24 15:52

Cisco Systems Inc. v Lianra Technologies Ltd.
EX-1002 p.196

EAST Search History

S9	28	S7 and (packet near engine)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	ADJ	ON	2007/07/25 08:04

Cisco Systems, Inc. v. Lionra Technologies Ltd.
EX-1002 p.197

PLUS Search Results for S/N 10903785, Searched Tue Jul 17 08:34:09 EDT 2007

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

4423287 99
4885789 99
5619657 99
5822431 99
5884277 99
6092202 99
6115819 99
6199113 99
6247129 99
4386234 99
4755940 99
4864615 99
4864616 99
4870681 99
4901348 99
4910773 99
4933971 99
4956862 99
4965568 99
4985919 99
4997288 99
5008936 99
5012515 99
5016277 99
5022076 99
5032979 99
5201000 99
5235641 99
5241594 99
5261070 99
5268962 99
5301231 99
5359660 99
5416842 99
5436857 99
5506393 99
5553280 99
5588060 99
5590196 99
5596718 99
5633933 99
5657388 99
5675771 99
5684950 99
5724274 99
5742845 99
5774879 99
5778071 99
5781724 99
5784459 99

INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, SUITE 325
SCOTTSDALE, ARIZONA 85251
Telephone: (480) 385-5060
Facsimile: (480) 385-5061

RECEIVED
CENTRAL FAX CENTER
MAY 23 2005

FACSIMILE TRANSMITTAL SHEET

TO:	FROM:
	Paul D. Amrozowicz, Reg. No. 45,264
COMPANY: USPTO	DATE: MONDAY, MAY 23, 2005
FAX NUMBER: (703) 872-9306	TOTAL NO. OF PAGES INCLUDING COVER: 10
PHONE NUMBER: (703) 308-4357	SENDER'S REFERENCE NUMBER: 4224-25 US (044.0003)
RE: Third Submission of Revocation Of Power Of Attorney With Appointment Of New Power Of Attorney And Change Of Correspondence Address	REFERENCE NUMBER: 10/903,785

NOTES/COMMENTS:

FORMAL COMMUNICATION INTENDED FOR ENTRY

THIS MESSAGE IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED, AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL AND EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAWS. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, OR THE EMPLOYEE OR AGENT RESPONSIBLE FOR DELIVERING THE MESSAGE TO THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE AND RETURN ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA U.S. POSTAL SERVICE. THANK YOU.

BEST AVAILABLE COPY

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	John M. DAVIS et al.	Group Art Unit: 2135	
Serial No.:	10/903,785	Examiner: Unknown	
Filed:	July 30, 2004	Confirmation No.: 4954	

RECEIVED
CENTRAL FAX CENTER
MAY 23 2005

For: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Docket No.: 4224-25 US (044.0003)

Customer No. : 29906

CERTIFICATE OF MAILING OR TRANSMISSION UNDER 37 C.F.R. § 1.8(a)

I hereby certify that this correspondence is being transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) 872-9306.

on 5/23/05. Signature: _____
Paul D. Amrozowicz

THIRD SUBMISSION OF REVOCATION OF POWER OF ATTORNEY WITH APPOINTMENT OF NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On October 18, 2004, Applicant submitted a combined Revocation and Power of Attorney and Appointment of New Power of Attorney and Change of Correspondence Address (hereinafter "the Request") for 2 patents and 21 pending patent applications presently assigned to the Assignee of the instant application. The Request included a listing of each patent and patent application for which the requested change should be made.

PAGE 2/10 * RCVD AT 5/23/2005 12:18:07 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-38

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.200

Applicant's current representatives checked the Patent Application Information and Retrieval (PAIR) system and noted that the electronic file wrappers for each of the applications for which the requested change was made includes a copy of the Request. However, of the 21 applications included in the initial Request, only 3 had the requested correspondence address change implemented. Thus, Applicants filed a Second Submission of Revocation of Power of Attorney With Appointment of New Power of Attorney and Change of Correspondence Address on February 3, 2005.

Once again Applicant's current representatives have checked the Patent Application Information and Retrieval (PAIR) system and note that the electronic file wrappers for each of the applications for which the requested change was made includes a copy of the Request. However, of the 18 applications included in the Second Request, only 9 had the requested correspondence address change implemented.

In the interim, correspondence from the U.S. Patent and Trademark Office continues to be sent to the previous correspondence address(es) of record, resulting in wasted time and effort on the part of several involved parties. As such, the Assignee of the above-referenced application once again requests that the Office please:

- **Revoke all previous powers of attorney in this application;**
- **Appoint the practitioners associated with Customer Number 29906; and**
- **Change the correspondence address for this application to the address associated with Customer Number 29906.**

PAGE 3/10 * RCVD AT 5/23/2005 12:18:07 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-38

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.201

A copy of the Request that was submitted on October 18, 2004, which included a Statement under 37 CFR 3.73(b) from the Assignee, and a copy of the Second Request filed on February 3, 2005, are included herewith.

Respectfully submitted,

INGRASSIA FISHER & LORENZ

Dated: 5/23/05

By: _____

Paul D. Amrozowicz
Reg. No. 45,264
(480) 385-5060

PAGE 4/10 * RCVD AT 5/23/2005 12:18:07 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-38

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.202

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL FAX CENTER
MAY 23 2005

In re application of:	John M. DAVIS et al.	Group Art Unit: 2135	
Serial No.:	10/903,785	Examiner: Unknown	
Filed:	July 30, 2004	Confirmation No.: 4954	

For: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Docket No.: 4224-25 US (044.0003)

Customer No. : 29906

CERTIFICATE OF MAILING OR TRANSMISSION UNDER 37 C.F.R. § 1.8(a)

I hereby certify that this correspondence is being transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) 872-9306.

on 5/23/05 . Signature: _____
Paul D. Amrozowicz

SECOND SUBMISSION OF REVOCATION OF POWER OF ATTORNEY WITH APPOINTMENT OF NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On October 18, 2004, Applicant submitted a combined Revocation and Power of Attorney and Appointment of New Power of Attorney and Change of Correspondence Address (hereinafter "the Request") for 2 patents and 21 pending patent applications presently assigned to the Assignee of the instant application. The Request included a listing of each patent and patent application for which the requested change should be made.

PAGE 5/10 * RCVD AT 5/23/2005 12:18:07 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-38

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.203

Applicant's current representatives have checked the Patent Application Information and Retrieval (PAIR) system and note that the electronic file wrappers for each of the applications for which the requested change was made includes a copy of the Request. However, of the 21 applications included in the initial Request, only 3 have had the requested correspondence address change implemented. The instant application is not one of those three.

In the interim, correspondence from the U.S. Patent and Trademark Office continues to be sent to the previous correspondence address(es) of record, resulting in wasted time and effort on the part of several involved parties. As such, the Assignee of the above-referenced application once again requests that the Office please:

- **Revoke all previous powers of attorney in this application;**
- **Appoint the practitioners associated with Customer Number 29906; and**
- **Change the correspondence address for this application to the address associated with Customer Number 29906.**

A copy of the Request that was submitted on October 18, 2004, which included a Statement under 37 CFR 3.73(b) from the Assignee, is included herewith.

Respectfully submitted,

INGRASSIA FISHER & LORENZ

Dated: 2/8/05

By: _____
Paul D. Amrozowicz
Reg. No. 45,264
(480) 385-5060

PAGE 6/10 * RCVD AT 5/23/2005 12:18:07 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-38

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.204

RECEIVED
CENTRAL FAX CENTER
MAY 23 2005

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

REVOCATION OF POWER OF ATTORNEY WITH APPOINTMENT OF NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

REVOCATION OF POWER OF ATTORNEY WITH APPOINTMENT OF NEW POWER OF ATTORNEY

I hereby revoke all previous powers of attorney given in each of the pending U.S. patent applications listed in the attached Exhibit A and in each of the issued U.S. patents listed in the attached Exhibit B.

I hereby appoint the practitioners associated with Customer Number **29906** in each of the above-identified matters.

CHANGE OF CORRESPONDENCE ADDRESS

Please change the correspondence address for each of the pending U.S. patent applications listed in the attached Exhibit A and for each of the issued U.S. patents listed in the attached Exhibit B to the address associated with Customer Number **29906**.

I am the Assigneeof record of the entire interest of each of the pending U.S. patent applications each of the issued U.S. patents. A Statement under 37 CFR 3.73(b) is included.

Assignee of Interest: Corrent Corporation

Date: 10/6/2004

By: _____
Name: Richard Takahashi
Title: CEO, President

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.205

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

STATEMENT UNDER 37 CFR 3.73(b)

The undersigned is a representative authorized and empowered to act on behalf of Corrent Corporation (hereinafter "Assignee"), and states that it is the assignee of the entire right, title, and interest in and to each of the patent applications listed in the attached Exhibit A and each of the issued patents listed in the attached Exhibit B by virtue of the respective assignments from the inventor(s) of the patent applications/patents identified in the attached Exhibits. The assignments were each recorded in the U.S. Patent and Trademark Office at the Reel/Frame indicated in the attached Exhibits.

Date: 10/6/2004

By: _____
Name: Richard Takahashi
Title: CEO, President

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.206

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

EXHIBIT A

Serial Number	Filing Date	Reel/Frame
10/144,004	05/13/02	013437/0592
10/144,332	05/13/02	013562/0932
09/978,742	10/16/01	012675/0184
10/172,814	06/12/02	013223/0463
09/998,715	11/30/01	012344/0870
09/911,149	07/23/01	012045/0727
09/921,677	08/03/01	012061/0464
09/877,473	06/08/01	011908/0162
09/880,701	06/13/01	012281/0840
10/144,195	05/13/02	013457/0718
10/144,197	05/13/02	013562/0929
09/970,901	10/04/01	012582/0026
09/994,141	11/26/01	012749/0976
09/971,325	10/04/01	012239/0040
09/877,470	06/08/01	011907/0894
09/880,700	06/13/01	012272/0744
09/880,699	06/13/01	012272/0737
10/161,070	05/31/02	013255/0672
10/160,330	05/30/02	012972/0159
10/191,632	07/09/02	013457/0672
10/903,785	07/30/04	See attached Assignment

EXHIBIT B

Patent Number	Issue Date	Reel/Frame
6,507,247	02/27/01	011664/0214
6,760,739	03/01/01	011613/0694

INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, SUITE 325
SCOTTSDALE, ARIZONA 85251
Telephone: (480) 385-5060
Facsimile: (480) 385-5061

RECEIVED
CENTRAL FAX CENTER
FEB 0 3 2005

FACSIMILE TRANSMITTAL SHEET

TO:	FROM:
	Paul D. Amrozowicz, Reg. No. 45,264
COMPANY: USPTO	DATE: THURSDAY, FEBRUARY 03, 2005
FAX NUMBER: (703) 872-9306	TOTAL NO. OF PAGES INCLUDING COVER: 7
PHONE NUMBER: (703) 308-4357	SENDER'S REFERENCE NUMBER: 044.0003
RE: Second Submission of Revocation Of Power Of Attorney With Appointment Of New Power Of Attorney And Change Of Correspondence Address	REFERENCE NUMBER: 10/903,785

NOTES/COMMENTS:

FORMAL COMMUNICATION INTENDED FOR ENTRY

THIS MESSAGE IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED, AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL AND EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAWS. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, OR THE EMPLOYEE OR AGENT RESPONSIBLE FOR DELIVERING THE MESSAGE TO THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE AND RETURN ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA U.S. POSTAL SERVICE. THANK YOU.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.210

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED
CENTRAL FAX CENTER
FEB 0 3 2005

In re application of:	John M. DAVIS et al.	Group Art Unit: 2135	
Serial No.:	10/903,785	Examiner: Unknown	
Filed:	July 30, 2004	Confirmation No.: 4954	

For: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Docket No.: 4224-25 US (044.0003)

Customer No. : 29906

CERTIFICATE OF MAILING OR TRANSMISSION UNDER 37 C.F.R. § 1.8(a)

I hereby certify that this correspondence is being transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) 872-9306.

on 2/3/05. Signature: _____
Paul D. Amrozowicz

SECOND SUBMISSION OF REVOCATION OF POWER OF ATTORNEY WITH APPOINTMENT OF NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

On October 18, 2004, Applicant submitted a combined Revocation and Power of Attorney and Appointment of New Power of Attorney and Change of Correspondence Address (hereinafter "the Request") for 2 patents and 21 pending patent applications presently assigned to the Assignee of the instant application. The Request included a listing of each patent and patent application for which the requested change should be made.

PAGE 2/7 * RCVD AT 2/3/2005 2:00:13 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-10

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.211

Applicant's current representatives have checked the Patent Application Information and Retrieval (PAIR) system and note that the electronic file wrappers for each of the applications for which the requested change was made includes a copy of the Request. However, of the 21 applications included in the initial Request, only 3 have had the requested correspondence address change implemented. The instant application is not one of those three.

In the interim, correspondence from the U.S. Patent and Trademark Office continues to be sent to the previous correspondence address(es) of record, resulting in wasted time and effort on the part of several involved parties. As such, the Assignee of the above-referenced application once again requests that the Office please:

- **Revoke all previous powers of attorney in this application;**
- **Appoint the practitioners associated with Customer Number 29906;**

and

- **Change the correspondence address for this application to the address associated with Customer Number 29906.**

A copy of the Request that was submitted on October 18, 2004, which included a Statement under 37 CFR 3.73(b) from the Assignee, is included herewith.

Respectfully submitted,

INGRASSIA FISHER & LORENZ

Dated: 2/3/05

By: _____
Paul D. Amrozowicz
Reg. No. 45,264
(480) 385-5060

PAGE 3/7 * RCVD AT 2/3/2005 2:00:13 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-10

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.212

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

REVOCATION OF POWER OF ATTORNEY WITH APPOINTMENT OF NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

REVOCATION OF POWER OF ATTORNEY WITH APPOINTMENT OF NEW POWER OF ATTORNEY

I hereby revoke all previous powers of attorney given in each of the pending U.S. patent applications listed in the attached Exhibit A and in each of the issued U.S. patents listed in the attached Exhibit B.

I hereby appoint the practitioners associated with Customer Number **29906** in each of the above-identified matters.

CHANGE OF CORRESPONDENCE ADDRESS

Please change the correspondence address for each of the pending U.S. patent applications listed in the attached Exhibit A and for each of the issued U.S. patents listed in the attached Exhibit B to the address associated with Customer Number **29906**.

I am the Assigneeof record of the entire interest of each of the pending U.S. patent applications each of the issued U.S. patents. A Statement under 37 CFR 3.73(b) is included.

Assignee of Interest: Corrent Corporation

Date: 10/6/2004

By: _____
Name: Richard Takahashi
Title: CEO, President

PAGE 4/7 * RCVD AT 2/3/2005 2:00:13 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-10

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.213

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

STATEMENT UNDER 37 CFR 3.73(b)

The undersigned is a representative authorized and empowered to act on behalf of Corrent Corporation (hereinafter "Assignee"), and states that it is the assignee of the entire right, title, and interest in and to each of the patent applications listed in the attached Exhibit A and each of the issued patents listed in the attached Exhibit B by virtue of the respective assignments from the inventor(s) of the patent applications/patents identified in the attached Exhibits. The assignments were each recorded in the U.S. Patent and Trademark Office at the Reel/Frame indicated in the attached Exhibits.

Date: 10/6/2004

By: _____
Name: Richard Takahashi
Title: CEO, President

Best Available Copy

PAGE 5/7 * RCVD AT 2/3/2005 2:00:13 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-10

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.214

EXHIBIT A

Serial Number	Filing Date	Reel/Frame
10/144,004	05/13/02	013437/0592
10/144,332	05/13/02	013562/0932
09/978,742	10/16/01	012675/0184
10/172,814	06/12/02	013223/0463
09/998,715	11/30/01	012344/0870
09/911,149	07/23/01	012045/0727
09/921,677	08/03/01	012061/0464
09/877,473	06/08/01	011908/0162
09/880,701	06/13/01	012281/0840
10/144,195	05/13/02	013457/0718
10/144,197	05/13/02	013562/0929
09/970,901	10/04/01	012582/0026
09/994,141	11/26/01	012749/0976
09/971,325	10/04/01	012239/0040
09/877,470	06/08/01	011907/0894
09/880,700	06/13/01	012272/0744
09/880,699	06/13/01	012272/0737
10/161,070	05/31/02	013255/0672
10/160,330	05/30/02	012972/0159
10/191,632	07/09/02	013457/0672
10/903,785	07/30/04	See attached Assignment

EXHIBIT B

Patent Number	Issue Date	Reel/Frame
6,507,247	02/27/01	011664/0214
6,760,739	03/01/01	011613/0694

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OIPE JC1
DEC 10 2004
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	8

Application Number	10/903,785
Filing Date	July 30, 2004
First Named Inventor	John M. DAVIS
Art Unit	2135
Examiner Name	Unknown
Attorney Docket Number	4224-25 US (044.0003)

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☑ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☑ Other Enclosure(s) (please Identify below):
  PTO/SB/08A including 21 references.

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Ingrassia Fisher & Lorenz, PC		
Signature			
Printed name	Paul D. Amrozowicz		
Date	12/7/04	Reg. No.	45,264

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Paul D. Amrozowicz	Date	12/7/04

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OIPE JC10
DEC 10 2004
PATENT & TRADEMARK OFFICE

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of: John M. DAVIS — Art Unit: 2135

Serial No.: 10/903,785 — Examiner: Unknown

Filed: July 30, 2004 — Attny. Docket No.: 4224-25 US (044.0003)

For: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

on 12/7/04. Signature: *Paul D. Amrozowicz*

INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Commissioner:

In accordance with 37 C.F.R. 1.56 and in a manner prescribed by 37 C.F.R. 1.97 and 1.98, this Information Disclosure Statement IDS is being submitted herewith for consideration by the United States Patent and Trademark Office.

I. CONTENT
This IDS includes:

☒ A list of all patents, publications, applications, or other information submitted for consideration by the Office on PTO form SB/08A, which is included herewith;

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.218

☒ If required, a legible copy of: (i) each U.S. patent application publication and U.S. and foreign patent; (ii) each publication or that portion which caused it to be listed; and (iii) each cited pending U.S. application, the application specification including claims, and any drawing of the application, or that portion of the application which caused it to be listed including any claims directed to that portion; and (iv) all other information or that portion which caused it to be listed, unless subsequently provided in this IDS.

II. CONCISE EXPLANATION OF THE RELEVANCE (check at least one box)

☒ Except as may be subsequently indicated in this section II, a concise explanation is not required as all of the patents, publications, applications or other information are in the English language, or the degree of relevance of each is indicated in the English language version of the International Search Report, which accompanies this IDS.

☐ A concise explanation of the relevance, as it is presently understood by the individual designated in 1.56(a) most knowledgeable about the content of the information, of all patents, publications, applications or other information listed that is not in the English language.

☐ A copy of the translation of a non-English Language document, or portion thereof. (e.g., a translation of an abstract)

☐ Any patent, publication, pending U.S. application or other information that is listed on PTO form SB/08A, which are not enclosed herewith were previously cited by or submitted to the Office in one of the following applications that has been relied on for an earlier effective filing date under 35 U.S.C 120 and the IDS submitted in the earlier application complies with paragraphs (a) through (c) of 1.98:

U.S. Application Serial No.	U.S. Filing Date

III. THIS IDS IS BEING FILED UNDER 37 C.F.R. 1.97(b): (check one box)

☐ Within three months of the filing date of a national application other than a continued prosecution application under 1.53(d).

☐ Within three months of the date of entry of the national stage as set forth in 1.491 in an international application.

☒ Before the mailing date of a first Office Action on the merits. In the event that a first Office Action on the merits has been mailed, please consider this IDS under

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.219

37 C.F.R. 1.97(c) and see the statement under 1.97(e) **or** charge deposit account 50-2091 the fee specified by 37 C.F.R. 1.17(p) if such statement is not selected in Section VI.

