IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.
Petitioner,

v.

LIONRA TECHNOLOGIES LTD.
Patent Owner.

U.S. Patent Nos. 7,685,436 & 8,566,612

SYSTEM AND METHOD FOR A SECURE I/O INTERFACE

Inter Partes Review Nos.:
IPR2023-00673
IPR2023-00674

DECLARATION OF MARK E. CROVELLA IN SUPPORT OF PETITIONS FOR INTER PARTES REVIEW OF U.S. PATENT NOS. 7,685,436 &8,566,612.

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page001

Table of Contents

I. INTRODUCTION 1

II. QUALIFICATIONS 5

III. RELEVANT LEGAL STANDARDS 7

IV. OVERVIEW 11

V. BACKGROUND 15

A. Summary of the Patents 15

B. Claim Construction 23

C. Priority Date of the Challenged Claims 24

D. Person of Ordinary Skill in the Art 24

E. State of the Art 24

VI. IDENTIFICATION OF CHALLENGES 31

A. Challenged Claims 31

B. Statutory Grounds for Challenges 31

VII. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE 32

A. Ground 1: Claims 1, 2, 9-13, 16 and 22 are unpatentable over Pham in view of Wu. 32

1. The Pham Reference 32

2. The Wu Reference 35

3. The Motivation To Combine the Teachings of Pham with the Teaching of Wu with a Reasonable Prediction of Success 37

4. Detailed Application of Pham and Wu to Challenged Claims 1, 2, 9-13, 16 and 22 of each of the Patents. 44

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page002

a. Claim 1 44

b. Claim 13 64

c. Claim 2 69

d. Claim 9 69

e. Claim 10 71

f. Claims 12 and [22} 71

g. Claim 16 74

B. Ground 2: Claims 3, 14 And 21 Are Unpatentable Over Pham and Wu in Further View of Collins 76

1. The Collins Reference 76

2. Detailed Application of Pham and Wu And Collins 77

a. Claims 3 and 14 77

b. Claim 21 78

C. Ground 3: Claims 4, 7, 8 and 17 Are Unpatentable Over Pham, Wu and Collins and Further In View of Krishna 82

1. The Krishna Reference 82

2. Detailed Application Of Pham, Wu, Collins And Krishna 82

a. Claim 4 82

b. Claims 7 and 8 84

D. Ground 4: Claim 17 Is Unpatentable Over Pham and Wu and Further In View of Krishna 85

a. Claim 17 85

CONCLUSION AND DECLARATION I

APPENDIX A – MATERIALS RELIED UPON ..... A

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page003

APPENDIX B – RÉSUMÉ.....B

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page004

I, Mark E. Crovella, declare as follows:

I. INTRODUCTION

1. I am over the age of eighteen (18) and otherwise competent to make this Declaration.

2. I have been retained by Cisco Systems, Inc. (Petitioner) as an independent, technical expert consultant in this proceeding before the United States Patent and Trademark Office (USPTO). I am being compensated at my rate of $650 per hour for my services. No part of my compensation is dependent on my opinions or on the outcome of this proceeding. I have no financial interest in any of the parties to this proceeding.

3. This Declaration is in support of the Petition for *inter partes* review involving U.S. Patent 7,685,436 (the "'436 Patent") (EX-1001), and its child U.S. Patent .8,566,612 (the "'612 Patent") (EX-1012) both entitled "SYSTEM AND METHOD FOR A SECURE I/O INTERFACE" and listing John Davis and Richard Takahashi as the inventors.

4. For the purposes of this *inter partes* review as I discuss later, I have been instructed to assume that the effective filing date of the Claims of the '436 Patent and the '612 Patent challenged by the Petitioner in *inter partes* reviews is no earlier than October 2, 2003.

5. I understand that, according to USPTO records, the ’436 Patent and ’612 Patent are currently assigned to Lionra Technologies Ltd. (“Lionra” or “Patent Owner”). I assume for purposes of this proceeding that Lionra is the patent owner.

6. The ’436 Patent and the ’612 Patent are generally directed to a security processor handling encryption/decryption of packets and IDS to protect computing hardware from unauthorized access or attack. I am familiar with the technology described in the ’436 Patent and the ’612 Patent as of the earliest possible priority date of October 2, 2003, the filing date of Provisional Application No. 60/507,976.

7. In preparing this Declaration, I have reviewed the ’436 Patent (EX-1001) its prosecution history (EX-1002), the ’612 Patent (EX-1012) and its prosecution history (EX-1013) as well as the patents and documents cited herein, and I have considered these documents in light of the general knowledge in the art as of October 2, 2003. In formulating my opinions, I have relied upon my experience in the relevant art. I have also considered the viewpoint of a person of ordinary skill in the art (“POSA”) in the relevant field, as of October 2, 2003, who I describe below (§ V.D). For convenience, the materials I considered in arriving at my opinions are listed in Appendix A.

8. I have been asked to provide my technical expertise, analysis, insights and opinions regarding the ’436 Patent and the ’612 Patent and relevant references that form the basis of the arguments set forth in the accompanying Petitions for *inter partes* review of the ‘436 Patent and the ’612 Patent.

Opinions regarding the ’436 Patent

9. As described in detail below, I offer the following opinions in this Declaration with respect to the ’436 Patent:

- A POSA would have found Claims 1, 2, 9-13, 16 and 22 are unpatentable over *Pham* in view of *Wu* and a POSA would have been motivated to combine the teachings of these references.
- A POSA would have found Claims 3, 14 And 21 Are Unpatentable Over *Pham* and *Wu* in Further View of *Collins* and a POSA would have been motivated to combine the teachings of these references.
- A POSA would have found Claims 4, 7, 8 and 17 Are Unpatentable Over *Pham*, *Wu* and *Collins* and Further In View of *Krishna* and a POSA would have been motivated to combine the teachings of these references.

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page007

- A POSA would have found Claim 17 Is Unpatentable Over *Pham* and *Wu* and Further In View of *Krishna* and a POSA would have been motivated to combine the teachings of these references

Opinions regarding the ’612 Patent

10. I also offer the following opinions in this Declaration with respect to the ’612 Patent:

- A POSA would have found Claims 1, 2, 9-13, 16 and 22 are unpatentable over *Pham* in view of *Wu* and a POSA would have been motivated to combine the teachings of these references.
- A POSA would have found Claims 3, 14 And 21 Are Unpatentable Over *Pham* and *Wu* in Further View of *Collins* and a POSA would have been motivated to combine the teachings of these references.
- A POSA would have found Claims 4, 7, 8 and 17 Are Unpatentable Over *Pham*, *Wu* and *Collins* and Further In View of *Krishna* and a POSA would have been motivated to combine the teachings of these references.
- A POSA would have found Claim 17 Is Unpatentable Over *Pham* and *Wu* and Further In View of *Krishna* and a POSA would have been motivated to combine the teachings of these references

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page008

11. Unless otherwise indicated, the emphasis in quotations has been added.

II. QUALIFICATIONS

12. My qualifications for forming the opinions set forth in this declaration are summarized here and explained in more detail in my *curriculum vitae*, which is included as Appendix B. Appendix B also includes a list of my publications and patents.

13. I received a Ph.D. in Computer Science from the University of Rochester in October 1994. I also received a Master of Science degree in Computer Science in 1991, a Bachelor of Science degree from State University of New York at Buffalo in 1990 and a Bachelor of Science Degree from Cornell University in 1992.

14. For the last 17 years I have been Professor in the Department of computer Science at Boston University and Department Chair from 2013-2018. I was an Associate Professor between 2000 and 2006 and an Assistant Professor between 1994 and 2000/

15. Starting in 2022, I have been a Professor on the Faculty of Computing & Data Sciences at Boston University, of which I was one of the founding members. I presently serve as Chair of Academic Affairs for

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page009

the Faculty of Computing & Data Sciences. I was also a Data Science Faculty Fellow between 2019 and 2022.

16. My career in the area of computing and data analysis began in 1984 when I started work at Calspan Corporation in Buffalo., NY where I was eventually a Senior Computer Scientist. Between 2000 and April 2002, I was the Chief Architect for Webmanage Technologies of Chelmsford, MA. Webmanage was later acquired by Network Appliance for which I was a Technical Director. Between February 2012 and August 2014, I also served as Chief Scientist at Guavus Inc, a telecom analytics company.

17. Furthermore, I have served as a legal consultant for a number of companies. I have testified in Federal courts, the PTAB, and the ITC on behalf of leading companies such as Apple, Sony, Yahoo, RPX, Fortinet, Hulu, Netflix, Amazon, Samsung and Cisco.

18. I have been awarded several United States patents, including the following examples:

U.S. Pat. No.	Title
10,027,347,	Methods for storing and reading digital data on a set of DNA strands
8,869,276	Method and Apparatus for Whole-Network Anomaly Diagnosis and Method to Detect and Classify Network Anomalies Using Traffic Feature Distributions

8,533,167,	Compressed Set Representation for Sets as Measures in OLAP Cubes
7,747,741	Method and Apparatus for Dynamic Resource Discovery and Information Distribution in a Data Network
7,346,682	System for Creating and Distributing Prioritized List of Computer Nodes Selected as Participants in a Distribution Job
6,993,587	Method and Apparatus for Election of Group Leaders in a Distributed Network
6,748,447	Method and Apparatus for Scalable Distribution of Information in a Distributed Network
6,718,361	Method and Apparatus for Reliable and Scalable Distribution of Data Files in Distributed Networks
6,370,584	Distributed Routing
6,223,205	Method and Apparatus for Assigning Tasks in a Distributed Server System

19. Based on my above-described over three decades of experience in Computing and Data Sciences and the acceptance of my publications (200+) and professional recognition by societies in my field, I believe that I am qualified to be an expert in the field of computer security technology.

20. Based on my experience described above, and as indicated in my *curriculum vitae*, I am qualified to provide the following opinions with respect the patents in this case. Additionally, I am at least a person having ordinary skill in the art as of the priority date of the ’436 Patent and the ’612 Patent.

III. RELEVANT LEGAL STANDARDS

21. I do not provide any legal opinions in this Declaration. I have been informed and understand that certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims. I have been asked to provide my opinions regarding whether the claims of the ’436 Patent would have been obvious to a person having ordinary skill in the art at the time of the alleged invention, in light of the prior art.

22. Further, I have been informed and understand that a patent claim is not patentable as obvious (a requirement I understand to be governed by a statute, 35 U.S.C. § 103) if the differences between the patent claim and the prior art are such that the claimed subject matter as a whole would have been obvious at the time the claimed invention was made to a person having ordinary skill in the relevant art. Obviousness, as I have been informed and understand, is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and, to the extent that they exist, certain objective indicia of non-obviousness.

23. I understand that objective indicia can be important evidence regarding whether a patent is obvious or nonobvious, if it has an appropriate nexus to the claimed invention, i.e., is a result of the merits of a

claimed invention (rather than the result of design needs or market-pressure advertising or similar activities). Such indicia include: commercial success of products covered by the patent claims; a long-felt need for the invention; failed attempts by others to make the invention; copying of the invention by others in the field; unexpected results achieved by the invention as compared to the closest prior art; praise of the invention by the infringer or others in the field; the taking of licenses under the patent by others; expressions of surprise by experts and those skilled in the art at the making of the invention; the patentee proceeded contrary to the accepted wisdom of the prior art, and, the contemporaneous development of the subject matter claimed by others.

24. I have been informed that whether there are any relevant differences between the prior art and the claimed invention is to be analyzed from the view of a person of ordinary skill in the relevant art at the time of the invention. As such, my opinions below as to a person of ordinary skill in the art are as of the time of the invention, even if not expressly stated as such; for example, even if stated in the present tense.

25. In analyzing the relevance of the differences between the claimed invention and the prior art, I have been informed that I must consider the impact, if any, of such differences on the obviousness or non-

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page013

obviousness of the invention as a whole, not merely some portion of it. The person of ordinary skill faced with a problem is able to apply his or her experience and ability to solve the problem and also look to any available prior art to help solve the problem.

26. I have been informed that a precise teaching in the prior art directed to the subject matter of the claimed invention is not needed. I have been informed that one may take into account the inferences and creative steps that a person of ordinary skill in the art would have employed in reviewing the prior art at the time of the invention. For example, if the claimed invention combined elements known in the prior art and the combination yielded results that were predictable to a person of ordinary skill in the art at the time of the invention, then this evidence would make it more likely that the claim was obvious. On the other hand, if the combination of known elements yielded unexpected or unpredictable results, or if the prior art teaches away from combining the known elements, then this evidence would make it more likely that the claim that successfully combined those elements was not obvious.

27. I have been informed and understand that there are recognized, exemplary, rationales for combining or modifying references to show obviousness of claimed subject matter. Some of the rationales include the

following: combining prior art elements according to known methods to yield predictable results; simple substitution of one known element for another to yield predictable results; use of a known technique to improve a similar device (method or product) in the same way; applying a known technique to a known device (method or product) ready for improvement to yield predictable results; choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success; known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; and some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art teachings to arrive at the claimed invention.

IV. OVERVIEW

28. The ’436 Patent and the ’612 Patent (collectively “the Patents”) are directed to a security processor having a switching system (yellow), a cryptographic core (red) with a packet engine (green) for processing incoming and outgoing data packets interposed between the

switching system and cryptographic core:

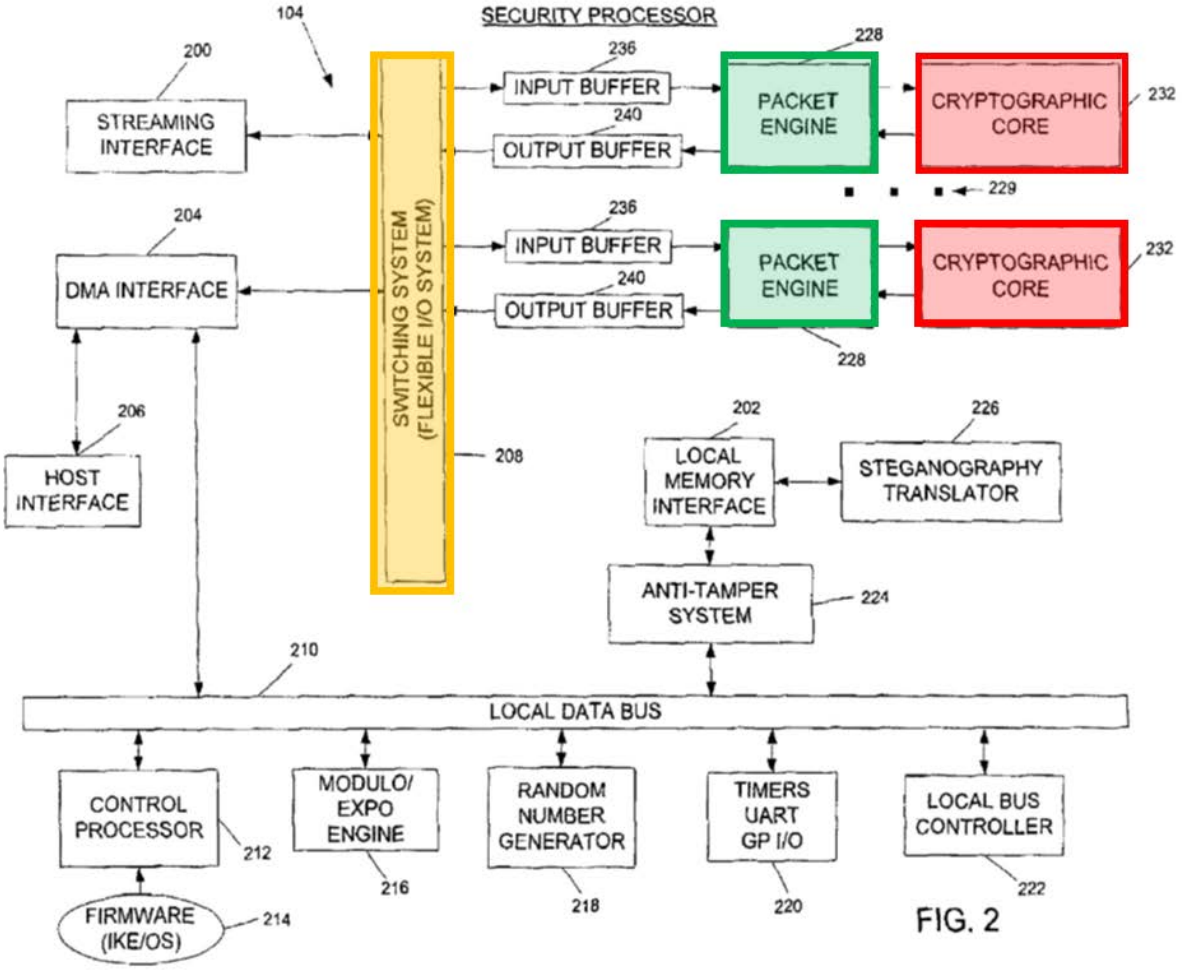
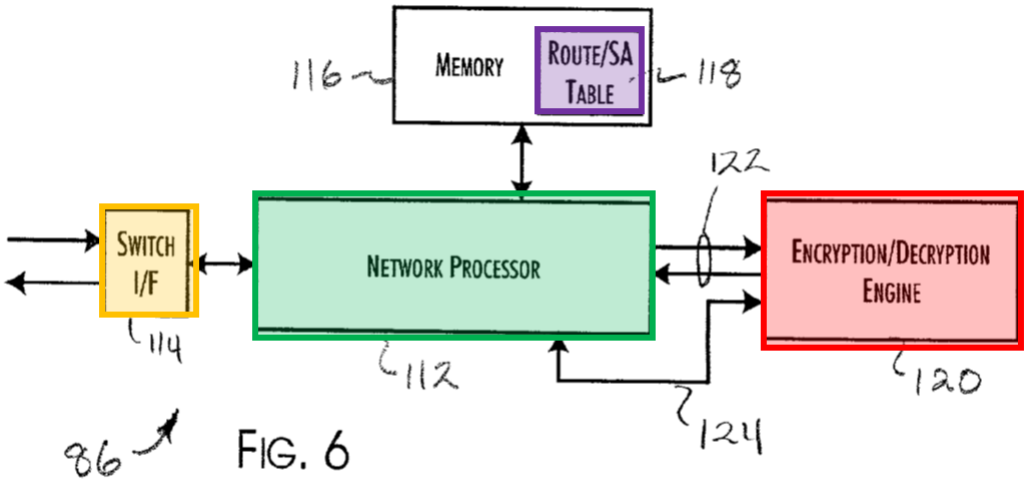


FIG. 2

29. The Patents also describes that an intrusion detection system using a signature database can be coupled between the packet engine and the cryptographic core to permit clear text packet capture either before or after encryption. EX-1001 19 5-8: EX-1012 18:64-19:1.