☐ Before the mailing of a first Office Action after the filing of a request for continued examination under 1.114.

IV. THIS IDS IS BEING FILED UNDER 37 C.F.R. 1.97(c):

☐ After the period specified in 27 C.F.R. 1.97(b) and before the mailing date of any of a final action under 1.113, a notice of allowance under 1.311 or an action that otherwise closes prosecution in the application, and accompanied by:

☐ a statement specified in 1.97(e) as subsequently provided in this IDS; or

☐ the fee set forth in 1.17(p).

V. THIS IDS IS BEING FILED UNDER 37 C.F.R. 1.97(d):

☐ After the period specified in 27 C.F.R. 1.97(c) and on or before the payment of the issue fee, and it is accompanied by a statement specified in 1.97(e) as subsequently provided in this IDS **and** the fee set forth in 1.17(p).

VI. Statement under 37 C.F.R. 1.97(e) (check only one box)
The undersigned hereby states that:

☐ Each item of information contained in the IDS was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this IDS.

☐ No item of information contained in the IDS was cited in a communication from a foreign patent office in a counterpart foreign application, and, to knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the IDS was known to any individual designated in 37 C.F.R. 1.56(c) more than three months prior to the filing of this IDS.

VII. PAYMENT OF FEES (check one box)

☐ A check in the amount of $_____ is enclosed for fees due with respect to this IDS.

☐ Please charge Deposit Account No.___in the amount of $_____ for the fees due with respect to this IDS. A duplicate copy of this paper is included with this IDS.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.220

VIII. CONCLUSION

It is respectfully submitted that the claims presently on file patently distinguish the present invention from each of these references cited in this IDS. The references cited in this IDS are being cited only in the interests of candor and without any admission that they constitute statutory prior art or contain matter which anticipates the invention or which would render the same obvious, either singly or in a combination, to a person of ordinary skill in the art. Furthermore the filing of this IDS should not be construed to be an admission that the information cited in this IDS is, or is considered to be, material to patentability as defined in 1.56(b). In addition, the filing of this IDS should not be construed as a representation that a search has been made.

If the Examiner has any questions concerning this IDS, the Examiner is requested to contact the undersigned at the telephone number associated with Customer No. 29906. If it is determined that this IDS has been filed under the wrong rule, the PTO is requested to consider this IDS under the proper rule, with a petition if necessary, and charge the appropriate fee to Deposit Account No. 50-2091.

Please charge any additional fees or credit any overpayment related to this IDS to Deposit Account No. 50-2091.

Respectfully submitted,

Date: 12/7/04

By: _____
Paul D. Amrozowicz
Reg. No. 45,264

Ingrassia Fisher & Lorenz, P.C.
Customer No. 29906

Enclosures:
- ☒ PTO-SB/08A
- ☒ References
- ☐ Foreign Search Report
- ☐ Fee
- ☐ Other:

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.221

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT & TRADEMARK OFFICE DEC 10 2004

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	10/903,785
Filing Date	July 30, 2004
First Named Inventor	John M. DAVIS
Art Unit	2135
Examiner Name	Unknown
Attorney Docket Number	4224-25 US (044.0003)

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number: Number - Kind Code[2] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-2002/0066014 A1	05/30/2002	Dworkin et al.	
		US-2002/0108059 A1	08/08/2002	Canion et al.	
		US-5,432,950	07/11/1995	Sibigtroth	
		US-5,737,760	04/07/1998	Grimmer, Jr. et al.	
		US-5,892,899	04/06/1999	Aucsmith et al.	
		US-5,940,626	08/17/1999	Sollars	
		US-6,041,122	03/21/2000	Graunke et al.	
		US-6,049,876	04/11/2000	Moughanni et al.	
		US-6,101,255	08/08/2000	Harrison et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] – Number[4] – Kind Code[5] (*if known*)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation in not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and selection option 2.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 | | 3

Complete if Known	
Application Number	10/903,785
Filing Date	July 30, 2004
First Named Inventor	John M. DAVIS
Art Unit	2135
Examiner Name	Unknown
Attorney Docket Number	4224-25 US (044.0003)

Examiner Initials*	Cite No.[1]	NON PATENT LITERATURE DOCUMENTS Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		MOTOROLA, Digital DNA, Technical Summary, MPC184TS/D, Rev. 1, 6/2002, MPC 184 Security Processor	
		Intel® IXP2400 Network Processor: Flexible, High-Performance Solution for Access and Edge Applications, pp. 1-7.	
		Intel® Addressing Next-Generation CPE Challenges, The Role of the Intel® XScale™ Technology-based Intel® IXP425 Network Processor in CPE, Intel® Internet Exchange Architecture, February 2002, pp. 1-8.	
		Delivering the Next Generation of Broadband Services over the Last Mile, Introducing a New Multi-Service Processor Architecture™, Brecis Communications, March, 2001, pp. 1-8.	
		C-PORT™ A Motorola Company, C-5™ Network Processor Data Sheet, Supporting C-5 Network Processor Version DO, January 21, 2002 - Preliminary Version, pp. 1-96.	
		DONALD L. EVANS, PHILLIP J. BOND, ARDEN L. BEMENT, Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, May 25, 2001 pp. i-viii, 1-61.	
		PATRICK CROWLEY, MARK A. FRANKLIN, HALDUN HADIMIOGLU, PETER Z. ONUFRYK, Network Processor Design Issues and Practices, Volume 1, Chapter 2, pp. 12-13, 148-154, 172-175; Chapter 9, pp. 192-218; Chapter 10, 220-248; and Chapter 12, 250-275, Morgan Kaufmann Publishers, 2003, San Francisco, California.	
		Corrent's Families of Security Processors [retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com>.	
		Comm Week. Startups take next step at NPU confab [online]. Robert Keenan [retrieved on 6/23/03]. Retrieved from Internet: <URL:www.eet.com>.	
		Corrent. The Security Processing Company. Corrent Introduces Industry's First Complete Security Processor Securing Next Generation Internet Transactions Today [online]. May 6, 2002, Las Vegas, NV [retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/press15.phtml>.	
		Corrent. The Security Processing Company. Socket Armor™ CR7020 SSL Security Processor [online]. [Retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/products_socket.phtml>.	
		Corrent. The Security Processing Company. Packet Armor™ CR7120 IPsec Security Processor [online]. [Retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/products_packet.phtml>.	
		Corrent. The Security Processing Company. Corrent Takes Industry Lead With Delivery Of Single-Chip Gigabit Speed Internet Security Processors [online]. December 10, 2001, Tempe, AZ [Retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/press8.phtml>.	
		Corrent. The Security Processing Company. Corrent Offers Gigabit-rate VPN/SSL Performance With a Cost-Effective Enterprise and Server PCI Card Solution [online]. December 2, 2002, Tempe, AZ [Retrieved on 4/10/03]. Retrieved from Internet: <URL:www.corrent.com/press20.phtml>.	
		Corrent. The Security Processing Company. Breakthrough Security Performance At Unparalleled Price Point From Check Point And Corrent [online]. March 24, 2003, Redwood City, CA and Tempe, AZ [Retrieved on 4/4/03]. Retrieved from Internet: <URL:www.corrent.com/press24.phtml>.	
		Intel® IXP425 Network Processor Family [online]. 2002 [Retrieved on 9/10/02]. Retrieved from Internet: <URL:www.intel.com/design/network/products/npfamily/ixp425.htm>.	
		EETimes. Developers Must Balance NPU Programmability and Performance Issues [online] August 5, 2002. {Retrieved on 9/10/02}. Retrieved from Internet: <URL:www.eetimes.com/in_focus/embedded_systems/OEG20020802S0032>.	
		TechWeb. Algorithm Hides Data Inside Unaltered Images [online] Colin Johnson, June 23, 1999 [Retrieved on 9/16/02]. Retrieved from Internet: <URL:www.techweb.com/wire/story/TWB19990623S0001>.	
		Electronic Engineering Times, Headline: Broadcom [online] March 4, 2002 [Retrieved on 9/6/02]. Retrieved from Internet: <URL:www.eetimes.com>.	

Examiner Signature		Date Considered	

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation in not in conformance and not considered. Include copy of this form with next communication to applicant.

[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO_9199 (1-800-786-9199) and selection option 2.

PTO/SB/08b (08-03)
Approved for use through 06/30/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	3	of	3

Complete if Known	
Application Number	10/903,785
Filing Date	July 30, 2004
First Named Inventor	John M. DAVIS
Art Unit	2135
Examiner Name	Unknown
Attorney Docket Number	4224-25 US (044.0003)

Examiner Initials*	Cite No.[1]	NON PATENT LITERATURE DOCUMENTS Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Electronic Engineering Times, Headline: Security chip speeds SSL/TLS record processing [online] July 8, 2002 [Retrieved on 9/6/02]. Retrieved from Internet: <URL:www.Broadcom.com>.	
		Motorola. MPC184: Security Processor [online] [Retrieved on 9/10/02]. Retrieved from Internet: <URL:www//e-www.motorola.com/webapp/sps/…/prod_summary.jsp?code=MPC184&nodeId=01M9732135977 2>.	

Examiner Signature		Date Considered	

*Examiner: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation in not in conformance and not considered. Include copy of this form with next communication to applicant.
[1]Applicant's unique citation designation number (optional). [2]Applicant is to place a check mark here if English language Translation is attached.
This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS.

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO_9199 (1-800-786-9199) and selection option 2.

OIPE JC111 NOV 2 2 2004 PATENT & TRADEMARK OFFICE

INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, SUITE 325
SCOTTSDALE, ARIZONA 85251
Telephone: (480) 385-5060
Facsimile: (480) 385-5061

BEST AVAILABLE COPY

FACSIMILE TRANSMITTAL SHEET

TO:	FROM:
	Paul D. Amrozowicz, Reg. No. 45,264
COMPANY: USPTO	DATE: MONDAY, NOVEMBER 22, 2004
FAX NUMBER: 703-746-4060	TOTAL NO. OF PAGES INCLUDING COVER: 8
PHONE NUMBER: 703-308-1202	SENDER'S REFERENCE NUMBER: 4224-25US (044.0003)
RE: Response to Notice to File Missing Parts of Application	APPLICATION NUMBER: 10/903,785

URGENT FOR REVIEW PLEASE COMMENT PLEASE REPLY PLEASE RECYCLE

NOTES/COMMENTS:

FORMAL COMMUNICATION INTENDED FOR ENTRY

THIS MESSAGE IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED, AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL AND EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAWS. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, OR THE EMPLOYEE OR AGENT RESPONSIBLE FOR DELIVERING THE MESSAGE TO THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE AND RETURN ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA U.S. POSTAL SERVICE. THANK YOU.

OIPE JC111
NOV 22 2004
PATENT & TRADEMARK OFFICE

BEST AVAILABLE COPY

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 7

Application Number	10/903,785
Filing Date	July 30, 2004
First Named Inventor	John M. DAVIS
Art Unit	2135
Examiner Name	Unknown
Attorney Docket Number	4224-25 US (044.0003)

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [x] Reply to Missing Parts/ Incomplete Application
  - [x] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please identify below):

Executed Declaration (2 sheets); and Copy of Notice to File Mising Parts.

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Ingrassia Fisher & Lorenz		
Signature			
Printed name	Paul D. Amrozowicz		
Date	11/22/04	Reg. No.	45,264

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Paul D. Amrozowicz	Date	11/22/04

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OIPE JC11 NOV 2 2 2004 PATENT & TRADEMARK OFFICE

BEST AVAILABLE COPY

PTO/SB/17 (10-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2005

Effective 01/01/2004. Patent fees are subject to annual revision.

[X] Applicant Claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 65.00

Complete if Known	
Application Number	10/903,785
Filing Date	July 30, 2004
First Named Inventor	John M. DAVIS
Examiner Name	Unknown
Art Unit	2135
Attorney Docket No.	4224-25US (044.0003)

METHOD OF PAYMENT *(check all that apply)*

[ ] Check [ ] Credit card [ ] Money Order [ ] Other [ ] None

[X] Deposit Account

Deposit Account Number: 50-2091

Deposit Account Name: Ingrassia Fisher & Lorenz, P.C.

The Director is authorized to: *(check all that apply)*

[X] Charge fee(s) indicated below [X] Credit any overpayments

[ ] Charge any additional fee(s) during the pendency of this application

[ ] Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	790	2001	395	Utility filing fee	
1002	350	2002	175	Design filing fee	
1003	550	2003	275	Plant filing fee	
1004	790	2004	395	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below		Fee Paid
Total Claims		-20**=		x 18.00 =	
Independent Claims		- 3**=		x 88.00 =	
Multiple Dependent				=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	88	2201	44	Independent claims in excess of 3
1203	300	2203	150	Multiple dependent claim, if not paid
1204	88	2204	44	**Reissue independent claims over original patent
1205	18	2205	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

** or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge – late filing fee or oath	65.00
1052	50	2052	25	Surcharge – late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	430	2252	215	Extension for reply within second month	
1253	980	2253	490	Extension for reply within third month	
1254	1,530	2254	765	Extension for reply within fourth month	
1255	2,080	2255	1,040	Extension for reply within fifth month	
1401	340	2401	170	Notice of Appeal	
1402	340	2402	170	Filing a brief in support of an appeal	
1403	300	2403	150	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive – unavoidable	
1453	1,330	2453	665	Petition to revive – unintentional	
1501	1,370	2501	685	Utility issue fee (or reissue)	
1502	490	2502	245	Design issue fee	
1503	660	2503	330	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify)

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($)65.00

SUBMITTED BY				Complete (if applicable)	
Name (Print/Type)	Paul D. Ancizowicz	Registration No. (Attorney/Agent)	45,284	Telephone	(480) 385-5060
Signature				Date	11/22/04

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 37 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

OIPE JC111 NOV 2 2 2004 PATENT & TRADEMARK OFFICE

BEST AVAILABLE COPY

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): John M. DAVIS et al.	
Application No.: 10/903,785	
Filed: July 30, 2004	
Title: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE	
Group Art Unit: 2135	
Attorney Docket No.: 4224-25US (044.0003)	

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is in response to a Notice to File Missing Parts of Application under 37 CFR 1.53(f). Enclosed is a copy of said Notice and the following documents and fees to complete the filing requirements of the above-identified application.

(X) Executed Declaration and Power of Attorney. The above-identified application is the same application which the inventor executed by signing the enclosed declaration.

( ) Statutory basic filing fee ( ) Utility ( ) Design

( ) Additional claim fees of $

(X) Missing Parts Surcharge $65.00

( ) A Petition for Extension of Time for reply to Notice of Missing Parts is attached.
- ( ) one month ($110.00)
- ( ) two months ($430.00)
- ( ) three months ($980.00)
- ( ) four months ($1,530.00)

Respectfully submitted,

By _____
Paul D. Amrozowicz, Reg. No. 45,264

Date: 11/22/04
Telephone No.: (480) 385-5060

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.228

BEST AVAILABLE COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/903,785	07/30/2004	John M. Davis	4224-25US

CONFIRMATION NO. 4954

29974
GAMMAGE & BURNHAM, PLC
c/o PortfolioIP
P.O. BOX 52050
Minneapolis, MN 55402

FORMALITIES LETTER

OC0000000014002701

OIPE
NOV 22 2004
PATENT & TRADEMARK OFFICE
JC111

Date Mailed: 10/05/2004

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of $65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is $65 for a Small Entity

- $65 Late oath or declaration Surcharge.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

*A copy of this notice **MUST** be returned with the reply.*

RECEIVED
OCT 08 2004
PORTFOLIO IP

10903785
11/24/2004 WABDELR1 00000093 502091
65.00 DA
01 FC:2051

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.229

BEST AVAILABLE COPY

John Ware

Customer Service Center
Initial Patent Examination Division (703) 308-1202
PART 2 - COPY TO BE RETURNED WITH RESPONSE

OIPE JC111 NOV 2 2 2004 PATENT & TRADEMARK OFFICE

BEST AVAILABLE COPY

IF&L Form - PTO/SB/01

United States Patent Application
Attorney Docket No.: 4224-25US (044.0003)
First Named Inventor: John M. Davis

COMBINED DECLARATION AND POWER OF ATTORNEY FOR A UNITED STATES PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, mailing address, and country of citizenship are stated below next to my full name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter, which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

the specification of which:
[ ] is attached hereto;
[X] was filed on July 30, 2004 and assigned U.S. application serial no. or PCT application no. 10/903,785;
[ ] and was amended on _____ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above, if any.

I hereby acknowledge the duty to disclose information which is material to patentability as defined by 37 C.F.R. § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. 119 or 365 of any foreign application(s) for patent, inventor's or plant breeders rights certificate(s), listed below and have also identified below, any foreign application for patent, inventor's or plant breeders rights certificate(s), or of any PCT international application having a filing date before that of the application of which priority is claimed:

Foreign Application No.	Country	Foreign Filing Date

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States Provisional applications listed below:

Application No.	Filing Date
60/507,976	10/02/2003

I hereby claim the benefit under 35 U.S.C. 120 of 365 of any United States application(s) or of any PCT international application designating the United States of America, listed below:

PAGE 5/8 * RCVD AT 11/22/2004 12:30:49 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/1 * DNIS:7464060 * CSID:4803855061 * DURATION (mm-ss):03-04

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.231

BEST AVAILABLE COPY

IF&L Form - PTO/SB/01

U.S. Parent Application or PCT Parent No.	Country	Foreign Filing Date

As a named inventor I hereby also appoint the practitioner(s) associated with Ingrassia Fisher & Lorenz, PC, Customer Number 29906 to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

I hereby declare that all statements made herein of my own knowledge are true and that all statements on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole or First Inventor: John M. Davis

Signature of Sole or First Inventor: _____ Date: 11/9/04

Residence City: Brentwood Residence State: TN

Residence Country: USA Citizenship: USA

Home or Business Post Office Address 1016 Highland Rd.

City: Brentwood State: TN Zip Code: 37027

Full Name of Second Joint Inventor: Richard Takahashi

Signature of Second Joint Inventor: _____ Date: Nov 9, 2004

Residence City: Phoenix Residence State: AZ

Residence Country: USA Citizenship: USA

Home or Business Post Office Address 14033 So. 35th Place

City: Phoenix State: AZ Zip Code: 85044

PAGE 6/8 * RCVD AT 11/22/2004 12:30:49 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-2/1 * DNIS:7464060 * CSID:4803855061 * DURATION (mm-ss):03-04

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.232

INGRASSIA FISHER & LORENZ, P.C.
7150 E. CAMELBACK, SUITE 325
SCOTTSDALE, ARIZONA 85251
Telephone: (480) 385-5060
Facsimile: (480) 385-5061

RECEIVED
CENTRAL FAX CENTER
OCT 0 8 2004

FACSIMILE TRANSMITTAL SHEET

TO:	FROM:
	Paul D. Amtozowicz, Reg. No. 45,264
COMPANY: USPTO	DATE: OCTOBER 8, 2004
FAX NUMBER: (703) 872-9306	TOTAL NO. OF PAGES INCLUDING COVER: 8
PHONE NUMBER:	SENDER'S REFERENCE NUMBER: 044.9999
RE: Revocation Of Power Of Attorney With Appointment Of New Power Of Attorney And Change Of Correspondence Address	REFERENCE NUMBER: See Exhibit

NOTES/COMMENTS:

RECEIVED
CENTRAL FAX CENTER
OCT 0 8 2004

FORMAL COMMUNICATION INTENDED FOR ENTRY

THIS MESSAGE IS INTENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY TO WHICH IT IS ADDRESSED, AND MAY CONTAIN INFORMATION THAT IS PRIVILEGED, CONFIDENTIAL AND EXEMPT FROM DISCLOSURE UNDER APPLICABLE LAWS. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, OR THE EMPLOYEE OR AGENT RESPONSIBLE FOR DELIVERING THE MESSAGE TO THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS COMMUNICATION IN ERROR, PLEASE NOTIFY US IMMEDIATELY BY TELEPHONE AND RETURN ORIGINAL MESSAGE TO US AT THE ABOVE ADDRESS VIA U.S. POSTAL SERVICE. THANK YOU.

10/12/04

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	Various
Filing Date	Various
First Named Inventor	
Art Unit	
Examiner Name	
Attorney Docket Number	Various

Total Number of Pages in This Submission: 7

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☑ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☑ Other Enclosure(s) (please identify below):

Statement Under 37 CFR 3.73(b); 1 Page Exhibit A; 1 Page Exhibit B; Copy of Assignment for S.N. 10/903,785.

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Ingrassia Fisher & Lorenz		
Signature			
Printed name	Paul D. Amrozowicz		
Date	October 8, 2004	Reg. No.	45,284

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Paul D. Amrozowicz	Date	October 8, 2004

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

REVOCATION OF POWER OF ATTORNEY WITH APPOINTMENT OF NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

REVOCATION OF POWER OF ATTORNEY WITH APPOINTMENT OF NEW POWER OF ATTORNEY

I hereby revoke all previous powers of attorney given in each of the pending U.S. patent applications listed in the attached Exhibit A and in each of the issued U.S. patents listed in the attached Exhibit B.

I hereby appoint the practitioners associated with Customer Number **29906** in each of the above-identified matters.

CHANGE OF CORRESPONDENCE ADDRESS

Please change the correspondence address for each of the pending U.S. patent applications listed in the attached Exhibit A and for each of the issued U.S. patents listed in the attached Exhibit B to the address associated with Customer Number **29906**.

I am the Assigneeof record of the entire interest of each of the pending U.S. patent applications each of the issued U.S. patents. A Statement under 37 CFR 3.73(b) is included.

Assignee of Interest: Corrent Corporation

Date: 10/6/2004

By: _____
Name: Richard Takahashi
Title: CEO, President

PAGE 3/8 * RCVD AT 10/8/2004 4:41:19 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-48

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.235

UTILITY PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

STATEMENT UNDER 37 CFR 3.73(b)

The undersigned is a representative authorized and empowered to act on behalf of Corrent Corporation (hereinafter "Assignee"), and states that it is the assignee of the entire right, title, and interest in and to each of the patent applications listed in the attached Exhibit A and each of the issued patents listed in the attached Exhibit B by virtue of the respective assignments from the inventor(s) of the patent applications/patents identified in the attached Exhibits. The assignments were each recorded in the U.S. Patent and Trademark Office at the Reel/Frame indicated in the attached Exhibits.

Date: 10/6/2004

By: _____
Name: Richard Takahashi
Title: CEO, President

PAGE 4/8 * RCVD AT 10/8/2004 4:41:19 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:4803855061 * DURATION (mm-ss):02-48

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.236

EXHIBIT A

Serial Number	Filing Date	Reel/Frame
10/144,004	05/13/02	013437/0592
10/144,332	05/13/02	013562/0932
09/978,742	10/16/01	012675/0184
10/172,814	06/12/02	013223/0463
09/998,715	11/30/01	012344/0870
09/911,149	07/23/01	012045/0727
09/921,677	08/03/01	012061/0464
09/877,473	06/08/01	011908/0162
09/880,701	06/13/01	012281/0840
10/144,195	05/13/02	013457/0718
10/144,197	05/13/02	013562/0929
09/970,901	10/04/01	012582/0026
09/994,141	11/26/01	012749/0976
09/971,325	10/04/01	012239/0040
09/877,470	06/08/01	011907/0894
09/880,700	06/13/01	012272/0744
09/880,699	06/13/01	012272/0737
10/161,070	05/31/02	013255/0672
10/160,330	05/30/02	012972/0159
10/191,632	07/09/02	013457/0672
10/903,785	07/30/04	See attached Assignment

EXHIBIT B

Patent Number	Issue Date	Reel/Frame
6,507,247	02/27/01	011664/0214
6,760,739	03/01/01	011613/0694

IF&L Form – Assignment

United States Patent Application
Attorney Docket No.: 044.0003
First Named Inventor: John M. Davis

ASSIGNMENT

WHEREAS, the undersigned inventor(s) (hereinafter individually and collectively referred to as "ASSIGNOR") have invented:

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

for which application for Letters Patent of the United States:

[ ] has been executed on even date herewith;
[ ] executed on _____;
[X] was filed on July 30, 2004, and assigned U.S. Application Serial No. 10/903,785 ;

AND WHEREAS, Cornent Corporation, a [X] corporation; [ ] partnership; individual [ ] having a place of business in Delaware (hereinafter "ASSIGNEE"), and successors, assigns, and legal representatives, is desirous of acquiring an interest therein;

AND WHEREAS, a "formal application," as referred to herein, shall mean any provisional, nonprovisional, continuation, continuation in part, continued prosecution, substitute, renewal, extension, divisional, reissue, reexamination, foreign, Patent Cooperation Treaty (PCT) or other patent application, inventor's certificate, or like document;

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, ASSIGNOR does hereby sell, assign and transfer unto ASSIGNEE, its successors, assigns and legal representatives, the full and exclusive right to the aforesaid application, to the invention as described in the aforesaid application, and to any formal application which may be filed based in whole or in part on the aforesaid application, in the United States and all foreign countries, together with the right of priority under any international agreements to which the United States currently adheres and adheres to in the future, and hereby authorizes and requests the Commissioner of Patents to issue said Letters Patent to ASSIGNEE, for the sole use and benefit of ASSIGNEE, its successors, assigns and legal representatives,

AND ASSIGNOR HEREBY AGREES to transfer, upon request of ASSIGNEE, its successors, assigns and legal representatives, and without further remuneration, a like interest in and to any improvements and formal applications based thereon, growing out of or relating to the invention; and, without further remuneration, to provide all reasonable assistance and execute any papers requested by ASSIGNEE, its successors, assigns and legal representatives, to preserve and/or acquire ASSIGNEE's full protection and title in and to the invention hereby transferred and any improvements therein,

ASSIGNOR AGREEING, FURTHERMORE, upon request of ASSIGNEE, and without further remuneration, to execute any and all papers desired by ASSIGNEE for the filing and granting of formal applications based on the invention or improvements therein, and the perfecting of title thereto in ASSIGNEE.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.239

IF&L Form – Assignment

EXECUTED as of the date(s) written below by ASSIGNOR:

John M. Davis Date: 10/8/04

Richard J. Takahashi Date: 10/8/2004

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.240

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/903,785	07/30/2004	John M. Davis	4224-25US

CONFIRMATION NO. 4954

FORMALITIES LETTER

OC000000014002701

29974
GAMMAGE & BURNHAM, PLC
c/o PortfolioIP
P.O. BOX 52050
Minneapolis, MN 55402

Date Mailed: 10/05/2004

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of $65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$65** for a Small Entity

- **$65** Late oath or declaration Surcharge.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice MUST be returned with the reply.

John Ware

Customer Service Center
Initial Patent Examination Division (703) 308-1202

PART 3 - OFFICE COPY

16085 U.S. PTO
073004

17302 U.S. PTO
10/903785
073004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: John M. Davis et al.
Title: SYSTEM AND METHOD FOR A SECURE I/O INTERFACE
Attorney Docket No.: 4224-25US

PATENT APPLICATION TRANSMITTAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following attached items and information (as indicated with an "X"):

X Return postcard.
X Utility Patent Application under 37 CFR 1.53(b) comprising:
X Specification (48 pgs, including claims numbered 1 through 29 , a 1 page Abstract and 7 pgs Appendix).
X Informal Drawing(s) (10 sheets).
X Unsigned Declaration (2 pgs).
X Charge Deposit Account No. 50-2412 in the amount of $509.00 to pay the filing fee.
X Applicant claims small entity status under 37 C.F.R 1.27.

The filing fee has been calculated below as follows:

	No. Filed	No. Extra	Rate	Fee
TOTAL CLAIMS	29-20	9	x 9.00 =	**$81.00**
INDEPENDENT CLAIMS	4-3	1	x 43.00 =	**$43.00**
[]MULTIPLE DEPENDENT CLAIMS PRESENTED				**$0.00**
BASIC FEE				**$385.00**
TOTAL				**$509.00**

Please charge any additional required fees or credit overpayment to Deposit Account No. 50-2412.

Customer No. 29974

By: _____
Atty: Bruce T. Neel
Reg. No. 37,406
(602) 256-4429

"Express Mail" mailing label number: EV539668205US
Date of Deposit: July 30, 2004
This paper or fee is being deposited on the date indicated above with the United States Postal Service pursuant to 37 CFR 1.10, and is addressed to The Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Related Application

This application is a non-provisional application claiming benefit under 35 U.S.C. sec. 119(e) of U.S. Provisional Application Serial No. 60/507,976, filed 10/02/2003 (titled SYSTEM AND METHOD FOR A SECURE I/O INTERFACE by John M. Davis et al.; attorney docket no. 4224-25PRV), which is incorporated by reference herein.

Field of the Invention

The present invention relates in general to data communications, and particularly to secure cryptographic communications, and more particularly to a secure input/output (I/O) interface system for a computing device such as, for example, a host computer communicating using internet protocol (IP) data packets or other datagrams.

Background of the Invention

Trusted internal computer networks are typically protected from un-trusted external computer networks by routers or other gateway systems that provide different types of firewall functionality. Security processing performed by related systems may also provide additional protection. For example, a computer in the internal network may establish a virtual private network (VPN) session with a computer in the external network. The host processor of the computer or a dedicated security processor coupled to the router or other gateway system typically performs the security processing necessary to support the VPN. In addition, a dedicated network processor may be coupled to the security processor and/or the host processor to handle network packet processing functions.

Network interface cards (NIC) often provide a computer's physical connection to its trusted internal network. More specifically, a NIC connects a personal computer,

server or workstation to a local area network (LAN) and has two primary interfaces: the network interface and the host bus interface. NICs are typically low-cost ASIC-based products designed for simple buffering and data transfer.

It is desired that communications to and from a trusted computer be secure and that communication speeds be improved. However, providing firewall, network processing and security functionalities in different systems, which are often made by different manufacturers, provides increased opportunities for snooping or other techniques that may permit an unauthorized person to gain access to ongoing communications or to discover key or other security data when it is exchanged between subsystems. For example, if certain security functions associated with securing communications over a NIC are handled by the computer's host processor and/or by other computers on the internal network, then the communications may be more easily attacked or otherwise accessed or interfered with by an unauthorized person, who may attempt to exploit easier snooping access or other vulnerabilities presented by the processing of security functions by a host processor or another server on the network.

The use of different systems to perform different portions of security and network processing also requires additional processing and interfaces for coordinating communications processing between the systems. Such additional processing and interfaces increase processing demands, which limits communication speed and increases the size of the chips and systems necessary to implement secure communications.

As a specific example, when using a separate security processor and I/O card connected to a backplane bus of a host, input encrypted data is typically transferred using direct memory access (DMA) from the I/O card, under control of the host, to memory coupled to the host. Then, the data is transferred by DMA from the memory via the host to the security processor. After the data is decrypted, and possibly a public key generated, the data is transferred by DMA from the security processor to memory again via the host. Finally, the decrypted data is transferred by DMA from the memory to the I/O card for output to another destination. This large number of data transfers

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.245

creates a bottleneck on the backplane bus, which includes multiple data transactions, many interrupts, and heavy usage of memory to store the data.

The use of secure communications in broadband networks will increasingly require high-speed security and network processing. Further, the use of portable devices that securely connect to networks will require smaller chip and system sizes that can meet security and networking processing demands while at the same time retaining easy portability. In light of the foregoing, there is a general need for a secure I/O interface system and method that improve the security of communications to and from trusted hardware, improve communication speed, reduce the number of different systems required for secure communications, and reduce the extent of the bottleneck on the backplane bus.

Brief Description of the Drawings

The invention is pointed out with particularity in the appended claims. However, for a more complete understanding of the present invention, reference is now made to the following figures, wherein like reference numbers refer to similar items throughout the figures:

FIG. 1 illustrates a simplified functional block diagram of a system architecture suitable for use in implementing embodiments of a security processing system and method in accordance with an embodiment of the present invention;

FIG. 2 illustrates a high-level simplified functional block diagram of a security processor in accordance with an embodiment of the present invention;

FIG. 3 illustrates a more-detailed functional block diagram of a network intrusion detection system used in a portion of the security processor of FIG. 2 in accordance with an embodiment of the present invention;

FIG. 4 illustrates a simplified flow diagram of packet flow in the security processor of FIG. 2;

FIG. 5 illustrates a data representation convention used herein;

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.246

FIG. 6 is a block diagram illustrating the GDMA block, which incorporates an EDMA block, in accordance with an embodiment of the present invention;

FIG. 7 is a block diagram illustrating the EDMA block in accordance with an embodiment of the present invention;

FIG. 8 is a block diagram illustrating the ER block in accordance with an embodiment of the present invention;

FIG. 9 is a block diagram illustrating the OPC interfaces in accordance with an embodiment of the present invention;

FIG. 10 is an internal block diagram illustrating the OPC in accordance with an embodiment of the present invention;

FIG. 11 is a block diagram illustrating the relationship of the ER block to the cryptographic core and memory in accordance with an embodiment of the present invention; and

FIG. 12 is a block diagram illustrating the relationship between the ER block, the EDMA block, the cryptographic core, and memory in accordance with an embodiment of the present invention.

The exemplification set out herein illustrates an embodiment of the invention in one form, and such exemplification is not intended to be construed as limiting in any manner.

Detailed Description of the Drawings

The following description and the drawings illustrate specific embodiments of the invention sufficiently to enable those skilled in the art to practice it. Other embodiments may incorporate structural, logical, electrical, process and other changes. Examples merely typify possible variations. Individual components and functions are optional unless explicitly required, and the sequence of operations may vary. Portions and features of some embodiments may be included in or substituted for those of others. The scope of the invention encompasses the full ambit of the claims and all available equivalents.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.247

The present invention is described and claimed herein primarily with reference to the processing of "packets". However, as used herein, it is intended that the term "packet" or "packets" have the meaning and scope of the more generic term "datagram" or "datagrams."

In one embodiment, the present invention provides, among other things, a system and method for connecting a trusted piece of hardware, such as, for example, a personal computer, server, router, personal digital assistant (PDA), cellular phone, network-enabled device or other computing or communication device, to a network using an I/O interface or system that provides improved security for all or substantially all communications received and sent by the trusted hardware. The secure I/O system preferably may perform all security and network processing necessary to maintain secure communications by the hardware with other devices on internal or external networks. Alternatively, it may perform the network security processing essential to be segregated from other processing to ensure safe (i.e., protected) and efficient system or device operation. For example, the secure I/O system permits establishing a VPN with a computer on an external network. The VPN may be established using, for example, the standard IPSec internet protocol security, as described in "Request for Comment" (RFC) 2401, 2402 and 2406, which are incorporated herein by reference.

The secure I/O system of the present invention permits performing all or substantially all network processing functions and off-loads all or substantially all security functions associated with network address translation (NAT), the providing of a firewall, intrusion detection/protection system functionality, traffic proxying, and encryption from a host or network processor onto a single system or card, for example a NIC. This card may be inserted into each of the servers and other computers connected on an internal network.

The security processing performed by the secure I/O system typically may include encryption, decryption, signing and verification of packets at, for example, 100 megabits per second full duplex and greater speeds. For example, the secure I/O system of the present invention may provide wire speed performance, for example, of about 2-3

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.248

gigabits per second firewall and VPN throughput. The secure I/O system may simplify the deployment of security solutions on open platforms and appliances.

The elements that implement the various embodiments of the present invention are described below, in some cases at an architectural level. Many elements may be configured using well-known structures. The functionality and processes herein are described in such a manner to enable one of ordinary skill in the art to implement the functionality and processes within the architecture.

FIG. 1 illustrates a simplified functional block diagram of a system architecture suitable for use in implementing a security processing system and method in accordance with an embodiment of the present invention. Architecture 100 includes security processing system 102 comprising security processor 104, which may consolidate the processing of discrete or consolidated security functions and maintain the relationships and integrity of the stored security context and other information in memories 106, 108, and 110. Memories 106, 108 and 110 are coupled to security processor 104. Memories 106, 108 and 110 store, for example, cryptographic keys and other data used in security functions by security processor 104, and also store security associations and connection entries used in maintaining multiple security sessions with other computers. Memories 106, 108 and 110 also may be used to buffer inbound or outbound data packets awaiting security processing by security processor 104. Memory 108 may be used to support classification processing by security processor 104.

Security processing system 102 is preferably contained within cryptographic boundary 112 and provides a secure I/O interface for computing or communications hardware as described above. Cryptographic boundary 112 preferably complies with Federal Information Processing Standards Publication (FIPS PUB) 140-2 titled "Security Requirements for Cryptographic Modules", issued May 25, 2001, by National Institute of Standards and Technology (NIST), which is incorporated by reference herein.

Security processing system 102 may be coupled to internal network 116 by I/O interface 114 and to external network 120 by I/O interface 118. Interfaces 114 and 118

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.249

may perform physical (PHY) layer processing to convert a digital bit stream to or from an analog or photonic signal for transmission over a physical medium such as, for example, copper wire pairs, co-axial cable, fiber or air. Interfaces 114 and 118 are, for example, streaming data interfaces such as a Packet-Over-SONET Physical-Layer Three (POS/PHY3) type streaming interface, although 10/100 megabit (Mb) Ethernet, 1 Gigabit (Gb) Ethernet, UTOPIA, LX SPI-4 and other interface types may be suitable. By routing all or substantially all I/O to and from host processor 130 and/or internal network 116 through security processing system 102, host processor 130 and internal network 116 are substantially protected against unauthorized access or other security breaches, protecting the security information integrity, and providing processing and storage efficiency from information consolidation.

IP data packets are received from and transmitted to external network 120 and internal network 116 over interfaces 114 and 118. In other embodiments, security processing system 102 may include a number of additional interfaces to internal or external networks. Security processor 104 performs, for example, routing of data packets from external network 120 to appropriate destinations in internal network 116 and handles IPSec processing for both inbound and outbound data packets. Security processor 104 preferably handles all network and security processing functions for the data packets to provide the most secure I/O interface. However, in alternative embodiments, certain selected networking and/or security functions may be handled by other processors such as, for example, host processor 130. Examples of network and security processing systems and methods, and related communications interfaces and protocols, suitable for implementation in and with security processing system 102 are described in U.S. patent applications serial no. 09/880,701 (entitled "METHOD AND SYSTEM FOR HIGH-SPEED PROCESSING IPSEC SECURITY PROTOCOL PACKETS" filed by Lee P. Noehring et al. on June 13, 2001) and serial no. 10/160,330 (entitled "SYSTEM AND METHOD FOR MANAGING SECURITY PACKET PROCESSING" filed by Lee P. Noehring et al. on May 30, 2002), which applications are incorporated by reference herein.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.250

Security processing system 102 may process packets delivered from internal or external networks 116 or 120 or from host processor 130. System 102 may, for example, handle thousands of separate IPSec tunnels at various packet sizes from 64 bytes and higher at a throughput of, for example, about 300 Mb per second or greater. System 102 may handle transport or tunnel mode IPSec.

Other computing devices may be coupled to external network 120. For example, user devices 122 and 124 may correspond to devices that may establish secure communication sessions with host processor 130 or another device on internal network 116. User device 124 may be protected using a secure I/O interface 126, which may be a hardware system similar to security processing system 102. User device 122 may use only its host processor and software to process secure communications through external network 120.

Security processor 104 may handle both so-called fast path and slow path processing functions. Fast path functions include time-sensitive processing such as, for example, packet classification, modification and forwarding, and slow path functions include, for example, system management and alarm functions and time-insensitive packet processing functions such as route calculation, unknown address resolution, firewall rule management, and routing table management. Packet classification generally involves matching information from an incoming packet to a table of connection entries (which may include state and context elements, and relations to encryption associations) stored in, for example, memory 106 or 108.