30. However, this security processor described in the Patents was a combination of conventional components performing their intended purpose. Specifically, U.S. 2003/0074473 ("Pham") discloses a security

processor having a switching system (yellow), a cryptographic core (red) with a packet engine (green) for processing incoming and outgoing data packets interposed between the switching system and cryptographic core.



EX-1004 Fig. 6

31. A POSA would understand that the intrusion detection system of Wu would be suitable for use with the packet engine of Pham. For example, Wu discloses a signature-based intrusion detection system with a signature database and describes that "intrusion detection system 14 may be used alone or in combination with a data monitoring and analysis device configured to perform fault and network performance management." EX-1005 4:4-7.

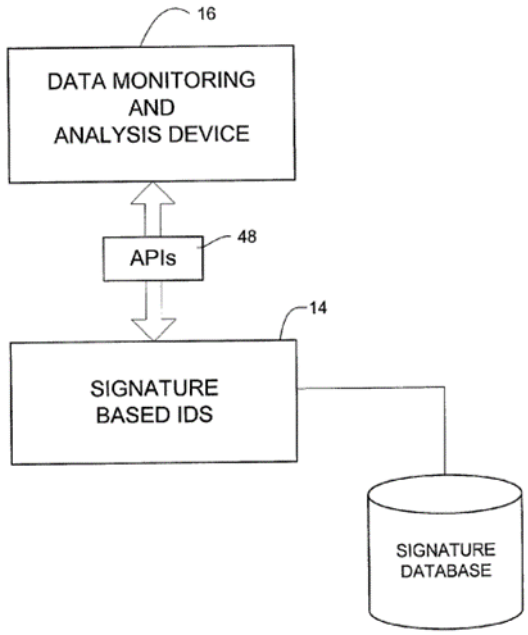


FIG. 2

EX-1005 Fig. 2.

32. U.S. Patent Publication 20020073316 ("Collins") discloses features recited in the dependent claims of the Patents directed to details of a cryptographic engine for performing "fast modular exponentiation" and that Collins describes that its design and operation are known to a POSA. EX-1008 [0048]. U.S. Pat. No. 7,996,670 ("Krishna") Krishna discloses features recited in the dependent claims of the Patents directed to a packet engine, a cryptographic core and other components of a security processor contained on a single chip. EX-1006 FIG. 2; 3:43-50.

33. As I describe in detail below, because these references are all directed to the same problems described in the Patents and describe the

same solutions and features proposed in the Patents, these references are analogous art and a POSA would be motivated to combine their teachings with a high likelihood of success.

V. BACKGROUND

A. Summary of the Patents

34. FIG. 2, in the Patents, illustrates a high-level simplified functional block diagram of one embodiment of a security processor 104. The ’436 Patent describes that security processor 104 is preferably, though not necessarily, formed on a single chip. EX-1001 6:38-45; EX-1012 6:38-45.

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page019

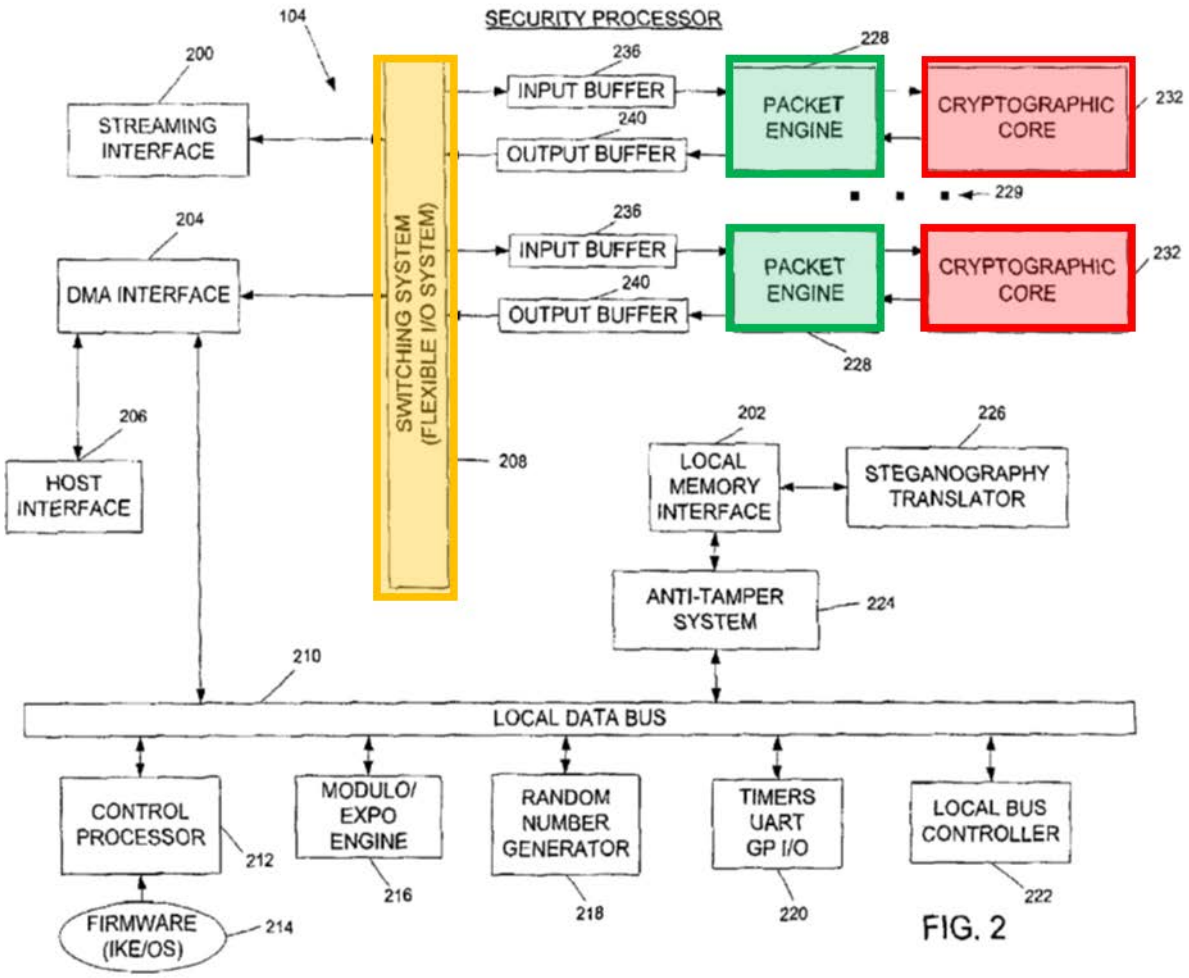


FIG. 2

35. Switching system 208 (orange) provides a switching mechanism to route packets and data to and from any of the I/O interfaces of security processor 104 and local data bus 210. EX-1004 6:58-61. The ’436 Patent admits that the switching system 208 is known in the art and can be implemented using conventional switches. EX-1001 7:33-48; EX-1012 7:33-47.

36. Packet engines 228 (green) may each be interposed between a cryptographic core 232 (red) and the switching system 208. Packet

engines 228 may each comprise microprocessors customized for packet operations such as, for example, packet processing and classification. The ’436 Patent explains that suitable packet engines are known in the art, which process packets needing network address translation processing and firewall table processing, and process IPSec packets. Ex-1001 9:60-10:8; EX-1012 9:60-10:6.

37. 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 header altering to be done. EX-1001 10 8-13; EX-1012 10:6-12.

38. 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). EX-1001 10:14-20; EX-1012 10:13-19.

39. 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. EX-1001 10:21-34; EX-1012 10:20-33.

40. Cryptographic cores 232 provide security processing to perform 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. The Patents describe that suitable cryptographic cores were known. EX-1001 11:23-47; EX-1012 11:23-45.

41. The Patents describes that in one embodiment, 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. EX-1001 11: 59-63; EX-1012 11:57-61.

42. 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. EX-1001 12:6-18; EX-1012 12:4-16.

43. 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. EX-1001 12:19-24; EX-1012 12:17-22.

44. 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 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. Ex-1001 7:60-8:2; EX-1012 7:59-8:9.

45. The ’436 Patent issued with 22 Claims. Claims 1 and 13 are the only independent claims and recite a “security processor” and “security

processing system" respectively. Claims 1 and 13 are substantially similar with Claim 13 reciting the well-known limitations of a local data bus and memory on top of the limitations of Claim 1.

46. Claim 1 is representative:

1. **[i.pre]** A security processor to process incoming packets and outgoing packets, the security processor comprising:

[ii.] a switching system to send the outgoing packets and receive the incoming packets;

[iii.] 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,

[iv.] 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 **[v.]** 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;

[vi.] 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,

[vii.] wherein the packet engine is interposed between the switching system and the cryptographic core;

[viii.] 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.

47. The ’612 Patent issued with 26 Claims. Claims 1 and 13 are independent claims and recite a “security processor” and “security processing system” respectively. Claims 1 and 13 are substantially similar with Claim 13 reciting the well-known limitations of a local data bus and memory on top of the limitations of Claim 1. Claim 1 is representative:

1. **[i.pre]** A security processor to process incoming packets and outgoing packets, the security processor comprising:

[ii.] a switching system to send the outgoing packets and receive the incoming packets;

[iii.] 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,

[iv.] 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;

[v.] 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,

[vi.] wherein the packet engine is interposed between the switching system and the cryptographic core;

[vii.] 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.

B. Claim Construction

48. I have been informed to give each claim term in the Challenged Claims its plain and ordinary meaning in this proceeding. It is my opinion that no specific construction of any claim term is required because the prior art I have relied upon meets each of the claim terms under any reasonable construction.

C. Priority Date of the Challenged Claims

49. The ’436 Patent claims the benefit of U.S. Provisional Application Ser. No. 60/507,976, filed on October 2, 2003. The ’612 Patent claims priority of its parent, the ’436 Patent as well as U.S. Provisional Application Ser. No. 60/507,976, Solely for the purposes of this IPR, I have been instructed to assume the priority dates for the Patents are October 2, 2003.

D. Person of Ordinary Skill in the Art

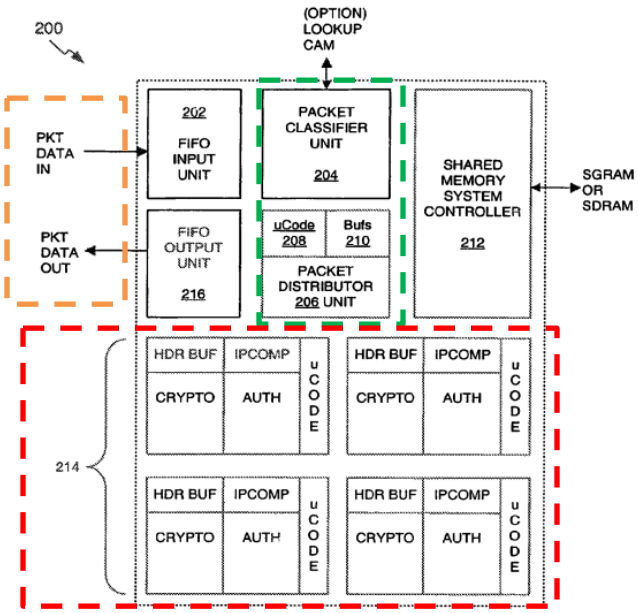
50. With respect to the Patents, a POSA would have a Bachelor’s degree in computer science, computer engineering, or a related discipline, and 3-4 years of experience in computer networking with an emphasis on packet processing systems including traffic monitoring, inspection, and encryption/decryption systems. More experience could compensate for less formal education and vice versa.

E. State of the Art

51. In the following section I describe the state of the art for packet processing systems as of October 2003. The prior art references, and the discussions of what was known to a POSA, provide the factual support for the general description of the state of the art at the time of the invention, provide additional motivation to modify or combine the reference Accordingly, these references should be considered by the Board.

1. The use of packet engines and cryptographic cores

52. By October 2003, the use of packet processors for handling encrypted packets was well-known. In one such system (Krishna), a packet engine (green) received packets from a switching system (orange) and provided them to a cryptographic core(red).



EX-1006, Fig 2.

53. The packet engine included a packet classifier unit and a packet distributor. Packet header information from packets received from the switching system is sent to a packet classifier unit 204 where a classification engine rapidly determines security association (SA) information required for processing the packet, such as encryption keys,

data, etc. The classification engine performs lookups from databases stored in associated memory and the security association information determined by the packet classifier unit 204 is sent to a packet distributor unit 206. EX-1006, 5:37-53. Packet classification and use of SA information in the Krishna system is the same as described in the '436 Patent, as discussed with respect to the prosecution history above. Krishna describes that the function of the packet classifier is to perform IPSec-specified lookup as well as IP packet fragmentation lookup. These lookups are used by the distributor engine. EX-1006, 9:33-50. "The distributor unit 206 determines if a packet is ready for IPSec processing, and if so, distributes the security association information (SA) received from the packet classifier unit 204 and the packet data among a plurality of cryptography processing engines 124, in this case four, on the chip 200, for security processing " EX-1006, 5:54-60.

54. Moreover, by October 2003, a POSA understood that cryptographic processing was moving away from discrete processors and was being implemented on a single chip. EX-1010, Fig. 1, Abstract.

2. The use of intrusion and detection systems

55. By October 2003, the use of intrusion detection systems were well-known. In one such system, U.S. 6,279,113 ("Vaidya"), a signature

based dynamic network intrusion detection system (IDS) includes attack signature profiles which are descriptive of characteristics of known network security violations. The attack signature profiles are organized into sets of attack signature profiles according to security requirements of network objects on a network. Each network object is assigned a set of attack signature profiles which is stored in a signature profile memory together with association data indicative of which sets of attack signature profiles correspond to which network objects. A monitoring device monitors network traffic for data addressed to the network objects. Upon detecting a data packet addressed to one of the network objects, packet information is extracted from the data packet. The extracted information is utilized to obtain a set of attack signature profiles corresponding to the network object based on the association data. A virtual processor executes instructions associated with attack signature profiles to determine if the packet is associated with a known network security violation. An attack signature profile generator is utilized to generate additional attack signature profiles configured for processing by the virtual processor in the absence of any corresponding modification of the virtual processor. EX-1007, Abstract.

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page031

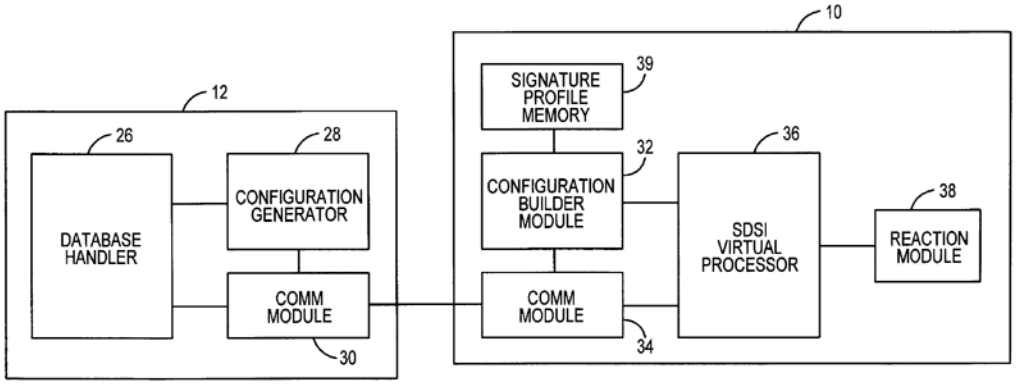


FIG. 2

EX-1007, Fig. 2.

56. It was also well known to locate IDS systems at various locations in the networks, but in particular proximate the ingress of the network to facilitate detection prior to deeper intrusion by a malicious packet. EX-1007, 5-26. It was well known that, encryption turns malicious traffic indistinguishable from non-harmful traffic, thus the monitoring taps of the IDS are preferably placed at the endpoints where encryption and decryption are performed such that it can inspect unencrypted traffic ("the IDS function in servers 720, 740 has access to clear text data so that IDS evaluation can occur." (EX-1015 [0079])). EX-1015 [0012, 0079].

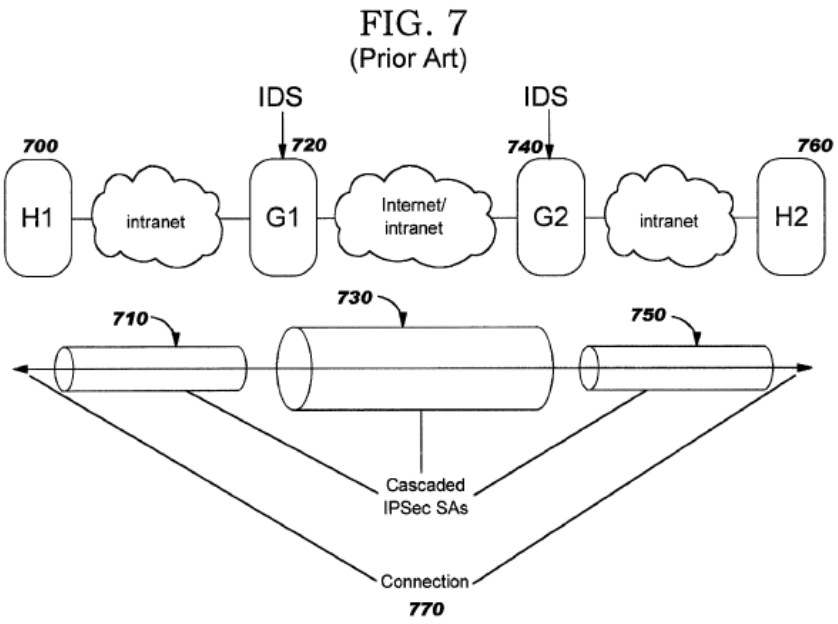
57. Bruton describes that sniffers and scanners that are used to detect data matching signatures cannot evaluate data that is encrypted.

Network sniffers (such as elements 210, 230, 240 in FIG. 2) cannot evaluate data that is encrypted unless the Sniffer and the encryption endpoint are located at the same node. Because Sniffers are not typically co-located with the packet destination, providing an encryption endpoint at the Sniffer is contradictory with the goal of end-to-end encryption (that is, encryption where the endpoints are the client and application server. EX-1015 [0012]

58. Bruton also describes decrypting and re-encrypting for IDS in an end-to-end encryption tunnel so as to access the clear text.

As shown therein, "cascaded" IPSec SAS are used to provide end-to-end encryption for the connection. That is, three IPSec SAS 710, 730, 750 are established in a Series from end to end, with the SAS ending in network devices (gateway servers 720, 740, in this example) that are performing intrusion detection. In the scenario of FIG. 7, the IDS

function in servers 720, 740 has access to clear text data so that IDS evaluation can occur. EX-1015 [0079]



EX-1015 Fig. 7

59. A POSA further understood creating a signature database that allowed for signature matching of encrypted data was impractical given the vast number of possible combinations of bytes. For example, when a sequence of bytes (which may contain an attack signature, *i.e.* a "pattern" in Vaidya) is sent over an encrypted connection, the specific encrypted bytes will depend on the encryption key. Because a different key is used for each connection (in general), the same signature will appear as a completely different sequence of bytes on different connections. Given the exponential growth in byte sequences required, a signature database cannot

be built that operates on encrypted data, because the encrypted signature changes each time it is transmitted over a new connection.

VI. IDENTIFICATION OF CHALLENGES

A. Challenged Claims

60. Claims 1-4, 7-14, 16, 17, 21 and 22 of the ’436 Patent as well as the ’612 Patent are challenged in this Petition.

B. Statutory Grounds for Challenges

Challenges to the ’436 Patent.

Ground	Claims	Basis	Reference
1	Claims 1-2, 9-13, 16 and, 22,	§ 103	Pham in view Wu
2	3, 14, 21	§ 103	Pham in view of Wu and Collins
3	4, 7, 8	§ 103	Pham in view of Wu and Collins and Krishna
4	17	§ 103	Pham in view of and Wu and Krishna

Challenges to the ’612 Patent.

Ground	Claims	Basis	Reference
1	Claims 1-2, 9-13, 16 and, 22,	§ 103	Pham in view Wu
2	3, 14, 21	§ 103	Pham in view of Wu and Collins
3	4, 7, 8	§ 103	Pham in view of Wu and Collins and Krishna
4	17	§ 103	Pham in view of and Wu and Krishna

C. Prior Art Basis

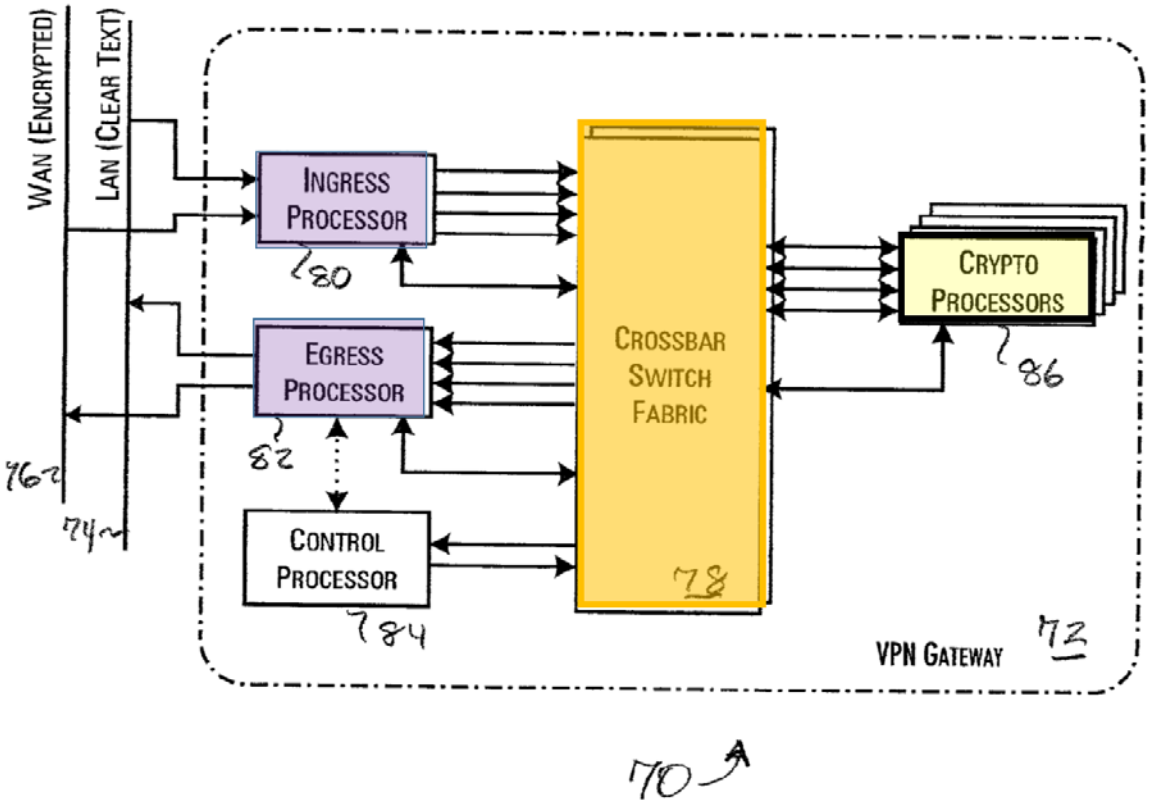
61. I have been informed that Published Application U.S. Patent Publication 2003/0074473 ("Pham"), U.S. Patent No. 7,424.744 ("Wu"), U.S. Patent Publication 2002/0073316A1 ("Collins") and U.S. Patent No. 7,996,670 ("Krishna") qualify as prior art under §102 for purposes of this IPR.

VII. IDENTIFICATION OF HOW THE CHALLENGED CLAIMS ARE UNPATENTABLE

A. Ground 1: Claims 1, 2, 9-13, 16 and 22 are unpatentable over Pham in view of Wu.

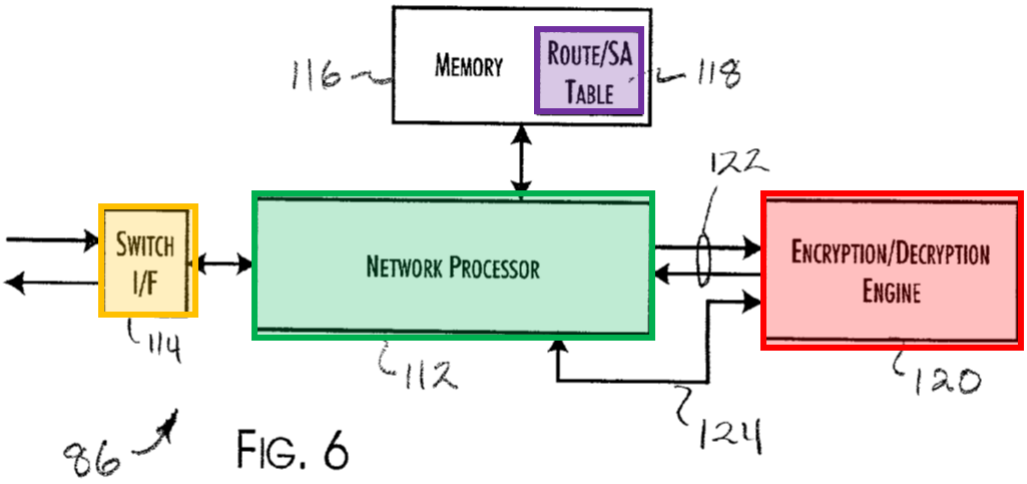
1. The Pham Reference

62. Pham is directed to a network data processor system in the form of a virtual private network gateway that includes a plurality of data packet processors in the form of crypto processors (yellow) coupled through a data switch fabric (orange) between network connection processors (purple). Ex-1004 Abstract.



EX-1004 Fig. 4.

63. The crypto processors each include a data processing engine configured to perform a data processing function over data contained within predetermined data packets and to perform hardware encryption and decryption algorithms called for by the IPsec protocol. EX-1004 Abstract. Figure 6 illustrates one embodiment of a crypto processor that corresponds to the security processing system described in the Patents:



EX-1004 Fig. 6.

64. The network processor 112 (green) connects to and supports high-speed data interchange with a dedicated encryption/decryption engine 120 (red). The network processor 112 controls and monitors the engine 120. EX-1004 [0052] ; A memory array 116 is provided for the external memory and program requirements of the network processor and provides storage space for various secure authority (SA) parameters for the encryption and decryption of data, SA parameter data table 118 (purple). EX-1004 [0051].

65. In one embodiment, the SA parameter association task is performed by the crypto processors 86. The control processor 84 explicitly propagates identical copies of the SA parameter data to each of the crypto

processors 86, enabling the crypto processors 86 to process any data packet received." EX-1004 [0051].

66. The network processor 112 connects to and supports high-speed data interchange with a dedicated encryption/decryption engine 120 through a direct data transfer bus 122. The network processor 112 controls and monitors the encryption/decryption engine 120 via control and status lines 124. EX-1004 [0052].

2. The Wu Reference

67. Wu discloses a signature based instruction detection system that stores signature profiles identifying patterns associated with network intrusions in a signature database and generates classification rules based on the signature profiles. Data packets transmitted on the network and having corresponding classification rules are classified according to generated classification rules. Classified packets are forwarded to a signature engine for comparison with signature profiles. EX-1005 2:39-49. Any problems detected are sent to an alert log 68 and appropriate action is taken. EX-1005 1-3.

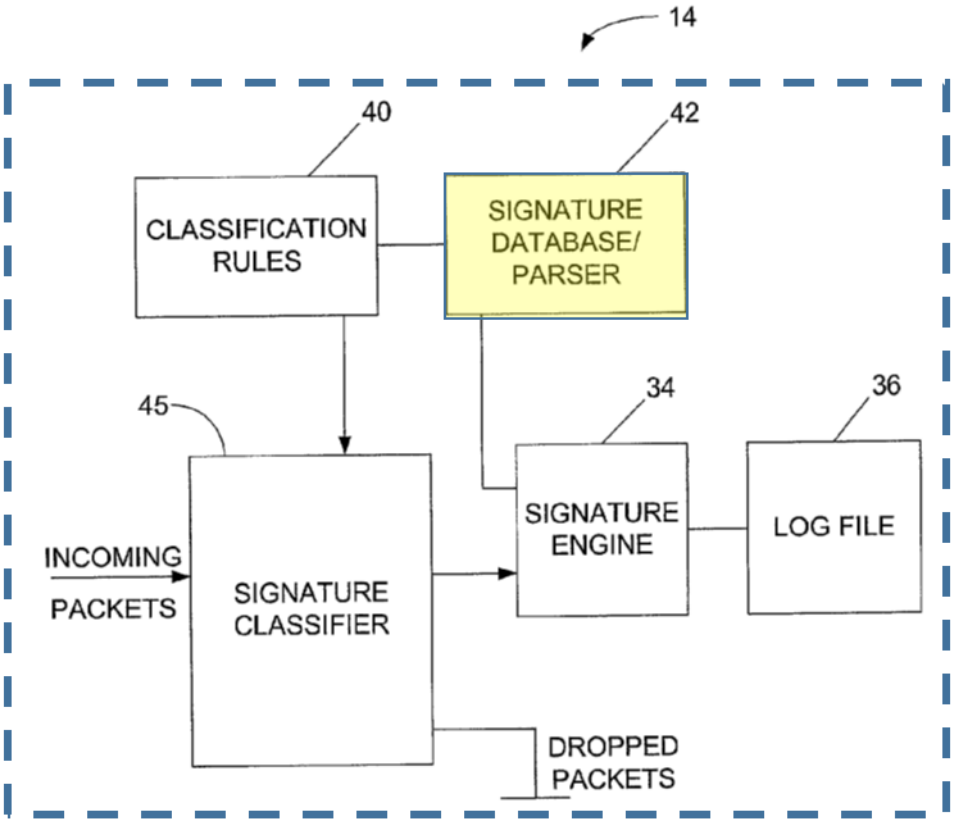


FIG. 1

EX-1005 Fig. 1.

68. The system includes a signature engine 34, classification rules database 40, signature database/parser 42 (yellow), log file 36 and signature classifier 45. The signature classifier 45 filters out incoming packet streams in accordance with classification rules generated from the signature database 42. Only packets matched with the classification rules move to the signature engine 34, while no further processing is performed

on the rest of packets. The workload of the signature engine 34 is thus reduced. EX-1005 3:52-4:3. Signatures (or patterns) of all known attacks are described in an abstract form and included within the signature database 42. EX-1005 4:4-7.

69. Wu discloses that the network intrusion detection system "may be placed at key points throughout the network" and "may be used on different types of networks and placed in various locations throughout the network." EX-1005 4:46-47; 4:66-67. A POSA understood, as discussed in the state of the art, IDS systems may be placed at various location but requires inspection of unencrypted traffic (packets), thus any placement would be predicated on access to unencrypted data (clear text) near and preferable towards the endpoint of the local network.

3. The Motivation To Combine the Teachings of Pham with the Teaching of Wu with a Reasonable Prediction of Success

70. The Patents, Pham and Wu are analogous art, all directed to network protection, operating at the packet level to ensure transported data to the network is secure and not malicious. Wu describes that as Internet access costs have decreased, corporations are increasingly using the Internet for corporate data and communications with external networks. EX-1005 1:8-13. It identifies that network security is increasingly

becoming a critical issue in enterprise and service-provider networks as usage of public networks for data transport increases and new business applications such as e-commerce sites are deployed. Security measures are required, for example, to prevent hackers from gaining unauthorized access to a corporation's information resources or shutting down an e-commerce web site via a distributed denial of service attack. EX-1005 1:13-22. Wu describes that corporations continue to deploy firewalls to prevent unauthorized users from entering their networks, but are looking for additional security technologies to protect their system's vulnerability that firewalls alone cannot address. EX-1005 1:22-26.

71. Wu describes that one of these additional security measures is an intrusion detection system (IDS). Wu describes that as network attacks have increased in number and severity, intrusion detection systems have become a necessary addition to the security infrastructure of most organizations. Intrusion detection allows organizations to protect their systems from threats that come with increasing network connectivity and reliance on information systems. Intrusion detection systems include software or hardware systems that automate the process of monitoring events occurring in a computer system or network, and analyzing them for signs of security problems. Wu explains that because intruders attempt to

compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network, intrusion detection technology has become a necessary addition to every large organization's computer network security infrastructure. EX-1005 1:27-45.