Security processing system 102 may be implemented, for example, as a stand-alone system box or as a card such as, for example, a NIC, that connects to a slot in the motherboard of a host system. Security processing system 102 may be coupled to host processor 130 using host bridge or interface 128. Host processor 130 may be coupled to hard drive 132, digital content input device 134, and authentication input device 136. Hard drive 132 may store, for example, a software application that communicates with the application program interface (API) of security processing system 102. Security

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.251

processor 104 may send security-related information and data as requested to host processor 130, and may switch its I/O ports as requested by host processor 130.

Host bridge 128 may couple security processor to host processor 130 of, for example, a personal computer, server, or other computing or communications device. Host bridge 128 may be, for example, a peripheral component interconnect (PCI) interface, and in one embodiment, may be a 32 bit, 66 MHz PCI interface.

Authentication input device 136 may be, for example, a physical key or token, a smart card, or a biometric identification sensor. Authentication input device 136 may enable the authentication of a user attempting to access host processor 130. Authentication input device 136 may be directly attached, for example, to a serial, network, or EEPROM interface of host processor 130 using a physically segregated or covered transmission channel. Authentication input device 136 may act as a mechanism for enabling or modifying the functions of security processor 104, or as an information-loading mechanism, used for example in loading keys, uncovering keys, or modifying rules for device operation.

Digital content input device 134 may be, for example, a CD-ROM, portable storage device, or keyboard and provides digital data such as program code or security data to host processor 130.

Security processor 104 may provide the first inspection of incoming data from external network 120 to determine, for example, if the data is encrypted or in plain text form, and the type of security processing required, as may be determined by reading the header or other content of incoming data packets, and to set up a secure channel or process to handle the data, as may be requested for a security policy.

Security processing system 102 may include a unique identification (ID) number stored on a chip containing security processor 104 or stored in encrypted form in, for example, memory 110. Security processing system 102 may perform protected key generation in hardware, and protected keys are preferably never output from security processor 104 in plain text form.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.252

Security processing system 102 may also serve as a trusted hardware device to authenticate another hardware security token connected on, for example, a common network. Security processing system 102 may be authenticated using authentication input device 136 and may provide the cryptographic processing for such authentication. Security processing system 102 may communicate verification or other information regarding the authentication status of input device 136 to host processor 130.

By performing all or most security and networking processing for I/O communications to host processor 130 in security processing system 102, a large proportion, for example, of greater than about 50-90 percent of VPN and firewall I/O data loops may be handled in security processing system 102 without intervention by host processor 130. In addition, all or most security and network exception processing may be handled by security processing system 102.

Security Processor

FIG. 2 illustrates a high-level simplified functional block diagram of security processor 104 in accordance with an embodiment of the present invention. In other embodiments of the present invention, other security processor configurations may be used in the system architecture of FIG. 1. Security processor 104 is preferably, though not necessarily, formed on a single chip.

Streaming interface 200 may be coupled for input and output to physical I/O interfaces 114 and 118 and supports fast path data flow to security processor 104. Host interface 206 may be coupled to physical host bridge 128 and supports slow path data flow and system management by host processor 130. Host interface 206 may be coupled to DMA interface 204. Both streaming interface 200 and DMA interface 204 may be coupled to switching system 208. Although only a single streaming and DMA interface are illustrated, more than one interface of each type may be used. For example, in one embodiment, streaming interface 200 may comprise three 10/100 Ethernet interfaces, and DMA interface 204 may comprise two DMA interfaces. Switching system 208 may be used to provide a switching mechanism to route packets

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.253

and data to and from any of the I/O interfaces of security processor 104 and local data bus 210.

Local data bus 210 may be coupled to DMA interface 204 and operate under control of local bus controller 222. Local memory interface 202 may be coupled to local data bus 210 and may couple security processor 104 to memories 106, 108, and 110, which are typically provided on one or more separate chips although operating portions of memories 106, 108 and/or 110 may be provided on-chip with security processor 104. In other embodiments, more than one local data bus 210 may be used.

Local memory interface 202, and DMA interface 204 may be used, for example, by packet engines 228 to access memories 106 and 108 for classification processing and by control processor 212 for accessing firmware 214. Memory 106 may be, for example, a DDR SDRAM, and memory 108 may be, for example, an SRAM. Memory 106 may be made available to control processor 212 for operating system and code storage (for example, for firewall and internet key exchange (IKE) functionality, routing and network address translation (NAT) information, and firewall table entries). Memory 106 may be made available to packet engine 228 for access to specific firewall information, and stored security policies and associations. Memory 106 may be made available to cryptographic core 232 to store security association and key information. Memory 106 may also be made accessible via host interface 206 to host processor 130. Alternatively, a portion or all of the security association data may be stored in a memory, for example an SRAM (not shown), on-chip in security processor 104.

Memory 108 may be made available to both control processor 212 and each packet engine 228. Memory 108 may be used to aid in rapid lookups supporting packet engine 228 in classification and forwarding decisions. Memory 110 may be, for example, flash memory to provide non-volatile storage, for example, for boot memory and certain key storage. The boot code used to load firmware for execution by security processor 104 may optionally be authenticated using a mechanism internal to security processor 104 prior to its operation.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.254

Switching system 208 may provide a flexible I/O system that allows packet processing engines or packet engines 228 to communicate high-speed data with several different types of interfaces including, for example, streaming interface 200 and direct memory access (DMA) interface 204. A non-limiting example of a switching system and method that are suitable for use with the present invention is described in U.S. patent application serial no. 10/172,814 (entitled FLEXIBLE I/O INTERFACE AND METHOD FOR PROVIDING A COMMON INTERFACE TO A PROCESSING CORE, filed by Swaroop Adusumilli et al. on June 12, 2002), which is hereby incorporated by reference. Alternatively, switching system 208 may be implemented using conventional switches. Switching system 208 may provide a common bus interface to packet engines 228.

More specifically, switching system 208 may arbitrate between streaming and DMA interfaces to provide a common interface for packet engines 228 to permit communication of differing types of data over a plurality of bus types that implement different bus protocols and/or standards. The use of switching system 208 with DMA interface 204 may permit packets and other data to be routed using direct memory access among control processor 212, each of packet engines 228, and external memory such as memories 106 and 108. In one embodiment, individual packets may be routed within security processing system 102 using DMA.

Switching system 208 may select the I/O port or interface, including host interface 206, to use for data packets based on the results of cryptographic or other security or network processing. For example, packets classified for forwarding to another destination after a security operation (such as encryption or new connection validation) could be directed to the proper egress port, while packet data requiring host inspection (such as IKE messages, or exception or initial packets for firewall classification) could be redirected to DMA interface 204. In contrast to prior systems that rely on external bus interfaces to re-direct packet traffic to varying packet processing devices, the present invention may permit simplifying or collapsing the schema and protocols used, for example, in firewall, routing, NAT and IPSec

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.255

processing with the result that lookups, transforms, and other application activity are more efficient. Prior systems typically require context labeling or other data envelopment or tagging to manage packet workflow among varying processing devices.

Switching system 208 may also include the ability to perform packet spanning. Spanning generally refers to a capability in managing network data flow that duplicates a selected traffic flow through an additional port for analysis by a traffic analyzer or intrusion detection system. The term "spanning" includes within its meaning, but is not necessarily limited to, functionality associated with the use of switched port analysis (often designated by the acronym "SPAN"). Unlike the all-or-nothing port duplication capabilities of typical existing network switches having a SPAN capability, the spanning function of switching system 208 may selectively identify flows of traffic and then stream duplicate packets or other datagrams via DMA interface 204 to control processor 212 or to, for example, another integral MIPS or associated control processor (not shown) that may be included in security processor 104.

Typical data traffic that will not be spanned (i.e., non-spanned traffic) flows from one of packet engines 228 to, for example, an output packet cache (OPC). The OPC is an intermediate buffer to switching system 208 for outgoing packet traffic that will leave security processor 104 through DMA interface 204 or streaming interface 200. FIG. 9 is a block diagram illustrating the OPC interfaces.

At the OPC, this outgoing packet traffic may be placed on an active list (for example, a list of 64-byte memory structures residing in the OPC) for transmission out of interface 204 or 200 (for example, a PDMA or GMII interface). The OPC may be implemented, for example, as an embedded memory structure or in external memory and may be coupled between a packet engine 228 and one of the external interfaces of security processor 104. The use of the spanning feature is preferably configurable and may be selected by the system or operator. This feature is preferably implemented primarily using the OPC. FIG. 10 is an internal block diagram illustrating the OPC.

More specifically, the OPC may include an output packet buffer (OPB) memory (e.g., a RAM) for buffering output data, and a buffer control block (BCB). The BCB is

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.256

typically a set of pointers stored in memory that each refer to memory locations of the output data. The BCB may maintain metadata such as, for example, start-of-packet, end-of-packet, error, sequence number, pointer to next BCB in chain, and other metadata. The BCB is preferably used to manage the active lists and the free list for the linked-list allocation scheme. When logically dictated during the operation of security processor 104 such as, for example, in the case of a five-tuple match result from a lookup engine, a NIDS engine match to packet type, or particular TCP state, or some other pattern within a datagram that is of interest to the system operator, a control bit or flag (sometimes referred to as a "SPAN bit" herein) may be set or some other notification may be sent by packet engine 228 to notify the BCB for packet data that is transiting the OPB memory, including the output device or interface that will be used. When a packet that will not be spanned (i.e., a "non-span packet") is stored in the OPC, a "DONE" flag, for example, is set to zero for each such non-span packet, and each non-span packet may be queued for egress out through an appropriate interface (i.e., streaming interface 200 or DMA interface 204).

After the memory pointed to by the BCB is drained (i.e., data is read or outputted out of that location into another location), the BCB "DONE" flag may be set to allow the memory to be overwritten. Alternatively, another method may be used to move output buffer data from the "active list" to the "free list". When a spanned packet is sent to the OPC from packet engine 228, a separate bit may be set (this separate bit is referred to herein as a "SPAN" bit). The SPAN bit may be used to initiate alteration of the behavior of the OPC. The packet may be streamed out through the original targeted egress interface (e.g., streaming interface 200 or data interface 204), but before releasing the data memory area pointed to by the BCB, the data may be drained out via a designated interface, for example DMA interface 204 to control processor 212 or to host processor 130. After such a packet is successfully duplicated using DMA interface 204, the BCB may be set to free the memory to be overwritten as described above.

In an alternate embodiment, the BCB or some other memory control mechanism could maintain an active list and a free list and place the active data blocks of OPB

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.257

memory (i.e., re-map the pointers) from the active list to the free list when the packet data is streamed out. When the SPAN bit is set, the data would first be streamed to the alternate interface (such as, for example, DMA interface 204) in addition to its primary target output interface prior to moving the data blocks to the free list. After spanned data has been drained to control processor 212 or host processor 130, the spanned data is available to other processors or systems for any desired subsequent actions such as, for example, logging, analysis for intrusion detection, or transcription.

The foregoing approach may be particularly useful for network intrusion detection functions. When one of the defined actions for a certain packet traffic type is to log the packet, the above approach permits security processor 104 to act substantially as an in-line tap, which permits selectively duplicating streams of data that may be of interest based on specific pre-selected criteria. When NIDS 302 returns a potential signature match to one of packet engines 228, and that packet engine 228 is able to verify that the potential signature match is a true positive match, packet engine 228 may set the SPAN bit for that packet so that it is duplicated to control processor 212 and/or host processor 130 as discussed above. This verification may, for example, be based on the protocol of the packet or other appropriate criteria. Control processor 212 and/or host processor 130, as is applicable, may then run further analysis on the packet or the packet stream, and/or may forward it to a centralized IDS collector for enterprise intrusion detection.

Alternatively, the packet or packet stream may be re-directed or duplicated to host processor 130 for further processing. Such processing may include, for example, upper-layer cross-packet analysis, packet normalization, data mangling, or other operations. The packet may be forwarded out through the appropriate interface (e.g., streaming interface 200 or DMA interface 204) after such post-analysis or post-processing.

Packet engines 228 may each be coupled to a cryptographic core 232. Packet engines 228 may each comprise microprocessors customized for packet operations such as, for example, packet processing and classification. Examples of packet engines

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.258

suitable for use with the present invention are described in detail in U.S. patent application serial no. 09/880,701 (entitled "METHOD AND SYSTEM FOR HIGH-SPEED PROCESSING IPSEC SECURITY PROTOCOL PACKETS" filed by Lee P. Noehring et al. on June 13, 2001), which is incorporated by reference herein. Each packet engine 228 may, for example, process packets needing initial NAT processing and firewall table entry setup, process packets corresponding to existing NAT and firewall tables, and process IPSec packets.

More specifically, each packet engine 228 may perform hash table lookups to a firewall connection table entry, which may contain state information, a rule to be applied to a packet, optional security association information, routing information (for example, for MAC overlay), and any application level gateway (ALG) packet mangling to be done.

For outbound IPSec traffic, each packet engine 228 may provide a pointer to security association data for an IP packet, load a security association database entry into a local buffer located on or off-chip, construct and add an outer IP header and IPSec header, perform lifetime checks, and update an associated security association database (SAD) entry (for example, the sequence number and byte count).

For inbound IPSec traffic, each packet engine 228 may locate an associated SAD entry by using a security policy index (SPI) number from the IPSec header or by an SAD address provided by the classification of the destination address, protocol and SPI. In order to use the SPI number, IKE firmware 214 may define the inbound SPI number from the API provided for security processor 104 during security association establishment. Packet engine 228 may then load the SAD entry into a local buffer, perform anti-replay checks and lifetime checks, and then update the SAD entry. Each cryptographic core 232 may remove tunnel IP headers, ESP or AH headers, and ESP trailers. The packet may then optionally be redirected through packet engine 228 for a firewall connection table lookup.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.259

Packet engines 228 in FIG. 2 represent one or more packet engines that may be provided in parallel in security processor 104. The optional presence of additional packet engines 228 is indicated in FIG. 2 by ellipsis 229.

Input and output buffers 236 and 240 may be provided to couple each packet engine 228 to switching system 208. Buffers 236 and 240 may be, for example, FIFO buffers. In one embodiment, each of output buffers 240 may read control data prepended to the data payload as an in-band instruction set that determines the distribution direction or interface of the packet by switching system 208. Input and output buffers 236 and 240 may each have a size of, for example, 16-32 kilobytes (KB). An alternative is to have a direct control interface provided to couple each packet engine 228 to switching system 208, for out-of-band signaling of the packet data distribution direction. Roughly stating the foregoing in another way, instructions may be sent either from a packet engine 228 to switching system 208 either in-band, as prepended control words, or out-of-band, via a discrete control channel.

Packet engines 228 may be interconnected at the packet level for passing a packet and associated context information to other functional blocks or to each other for specific processing. In parallel operation, the individual packet engines 228 may each independently process discrete packets and forward the packets to other devices, such as cryptographic processing cores or switches. Two or more microprocessors could, for example, be serialized to perform discrete functional tasks as the packet transits from one functional block to another. Packet engines 228, in conjunction with cryptographic cores 232 and under the common control of control processor 212, may perform, for example, firewall lookup and statistics, IPSec and secure sockets layer (SSL) processing, quality of service (QoS), traffic management, and public key processing. Packet engines 228 may be programmable through registers (not shown), which may be configured by an external driver or initialization program. Each packet engine 228 may perform any needed datagram modification prior to sending a packet out from security processor 104. For example, packet engine 228 may write a MAC destination address to a packet as it streams out of processor 104.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.260

In one embodiment, all incoming packets to security processor 104 may be initially processed by one of packet engines 228. Each packet engine 228 may classify the packet based upon a lookup table result and then may apply a variety of operations including, for example, forwarding with necessary transform parameters to cryptographic core 232, or forwarding to control processor 212 for application level processing. Such operations may further include overwriting portions of the packet with new data such as, for example, the media access control (MAC) header for forwarding and the IP header for NAT, and may also include dropping the packet, or passing the packet through security processor 104 to an egress interface, such as, for example, streaming interface 200, unchanged.

Cryptographic cores 232 may provide security processing to perform, for example, IPSec and/or SSL processing. Each cryptographic core 232 may provide high-speed fixed function encryption and authentication hash processing for packet data. Each cryptographic core 232 may receive instructions and key address information affixed to a packet for applying appropriate transforms. Examples of cryptographic cores 232 suitable for use with the present invention are described in the following U.S. patent applications, all of which are incorporated herein by reference: serial no. 10/144,004 (entitled "SINGLE-PASS CRYPTOGRAPHIC PROCESSOR AND METHOD" filed by Satish N. Anand et al. on May 13, 2002); serial no. 10/144,332 (entitled "SECURITY ASSOCIATION DATA CACHE AND STRUCTURE" filed by Satish N. Anand et al. on May 13, 2002); serial no. 10/144,195 (entitled "APPARATUS AND METHOD FOR A HASH PROCESSING SYSTEM USING MULTIPLE HASH STORAGE AREAS" filed by Satish N. Anand on May 13, 2002); and serial no. 10/144,197 (entitled "APPARATUS AND METHOD FOR A HASH PROCESSING SYSTEM USING INTEGRATED MESSAGE DIGEST AND SECURE HASH ARCHITECTURES" filed by Satish N. Anand on May 13, 2002).

It should be noted that each cryptographic core 232 is preferably accessible only through a corresponding packet engine 228. Alternatively, several packet engines 228 may access a single cryptographic core in a round robin or other arbitrated flow

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.261

mechanism. Accordingly, all or substantially all packet and data flow may return to the corresponding packet engine 228 from cryptographic core 232 prior to output from security processor 104. Also, in a preferred embodiment according to the present invention, all I/O data to security processor 104 transits one of cryptographic cores 232 whether or not the data needs encryption/decryption or other security processing. After exiting cryptographic core 232, a packet may be assigned its distribution directions (for example, to a destination of one of several streaming interfaces 200 or control processor 212) by packet engine 228 for distribution through switching system 208.

Streaming interface 200, switching system 208, packet engines 228 and cryptographic cores 232 may provide fast path data flow for security processing system 102. This fast path data flow may provide both firewall and virtual private network (VPN) functionality along with network intrusion detection functionality as described further below. Control processor 212 and firmware 214 may provide all or substantially all control for these firewall, VPN and network intrusion functions.

Initial packets for a data flow may transit from packet engine 228 and cryptographic core 232 to control processor 212 for an initial classification. Control processor 212 may perform firewall, NAT, and routing classification for the packet, and further may create a connection table and hash entry in memory 106 for use by packet engine 228 on subsequent packets in the data flow. This may include the building of more than one connection table entry, depending on the application. Examples of this include preemptively constructing inbound and outbound entries, as well as a data channel entry for certain protocols. Control processor 212 may also trigger IKE processing as a result of the classification of the initial packet.

The connection table entries above provide a mechanism that allows the acceleration of security operations, such as firewall or NAT decision processing for packets. Connection entries may have a relationship (for example, one-to-one or many-to-one) to IPSec SAD entries in support of IPSec operations as a result of classification.

Control processor 212 may provide control plane operations for security processing system 102 and may run an embedded operating system or simple task

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.262

scheduler to handle complex packet applications such as, for example, firewall and intrusion detection system applications, a TCP/IP stack including routing functions, and support applications such as IKE and user interfaces for configuration, for example, from host processor 130. The use of control processor 212 in the foregoing manner may permit the complete containment of all key generation, public key and symmetric key encryption and decryption processing within the hardware of security processing system 102 and within cryptographic boundary 112. Control processor 212 allows the flexibility of general purpose processing for non-real-time, demand-driven or OS-based applications to be executed.

Modulo/expo engine 216 may be coupled to local data bus 210 to provide processing for streaming and modular exponentiation. Control processor 212 may provide public key macro acceleration by providing pre-processing for modulo/expo engine 216, which would permit host processor 130 to request high-level public key acceleration calls that are handled completely by security processing system 102. Modulo/expo engine 216 may be made accessible to control processor 212 and also host processor 130. The interconnectivity of operations that may be provided by control processor 212, specifically the providing of key management functions, modulo/expo engine operation and local access to encrypted/protected memory, allows security processor 104 to keep all unprotected cryptographic keys and operations within the boundary of security processor 104. In other embodiments, a dedicated key management processor (not shown), which may be coupled to local data bus 210, and associated firmware may be integrated and made accessible to modulo/expo engine 216 in addition to or even in the absence of control processor 212.

Firmware 214 may be executed by control processor 212 and may provide operating system software and other software to provide IKE and other functions and additional functions known to one of skill in the art. Control processor 212 may be, for example, a general purpose processor such as a 32-bit RISC processor. Other types of processors may also be used. Other software stored as part of firmware 214 may be used to permit control processor 212 to provide VPN, firewall, intrusion

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.263

detection/prevention, and SSL protocol communications, virus protection, digital rights management, content filtering, access control, verifying of application integrity, and management of public key infrastructure (PKI) exchanges.

Additional software stored as part of firmware 214 may permit a wide variety of data analysis functions including, for example, packet analysis, pattern matching, or other data analysis. Statistics may be generated by such functions and/or other functions and the results communicated to host processor 130 or another device (not shown) for central data collection of activity on devices coupled to internal network 116.

Firmware 214 may include control plane software that runs on control processor 212. The control plane software may communicate with the data plane software using a set of application program interfaces (APIs) and a message-based protocol. The data plane software may include forwarding software responsible for performing high-speed packet processing that handles the data plane steady-state portion of networking applications, such as, for example, IP packet forwarding protocols. The functionalities provided by security processing system 102 may be changed and/or updated by updating firmware 214. Such updating may be done, for example, as new industry or government security standards are developed or modified. Also, the resources devoted to each of the security and networking processing functions may be customized for each host computing device or by the location of a device on a network, for example a location at either a gateway or at an edge of the network.

Security processor 104 may include random number generator (RNG) 218 and timers, universal asynchronous receiver/transmitter (UART), and general purpose I/O 220 coupled to local data bus 210. RNG 218 may be a true digital random-number generator. RNG 218 may be made available to control processor 212 and also to host processor 130. Timers 220 may operate most operations in the core of security processor 104 and may run, for example, at a frequency of about 150 MHz. A separate reference clock (not shown) may be coupled to control processor 212, which may be bridged to the security processor 104 core, and run, for example, at about 250 MHz.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.264

Security processor 104 optionally may include anti-tamper system 224. Anti-tamper system is controlled by control processor 212 and may include detection circuits for voltage, temperature and physical probing forms of tampering. More specifically, anti-tamper system 224 may comprise hardware tamper circuits and firmware routines to check the integrity or health of stored flash content. The firmware routines may check the general integrity or health of the flash content using, for example, both DES-MAC or AES-MAC security methods or other hashing and authentication techniques. Anti-tamper system 224 may be implemented as a network of detection circuits tied to a fail-safe fault collector (not shown).

Translator 226, which may be, for example, a steganography translator or another memory obfuscation device or encryption translator, such as an encryption filter, may optionally be coupled to local memory interface 202 to use known steganographic or encryption techniques, as applicable to the type of device 226 used, in the writing and reading of security keys and other data to and from memories 106, 108 and/or 110. For example, an encryption key of, for example, about 112 bits may be distributed in an SRAM memory 108 in a data block size of, for example, about 100,000 bits and only be retrievable from memory 108 using a translation algorithm implemented in software in translator 226.

Encrypted Memory System

A hardware encryption path may be included between local data bus 210 and a memory controller block in security processor 104. This path may consist of two main components: (i) an encryption DMA block (EDMA) that may be a write-only path between a local host and off-chip memory (e.g., memory 106) for securely storing SA (security association) keying material; and (ii) an "ER" block that may be a read path from the memory controller block to the block from which a calling function is originating (for example, a cryptographic function running in cryptographic core 232 that uses SA keys for IPSec processing). The hardware encryption path as described herein may in general be useful with any off-chip memory, including for example,

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.265

memory 106, 108, or 110. FIG. 12 is a block diagram illustrating the relationship in this embodiment between the ER block, the EDMA block, cryptographic core 232, and memory. The division of memory access shown could be physical (block connection) or logical (access to targeted address ranges that are encrypted).

The EDMA block may consist of several blocks including an AES encryption block (e.g., 18-round AES with a 64-bit block size), an address expansion block, a control block, and a configuration block. The EDMA may sit between DMA interface 204 and an "AHB master block" (see FIGs. 6 and 7), which is coupled to the memory controller block (as discussed in more detail below). As discussed in more detail below and as illustrated in the figures, the AHB may be an internal AMBA host for the chip. AMBA refers to the Advanced Microcontroller Bus Architecture.

The EDMA block monitors signals from, for example, DMA interface 204 to determine if the current write request from DMA interface 204 to the AHB master block is, for example, for an IPSec SA, and/or SSL SA, or for a transfer which does not contain any SA data. This distinction may be controlled by two control bits in a control word associated with DMA interface 204 and used for each transfer. If the transfer is for an IPSec SA, the EDMA logic may hold off the request going to the AHB master block until the AES block is ready e.g., when the initial 10 rounds of AES processing are complete). The AES block may use the SA source address and an internally generated key (K) to complete the initial 10 rounds. On completion of the 10 rounds, 64-bits, for example, of Cipher Text 0 (CT0) will be produced, and the write request will be allowed to pass to the AHB master block. The AHB master block will assert its read signal and the first 8 bytes of data (a Basic Command Word [BCW], which is control data not needing confidentiality protection) will be allowed to transfer as cleartext. On each of the remaining transfers, the AES block will step one round of the AES algorithm per each transfer, and the data will be XOR'ed with CT_n (n=0...8) to produce a value $EDMA_K [Data_n]$ (n=0...8) for a total transfer of 80-bytes, of which 72 bytes are encrypted. The EDMA preferably will not encrypt any transfer where the source address equals the destination address.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.266

The ER block may provide a path from memory 106 (e.g., off-chip SA DDR) to cryptographic core 232 for decrypting SA's that are located within memory 106. The ER block may consist of several blocks including an AES encryption block (e.g., 18-round, 64-bit AES), an address expansion block, a variable FIFO, a control block, and a configuration block. The ER block may be located between the calling functional block (e.g., cryptographic core 232 or another block) and memory 106. The ER block may be read-only, or it may be read-write, if necessary to, for example, copy back state information. FIG. 11 is a block diagram illustrating the relationship in this embodiment of the ER block to the cryptographic core and memory.

The ER block may monitor the calling functional block's request signals to memory 106. If the request is a read, the ER block will hold off the completion of the read by de-asserting its ready signal (***"ER_rdy"***) to a memory arbiter until the AES block is ready (i.e., when the initial 10 rounds of the AES algorithm are complete). The memory arbiter (e.g., a RAM arbiter) brokers access requests from the requestors of memory (e.g., a MIPS processor, one of packet engines 228, or cryptographic core 232). Signal ***ER_rdy*** may be transmitted to the memory controller (see the "CRA" block in Fig. 12) from the EDMA or the ER control element.

The AES block may use the SA source address provided from the interface to cryptographic core 232 and the K key to complete the initial 10 rounds of the AES algorithm. On completion of the 10 rounds, 64-bits of Cipher Text 0 (CT0) will be produced and the ready signal (***ER_rdy***) may be asserted allowing the read request to pass to the memory arbiter. The memory arbiter will assert its data ready signal and the first 8-bytes of data (the BCW) will be allowed to transfer in the clear. On each of the remaining transfers, the AES block will step one round of the 64-bit AES algorithm per transfer, and the data will be XOR'ed with CT_n (n=0...8) to produce values $E1_K$ [$Data_n$] (n=0...8) for a total transfer of 80 bytes, of which 72 bytes are decrypted. More generally, the ER block may decrypt or encrypt to arbitrary offsets per each read or write request, intermingling data stored in the clear with data stored in an encrypted form so as to make a clear text delivery to the calling functional block.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.267

Now discussing an encrypted hardware path according to the present invention in more detail, an encrypted memory system may be implemented as a multi-block system tasked with the selective encryption of memory structures to protect data that may reside in off-chip memory (e.g., memory 106, 108, or 110, as mentioned above) from use by anything other than the intended block and/or logic that resides in the system itself. It is particularly useful in encryption devices and applications such as with the IP Security protocol where one wishes to achieve FIPS 140-2 level 2 or similar levels of protection for data and process contents.

The specific embodiment of the present invention discussed here preferably has two primary blocks. First, the EDMA block may provide logic and a protected path from, for example, a host general purpose DMA interface to the memory controller. This is the path over which the encrypted data may be written to memory. The utility of the EDMA block is to provide a method of inserting data into memory, encrypting it enroute. Second, the ER block may provide a fast decryption path for data read from external memory. The ER block is accessible only to trusted requestor blocks within the chip, making retrieval and decryption of certain protected memory data discriminatory, based on purposeful hardware design. An encryption key K may be used for encryption and decryption of the externally stored data. K is preferably internally generated at initialization and not visible nor accessible outside the system.

Data Representation Conventions

FIG. 5 illustrates the data representation convention used herein for purposes of explanation. Other conventions may be used in different embodiments. Throughout the description herein, all data vectors and one-dimensional data structures are represented with the Most Significant Bit (MSb) in the leftmost position and the Least Significant Bit (LSb) in the rightmost position. All two-dimensional data structures are represented with the MSb in the upper leftmost position and the LSb in the lower rightmost position.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.268

EDMA Block (GDMA to Off-Chip Memory)

The EDMA block may provide a write-only path between a local host or other data generating device and the off-chip memory for securely storing protected information, such as SA keying material. It may consist of several blocks that include an N round B block AES encrypt (where B is the width of the memory interface), address expansion, control, and configuration. An AES algorithm of 128-bit key size is typically used though other key sizes may be used with the appropriate adjustment in key expansion rounds. Likewise, some other streaming or block cipher may be used in an alternate implementation. The EDMA block sits between the interface from the data path and the bus to the memory controller. In one implementation the EDMA may be located between the "GDMA" block and the "AHB" block (see FIGs. 6-8). The GDMA (general purpose DMA) block may interface the internal or external host to the AHB. The AHB master is the mechanism for the functional block (e.g., the GDMA block or packet DMA [PDMA]) to take control of the bus for signalling and data transmission. Alternatively, in a multi-path (parallelizing) design, the EDMA block could be located between the GDMA Slice0 (gda_sclice0) and the GDMA multiplexer (mux) as illustrated in FIG. 6.

The EDMA block monitors the incoming data bus (e.g., GDMA signals) to determine if the current write request is protected data or a transfer which does not contain any protected data. This distinction may be controlled by signaling, for example, two control bits in a GDMA control word for each transfer. The signaling may also determine whether or not there is an offset to the beginning of encryption, allowing a block-sized multiple of clear text to precede the encrypted data in a single transaction. If the transfer is to be encrypted, for instance for an IPSec SA, the EDMA logic will hold off the request going to the AHB Master until the AES is ready, that is when the initial 10 rounds of AES are complete, and the block multiple clear text offset is reached, if it exists. The AES block will use the incoming data's Source Address (M) and K key to complete the initial 10 rounds. On completion of the 10 rounds, B bits of Cipher Text 0 (CT0) will be produced and the write request will be allowed to pass to

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.269

the AHB Master. The AHB Master (in this example) will assert its read signal and the first 8-bytes of data will be allowed to transfer. On each of the remaining transfers the AES block will step one round of the AES algorithm per transfer and the data will be XOR'ed with CT*n* (n=0...i) to produce E_K[Data*n*] for a total transfer of n x 8 bytes being encrypted. The EDMA block will not encrypt any transfer where the source address equals the destination address. A more detailed block diagram is illustrated in FIG. 7. The sections below describe each of these blocks in more detail.

RND_{mix}

The RND_{mix} value will be initialized during the boot-up sequence as a 64-bit (or block size) random or pseudo-random number and then written to the EDMA RND_{mix} register. The RND_{mix} will be XOR'd with the cipher text XOR data and then be sent to the EDMA mux, providing additional mix protection to mitigate the weakness of "to 000 or FFF" writes to memory.

AES64 Encryption Block

The AES block preferably uses a reduced block size, 64-bit block AES (128-bit key) algorithm as defined in the Appendix to this application (AES64 Specification). Although the embodiment of the present invention is discussed in the context of this specific AES algorithm, one of skill in the art will recognize that other algorithms (e.g., other than AES) may be used in other embodiments. Although in the Appendix the number of rounds for the AES algorithm is defined as 10, for the EDMA or ER blocks the AES64 may be extended to support an 10+n round cipher, as determined by the size of the encrypted data transaction. For more detail, see the following table:

PreAdd round 1	SubBytes
round 1	ShiftRows

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.270

round 1	MixColumn
round 1	AddKey
...	
round n	SubBytes
round n	ShiftRows
round n	(No MixColumn On Last Round)
round n	AddKey

The output of rounds 11 through n will produce CT_0 through CT_n which will be used to XOR with the eight byte blocks (for a 64-bit memory width) of the data transaction being written to off-chip memory. An initial, block multiple amount of data may be allowed to pass in the clear prior to the active encryption, based on any offset programmed into the transaction signaling.

EDMA Address Expansion Block

The address expansion block takes n_m-bits of address data together with some amount of K data and produces block-sized bits of address expansion data for input to the AES block. The address expansion block may use S-Box and E-Box functions to accomplish the expansion, though other substitution or expansion algorithms may be used as long as they introduce sufficient variability. The address is typically expanded through the E-Box or some other expansion function. Some mixing bits are selected from K and run through a number of S-Box's or some other substitution function to produce data that will be XOR'd with the expanded address seed from the E-Box. The output from the XOR is then appended to the address (or data that is address dependant) to form a block-sized amount of output (***ax_data[B:0]***). In more detail, in formula form: $ax\_data[B:0] = \{gdma\_EDMA\_amemory[m_i:0], X_i[(B-m_i):0]\}$

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.271

ER Block (Cryptographic Core to/from Security Association (SA) Memory)

The ER block (e.g., for a four-channel slice) provides a read-only (e.g., IPSec) path from off-chip memory to the functional block or device reading the memory, for example, in the case where cryptographic core 232 would need to decrypt SA's that are located within off-chip memory. It may consist of several blocks that include an n-round, B-bit AES encrypt, address expansion, variable FIFO, control, and configuration. The ER block may be located between the memory-consuming function (e.g., cryptographic core 232) and off-chip memory as illustrated in more detail in FIG. 8. Multiple function blocks or devices may have their own or a shared ER block to memory.

The ER block monitors the calling block's request signals to the off-chip memory. If the request is a read, the ER block will hold off the completion of the read by de-asserting its ready signal (***ER_rdy***) to a memory arbiter until the AES block is ready (i.e., when the initial 10 rounds of AES64 are complete). The AES block will use the memory Source Address provided from the cryptographic core interface and the K key to complete the initial 10 rounds of AES64. On completion of the 10 rounds, 64 bits of Cipher Text 0 (CT0) will be produced and the ready signal (***ER_rdy***) will be asserted allowing the read request to pass to the memory arbiter. The memory Arbiter will assert its data ready signal and the data will be allowed to transfer. If an offset is included in the request signal, then a block multiple of data may precede the decrypted information in the clear. On each of the remaining transfers the AES block will step one round of the AES algorithm per transfer and the data will be XOR'ed with CT*n* (n=0...8) to produce $E1_K$[Data*n*] for a total transfer of 8 x n bytes being decrypted.

Host Configuration Interface (I/F)

A host configuration interface provides read/write access to local configuration and status registers.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.272

RND_{mix}

The RND_{mix} value will be initialized during the boot-up sequence as a 64-bit (or block size) random or pseudo-random number and then be written to the EDMA RND_{mix} register. The RND_{mix} will be XOR'd with the cipher text XOR data and then be sent to the EDMA mux, providing additional mix protection to mitigate the weakness of "to 000 or FFF" writes to memory.

AES Encryption Block

The AES block preferably uses a reduced-block size, 64-bit AES algorithm as defined in the Appendix to this application (AES Specification). Although the discussion in the Appendix defines the number of rounds as 10, for the ER block the AES block is able to support a 10+n round cipher, where n represents the number of bus width blocks of memory to be retrieved.

ER Address Expansion Block

The ER address expansion block may be implemented in the same way as the EDMA address expansion block.

Network Intrusion Detection System

FIG. 3 illustrates a more-detailed functional block diagram of a network intrusion detection system that may be used in a portion of security processor 104 in accordance with an embodiment of the present invention. FIG. 3 illustrates, for example, three packet engines 228 in parallel and each connected to a cryptographic core 232.

Network intrusion detection system (NIDS) 302 has taps 303 that may couple to the input/output of each of packet engine 228 and cryptographic core 232 pair. Signature database 304 is a defined set of patterns stored in on and/or off-chip memory.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.273

NIDS 302 attempts to match parts of the data stream (for example, the header, payload, or trailer) against the stored set of patterns.

According to the present invention, by passing all I/O traffic to host processor 130 and/or internal network 116 through security processing system 102, and including NIDS 302 within system 102, undesirable intrusions may be detected in-line with such I/O traffic, such as, for example, it passes through an NIC. By being in-line in this manner, intrusions identified by NIDS 302 may be stopped in the I/O traffic flow and any further related improper intrusion prevented from passing to host processor 130 and/or internal network 116.

Each computer or computing device (not shown) connected, for example, to internal network 116 may be protected by security processing system 102, such as, for example, using an NIC containing security processing system 102 for all I/O traffic for each device. Each such distributed NIC may communicate with a central server (not shown) connected to internal network 116 to accumulate performance, security, network processing and other data related to activities reported by each such security processing system 102. Additionally, such accumulated data may be processed and/or analyzed by the central server and then new or modified control signals sent to all, or a selected portion, of the security processing systems 102 of each device on internal network 116.

Having a tap on each of the input and output paths to each cryptographic core 232 permits the capture of clear text packets either before or after encryption, depending on whether the packets are inbound or outbound. Thus, signature matching may be done on clear text data. NIDS 302 may flag a packet as having a potential signature match to a pattern in signature database 304. The flagged packet may either be dropped (and the flow of subsequent packets in the same data flow stopped) or continue to its next destination, with a logging report to host processor 130 in either case indicating the status of the packet. Also, in addition to being sent to its next destination, the flagged packet may be redirected or duplicated and receive further slow path processing by control processor 212. The logging report may be used to form an audit trail for

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.274

collective or heuristic analysis and future packet inspection by a centralized intrusion detection system or other process or device. If a packet has been identified as undesirable, intrusion prevention may be provided by dropping related future packets in packet engines 228.

NIDS 302 may be coupled to a separate control channel 305 coupled back to one or more, and preferably all, of packet engines 228. Control channel 305 is a special path to send packets that have been flagged by NIDS 302 to the control plane on local data bus 210 (and then optionally on to host processor 130) for logging or other administrative tasks, including, for example, providing data for use by a network administrator in managing and improving network intrusion detection and prevention by security processing system 102.

Flagging of a packet or a packet data structure may be done by setting a bit flag in a control word corresponding to the packet. By examining this bit flag for a packet, control processor 212 may direct the packet to a certain location for logging. Results from packet classification performed by each packet engine 228 (for example, to determine that the packet is network file system (NFS) traffic) may be used to select from one of many rules sets or signature sets in signature database 304.

Based on comparisons to the selected rules or signature sets, control channel 305 may indicate one or more types of initial potential intrusion violations associated with a packet. After indicating flagged packets to one or more of packet engines 228 through control channel 305, each packet engine 228 may further classify the packet by comparison to the one or more types of other potential intrusion violations provided for the packet by control channel 305, and use information from prior classification processing for the packet by the packet engine 228 to narrow or eliminate the set of potential intrusion violations.