72. Pham also recognizes the challenges presented by the growth of the Internet and proliferation of private distributed intranets, and specifically identifies increasing the speed, security, and transactional reliability of network data transmissions as a fundamental concern and continuing consideration in the development of new network infrastructure. EX-1004 [0005]. Pham is directed to a virtual private network gateway having data packet processors for processing packets coming from external data networks. EX-1004 Abstract. Pham specifically identifies that its technology is useful for the type of corporate intranet environments that connect to the Internet that are identified by Wu. EX-1004 [0008].

73. A POSA would be motivated to modify the teachings of Pham to include the teachings of Wu to include an intrusion detection system to achieve the advantages expressly described above by Wu for increasing security of the network protected by Pham's gateway. Wu describes that a "signature based intrusion detection system 14 may be used alone or in

combination with a data monitoring and analysis device configured to perform fault and network performance management." EX-1005 4:4-7. In one embodiment, Wu describes that application program interfaces (APIs) can be used to open applications of the network analysis device 16. EX-1005 4:26-27.

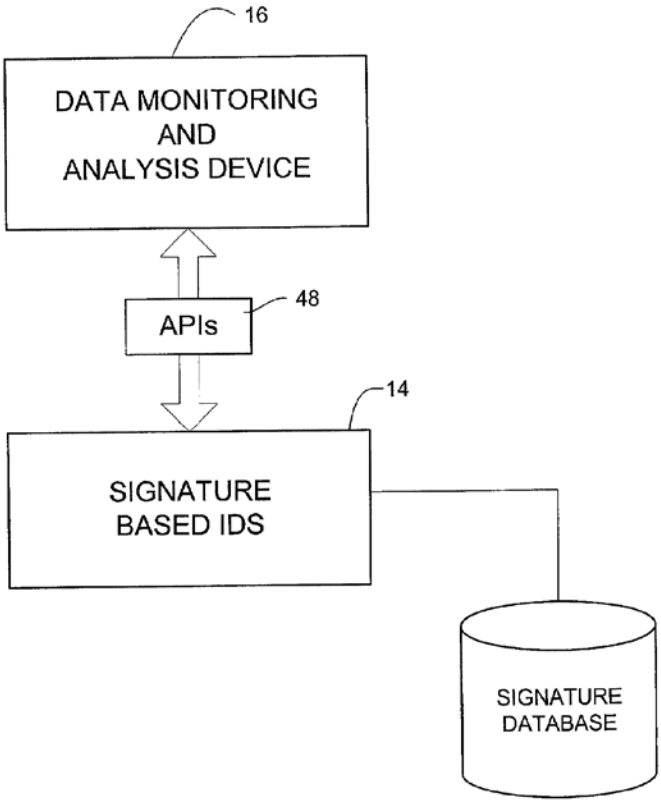


FIG. 2

EX-1005 Fig. 2.

74. The APIs are used to parse, generate and load signatures, invoke corresponding signature detection methods from appropriate protocol contexts, access states required for stateful intrusion detection,

and access alerts/alarms management facilities. Wu also teaches in another embodiment that the signature based intrusion detection system 14 may be used without the network analysis device 16, and instead perform the function of device 16, such as packet decoding. EX-1005 4:28-38.

75. Pham describes that the network processor 112 connects to and supports high-speed data interchange of incoming and outgoing packets with a dedicated encryption/decryption engine controls and monitors the engine encryption/decryption 120. EX-1004 [0052]. A memory 116 is provides for the external memory and program requirements of the network processor. EX-1004 [0051]. A POSA understood that to implement the teachings of Wu with Pham, the IDS would be coupled between the network processor 112 and the cryptographic core because Wu expressly discloses that network intrusion detection system may be "placed in various locations throughout the network" (EX-1005 4:65-67), and "may be used alone or in combination with a data monitoring and analysis device configured to perform fault and network performance management." EX-1005 4:4-7. Placing the intrusion system in line with the network processor of Pham is advantageous because it allows actions to be taken on packets that match a signature in the signature database before the packet is accepted into a network or sent to a network.

Importantly as discussed in the state of the art, IDS systems such as Wu must necessarily be placed where it can inspect unencrypted traffic (packets), thus placement between the encryption engine and the network processor would have allowed access to unencrypted data (clear text) near and endpoint of the local network. EX-1015 [0012, 0079]. As noted in Wu, the IDS is configured to analyze packets flowing through a network that may be overlooked by the firewall's simplistic filtering rules. EX-1005 1:50-54. For incoming encrypted packets, a tap location between the Pham's network processor 112 and encryption/decryption engine 120 is the first instance a clear text packet may be analyzed, conversely for outgoing packets that will be encrypted, the tap location between the network processor 112 and the encryption/decryption engine 120 is the last opportunity to analyze the packets prior to encryption and transmission out of the LAN. Further, external memory 116 of Pham is described as including to store and share other information between the crypto processors and, generically, data processors. EX-1004 [0053]. Thus, a POSA understood that the signature database could be included in memory 188, as contemplated by Pham, or as a standalone database.

76. In view of the above, a POSA would be motivated to combine the teachings of Pham with Wu, with a reasonable expectation of success because:

i. Wu expressly provided the teaching, suggestion, and motivation that "intrusion detection technology has become, a necessary addition to every large organization's computer network security infrastructure" and would have led a POSA to modify Pham's network data processor with an intrusion detection system with a signature database before allowing a data packet to enter the internal network to increase security and achieve the benefits expressed described by Wu.

ii. The general knowledge in the art that the use of intrusion detection systems and signature databases to protect internal networks from external threats was an accepted, known and predictable mechanism to increase the security of Pham's network processor.

iii. Wu's known technique of using APIs in conjunction with a network processor to implement the intrusion detection system would readily improve the security of the network processor taught by Pham with predictable results; and,

iv. The location between the network processor and the encryption/decryption engine allows the IDS access to the unencrypted packet at a point near the endpoint at the first possible point after decryption thus allowing the earliest indication of an incoming threat and allows action to be taken before a malicious packet is received into the network. Similarly, this location allows the IDS access to the unencrypted packet at a point near the endpoint at the last possible point prior to encryption thus allowing action to be taken before a malicious packet is sent into to another network.

4. Detailed Application of Pham and Wu to Challenged Claims 1, 2, 9-13, 16 and 22 of each of the Patents.

a. <u>Claim 1</u>

i. [pre]A security processor to process incoming packets and outgoing packets, the security processor comprising:

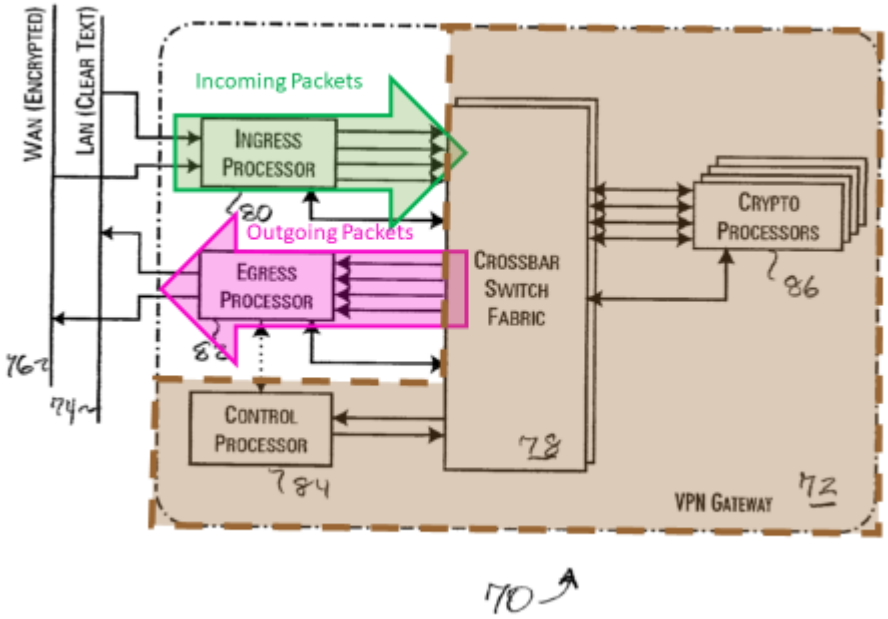
77. To the extent the preamble is limiting, Pham discloses a security processor for ingress and egress processing of packets. (*process incoming packets and outgoing packets*)

A VPN gateway 72 provides a single physical LAN 74 connection supporting multiple logical connections over a local clear text network and a single physical WAN 76 connection, extending encrypted network connections over the Internet. The VPN gateway 72 utilizes IBM Packet Routing Switches PRS28.4G (IBM Part Number

IBM3221L0572), available from IBM Corporation, Armonk, N.Y., as the basis for a central crossbar switch fabric 78 interconnecting an ingress processor 80, an egress processor 82, a control processor 84 and an array of two to sixteen crypto processors 86.

EX-1004 ¶[0045].

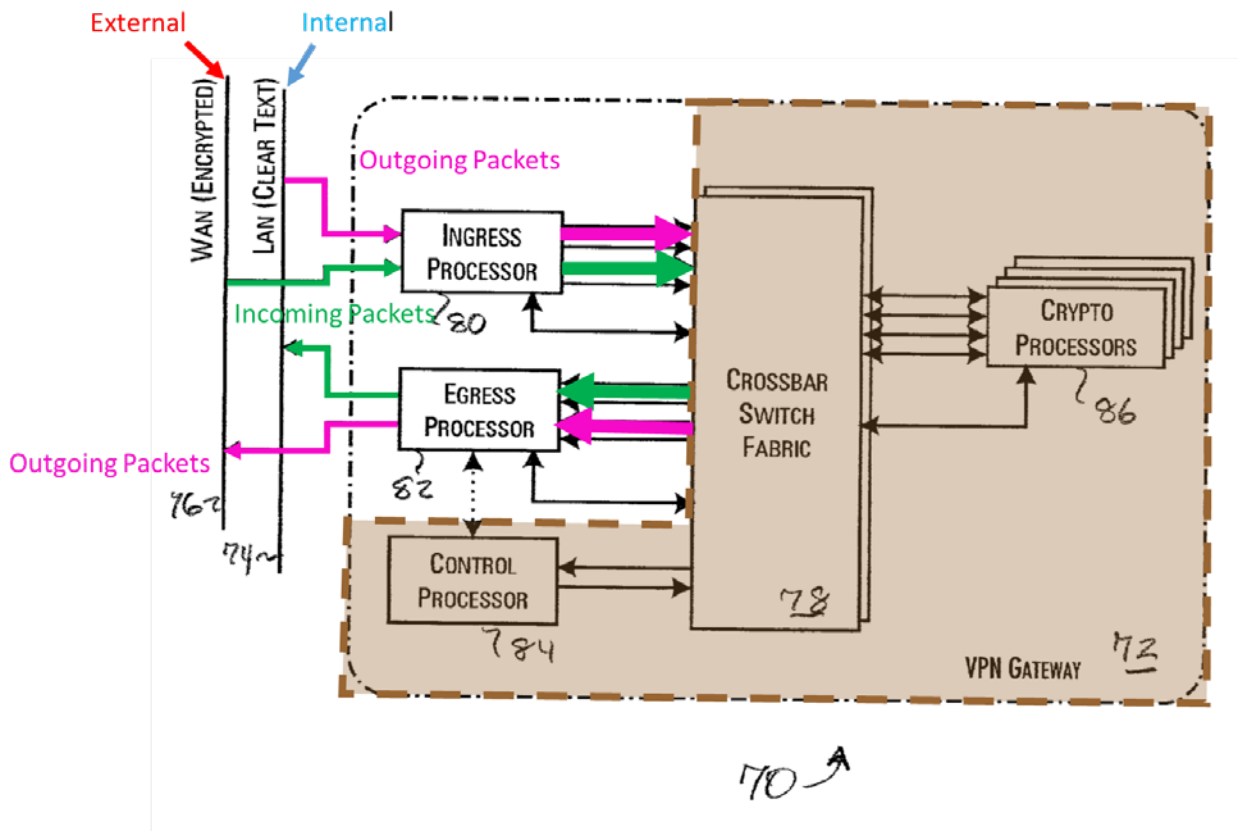
78. In Pham, as shown in annotated Fig. 4, the security processor (brown) processes incoming packets (green) and outgoing packets (pink).



EX-1004 Fig. 4.

79. Alternatively, to the extent the PO argues the incoming/outgoing packet distinction is with respect to the internal/external network perspective, the incoming packets may be the encrypted packets received from the external network (i.e. the WAN 76)

and the outgoing packets may be the clear text packets received from the internal network (i.e. the LAN 74).



EX-1004 Fig. 4.

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

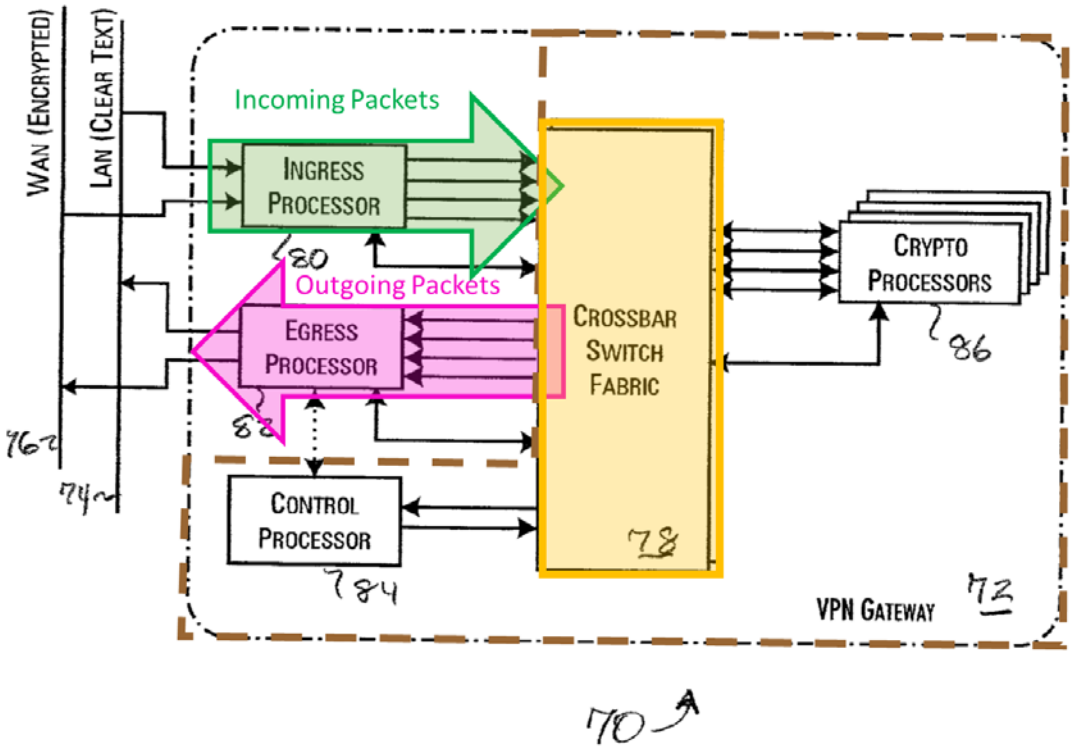
80. Pham discloses a switch fabric 78 (*switching system*) to send the egress packets (*outgoing packets*) and received in ingress packets (*incoming packets*).

Thus, for 4 Gbps network 74, 76 connections, each ingress processor 80 implements at least three port connections to the switch fabric 78.

Likewise, each egress processor 82 receives at least three output port connections to the switch fabric 78.

EX-1004 [0047].

81. As shown in Fig 4. The switch fabric 78 (orange) sends outgoing packets (pink) and receives incoming packets (green)



EX-1004 Fig. 4.

82. Pham discloses that the switch fabric is made up of conventional packet routing switches (EX-1004 [0045]), which is consistent with the disclosure of the Patents that the switching system 208

is known in the art and can be implemented using conventional switches.