Packet/Data Flow

FIG. 4 illustrates a simplified flow diagram of typical packet or data flow for one embodiment of security processing system 102. Each packet engine 228 may

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.275

comprise a packet processor and a classification engine. Circles 404 and 406 generally correspond to the functionality provided by the classification engine and the packet processor, and such functionality is referred to herein as classification engine 404 and packet processor 406.

Classification engine 404 may provide lookup and decision logic for, among other things, security policy database (SPD) lookup, firewall connection table lookup, NAT table lookup, routing, and limited application level gateway (ALG) rule application and data mangling. Any or all of the foregoing classification engine functions may be subsumed in a single connection table entry. Once an initial data flow is defined, the foregoing classification engine functions may be made integral to the data flow.

Packet flow through security processing system 102 typically begins when a packet enters switching system 208 via one of streaming interfaces 200 or DMA interfaces 204. Each packet may be inserted into an active list waiting for the next available packet engine 228. The same active list may be an insertion path for control processor 212 to direct packet traffic into a packet engine 228. Regardless of destination, whether, for example, it is to streaming interface 200, host interface 206, control processor 212, or a loop through a packet engine 228, all packet data preferably flows to a packet engine 228 and then to a corresponding cryptographic core 232. Tagging of the packet upon ingress to the packet engine 228 may determine the egress path from cryptographic core 232. More specifically, the incoming and outgoing packets may be provided with a tag upon ingress to one of packet engines 228 and the tag may be used to determine the egress path upon exit from the corresponding cryptographic core 232.

Classification hash lookup data and a detailed connection flow table and security policy/association data may be stored, for example, in memory 106. Upon receiving a packet, packet engine 228 may find a match in the connection table, fetch the connection information (including SAD information as appropriate), and apply the appropriate rules and transforms. This may include forwarding the packet to control

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.276

processor 212. If no match is found in the connection table, then the packet is preferably forwarded to control processor 212.

Outbound packets may be buffered after transit through packet engine 228 and cryptographic core 232 for sending out to streaming interface 200 or to host interface 206. Outbound packets may have made a single trip through packet engine 228 and core 232, may have made a second trip through packet engine 228 and core 232 after prior processing by control processor 212, or may have made a second trip through packet engine 228 for firewall inspection following decryption in cryptographic core 232.

Initial packets needing classification to create a NAT lookup table entry and/or firewall connection table entry may be forwarded to control processor 212 for processing, then back to classification engine 404, and then to packet processor 406 prior to output from security processor 104 (unless dropped in accordance with the firewall rules in effect). If such initial packets also need IPSec processing, they may be forwarded to packet engine 228 after initial processing by control processor 212, then back to an egress interface.

For packets that are already in an existing data flow, for example, already having connection table entries or NAT global mapping in existence, a successful lookup may result in a direct forwarding to packet processor 406 for modification, and then classification by classification engine 404 for egress from security processor 104. Outbound IPSec packets in an existing flow transit to packet engine 228 and cryptographic core 232 after egress classification and firewall packet processing. Inbound IPSec packets in an existing flow are forwarded to packet engine 228 and cryptographic core 232, then to the classification engine 404 and packet processor 406 for SPD validation, routing, and optionally, firewall and NAT processing prior to egress.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.277

APPENDIX

An APPENDIX is included at the end of this application, which is incorporated by reference in full herein. The APPENDIX describes the AES64 algorithm referenced above. The APPENDIX presents information regarding a specific algorithm and is not intended to be limiting in any way. Other implementations of the present invention may be made.

CONCLUSION

By the foregoing description, an improved secure I/O interface system and method have been described. The system and method may improve the security of communications to and from trusted hardware, improve communication speed, reduce the number of different systems required for secure communications, and reduce the extent of the bottleneck on the backplane bus.

The foregoing description of specific embodiments reveals the general nature of the invention sufficiently that others can, by applying current knowledge, readily modify and/or adapt it for various applications without departing from the generic concept. Therefore, such adaptations and modifications are within the meaning and range of equivalents of the disclosed embodiments. The phraseology or terminology employed herein is for the purpose of description and not of limitation. Accordingly, the invention embraces all such alternatives, modifications, equivalents and variations as fall within the spirit and scope of the appended claims.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.278

CLAIMS

What is claimed is:

1. A security processor to process incoming and outgoing packets, the security processor comprising:

a switching system to send and receive packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming and outgoing packets; and

a cryptographic core, coupled to the packet engine, to provide encryption and decryption processing for packets received from the packet engine.

2. The security processor of claim 1 wherein the packet engine is further operable to handle security context management processing for the incoming and outgoing packets.

3. The security processor of claim 1 further comprising:

a local data bus coupled to the switching system; and

a modulo engine coupled to the local data bus.

4. The security processor of claim 1 wherein the packet engine is one of a plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit one of the plurality of packet engines.

5. The security processor of claim 4 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the plurality of packet engines and substantially all of the incoming and outgoing packets to the security processor transit a corresponding one of the plurality of cryptographic cores after transiting one of the plurality of packet engines.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.279

6. The security processor of claim 4 wherein the incoming and outgoing packets are provided with a tag upon ingress to one of the plurality of packet engines and the tag determines the egress path within the security processor upon exit from the corresponding one of the plurality of cryptographic cores.

7. The security processor of claim 3 wherein the packet engine, the cryptographic core, and the modulo engine are formed on a single chip.

8. The security processor of claim 7 further comprising a control processor, coupled to the local data bus, for exception handling of the incoming and outgoing packets.

9. The security processor of claim 7 further comprising a key management engine coupled to the local data bus.

10. The security processor of claim 1 further comprising an intrusion detection system coupled between the cryptographic core and the packet engine.

11. The security processor of claim 7 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

12. The security processor of claim 11 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

13. The security processor of claim 1 further comprising an intrusion detection system coupled between the cryptographic core and the packet engine.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.280

14. A security processing system comprising:

(a) a security processor comprising:

a switching system to send outgoing and to receive incoming packets;

a packet engine, coupled to the switching system, to handle classification processing for the incoming and outgoing packets;

a cryptographic core, coupled to the packet engine, to provide encryption and decryption processing for packets received from the packet engine; and

a local data bus coupled to the switching system; and

(b) a memory coupled to the local data bus.

15. The security processing system of claim 14 further comprising a modulo engine coupled to the local data bus.

16. The security processing system of claim 15 further comprising a key management engine coupled to the local data bus.

17. The security processing system of claim 14 wherein the memory and the security processor are within the same cryptographic boundary.

18. The security processing system of claim 14 wherein the security processor is formed on a single chip.

19. The security processing system of claim 14 further comprising:

a memory interface coupled to the local data bus, wherein the memory is coupled to the local data bus using the memory interface; and

a translator coupled to the memory interface to perform translation of data received by the memory interface from the memory.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.281

20. The security processing system of claim 19 wherein the translator performs steganographic translation of the received data.

21. The security processing system of claim 19 wherein the translator performs encryption translation of the received data.

22. The security processing system of claim 14 wherein the security processor is operable to (i) execute boot code to load firmware for execution by the security processor and (ii) authenticate the boot code using a mechanism internal to the security processor prior to operation of the security processor.

23. A security processor to connect a trusted network to an un-trusted network for data packet communication, the security processor comprising:

a first interface to couple to the trusted network and to the un-trusted network;

a second interface to couple to a host processor;

a switching system operable to selectively couple to the first interface or the second interface;

a local data bus, coupled to the switching system;

a plurality of packet engines coupled to the switching system;

a plurality of cryptographic cores each coupled to one of the plurality of packet engines; and

a control processor, coupled to the local data bus, to control data packet flow within the security processor.

24. The security processor of claim 23 wherein the security processor is operable to act as a firewall to deny or accept a data packet and to implement a secure communication channel with another computing device in the un-trusted network.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.282

25. The security processor of claim 24 wherein the security processor implements data packet security and authentication functions to support the secure communication channel.

26. A communication system comprising:

a trusted network; and

a secure interface coupled to the trusted network to carry all incoming and outgoing communications of the trusted network, wherein the secure interface comprises a security processor to handle substantially all security processing for the incoming and outgoing communications.

27. The communication system of claim 26 wherein the security processor performs substantially all network processing for data packet communications traveling to and from the trusted network.

28. The communication system of claim 27 wherein the secure interface handles substantially all security processing for the incoming and outgoing communications.

29. The communication system of claim 28 wherein the information security processing comprises IPSec processing.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.283

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Abstract

A security processor performs all or substantially all security and network processing to provide a secure I/O interface system to protect computing hardware from unauthorized access or attack. The security processor sends and receives all incoming and outgoing data packets for a host device and includes a packet engine, coupled to a local data bus, to process the incoming and outgoing packets. The processor further comprises a cryptographic core coupled to the packet engine to provide encryption and decryption processing for packets processed by the packet engine. The packet engine also handles classification processing for the incoming and outgoing packets. A modulo engine may be coupled to the local data bus.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.284

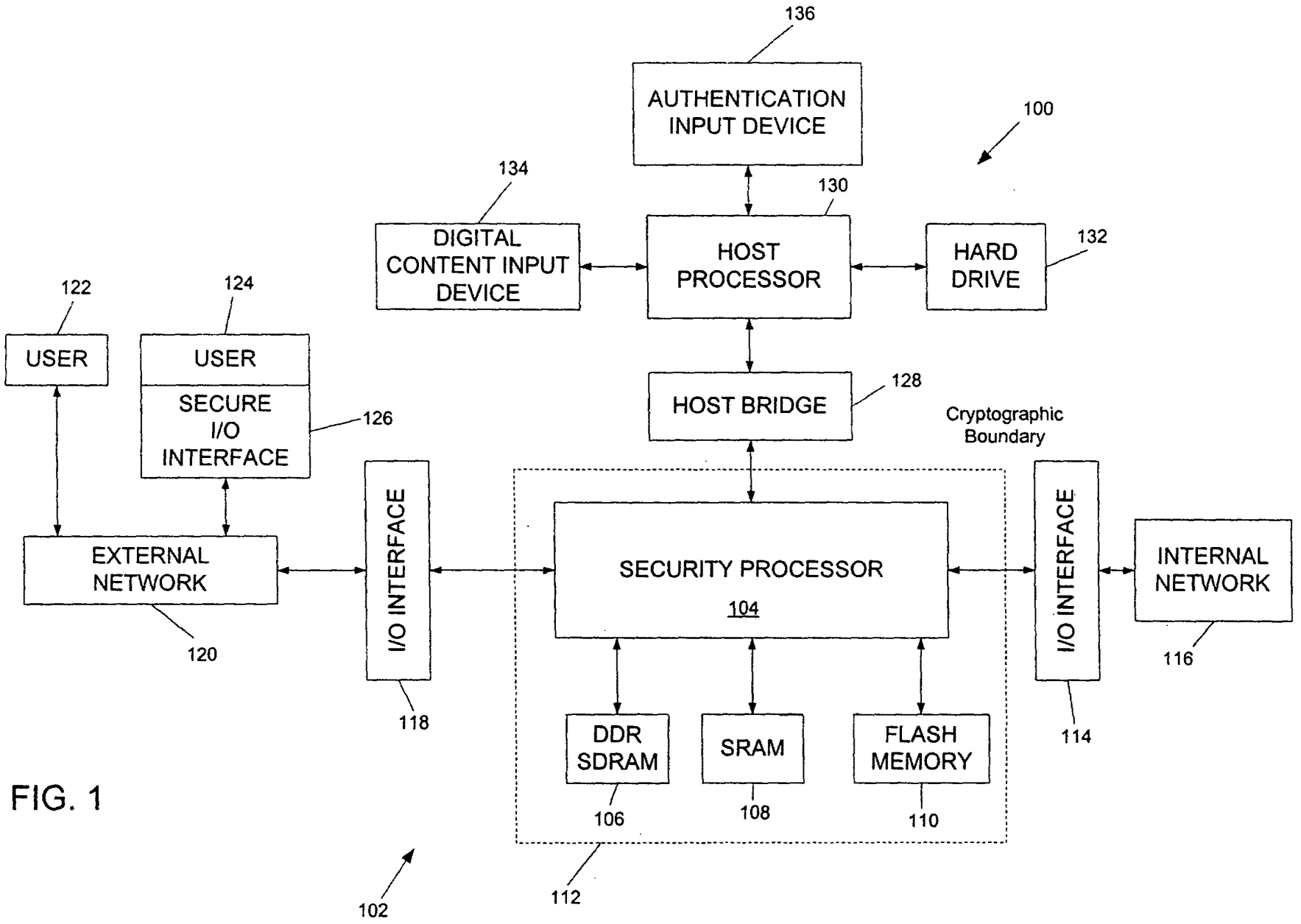

136
AUTHENTICATION INPUT DEVICE
100
134
130
DIGITAL CONTENT INPUT DEVICE
HOST PROCESSOR
HARD DRIVE
132
122
124
USER
USER
SECURE I/O INTERFACE
126
HOST BRIDGE
128
Cryptographic Boundary
EXTERNAL NETWORK
120
I/O INTERFACE
118
SECURITY PROCESSOR
104
I/O INTERFACE
114
INTERNAL NETWORK
116
DDR SDRAM
106
SRAM
108
FLASH MEMORY
110
102
112

FIG. 1

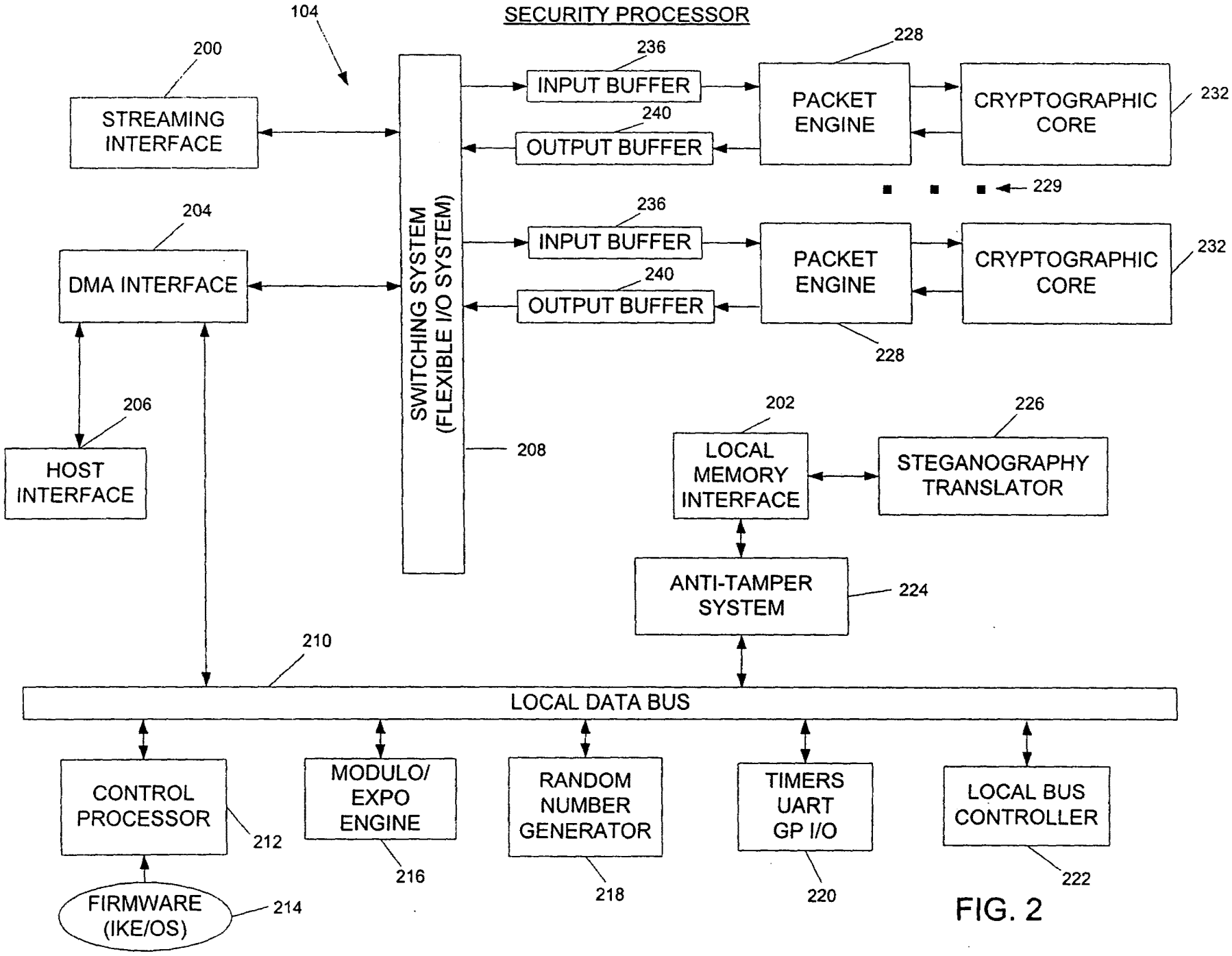

SECURITY PROCESSOR
104
200
STREAMING INTERFACE
204
DMA INTERFACE
206
HOST INTERFACE
SWITCHING SYSTEM (FLEXIBLE I/O SYSTEM)
208
236
INPUT BUFFER
240
OUTPUT BUFFER
228
PACKET ENGINE
CRYPTOGRAPHIC CORE
232
229
236
INPUT BUFFER
240
OUTPUT BUFFER
PACKET ENGINE
CRYPTOGRAPHIC CORE
232
228
202
LOCAL MEMORY INTERFACE
226
STEGANOGRAPHY TRANSLATOR
ANTI-TAMPER SYSTEM
224
210
LOCAL DATA BUS
CONTROL PROCESSOR
212
FIRMWARE (IKE/OS)
214
MODULO/ EXPO ENGINE
216
RANDOM NUMBER GENERATOR
218
TIMERS UART GP I/O
220
LOCAL BUS CONTROLLER
222

FIG. 2

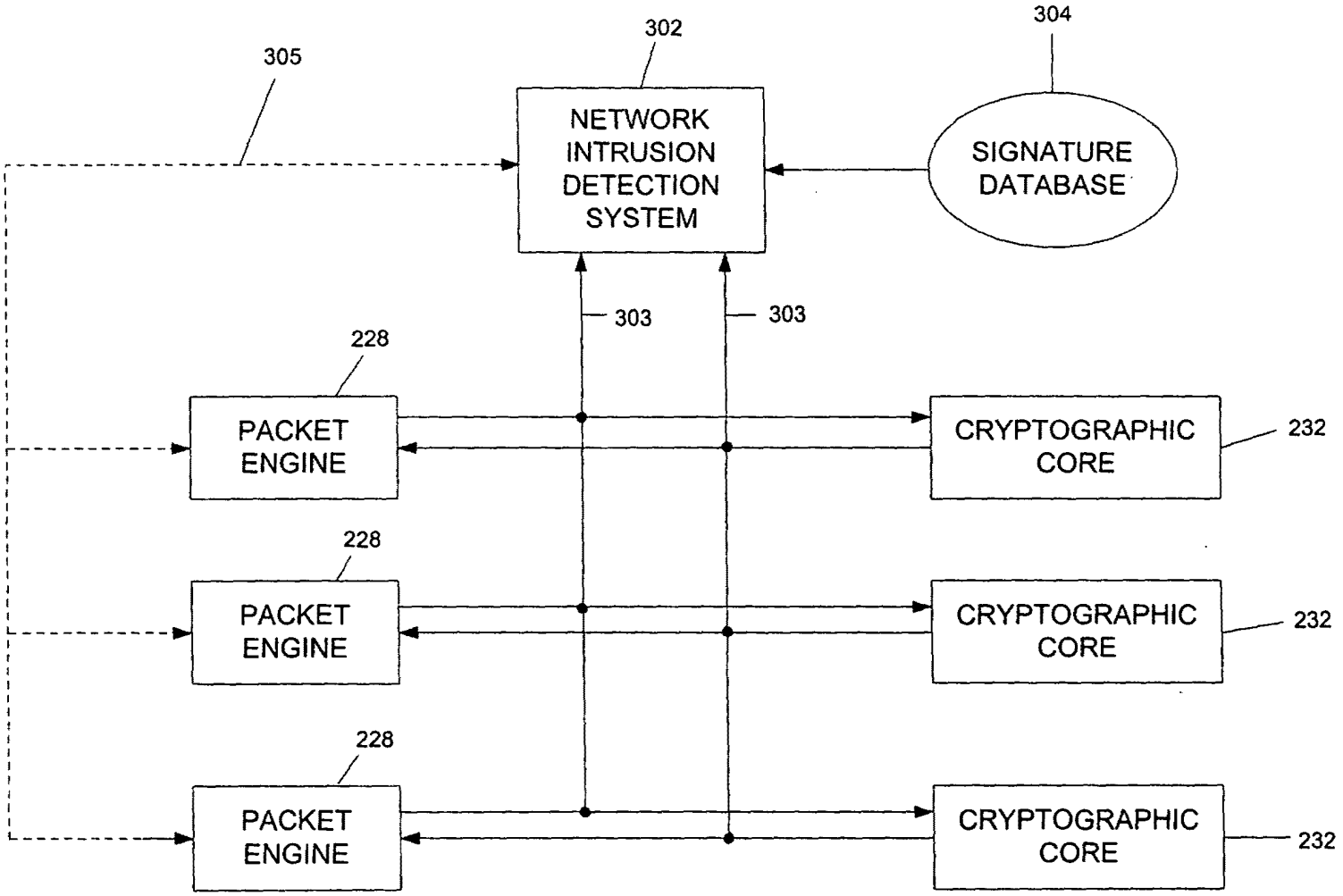

305
302
304
NETWORK INTRUSION DETECTION SYSTEM
SIGNATURE DATABASE
303
303
228
PACKET ENGINE
CRYPTOGRAPHIC CORE
232
228
PACKET ENGINE
CRYPTOGRAPHIC CORE
232
228
PACKET ENGINE
CRYPTOGRAPHIC CORE
232

FIG. 3

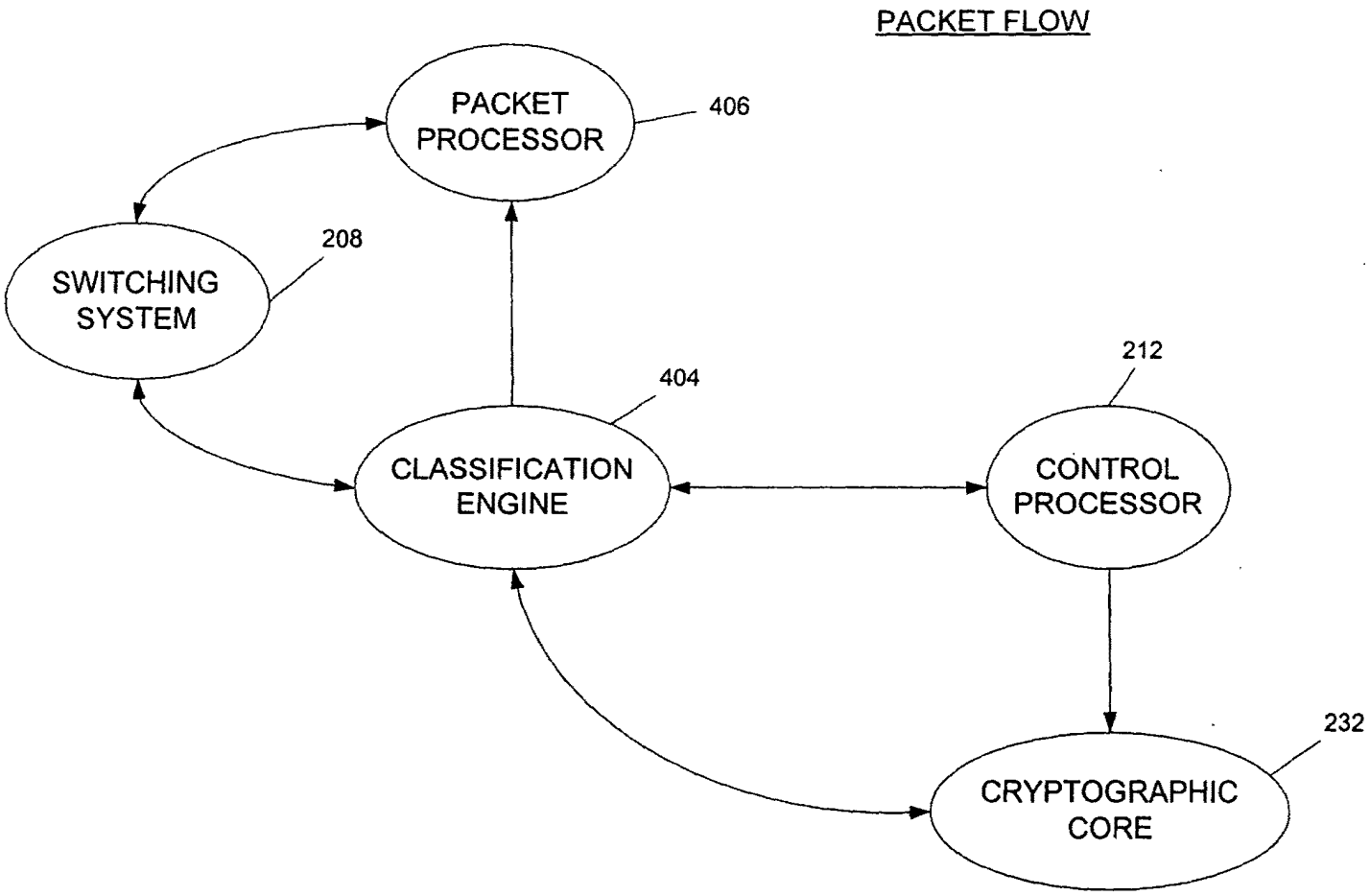

PACKET FLOW
PACKET PROCESSOR
406
SWITCHING SYSTEM
208
CLASSIFICATION ENGINE
404
CONTROL PROCESSOR
212
CRYPTOGRAPHIC CORE
232

FIG. 4

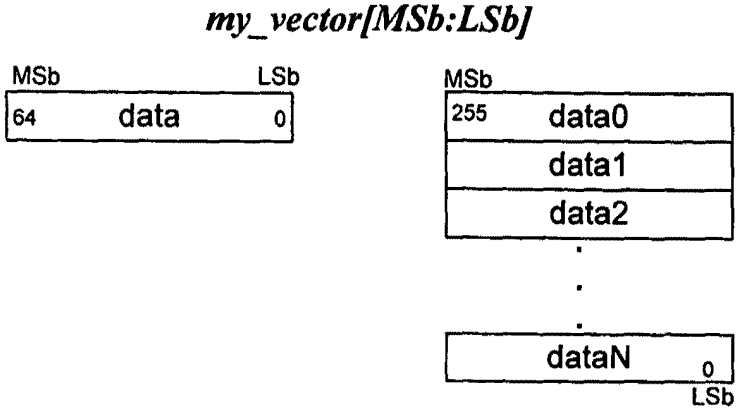

my_vector[MSb:LSb]
MSb
LSb
64
data
0
MSb
255
data0
data1
data2
dataN
0
LSb

FIG. 5

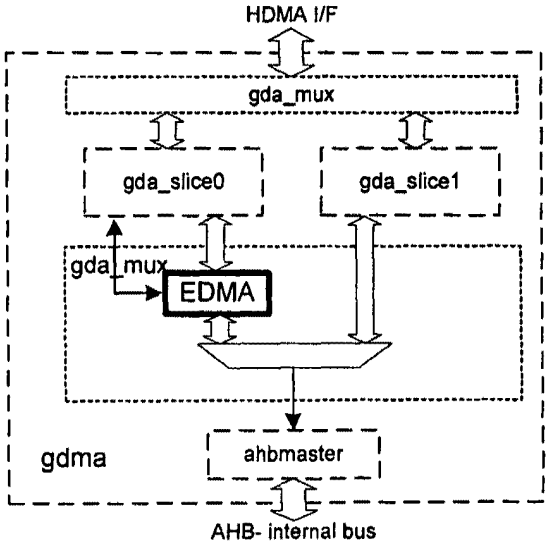

HDMA I/F
gda_mux
gda_slice0
gda_slice1
gda_mux
EDMA
gdma
ahbmaster
AHB- internal bus

FIG. 6

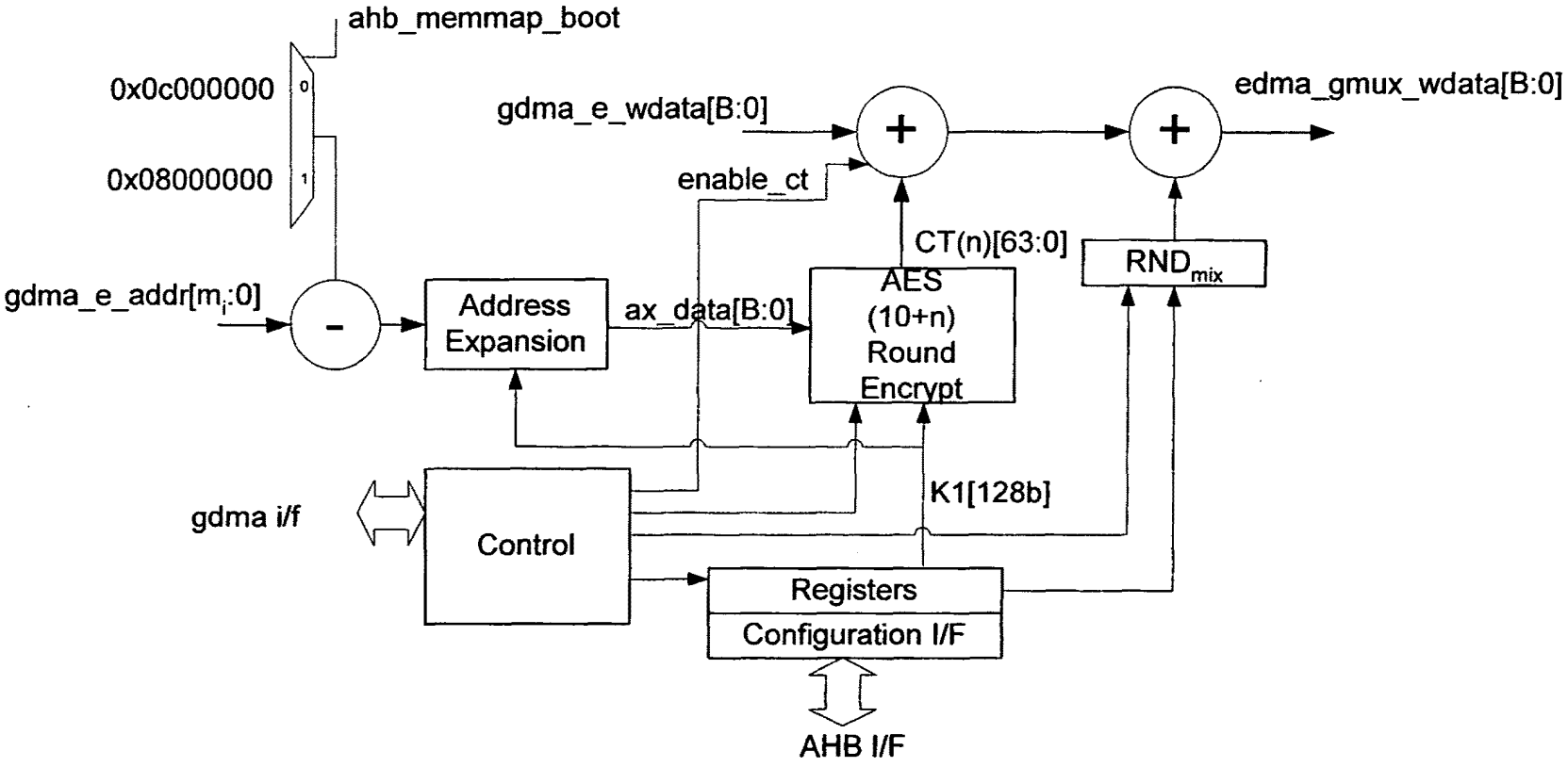

ahb_memmap_boot
0x0c000000
0x08000000
0
1
gdma_e_wdata[B:0]
edma_gmux_wdata[B:0]
enable_ct
CT(n)[63:0]
RND mix
gdma_e_addr[m i:0]
Address Expansion
ax_data[B:0]
AES (10+n) Round Encrypt
gdma i/f
Control
K1[128b]
Registers
Configuration I/F
AHB I/F

FIG. 7

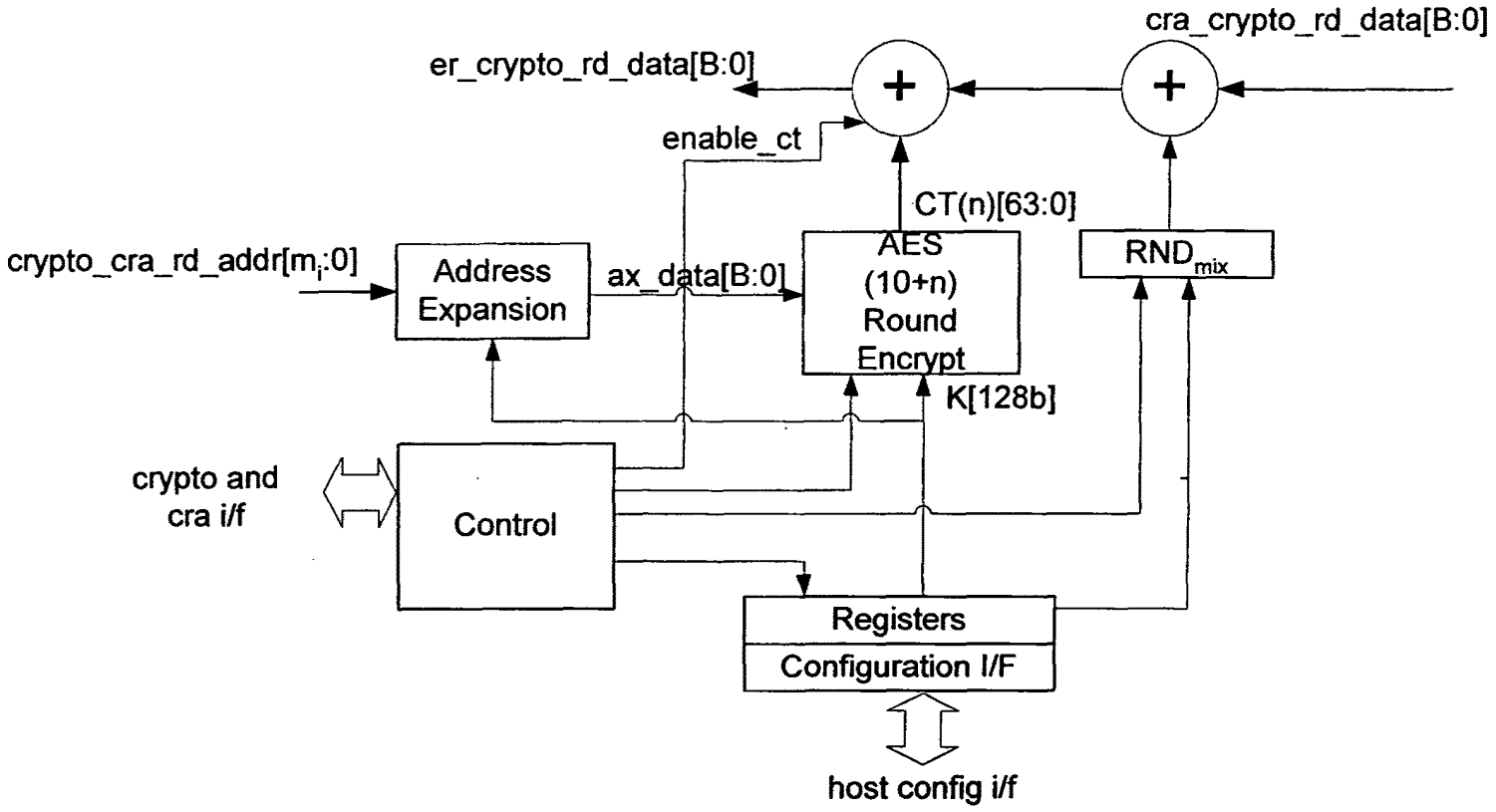
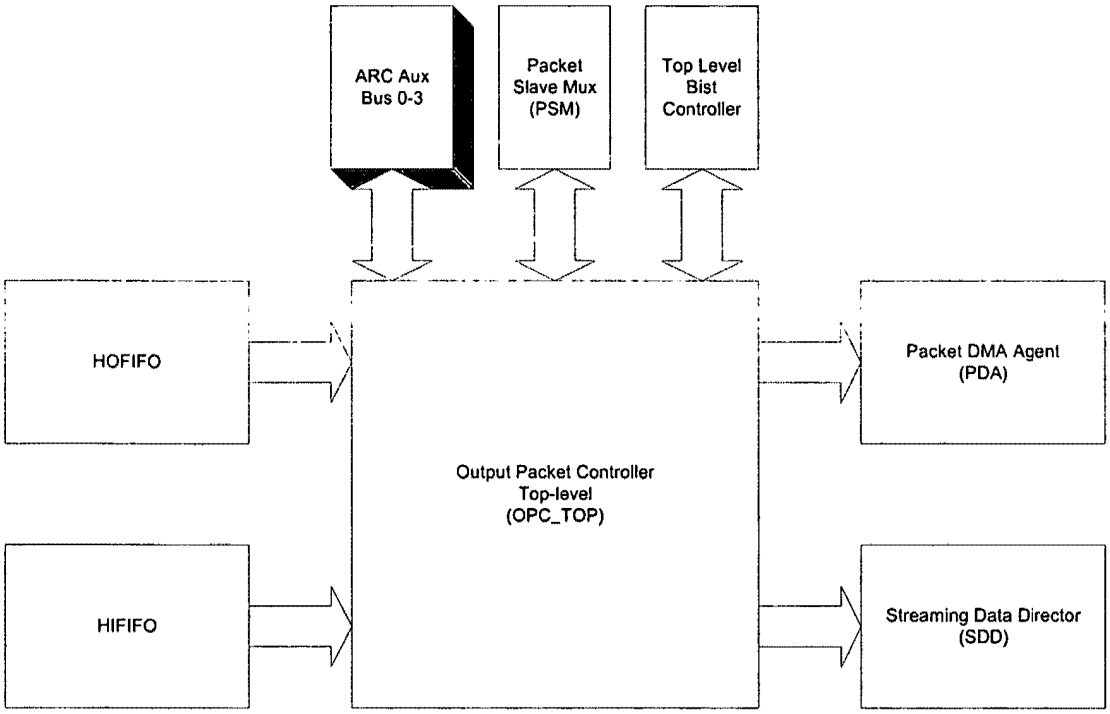

cra_crypto_rd_data[B:0]
er_crypto_rd_data[B:0]
enable_ct
CT(n)[63:0]
crypto_cra_rd_addr[m_i:0]
Address Expansion
ax_data[B:0]
AES (10+n) Round Encrypt
RND_mix
K[128b]
crypto and cra i/f
Control
Registers
Configuration I/F
host config i/f