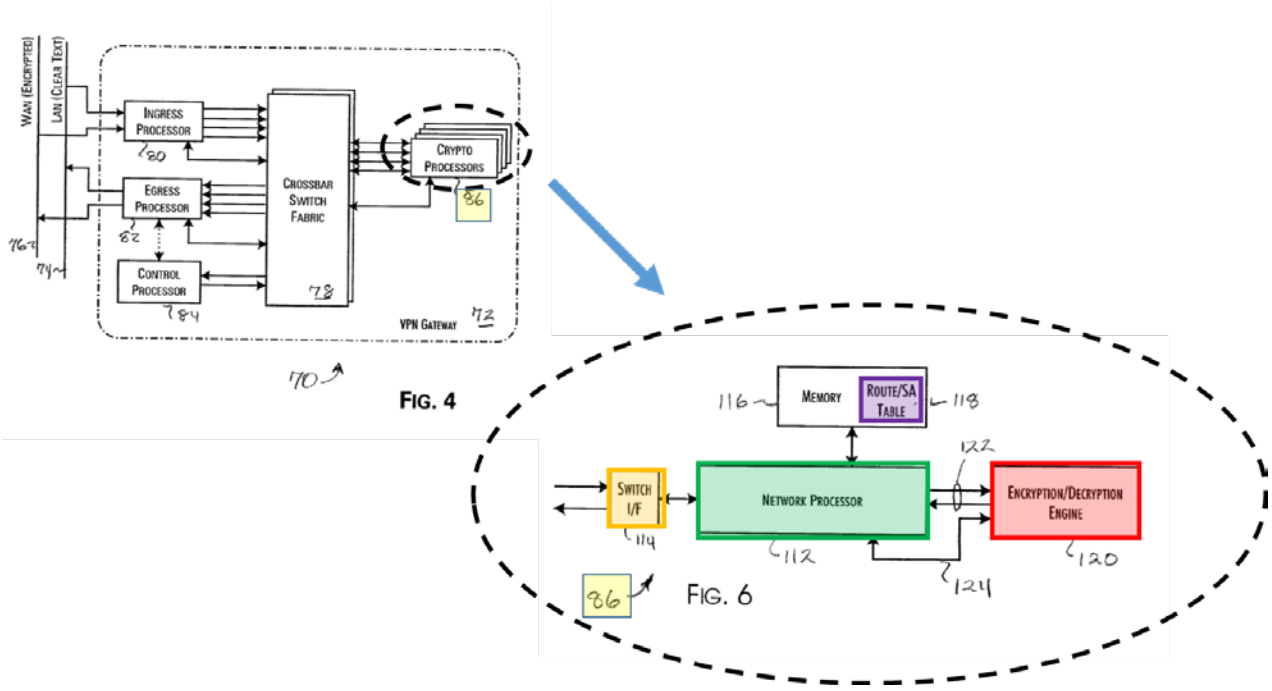
EX-1001 7:33-48; EX-1012 7:33-47.

iii. 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,

83. Pham discloses an implementation of a crypto processor 86 which includes a network processor 112 (*packet engine*) coupled to the switch fabric 78 (switching system).

The preferred implementation of a crypto processor 86 is shown in. FIG. 6.

EX-1004 [0051].



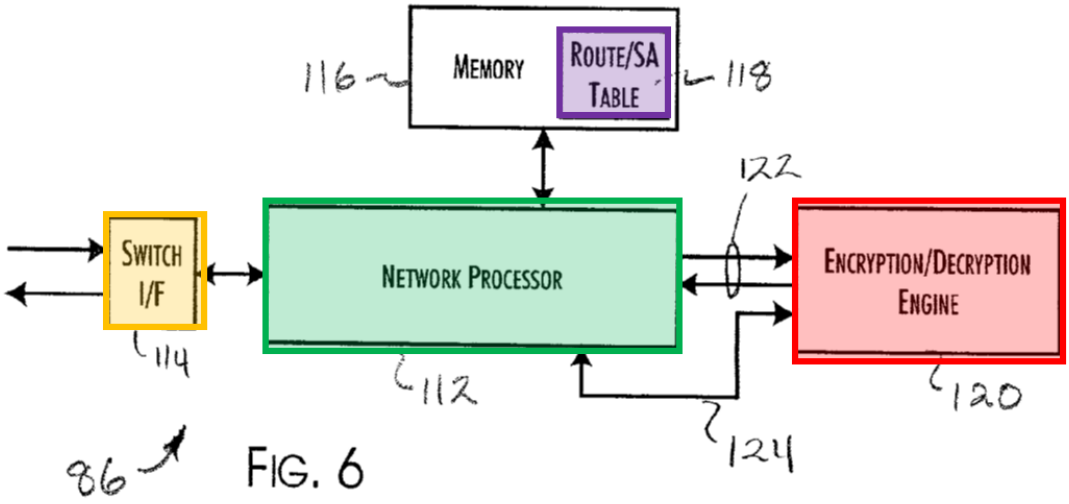
EX-1004 Figs. 4 and 6.

84. Pham discloses the network processor 112 (*packet engine*) processes the incoming packets received from the switch fabric (*switching system*) and the outgoing packets sent to the switch fabric (*switching system*). The network processor includes the association of secure authority (SA) parameters task (*classification processing*). The SA parameter data from table 118 is used to dynamically create and attach SA headers to each received IPSec data packet to allow for IPsec protocol processing by encryption/decryption engine 120. EX-1004 [0049]-[0051].

85. Pham's description of classification processing is consistent with the Patents' disclosure that 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. EX-1001 5:23-35; EX-1012 5:23-35.

86. As shown in Fig. 6, the network processor 112 (green) is connected to the switching fabric 78 via the switch fabric interface 114 (orange) (the interface 114 may be considered part of the switching fabric 78) and processes the incoming and outgoing packets (green and pink) for association with the SA parameters stored in the memory 116/ SA

parameter data table 118 (purple). An encryption/decryption engine 120 (red) is connected to the network processor.



EX-1004 Fig. 6.

87. Pham describes that the network processor 112 can be a commercially available processor including a switch fabric interface 114, *e.g.,* IBM PowerNP NP4GS3 Network Processor. EX-1004 [0049], [0051]. Pham's disclosure of a conventional network processor is consistent with the Patents' disclosure that suitable packet engines were known in the art to process packets needing network address translation processing and firewall table processing, and processed IPSec packets. Ex-1001 9:60-10:8; EX-1012 9:60-10:6.

iv. 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

88. Pham discloses multiple crypto processors 86 which each include a respective network processer (*packet engines*).

> The VPN gateway 72 utilizes IBM Packet Routing Switches PRS28.4G (IBM Part Number IBM3221L0572), available from IBM Corporation, Armonk, N.Y., as the basis for a central crossbar switch fabric 78 interconnecting an ingress processor 80, an egress processor 82, a control processor 84 and an array of two to sixteen crypto processors 86."

EX-1004 ¶[0045].

> The preferred implementation of a crypto processor 86 is shown in FIG. 6.

EX-1004 ¶[0051].

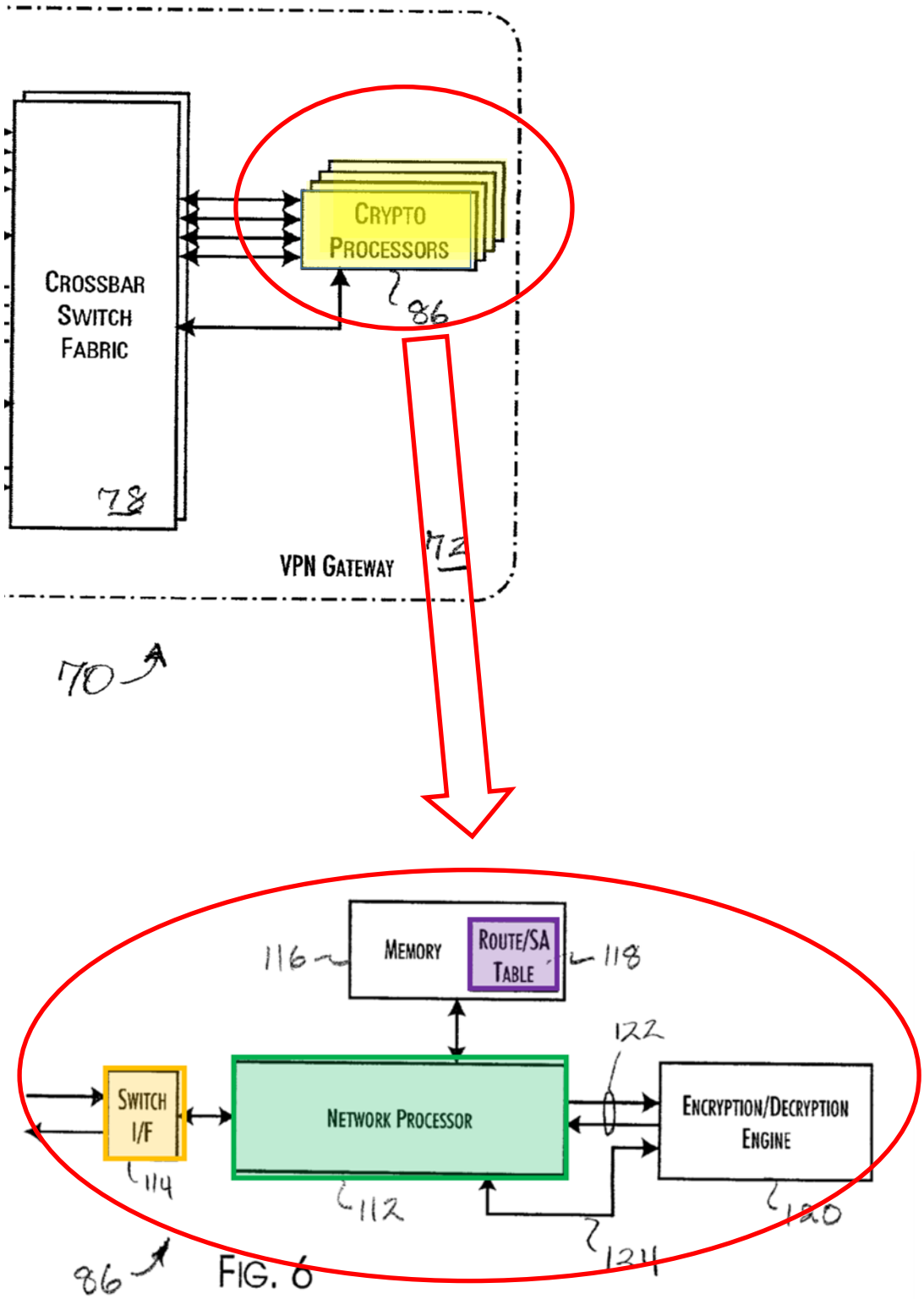

CROSSBAR SWITCH FABRIC
78
CRYPTO PROCESSORS
86
VPN GATEWAY
72
70
MEMORY
ROUTE/SA TABLE
116
118
122
SWITCH I/F
114
NETWORK PROCESSOR
112
ENCRYPTION/DECRYPTION ENGINE
120
124
86

FIG. 6

EX-1004 Figs. 4 and 6.

89. Pham discloses that the network processors 112 process substantial all the data packet received and transmitted by the VPN Gateway. For example, in one embodiment, Pham discloses that ingress processor 80 (Fig. 5) and network processor 112 in crypto processor 86 (Fig. 6) use the identical conventional processors and identical routing and SA tables to allow functions of the ingress processor to be offloaded to network processor 112, such as packet routing, SA parameter association and compression and decompression. EX-10044 Figures 5, 6 [0049], [0051], [0053]. Thus, all packets, both clear text and encrypted can be sent to network processor 112 for routing using routing and SA table 118.

90. Further, as discussed below, when the intrusion detection system is interposed in line with the network processor between the network processor and the cryptographic core, all incoming and outgoing packets would be sent through the intrusion detection system, via the network processor to ensure that malicious packets can be identified before being sent into or from the network.

v. 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;

91. This limitation only applies to the Challenged Claims of the ’436 Patent.

92. Pham discloses the incoming packets and outgoing packets are provided with SA header information and an IP tunneling header (*tag*) upon ingress to one of the plurality of network processors (*packet engines*). Pham also discloses the SA header including the IP tunneling header (*tag*) determines the egress path within the security processor to an appropriate egress processor upon exit from the encryption/decryption engine 120 (*cryptographic core*). EX-1004 [0051, 0071 and 0072].

93. Pham, with respect to one embodiment, discloses adding an IP tunneling header to the packet at the ingress processor using the routing and SA parameter table.

The relevant SA parameters are retrieved 266 from the SA context store and formatted into a SA header 268. A tunneling IP header 270, IPsec control fields 271, padding field 272, and Message Authentication Code (MAC) field 273 are also created.

EX-1004 [0071].

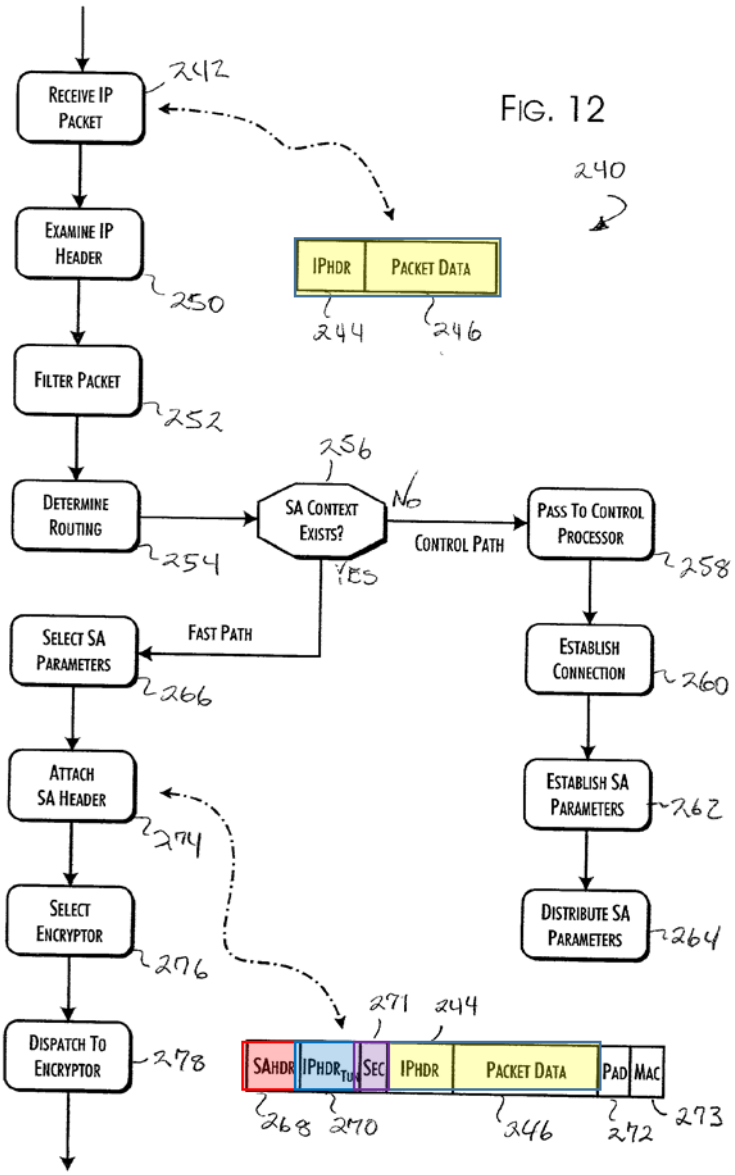
94. Figure 12 of Pham illustrates the use of the routing and SA table (102) used by the ingress processor (Figure 5) upon receipt of a clear text packet. However, Pham discloses that in an alternative embodiment, the routing and SA table 118 of the crypto processor can be used (Fig. 6) in

the network processor 112 and associated memory 116 with route/SA table 118.

In this alternate embodiment, the SA parameter association task is off-loaded from the ingress processors 80 and performed by the crypto processors 86. The control processor 84 explicitly propagates identical copies of the SA parameter data to each of the crypto processors 86, enabling the crypto processors 86 to process any data packet received. EX-1004 [0051].

95. Thus, Figure 12 applies equally to a clear text data packet received at network processor 112 using routing and SA table 118, and discloses the creation and attachment of the headers to each data packet by network processor 112 in a crypto processors 86 for each packet received (*upon ingress to one of the plurality of packet engines*) rather than by the ingress processors.

96. The headers added to the ingress packet (yellow) as disclosed in Pham include at least the SA header (red) and tunneling IP header (blue) and the IPsec control fields (purple), i.e. **SA**HDR (268) **IP**HDR$_{TUN}$ (270) and **S**EC (271). EX-1004 [0072], Figs. 12, 13.



EX-1004 Fig. 12.

97. Pham discloses the SA Header includes a tunneling IP header 270 (*tag*) that determines an egress path within the security processor upon exit from a corresponding encryption/decryption engine 120 (*cryptographic core*);

> The selection of an appropriate egress processor 82, where multiple egress processors 82 are present, is determined by the crypto processor 86 from the route identification information contained in the tunneling IP header 270.

EX-1004 [0072].

98. The tunneling IP header disclosed in Pham corresponds to the identification of the IPsec tunnels described in the '436 Patent. Similarly the routing and SA parameter table of Pham corresponds with the connection flow table and security policy/association data" of the '436 Patent. EX-1001, 5:7-14, 20:21-26.

vi. 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,

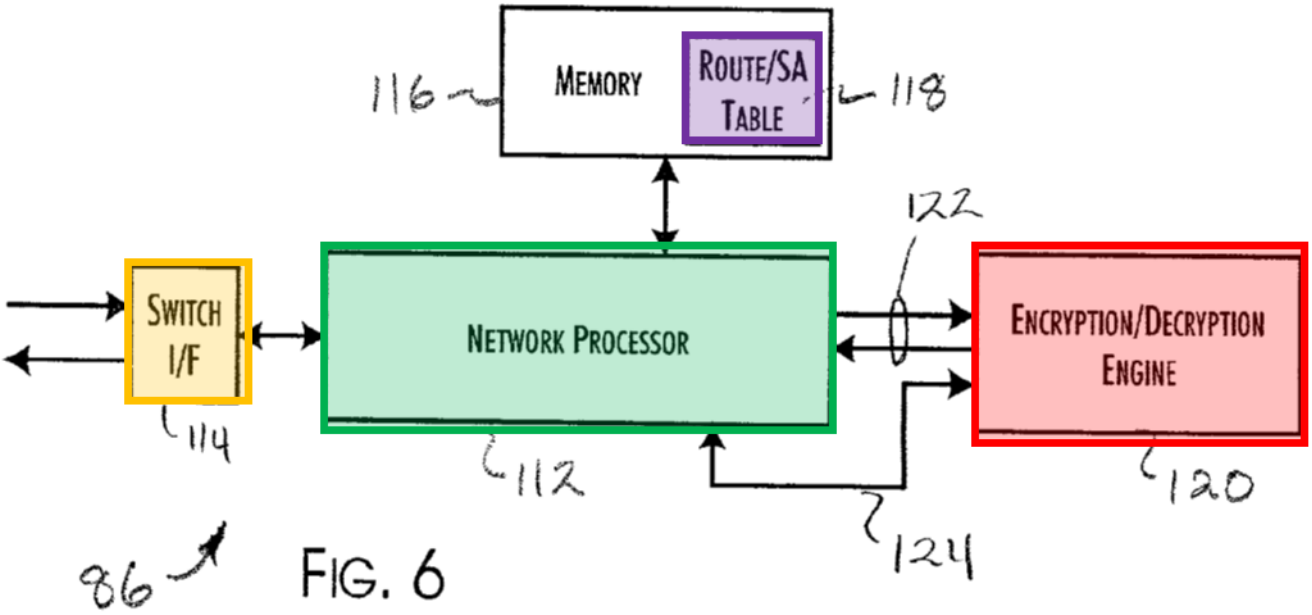
99. Pham discloses the crypto processor 86 includes an encryption/decryption engine 120 (*cryptographic core*) coupled to the network processor 112 (*packet engine*) which receives incoming packets from the switch fabric 78 (*switching system*) via the network processor 112 and communicating the outgoing packets to the switch fabric 78 via the

network processor 112, and provides encryption and decryption processing of packets received from and sent to the network processor.

The network processor 112 connects to and supports high-speed data interchange with a dedicated encryption/decryption engine 120 through a direct data transfer bus 122. The network processor 112 controls and monitors the engine 120 via control and status lines 124. Preferably, the engine 120 is a BCM5840 Gigabit Security Processor, available from Broadcom Corporation, Irvine, Calif. The BCM5840 processor implements a highly integrated symmetric cryptography engine providing hardware support for IPsec encryption and decryption operations. Utilizing the BCM5840, each crypto processor 86 is capable of a minimum sustained effective IPsec encryption/decryption and IPsec authentication rate of 2.4 Gbps."

EX-1004[0052].

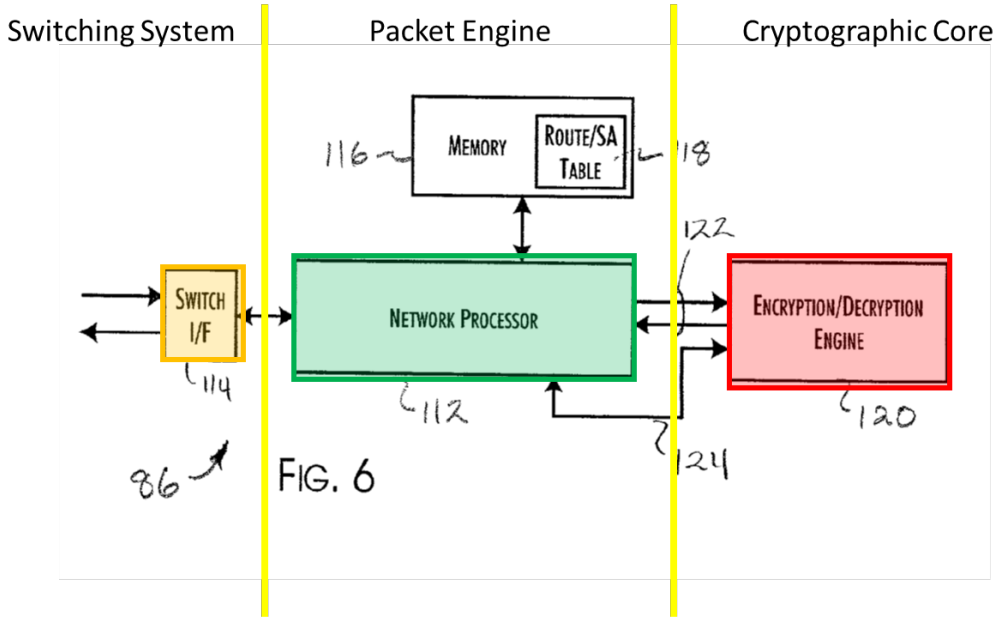
100. Fig. 6 illustrates the arrangement of the encryption/decryption engine 120 (red) and flow of packets with respect to the network processor (green), and switch fabric/interface (orange).



EX-1004 Fig. 6.

vii. wherein the packet engine is interposed between the switching system and the cryptographic core;

101. Pham discloses the network processor (*packet engine*) is interposed between the switch fabric/interface (*switching system*) and the encryption/decryption engine (*cryptographic core*).



EX-1004 Fig. 6.

102. Pham's arrangement shown in Fig. 6 corresponds with the architecture disclosed in the Patents which the applicant argued demonstrated the "Packet engines 228 may each be <u>interposed between/coupled to</u> a cryptographic core 232 <u>and the switching system 208 as shown in Figure 2.</u>

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.

EX-1002 OA response pp. 68-77.

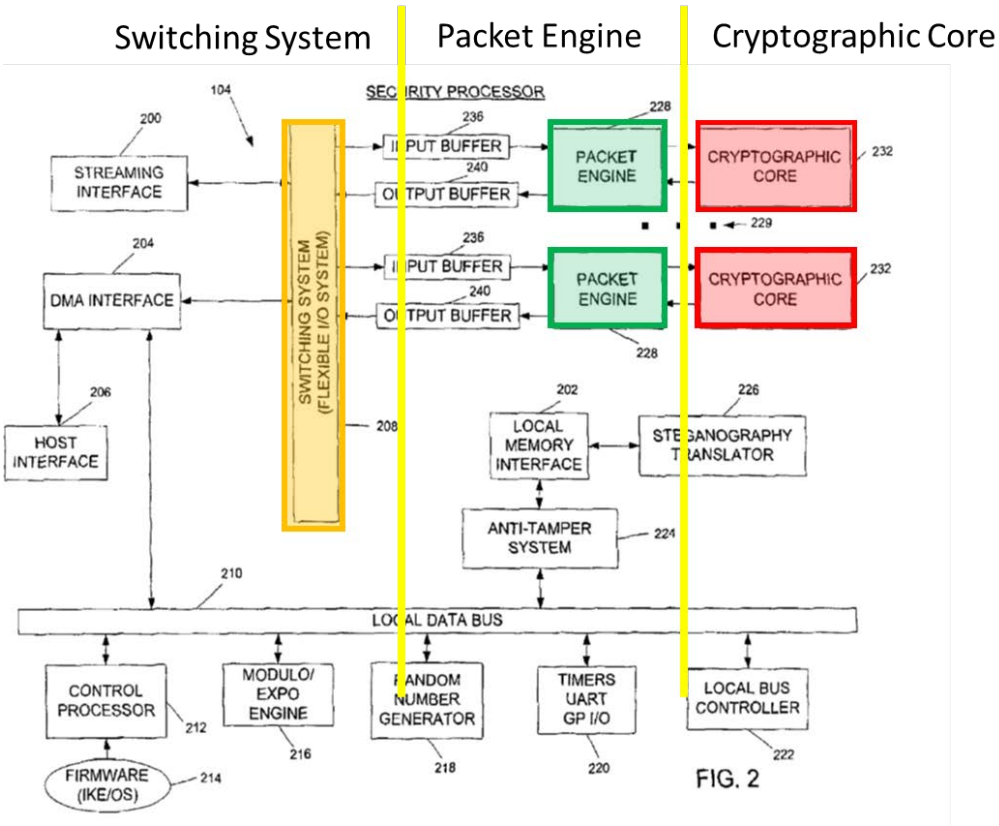


FIG. 2

EX-1001 Fig. 2; EX-1012 Fig. 2.

viii. 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.

103. Wu discloses a signature based intrusion detection system 14 (blue) with a signature database (yellow).

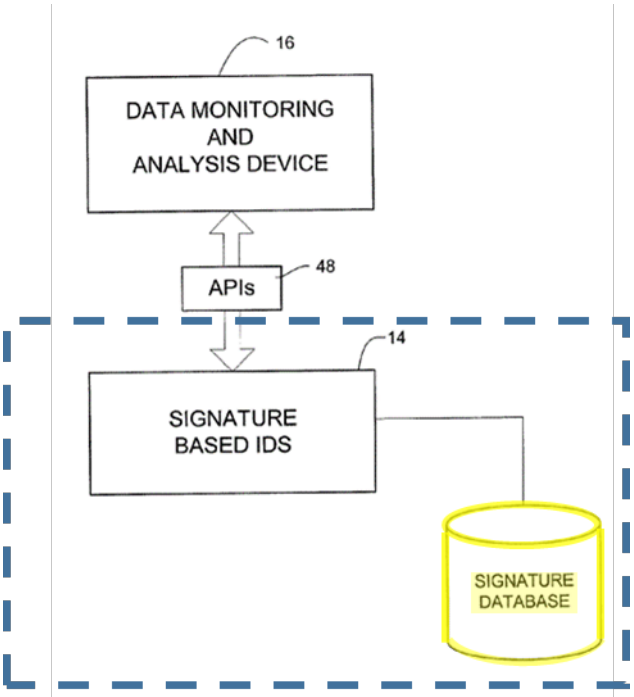


FIG. 2

EX-1005 Fig. 2.

104. Wu discloses a signature based instruction detection system 14 including a signature database 42. EX-1005 3:52-4:3.

105. The system of Wu is responsive to captured packets matching a signature stored in the signature database.

Signatures (or patterns) of all known attacks are described in an abstract form and included within the signature database 42. These patterns are used to identify an intrusion. Additional signatures are identified by studying system audit information in order to find matching patterns of known system intrusions. In a similar manner indications of other attacks can be figured out. They are represented in a specified form and coded to the intrusion detection system. A signature analysis or pattern matching algorithm is used upon the

packets, wherein the packets are compared to "attack signatures", or signatures of known policy violations or patterns of misuse. Signature engine 34 compares monitored traffic with attack signatures. Attack signatures can comprise, for example, a rules-based hierarchy of traffic signatures of known policy violations. The signature engine 34 compares packets from the network traffic with such attack signatures such that policy violations can be discovered.

EX-1005 5:23-39.

106. Wu discloses locating the intrusion detection system at key locations in the network and notes that the system may be "placed in various locations throughout the network." EX-1005 4:65-67.

The network intrusion detection system (NIDS) 18 may be placed at key points throughout the network. The units monitor network traffic, perform local analysis of the traffic, and report attacks to a central management station (e.g., system administrator). The network intrusion detection systems 18 are preferably placed on the network perimeter including both sides of a firewall 20 (e.g., between router 22 and the Internet), near a web server 26, and on links to internal or partner networks (e.g., between router 28 and internal corporate network 24). For example, NIDS 1 monitors all traffic passing into and out of the internal network. NIDS 1 provides an early warning since it detects reconnaissance port scans that typically indicate the start of hacker activity. From this point, NIDS 1 can document the number and types of attacks originating on the Internet that target the network. NIDS 2 monitors traffic that has passed through the firewall

20. NIDS 3 monitors traffic passing into and out of internal corporate LAN 24. It is to be understood that the network of FIG. 3 is only one example illustrating placement of NIDSs within a network and that the present invention may be used on different types of networks and placed in various locations throughout the network.

EX-1005 4:46-67.

107. It would have been obvious to modify the teachings of Pham with the teachings of Wu to add an intrusion detection system and signature database to the network data processor system AND to functionally locate the IDS between the network processor (*packet engine*) and the encryption/decryption engine (*cryptographic core*) as I discussed above in the motivation to combine section VII.A.3.

b. Claim 13

i. [pre] A security processing system comprising: a security processor comprising:

108. Pham discloses a security processing system including a security processor. *See* Claim 1 [pre]

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

109. *See* Claim 1.ii

iii. 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,

110. *See* Claim 1.iii

iv. 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

111. *See* Claim 1.iv

v. 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;

112. *See* Claim 1.v, this limitations applies only to the '436 Patent.

vi. 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,

113. *See* Claim 1.vi

vii. wherein the packet engine is interposed between the switching system and the cryptographic core;

114. *See* Claim 1.vii

viii. 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

115. Wu discloses an intrusion detection system meeting the limitation as described in detail above with respect to Claim 1.viii limitation.

116. It would have been obvious to a POSA to combine Pham and Wu as described above to arrive at the claimed invention for the same reasons as described above with respect to Claim 1.

ix. a local data bus coupled to the switching system; and

117. Pham discloses a direct data transfer bus 122 (*local data bus*).

> The network processor 112 connects to and supports high-speed data interchange with a dedicated encryption/decryption engine 120 through a direct data transfer bus 122."

EX-1004 [0052].

118. The direct data transfer bus 122 is coupled to the switch fabric 78 (*switching system*) via the network processor 112.

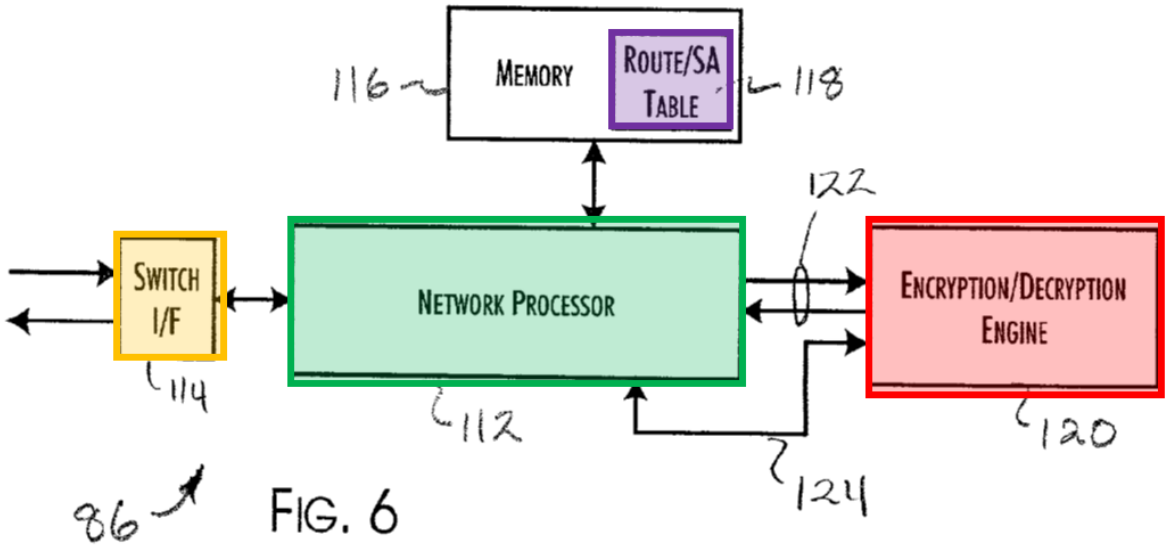


FIG. 6

119. This is consistent with the Patents' use of the word "coupling" with respect to the data bus, in that it includes direct coupling as well as coupling through an intermediate element. For example, the Patents describe that in Figure 2, local memory interface 202 is "coupled to local data bus 210" even though it is coupled through anti-tamper system 224. EX-1001 6:63-64; EX-1012 6:63-64.

120. To the extent the PO argues the local data bus must be directly coupled to switching system, it would have been obvious to a POSA to provide a direct data transfer bus as taught by Pham between the network processor and encryption/decryption engine to handle packets between the switching fabric and other entities in the security processor of

Pham, such as to connect the network processor and/or memory 116. A POSA would have been motivated to provide the bus to effectively handle data transfers between the switch fabric, network processor and memory as is known in the art, furthermore being downstream of the switch fabric, the local data bus fails to be subject to the deleterious saturation issues noted by Pham regarding prior art peripheral buses. EX-1004 [0010].

x. a memory coupled to the local data bus.

121. Pham discloses a memory array 116. EX-1004 [0051], Fig. 6.

> A memory array 116 is provided for the external memory and program requirements of the network processor. Optionally, in accordance with an alternate embodiment of the present invention, the memory array 116 also provides storage space for an SA parameter data table 118."

EX-1004 [0051].

122. The memory array 116 is coupled to the local data bus via the network processor 112. EX-1004 Fig. 6.

123. To the extent the PO argues the memory must be directly coupled to the local data bus, it would have been obvious to directly couple the local data bus to both the memory and switching fabric as discussed above.

c. Claim 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.

124. As discussed above with respect to Claim element 1.iii, Pham describes the network processor (*packet engine*) provides SA parameters (*security context management processing*) for the ingress and egress packets (*incoming and outgoing packets*).