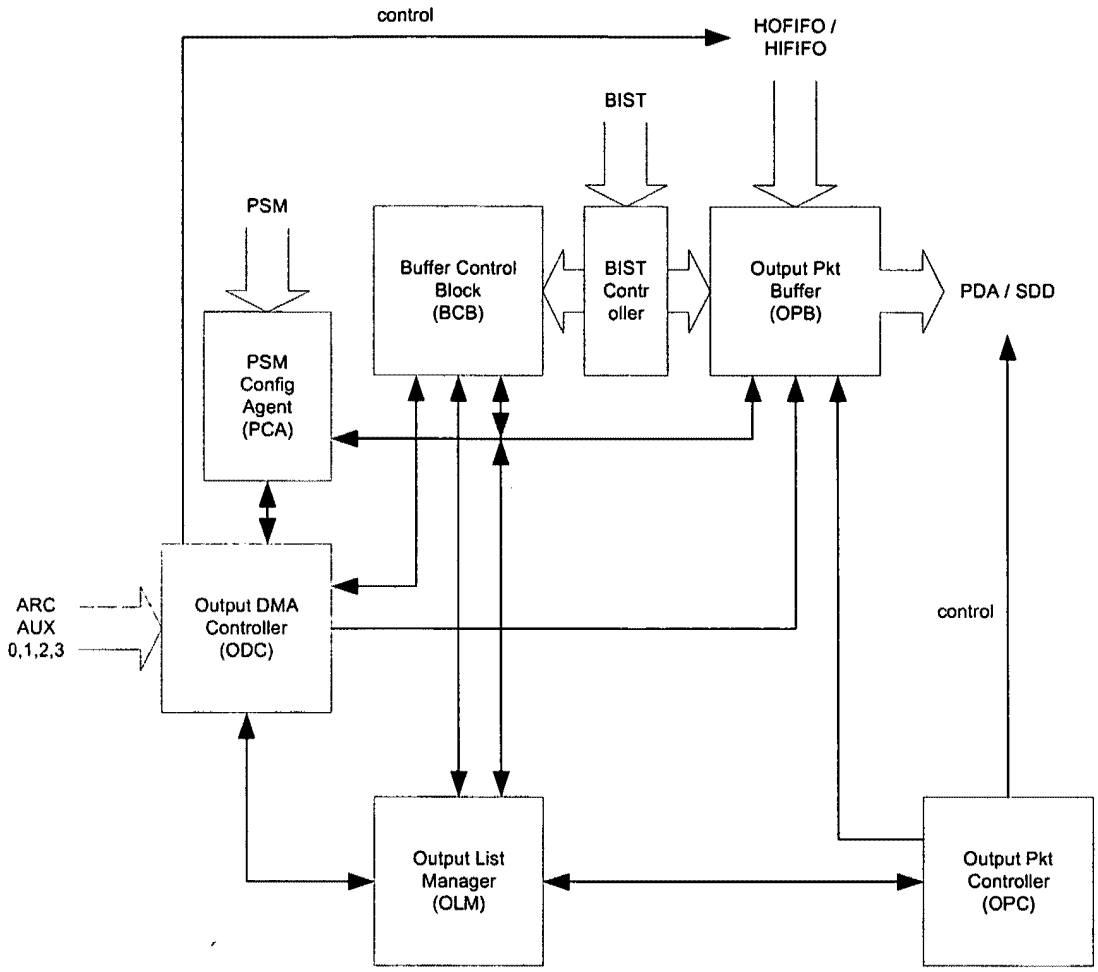
FIG. 8



OPC Interfaces

FIG. 9

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.292



OPC Internal Block Diagram

Notation:
PDA=Packet DMA Agent, forwards packets to host or connected entity via DMA.
SDD=Streaming Data Director. The SDD transfers packets to Streaming IO (e.g. GMII, PL-3, etc).
PCA= PSM Config Agent module enables host access to some of the OLM registers, and it contains a few configuration registers itself. Also, the PSM can access the OPB and the BCB RAMs (allowing host access).

FIG. 10

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.293

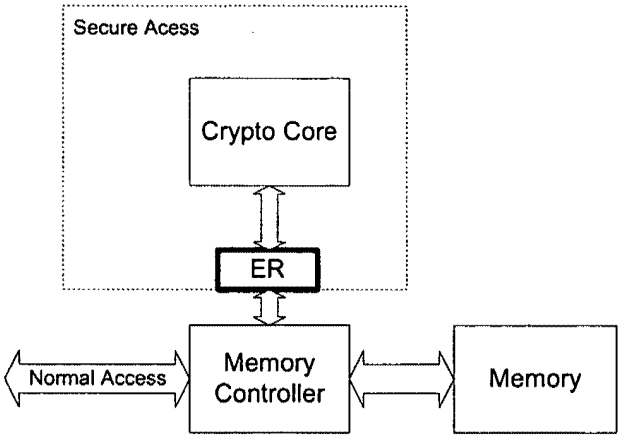


FIG. 11

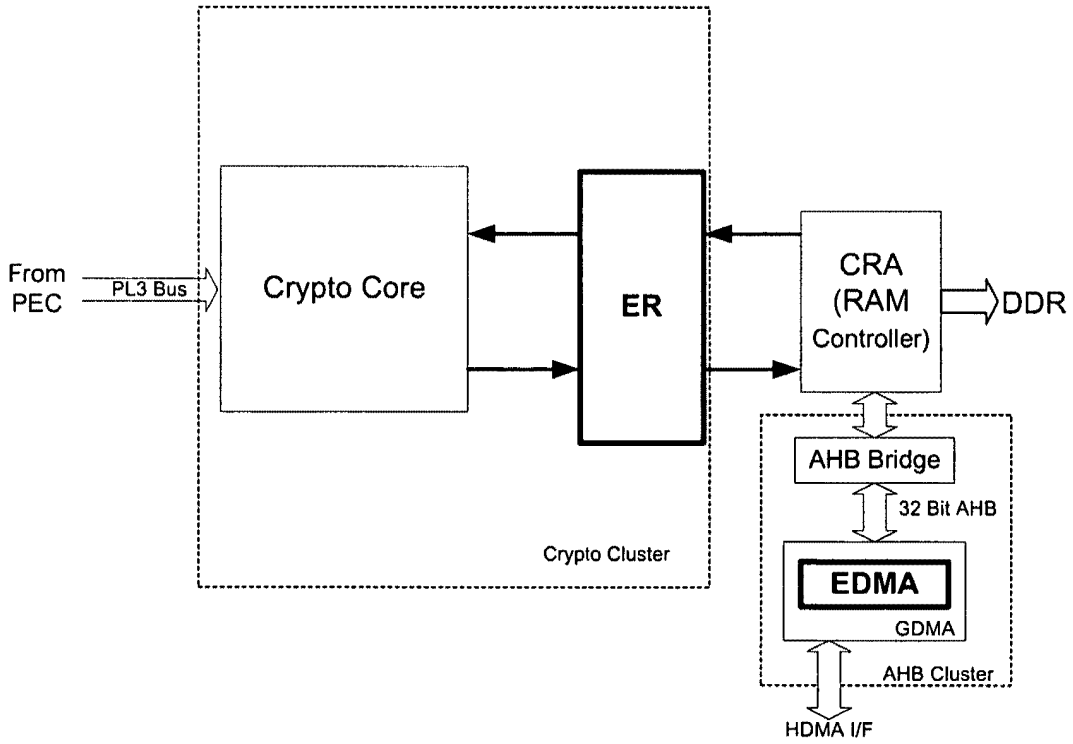


FIG. 12

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.294

PTO/SB/01 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION (37 CFR 1.63)

☑ Declaration Submitted With Initial Filing **OR** ☐ Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)

Attorney Docket Number	4224-25US
First Named Inventor	John Davis
COMPLETE IF KNOWN	
Application Number	Unknown
Filing Date	Herewith
Art Unit	Unknown
Examiner Name	Unknown

I hereby declare that:

Each inventor's residence, mailing address, and citizenship are as stated below next to their name.

I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

(Title of the Invention)

the specification of which

☑ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) ☐ as United States Application Number or PCT International Application Number ☐ and was amended on (MM/DD/YYYY) ☐ (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? Yes	Certified Copy Attached? No
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

PTO/SB/01 (08-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☑ Customer Number: 29974			*OR* ☐ Correspondence address below
Name			
Address			
City		State	ZIP
Country	Telephone	Fax	

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any]) John M.		Family Name or Surname Davis	
Inventor's Signature			Date
Residence: City Brentwood	State TN	Country US	Citizenship US
Mailing Address 1016 Highland Road			
City Brentwood	State TN	ZIP 37027	Country US

NAME OF SECOND INVENTOR:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any]) Richard J.		Family Name or Surname Takahashi	
Inventor's Signature			Date
Residence: City Phoenix	State AZ	Country US	Citizenship US
Mailing Address 14033 South 35th Place			
City Phoenix	State AZ	ZIP 85044	Country US

☐ Additional inventors or a legal representative are being named on the _____ supplemental sheet(s) PTO/SB/02A or 02LR attached hereto.

APPENDIX

(AES64 Specification)

REF: The Rijndael Block Cipher (Joan Daemen and Vincent Rijmen)

Intro
*****

This paper describes a codebook algorithm denoted AES64. AES64, which is derived from AES (formerly called Rijndael), operates on a reduced block size of 64 bits. Although AES is defined for block sizes of 128, 192, and 256 bits, all of the operations apply equally well to a block size of 64 bits, with the possible exception of the ShiftRow() transformation -- since this becomes somewhat trivial for the AES64 case of two bytes per row, ShiftRow() has been changed to operate on nibbles within a row instead of bytes. The security of AES64 rests on the widely accepted security of AES.

For AES64, we specify the following parameters:

(1) blocksize: 64 bits (8 bytes)
(2) key length: 128 bits (16 bytes)
(3) number of rounds: 10
(4) mode: ECB (Electronic Code Book)

Notation
****

Throughout this note as well as the accompanying source code, all values are viewed as byte sequences:

Block: BYTE *a = (a0 a1 a2 ... a7)
Key: BYTE *k = (k0 k1 k2 ... k15)
Expanded key: BYTE *W = (w0 w1 w2 ... w87)

Block values include input, output, and intermediate cipher; REF typically refers to all of these values as "state."

Using this notation, the round keys break out as:

Round 0 (w0 w1 w2 w3 w4 w5 w6 w7)
Round 1 (w8 w9 w10 w11 w12 w13 w14 w15)
Round 2 (w16 w17 w18 w19 w20 w21 w22 w23)

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.297

Round 3 (w24 w25 w26 w27 w28 w29 w30 w31)
.....
Round 13 (w72 w73 w74 w75 w76 w77 w78 w79)
Round 14 (w80 w81 w82 w83 w84 w85 w86 w87)

The Round 0 key is the "preadd" key. Because the AES64 blocksize is small relative to the key length, the first two rounds are actually just the input key (i.e. w(i) = k(i) for i=0,...,15).

In REF, the basic transformations (KeyAdd, ByteSub, ShiftRow, MixColumn) are described as operating on byte-valued state matrices all with exactly four rows. Each column corresponds to a 32-bit word (type unsigned int in C). To map one of the byte sequences described above to a state matrix, inscribe the bytes down the columns moving top to bottom and left to right -- that is, an input byte string

a[8] = a0 a1 a2 a3 a4 a5 a6 a7

corresponds to the state matrix

$$A[2][4] = \begin{matrix} a0 & a4 \\ a1 & a5 \\ a2 & a6 \\ a3 & a7 \end{matrix}$$

The KeyAdd and ByteSub transforms operate on individual bytes, so can be described in terms of either representation equally well. The ShiftRow and MixColumn transforms are defined in terms of the state matrix, with ShiftRow transforming rows and MixColumn transforming columns. In the source code, the mapping from byte string to state matrix is accomplished through indexing:

A[i][j] = a[4*i + j]

This may seem backwards -- index i refers to column and index j to row -- but this corresponds directly to the way that the C language stores multi-dimensional matrices.

Keys and Key schedule
****

AES64 uses the AES key schedule (as described in REF for the case Nk=4). The input key is 16 bytes long. AES64 requires 8 bytes of key for the pre-add and 8 bytes of key for each round, for a total of

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.298

11*8 = 88 bytes. Each round of the key scheduler produces 16 bytes of key. The routine aes64KeySched() actually computes 96 bytes of expanded key in six rounds and then copies the first 88 bytes into the output array. Comparing the pseudocode in REF to aes64KeySched() will probably lead to some confusion since REF describes it in terms of word operations, but these ops are all byte oriented so the translation is fairly straightforward using the equivalence

word W(i) == bytes w(4*i) w(4*i+1) w(4*i+2) w(4*i+3)

Component transforms
****

As noted above, AES64 consists of the same transformations as AES/Rijndael with the exception of ShiftRow(). In what follows, each transformation produces an eight byte output state (b0 ... b7) by operating on an eight byte input state (a0 ... a7):

- Key Addition -- XOR key material with data block
  b(i) = a(i) ^ w(8*r + i) for i=0,...,7
  where r denotes the round number.
- Substitution -- Apply the AES S-box function to data bytes
  b(i) = S[a(i)] for i=0,...,7
- InvSubstitution -- Apply Sinv box function to data bytes
  b(i) = Sinv[a(i)] for i=0,...,7
- MixColumn -- Matrix multiply (the state is a 4x2 byte matrix)

b0 b4		02 03 01 01		a0 a4	
b1 b5	=	01 02 03 01	x	a1 a5	over GF(256)
b2 b6		01 01 02 03		a2 a6	
b3 b7		03 01 01 02		a3 a7	

Or

b0 = mul(02,a0) ^ mul(03,a1) ^ mul(01,a2) ^ mul(01,a3)
b1 = mul(01,a0) ^ mul(02,a1) ^ mul(03,a2) ^ mul(01,a3)
b2 = mul(01,a0) ^ mul(01,a1) ^ mul(02,a2) ^ mul(03,a3)
b3 = mul(03,a0) ^ mul(01,a1) ^ mul(01,a2) ^ mul(02,a3)

b4 = mul(02,a4) ^ mul(03,a5) ^ mul(01,a6) ^ mul(01,a7)
b5 = mul(01,a4) ^ mul(02,a5) ^ mul(03,a6) ^ mul(01,a7)
b6 = mul(01,a4) ^ mul(01,a5) ^ mul(02,a6) ^ mul(03,a7)
b7 = mul(03,a4) ^ mul(01,a5) ^ mul(01,a6) ^ mul(02,a7)

where mul(x,y) is multiplication of x and y in GF(256).

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.299

· InvMixColumn -- like MixColumn, but uses inverse transform

```
b0 b4      0E 0B 0D 09      a0 a4
b1 b5  =    09 0E 0B 0D  x   a1 a5      over GF(256)
b2 b6      0D 09 0E 0B      a2 a6
b3 b7      0B 0D 09 0E      a3 a7
```

· ShiftRow -- Modified from AES to do nibble shifts vs. byte shifts

```
b0 b4      a0H a0L a4H a4L    rotate left 0 nibbles
b1 b5  =    a1L a5H a5L a1H    rotate left 1 nibbles
b2 b6      a6H a6L a2H a2L    rotate left 2 nibbles
b3 b7      a7L a3H a3L a7H    rotate left 3 nibbles
```

where a byte a0 is written as the high/low nibbles (a0H a0L)

· InvShiftRow -- The obvious thing; rotate right instead of left

```
b0 b4      a0H a0L a4H a4L    rotate right 0 nibbles
b1 b5  =    a5L a1H a1L a5H    rotate right 1 nibbles
b2 b6      a6H a6L a2H a2L    rotate right 2 nibbles
b3 b7      a3L a7H a7L a3H    rotate right 3 nibbles
```

Round Function
****

The round functions for AES64 are exactly as in AES. To encrypt,

· Initial key add (preadd, aka whitening)
· For r=1,...,9
  Substitution
  ShiftRow
  MixColumn
  KeyAddition
· Final (oddball) round
  Substitution
  ShiftRow
  KeyAddition

and to decrypt,

· Initial (oddball) round

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.300

KeyAddition
InvShiftRow
InvSubstitution

· For r=9,...,1

KeyAddition
InvMixColumn
InvShiftRow
InvSubstitution

· Final key add (strips off whitening)

An Example
****
Encryption
Input 0123456789abcdef
Key 000102030405060708090a0b0c0d0e0f

Key expansion algorithm (16 bytes per pass)
Pass 0: 00010203 04050607 08090a0b 0c0d0e0f
Pass 1: d6aa74fd d2af72fa daa678f1 d6ab76fe
Pass 2: b692cf0b 643dbdf1 be9bc500 6830b3fe
Pass 3: b6ff744e d2c2c9bf 6c590cbf 0469bf41
Pass 4: 47f7f7bc 95353e03 f96c32bc fd058dfd
Pass 5: 3caaa3e8 a99f9deb 50f3af57 adf622aa

Expanded key by round
Round 0: 00010203 04050607 (preadd)
Round 1: 08090a0b 0c0d0e0f
Round 2: d6aa74fd d2af72fa
Round 3: daa678f1 d6ab76fe
Round 4: b692cf0b 643dbdf1
Round 5: be9bc500 6830b3fe
Round 6: b6ff744e d2c2c9bf
Round 7: 6c590cbf 0469bf41
Round 8: 47f7f7bc 95353e03
Round 9: f96c32bc fd058dfd
Round 10: 3caaa3e8 a99f9deb

** input 01234567 89abcdef

** whitened 01224764 8daecbe8

** round 1 sub 7c93a043 5de41f9b

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.301

```
** round  1 shftd 7c3e1fb4 5d49a039
** round  1 mixed 1195bbd6 f80d047c
** round  1 added 199cb1dd f4000a73

** round  2 sub   d4dec8c1 bf63678f
** round  2 shftd d4e667fc bf3dc818
** round  2 mixed 1956e305 f29e211f
** round  2 added cffc97f8 203153e5
.....
** round  9 sub   28d45822 59fef902
** round  9 shftd 284ff922 59ed5820
** round  9 mixed 5a84e88a e650641e
** round  9 added a3e8da36 1b55e9e3

** round 10 sub   0a9b5705 affc1e11
** round 10 shftd 0abf1e10 afc95751
  (note no MixColumn last round)
** round 10 added 3615bdf8 0656caba

Output: 3615bdf80656caba

Decryption -- Key and expanded key identical to encryption above.
Input:  3615bdf80656caba

** input    8db33771 ac477fb5

** round 10 added   0abf1e10 afc95751
  (note no InvMixColumn first round)
** round 10 invshft 0a9b5705 affc1e11
** round 10 invsub  a3e8da36 1b55e9e3

** round  9 added   5a84e88a e650641e
** round  9 invmix  284ff922 59ed5820
** round  9 invshft 28d45822 59fef902
** round  9 invsub  ee195e94 150c696a
.....
** round  2 added   1956e305 f29e211f
** round  2 invmix  d4e667fc bf3dc818
** round  2 invshft d4dec8c1 bf63678f
** round  2 invsub  199cb1dd f4000a73

** round  1 added   1195bbd6 f80d047c
** round  1 invmix  7c3e1fb4 5d49a039
```


Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.302

** round 1 invshft 7c93a043 5de41f9b
** round 1 invsub 01224764 8daecbe8

** dewhitening 01234567 89abcdef

Output: 0123456789abcdef

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.303

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

08/04/2004 HTECKLU1 00000061 502412 10903785

01 FC:2001 385.00 DA
02 FC:2202 81.00 DA
03 FC:2201 43.00 DA

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 469-267/69033

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2003

Application or Docket Number: 10/903,788

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	29	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	29 minus 20=	* 9
INDEPENDENT CLAIMS	4 minus 3 =	* 1
MULTIPLE DEPENDENT CLAIM PRESENT		☐

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE	385.00	OR	BASIC FEE	770.00
XS 9=	81	OR	XS18=	
X43=	43	OR	X86=	
+145=		OR	+290=	
TOTAL	509	OR	TOTAL	

CLAIMS AS AMENDED - PART II

AMENDMENT A	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

(1) (19) (23) (26)

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X43=		OR	X86=	
+145=		OR	+290=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
***If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Cisco System Inc. v Lionra Technologies Ltd.
EX-1002 p.305