> The preferred implementation of a crypto processor 86 is shown in FIG. 6. The network processor 112 is also preferably an NP4GS3 Network Processor, including a switch fabric interface 114. A memory array 116 is provided for the external memory and program requirements of the network processor. Optionally, in accordance with an alternate embodiment of the present invention, the memory array 116 also provides storage space for an SA parameter data table 118. In this alternate embodiment, the SA parameter association task is off-loaded from the ingress processors 80 and performed by the crypto processors 86. The control processor 84 explicitly propagates identical copies of the SA parameter data to each of the crypto processors 86, enabling the crypto processors 86 to process any data packet received.

EX-1004 [0051].

d. Claim 9.

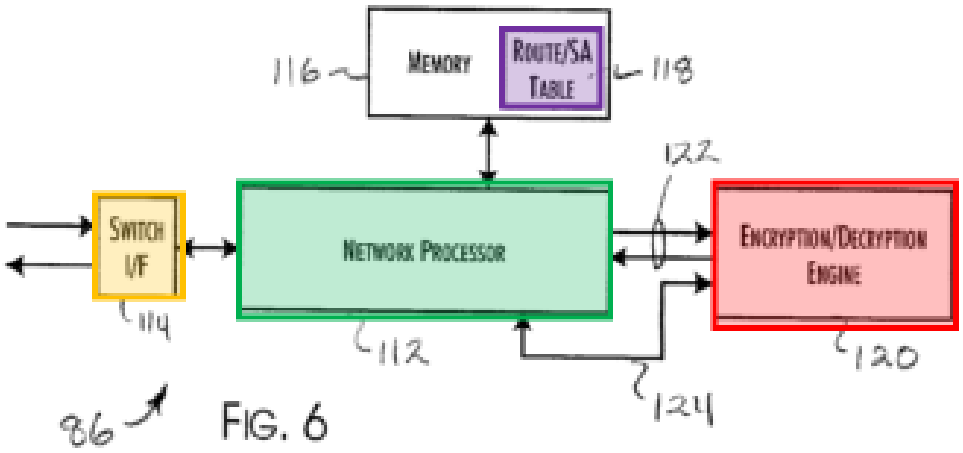
The security processor of claim 1 wherein the cryptographic core is one of a plurality of cryptographic cores coupled one-to-one to the

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.

125. As described with respect to Claim 1, Pham discloses multiple crypto processors 86 which each include a respective network processor [green] (*packet engines*) and encryption/decryption engine [red] (*cryptographic cores*)

> The VPN gateway 72 utilizes IBM Packet Routing Switches PRS28.4G (IBM Part Number IBM3221L0572), available from IBM Corporation, Armonk, N.Y., as the basis for a central crossbar switch fabric 78 interconnecting an ingress processor 80, an egress processor 82, a control processor 84 and **an array of two to sixteen crypto processors 86.**

EX-1004 ¶[0045].



EX-1004 Fig. 6.

126. Pham discloses that respective ones of the network processors 112 and encryption/decryption engines process substantially all the data packet received and transmitted. For example, in one embodiment, Pham discloses that ingress processor 80 (Fig. 5) and network processor 112 in crypto processor 86 (Fig. 6) use the identical conventional processors and identical routing and SA tables to allow functions of the ingress processor to be offloaded to network processor 112, such as packet routing, SA parameter association and compression and decompression. EX-1004 Figures 5, 6 [0049], [0051], [0053]. Thus, all packets, both clear text and encrypted can be sent to network processor 112 for routing using routing and SA table 118.

e. Claim 10.

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.

127. Pham discloses the network processor (packet engine) adds at least an IP_{tun} header (*IP header*) to the outgoing packets. *See* Claim 1 VII.A.4.a.iii and a.v.

f. Claims 12 and [22}

The security processor [processing system] of claim 1 [13], wherein the at least one packet matching the

signature stored in the signature database comprises a plain text packet.

128. Pham in view of Wu discloses an intrusion detection system including the signature database connected between the network processor and the encryption/decryption engine that "listens and analyzes all traffic in real-time as it travels across the network" for packets matching stored signatures as discussed above with respect Claims 1 and 13. Pham further discloses passing encrypted data packets and clear text data packets to the encryption/decryption engine.

> For the preferred IPsec processing embodiments of the present invention, clear text data packets forwarded from the LAN 38 through the VPN gateway 12 subject to the VPN encryption protection are routed by the ingress processor 30 through the Switch fabric 40 to an available encryption data packet processor 42. The encrypted data packet is then returned through the Switch fabric 40 to the egress processor 32 and passed onto the Internet 18. Conversely, encrypted data packets received from the Internet 18 are routed by the ingress processor 34 through the Switch fabric 40 to a decryption data packet processor 44. The resulting clear text data packet is then passed to the egress processor 36 for transferred onto the LAN 38.

EX-1004 [0041].

129. Wu further discloses its IDS, like conventional IDS, matches packets traversing the network against signatures in the signature database. EX-1005 2:11-13, 2:44-48, 7:51-67.

> Conventional signature based network intrusion detection systems treat signatures as passive items. When a packet is inspected, it is matched against a list of signatures.

EX-1005 2:11-13.

> Data packets transmitted on the network and having corresponding classification rules are classified according to generated classification rules. Classified packets are forwarded to a signature engine for comparison with signature profiles

EX-1005 2:44-48.

> The system preferably receives raw network packets and uses a network adaptor that listens and analyzes all traffic in real-time as it travels across the network.

EX-1005 5:41-44.

> Signatures (or patterns) of all known attacks are described in an abstract form and included within the signature database 42. These patterns are used to identify an intrusion.

EX-1005 5:23-25.

> Signature matching 66 is performed based on packet classifications to detect network intrusion. Any problems detected are sent to an alert log 68 and appropriate action is taken.

EX-1005 5:67-6:1.

> Action may include, for example, match packet with Subset of signatures (step 116), drop packet (step 118), generate alarm (120), or drop packet and update field of flow table (step 122).

EX-1005 7:64-67.

g. Claim 16.

The security processing system of claim 13 wherein the memory and the security processor are within the same cryptographic boundary.

130. Pham discloses the security processor and memory are within the same cryptographic boundary. A POSA understands a cryptographic boundary to mean an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all hardware, software, and/or firmware components of a cryptographic module. Pham discloses the memory 116 is within the security processor (brown) which forms the cryptographic module or part of the cryptographic module.

> A preferred VPN embodiment 70 of the present invention, representing a Specific implementation of the extended protocol

processor architecture 50, is shown in FIG. 4. A VPN gateway 72 provides a single physical LAN 74 connection supporting multiple logical connections over a local clear text network and a single physical WAN 76 connection, extending encrypted network connections over the Internet. The VPN gateway 72 utilizes IBM Packet Routing Switches PRS28.4G (IBM Part Number IBM3221L0572), available from IBM Corporation, Armonk, N.Y., as the basis for a central crossbar Switch fabric 78 interconnecting an ingress processor 80, an egress processor 82, a control processor 84 and an array of two to sixteen crypto processors 86.

131. The security processor as described previously includes the network processor 112, the encryption/decryption engine 120, and switch matrix 78 which enables the routing and processing of packets for encryption/decryption. The security processor and memory 116 is within the cryptographic boundary (red). EX-1004 [0045].

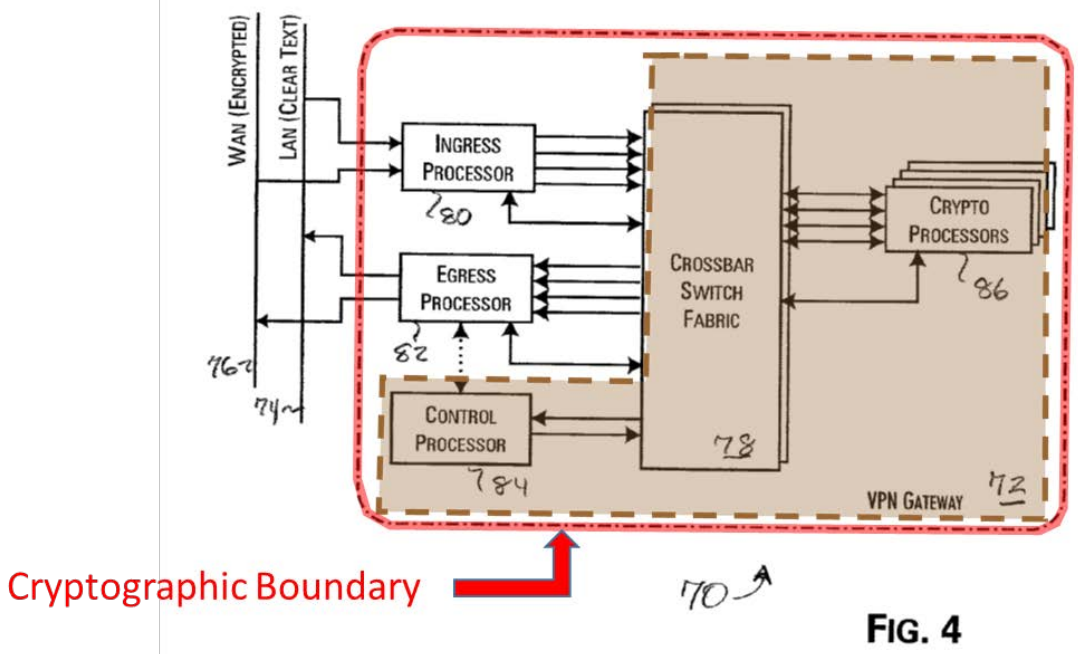


FIG. 4

EX-1004 Fig. 4.

B. Ground 2: Claims 3, 14 And 21 Are Unpatentable Over Pham and Wu in Further View of Collins

1. The Collins Reference

132. Collins describes a cryptographic system which includes an RSA engine. Collins describes that the RSA engine is a special purpose arithmetic unit designed and structured to perform "fast modular exponentiation" and that its design and operation are known to a POSA. EX-1008 [0048]. Collins explains that the RSA engine allows tasks to be performed in parallel to speed up the operation of the cryptographic system. EX-1008 [0050].

2. Detailed Application of Pham and Wu And Collins

a. <u>Claims 3 and 14</u>

> ***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.***
>
> ***14. The security processing system of claim 13 further comprising a modulo engine coupled to the local data bus.***

133. Pham in view of Wu renders Claims 1 and 13 obvious as discussed above. As described in Claim 13 Pham discloses a direct data transfer bus 122 (*local data bus*). EX-1004 [0052].

134. Pham and Wu do not explicitly disclose a modulo engine. However, a POSA understood that it was common to use a module engine to increase the speed of the cryptographic process, Collins discloses such modulo engine.

135. Collins discloses an arithmetic unit/exponentiation cells (*modulo engine*) to "perform fast modular exponentiation" for use in cryptographic processing coupled to a bus.

The RSA engine 260 is a special purpose arithmetic unit designed and structured to perform fast modular exponentiation. In the Specific embodiment, it performs 10 exponentiations per Second on a 1024 bit value. Its design and operation will be understood by one of skill in the art. If another encryption method besides RSA public key

> cryptography is provided by the System, other types of arithmetic units may be provided along with or instead of RSA engine 260.

EX-1008, [0048].

> As FIG. 3 further shows, the I/O controller router 310 of the cryptographic co-processor 115 is coupled by a data/control bus 320 to a DES cell 330 and a number of exponentiation cells 340.

EX-1008, [0057].

136. A POSA understood the arithmetic unit/exponentiation cell described in Collins to be a modulo engine.

137. It would have been obvious to a POSA to use the arithmetic unit (*modulo engine*) described in Collins to aid in the encryption/decryption of Pham. A POSA would be motivated to use a special purpose arithmetic unit to speed the encryption/decryption processes as expressly described by Collins as a benefit by allowing parallel processing, moreover it would have been obvious to a POSA to couple the arithmetic unit to the direct data bus of Pham to allow the transfer of data to and from the arithmetic unit in a conventional manner and would be no more than a design choice. Given the ubiquitous use of data buses, a POSA would also be highly confident of success.

b. <u>Claim 21</u>

The security processing system of claim 13 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.

138. Pham in view of Wu renders Claim 13 obvious as discussed above. Neither Pham nor Wu explicitly disclose executing and authenticating boot code. However, Collins does.

139. Collins discloses executing a loader program (*boot code*) on the cryptographic processor 110 (*security processor*) to load user applications programs (*firmware*). EX-1008 [0026, 58, 66]

> FIG. 6 is a flow diagram of a loader program (e.g., black-boot) that may be used to load user applications.

EX-1008 [0026].

> The black-boot program's main function is to load other user-application programs into flash memory 124, or to Start an application from flash memory 124 (if it is already there).

EX-1008 [0086].

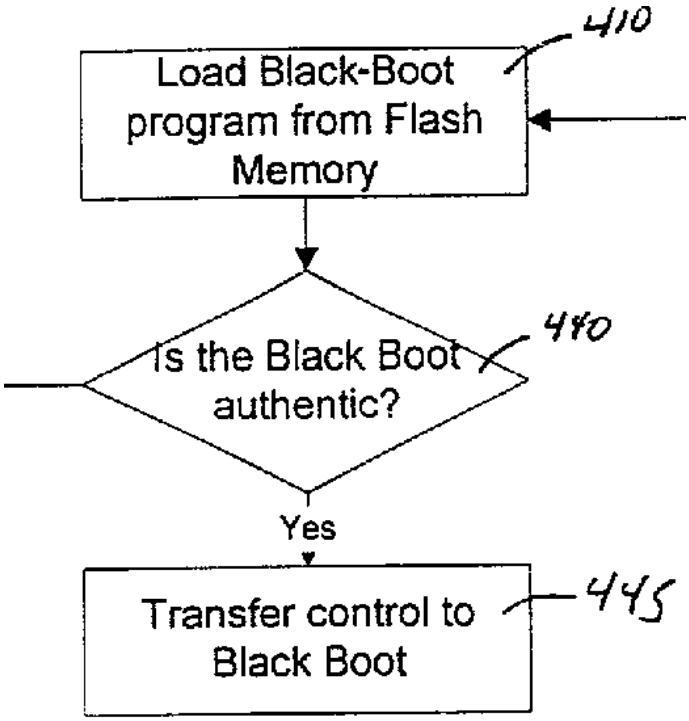
140. Collins discloses the loader program is loaded and authenticated by the cryptographic processor (*security processor*) prior to transferring control (*operation of the security processor*)

> CPU 210 proceeds to step 410 in which it loads a black-boot program from flash memory.

EX-1008 [0068].

> Referring again to FIG. 4, in step 440, once the black-boot program is loaded, CPU 210 determines if the black-boot is authentic using the same technique described above in Step 424. If it is not authentic, then operation is aborted to step 427 and the keys are zeroed (erased) and the cryptographic System 100 is placed in a non-functioning State awaiting a reset. If it is authentic, then the black-boot program is loaded into RAM, and control of CPU 210 is transferred to the black-boot program.

EX-1008 [0087].



EX-1008 Fig. 4.

141. It would have been obvious to a POSA to implement the boot authentication protocol taught by Collins into the security system of Pham and Wu. A POSA would have been motivated to implement the teachings of Collins in order to "provide a level of confidence" that boot code has not be altered or replaced by a fraudulent program" and "allows a great amount of flexibility, while still providing security" as expressly taught by Collins. EX-1008 [0081]. A POSA would have been confident of success implementing Collins authentication protocol given its use of well-known processes such as comparing the length of the program file, starting address, and hashes with known values. EX-1008 [0072].

C. Ground 3: Claims 4, 7, 8 and 17 Are Unpatentable Over Pham, Wu and Collins and Further In View of Krishna

1. The Krishna Reference

142. Krishna is directed to cryptographic processing on a single chip. EX-1006.

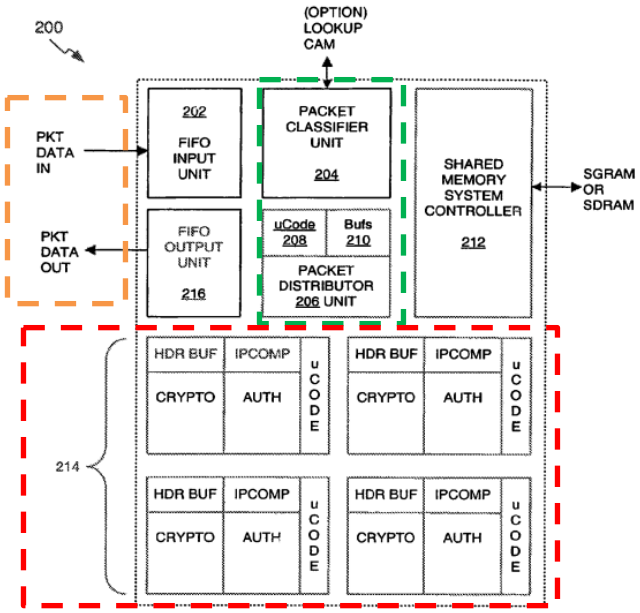
2. Detailed Application Of Pham, Wu, Collins And Krishna

a. Claim 4

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

143. Pham, Wu and Collins render Claim 3 obvious as described above including disclosing a network processor (*packet engine*), encryption/decryption engine (*cryptographic core*) and arithmetic unit (*modulo engine*). Pham, Wu and Collins do not explicitly disclose the packet engine, cryptographic core and modulo engine are formed on a single chip. However, Krishna discloses forming discrete components of the security processor on a single chip.

144. Krishna discloses a packet engine (green), a cryptographic core(red) and other components of a security processor upon a single chip.



EX-1006, Fig 2.

145. Krishna further describes incorporating components on a single chip may increase performance.

By incorporating both encryption and authentication functionality in a single accelerator chip, over-all system performance can be enhanced.

EX-1006 1:66-2:2

146. It would have been obvious to a POSA to form the network processor, encryption/decryption engine, and the arithmetic unit of Pham, Wu and Collins onto a single chip as taught by Krishna. A POSA would have been motivated to do so to increase performance as described by Krishna. As discussed in the State of the Art section, by October 2003

cryptographic processing had moved away from discrete processors to implementing on a single chip. EX-1010, Abstract.

147. A POSA would also be confident of success given Krishna's teaching and the ubiquitous nature of special purpose chips.

b. Claims 7 and 8

7. The security processor of claim 4 wherein the security processor handles substantially all security processing for the incoming and outgoing packets.

8. The security processor of claim 7 wherein the security processor further handles substantially all network processing for the incoming and outgoing packets.

148. Pham discloses the security processor includes network processor 112 that performs security processing and network processing. Pham also discloses that "[a]ll network traffic that is to be processed can be routed to and through the network gateway." EX-1004 ¶[0015].

The network processor 112 connects to and supports high-Speed data interchange with a dedicated encryption/decryption engine 120 through a direct data transfer bus 122. The network processor 112 controls and monitors the engine 120 via control and status lines 124. Preferably, the engine 120 is a BCM5840 Gigabit Security Processor, available from Broadcom Corporation, Irvine, Calif. The BCM5840 processor implements a highly integrated symmetric cryptography engine providing hardware Support for IPsec encryption and decryption operations.

EX-1004 [0052].

149. For example, in one embodiment, Pham discloses that ingress processor 80 (Fig. 5) and network processor 112 in crypto processor 86 (Fig. 6) use the identical conventional processors and identical routing and SA tables to allow functions of the ingress processor to be offloaded to network processor 112, such as packet routing, SA parameter association and compression and decompression. EX-1004 Figures 5, 6 [0049], [0051], [0053].

D. Ground 4: Claim 17 Is Unpatentable Over Pham and Wu and Further In View of Krishna

a. Claim 17.

The security processing system of claim 13 wherein the security processor is formed on a single chip.

150. Pham and Wu render obvious Claim 13 as described above. Pham and Wu do not explicitly disclose whether the security processor is formed on a single chip. Krishna as discussed above with respect to Claim 4 discloses forming a security processor including a switching system, a packet engine and a cryptographic core as well as other functions on a single chip. It would have been obvious to combine the teachings of Krishna with the system of Pham in view of Wu for the same reasons I discussed above with respect to Claim 4.

CONCLUSION AND DECLARATION

My findings and opinions set forth in this Declaration are based on my work and examination to date. I may continue my examinations in view of additional documents or other factual evidence over the course of this proceeding that may necessitate supplementing and/or refining my opinions. I reserve the right to add to, alter, or delete my opinions and my Declaration upon discovery of additional information. I reserve the right to make such changes as necessary.

In signing this Declaration, I understand that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in this case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and 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 Section 1001, of Title 18 of the United States Code.

[SIGNATURE ON FOLLOWING PAGE]

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page090

Date:_3/6/2023__ By: _____

Mark E. Crovella

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page091

APPENDIX A – MATERIALS RELIED UPON

Exhibit #	***Description***
1001	U.S. Patent No. 7,685,436 ("the '436 Patent")
1002	Prosecution history of the '436 Patent("'436 File History")
1004	U.S. 2003/0074473 ("Pham")
1005	U.S. 7,424,744 ("Wu")
1006	U.S. 7,996,670 ("Krishna")
1007	U.S. 6,279,113 ("Vaidya")
1008	U.S. Patent Publication 20020073316 ("Collins")
1009	U.S. 7,181,017 ("Nagel")
1010	US 2004/0039928A1 ("Elbe")
1011	Related Patents
1012	U.S. Patent No. 8,566,612 ("the '612 Patent")
1013	Prosecution history of the '612 Patent ("'612 File History")
1015	U.S. Patent Publication US 2003/0145225A1 ("Bruton")

APPENDIX B – RÉSUMÉ

MARK E. CROVELLA

Computer Science Department
Boston University
111 Cummington St
Boston, MA 02215
Office: (617) 353-8923
Department: (617) 353-8919

Date of Birth: October 28, 1959
Location: Buffalo, New York, USA
Nationality: USA

Current as of November 11, 2022

EDUCATION

Ph.D. Computer Science, University of Rochester, October 1994.

M.S. University of Rochester, May 1991.

M.S. State University of New York at Buffalo, May 1990.

B.S. Cornell University, May 1982.

SELECTED PROFESSIONAL EXPERIENCE

Professor Department of Computer Science, Boston University, 2006 to present. **Department Chair, Computer Science** 2013 – 2018; **Associate Professor** 2000 – 2006; **Assistant Professor** 1994 – 2000. On leave 2000 – 2001.

Professor Faculty of Computing & Data Sciences, Boston University, 2022 to present. **Chair of Academic Affairs, Faculty of Computing & Data Sciences** 2022 – present; **Founding Member, Faculty of Computing & Data Sciences**, 2020 – 2022; **Data Science Faculty Fellow** 2019 – 2022.

Chief Scientist Guavus, Inc., February 2012 to August 2014.

Technical Director Network Appliance, Tewksbury, MA. November 2000 to April 2002.

Chief Architect Webmanage Technologies, Chelmsford, MA. May 2000 to acquisition by Network Appliance in November 2000.

Senior Computer Scientist Calspan Corporation, Buffalo, NY. August 1984 to August 1994.

LEGAL CONSULTING

The following are cases in which I provided consulting and was disclosed. This list may not include certain confidential information as per written agreements.

Visual Networks v. Paradyne, 2005, District of Maryland.
Retained by Sughrue Mion, Washington DC on behalf of Visual Networks.
Provided Report on validity of Visual Networks patents.
Subject area: Communications networks. Settled.

Akamai Technologies and MIT v. Limelight Networks, 2007 - 2008, District of Massachusetts.
Retained by Choate, Hall and Stewart, Boston MA on behalf of Akamai.
Provided Infringement Report, Noninfringement Rebuttal, Deposition on expert reports, Testimony at trial (3 days).
Subject area: Content delivery networks. All claims were found infringed; no claims were found invalid; $45M award of lost profits.

Interval Research v. Apple, Google, AOL, et al, 2011, US PTO.
Retained by O'Melveny & Myers, San Francisco on behalf of Apple.
Provided expert report in support of re-examination claim.
Subject area: Web browsers. Settled.

Straight Path IP Group v. Sony Et. Al., 2013, International Trade Commission and ED Virginia.
Retained by Wolf Greenfield, Boston MA on behalf of Sony.
Provided declarations in support of petitions for Inter Partes Review to USPTO.
Subject area: Video streaming technology.
Case number: 2:13-cv-00427. Filing Date: 8/1/2013.
Settled.

PersonalWeb v. Microsoft and Yahoo!, 2013-2014, Eastern District of Texas.
Retained by Haltom and Doan, and GreenbergTraurig on behalf of Yahoo!, and Microsoft.
Provided Invalidity Report on PersonalWeb patents, Deposition.
Subject area: Search engine technology.
Case number: 6:12-CV-658, 6:12-CV-663. Filing Date: 9/17/2012.
Settled.

RPX Corporation v. Cedatech Holdings, 2015, Patent Trial and Appeal Board.
Retained by Wolf Greenfield, Boston MA on behalf of RPX.
Provided declaration in support of petition for Inter Partes Review.
Subject area: Web browser and media technology.
Case number: IPR2015-00736. Filing Date: 2/13/2015.
Cedatech responded by disclaiming all patent claims.

Fortinet v. Sophos, 2015, Eastern District of Texas.
Retained by Quinn Emanuel on behalf of Fortinet.
Provided Reports on Invalidity and Noninfringement, Deposition.
Subject area: Security products.
Case number: 3:13-cv-05831-EMC. Filing Date: 12/16/2013.
Settled.

RPX v. Applications In Internet Time, 2015, Patent Trial and Appeal Board.
Retained by Wolf, Greenfield, Boston MA on behalf of RPX.
Provided Declaration in Support of Petition for IPR, Deposition.
Subject area: Application architecture.
Case number: IPR2015-01750. Filing Date: 8/17/2015.
PTAB instituted all claims.

Akamai v. Limelight, 2016-2017, Patent Trial and Appeal Board.
Retained by Choate, Hall & Stewart and WilmerHale, Boston, MA on behalf of Akamai.
Provided Declarations in Support of Petition for IPR, Deposition.
Subject area: Content delivery networks.
Case number: IPR2016-01011. Filing Date: 5/13/2016.
PTAB held all claims unpatentable..

Limelight v. Akamai, 2016-2017, Patent Trial and Appeal Board.
Retained by WilmerHale, Boston MA on behalf of Akamai.
Provided Declaration in Support of Patent Owner Preliminary Response.
Subject area: Content delivery networks.
Case number: IPR2016-01711. Filing Date: 9/6/2016.
PTAB held all claims unpatentable..

Finjan v. Symantec, 2017, Northern District of California.
Retained by Quinn Emanuel, Chicago IL on behalf of Symantec.
Provided Damages Rebuttal Report, Deposition.
Subject area: Security products.
Case number: 4:14-cv-02998. Filing Date: 6/30/2014.
Dismissed 3/5/2018.

Sound View Innovations v. Hulu, 2017-2019, Central District of California.
Retained by O'Melveney & Myers on behalf of Hulu, LLC.
Provided Expert Reports on Noninfringement and Invalidity, Deposition.
Subject area: Database Technology.

Case number: LACV17-04146 JAK (PLAx). Filing Date: 6/2/2017.
Summary Judgment for Defendant.

RPX and Bank of America v. Publishing Technologies, 2018, PTAB.
Retained by Winston & Strawn on behalf of RPX Corporation.
Provided Declaration in support of Petition for Inter Partes Review.
Subject area: Content Management System.
Case number: IPR2018-01131 and IPR2018-01132. Filing Date: 5/31/2018.
PTAB held all claims unpatentable.

Intellectual Ventures v. BITCO and Great West (Old Republic), 2015-2019, Eastern District of Texas.
Retained by Sidley Austin on behalf of BITCO and Great West.
Provided Expert Reports on Invalidity and Noninfringement, Deposition, Testimony at Trial.
Subject area: Web Technology.
Case number: 6:18-cv-00298. Filing Date: 1/20/2015.
Jury Trial March 2019; ruling for plaintiff.

Centripetal Networks, Inc. v. Cisco Systems, Inc., 2019, Eastern District of Virginia, Norfolk.
Retained by Duane Morris on behalf of Cisco.
Provided Expert Reports on Invalidity and Noninfringement, Deposition, Testimony at Trial.
Subject area: Security Products.
Case number: 2:18-cv-00094-HCM-LRL. Filing Date: 3/29/2018.
Bench Trial May-June 2020; ruling for plaintiff.

British Telecommunications PLC v. Fortinet LLC, 2019, PTAB.
Retained by Duane Morris on behalf of Fortinet.
Provided Declaration in Support of IPR.
Subject area: Distributed Network Management.
Case number: IPR2019-01323. Filing Date: 7/11/2019.
PTAB denied institution.

Express Mobile v. Magento (X.commerce), 2019, Northern District of California.
Retained by Sidley Austin on behalf of Magento.
Provided Expert Reports on Invalidity and Ensnarement, Deposition.
Subject area: Web Authoring Software.
Case number: 17-cv-02605-RS. Filing Date: 2019.
Ongoing.

Ohio State Innovation Foundation v. Akamai, 2019, District of Massachusetts, PTAB.
Retained by Farella Braun & Martell on behalf of Akamai.
Provided Declaration in Support of IPR.
Subject area: Content Distribution and Prefetching.
Case number: 1:19-cv-11528. Filing Date: 2019.
Settled.

Askeladden v. Lightwire, 2020, PTAB.
Retained by Wilmer Hale on behalf of Askeladden.
Provided Declaration in Support of IPR.
Subject area: Identity Management in E-commerce. Filing Date: 2020.
PTAB Granted Institution.

CA, Inc. and Avago Technologies International Sales Pte. Limited v. Netflix Inc., 2020, Eastern District of Texas.
Retained by Keker, Van Nest & Peters on behalf of Netflix.
Provided Expert Reports on Invalidity and Non-infringement; Submitted Declaration on Claim Construction.
Subject area: Video Streaming.
Case number: 2:21-CV-80-JRG-RSP. Filing Date: 2021.

Sable Networks Inc et al v. Juniper Networks, Inc., 2020, Western District of Texas.
Retained by Farella Braun + Martell, LLP on behalf of Juniper.
Provided Prior Art Search and Analysis.
Subject area: Network Switch Technology.
Case number: 6:20-cv-00524. Filing Date: 2020.
Settled December 2020.

Sable Networks Inc et al v. Cloudflare, 2021, Western District of Texas.
Retained by Farella Braun + Martell, LLP on behalf of Cloudflare.
Provided Prior Art Search, Declaration in IPR.
Subject area: Network Switch Technology.
Case number: 6:21-cv-00261. Filing Date: 2021.

Eolas v. Amazon et al., 2021, Northern District of California.
Retained by Latham and Watkins, LLP on behalf of Amazon.
Provided Report on Invalidity, Deposition.
Subject area: Web Browser Technology.
Case number: 4-17-cv-03022. Filing Date: 2017.
Summary Judgment of Invalidity under Sec 101, May 2022.

RightQuestion, LLC v. Samsung Electronics Co., et al, 2021, Eastern District of Texas.
Retained by O'Melveny and Myers LLP on behalf of Samsung.
Provided IPR Declaration, Invalidity Report, Deposition.
Subject area: Authentication Management.
Case number: 2:21-cv-00238. Filing Date: 2021.

IBM v. Rakuten, 2021-2022, PTAB.
Retained by GreenbergTraurig, LLP on behalf of Rakuten.
Provided Declaration in Support of IPR.
Subject area: Personalization Methods.
Case number: IPR2022-00439. Filing Date: 2021.

IBM v. Rakuten, 2021-2022, PTAB.
Retained by GreenbergTraurig, LLP on behalf of Rakuten.
Provided Declaration in Support of IPR.
Subject area: Authentication Methods.
Case number: IPR2022-00646. Filing Date: 2022.

IBM v. Rakuten, 2022, District of Delaware.
Retained by GreenbergTraurig, LLP on behalf of Rakuten.
Provided Declaration in Support of Claim Construction.
Subject area: .
Case number: 1:21-00461. Filing Date: 2021.

PATENTS HELD

Methods for storing and reading digital data on a set of DNA strands, US Patent # 10,027,347, issued July 17, 2018.

Method and Apparatus for Whole-Network Anomaly Diagnosis and Method to Detect and Classify Network Anomalies Using Traffic Feature Distributions, US Patent # 8,869,276, issued October 21, 2014.

Compressed Set Representation for Sets as Measures in OLAP Cubes, US Patent # 8,533,167, issued September 10, 2013.

Method and Apparatus for Dynamic Resource Discovery and Information Distribution in a Data Network, US Patent # 7,747,741, issued June 29, 2010.

System for Creating and Distributing Prioritized List of Computer Nodes Selected as Participants in a Distribution Job, US Patent # 7,346,682, issued March 18, 2008.

Method and Apparatus for Election of Group Leaders in a Distributed Network, US Patent # 6,993,587, issued January 31, 2006.

Method and Apparatus for Scalable Distribution of Information in a Distributed Network, US Patent # 6,748,447, issued June 8, 2004.

Method and Apparatus for Reliable and Scalable Distribution of Data Files in Distributed Networks, US Patent # 6,718,361, issued April 6, 2004. European Patent # EP1305924 issued March 31, 2010.

Distributed Routing, US Patent # 6,370,584, issued April 9, 2002.

Method and Apparatus for Assigning Tasks in a Distributed Server System, US Patent # 6,223,205, issued April 24, 2001.

Selected Honors

Innovator of the Year, 2014, Boston University.

IEEE Fellow, 2011, "For contributions to the measurement and analysis of networks and distributed systems."

ACM Fellow, 2010, "For contributions to the measurement and analysis of networks and distributed systems."

Funding

Recipient of over 25 research grants from NSF, ARO, NGIA, Sprint, GTE, Xerox, and Hewlett-Packard totalling over $13.8 M.

Selected Professional Activities

Scientific Advisory Board of the Max Plank Institute for Software Systems, 2016 – present.

General Co-Chair, CoNEXT 2011.

Chair, ACM SIGCOMM 2007–2009.

Program Co-Chair, IFIP Networking 2010.

Program Committee Chair, Internet Measurement Conference 2003.

Books

M. Crovella and B. Krishnamurthy, "Internet Measurement: Infrastructure, Traffic, and Applications," John Wiley and Sons, 2006, 512 pp.

Published Articles

Author of over 200 published articles in Computer Science, cited more than 30,000 times according to Google Scholar.

Cisco Systems, Inc. v. Lionra Technologies Ltd
EX-1003 page098