

安全回應。

如果由安全引擎 110 鑑別週邊密碼鍵 142，方法 500 進至區塊 516，其中安全引擎韌體 152 使用現已鑑別的週邊密碼鍵 142 來鑑別週邊韌體 140。例如，在其中韌體 140 係經加密的實施例中，安全引擎 110 解密韌體 140。另外或或者，安全引擎 110 可使用週邊密碼鍵 142 基於例如韌體 140 之散列函數或之類來確保韌體 140 已事先被簽署過。

在區塊 518 中，SOC 102 判定安全引擎 110 成功鑑別週邊韌體 140。若否，方法 500 進至區塊 514，其中產生週邊驅動器載入錯誤，並將硬體週邊保持在重設模式中。然而，如果週邊韌體 140 經鑑別，則方法 500 進至區塊 520，其中安全引擎韌體 152 載入經鑑別（且經解密）的硬體週邊韌體 140 到關聯的韌體受保護記憶體區域 202 中並從重設模式釋放硬體週邊 120。依此方式，僅由 SOC 102 載入並執行硬體週邊的經鑑別韌體。另外，僅經鑑別的硬體週邊能存取受保護記憶體區域 200 及包含在其中之經解密的媒體內容。

茲參照第 6 圖，在已鑑別過硬體週邊 120 後，SOC 102 可傳遞內容至多媒體平台 100 的使用者。要這樣做，SOC 102 可執行用於在受信賴資料路徑中傳遞內容媒體之方法 600。方法 600 以區塊 602 開始，其中由 SOC 載入任何數位版權管理（DRM）韌體。DRM 韌體可支援待於多媒體平台 100 上傳遞之媒體內容的解密操作。於 DRM 韌

體的載入期間，用於解密媒體內容之應用加密鍵 162 係儲存於記憶體 104 中。在該例示實施例中，應用加密鍵 162 係以經加密形式儲存於記憶體 104 的未受保護記憶體 160 中。另外，待傳遞至使用者之經加密媒體內容可儲存在未受保護記憶體 160 中。

在區塊 606 中，SOC 102 判定使用者是否已請求媒體內容之傳遞。若是，方法 600 進至區塊 608，其中安全引擎 110 從記憶體 104 之未受保護記憶體 160 擷取經加密應用鍵 162。在區塊 610 中，安全引擎 110 解密應用鍵 162，並在區塊 612 中將經解密的應用鍵儲存在安全引擎 110 的安全記憶體 154 中。之後，在區塊 614 中，安全引擎 110 使用經解密的應用鍵 162 來解密經加密的媒體內容，其可儲存在未受保護記憶體 160 中。經解密的媒體內容係儲存在串流訊框緩衝器受保護記憶體區域 204 中。

在區塊 618 中，經鑑別之硬體週邊 120 存取受保護記憶體區域 200 中之經解密媒體內容，並由各個經鑑別之硬體週邊 120 處理媒體內容並傳遞至 SOC 102 的 A/V 輸出 134 以供播放給多媒體平台 100 的使用者。如此，應可認知到經解密的應用鍵 162 及經解密的媒體內容從未被置於未受保護狀態中。

應可認知到上述系統以安全且受保護的方式傳遞媒體內容。例如，經解密的媒體內容及經解密的應用鍵 162 每當在解密狀態中時係儲存在受保護且安全的記憶體位置中。另外，僅經鑑別的硬體週邊 120 能存取受保護記憶體

區域 200，其中在處理供傳遞之內容期間儲存有經解密的媒體內容。依此方式，媒體內容在傳遞程序期間保全於 SOC 102 本身內。

雖已於圖及前面的說明中詳細繪示並說明本公開，這種繪示及說明應視為示範而非限制性，可理解到僅顯示並說明例示的實施例，且希望保護與本公開及所述之申請專利範圍一致之所有改變及修改。

【圖式簡單說明】

舉例但非以限制的方式在圖中繪示在此所述之發明。為了圖解之簡單及清楚，圖中所示之元件並非一定按照比例繪製。例如，為求清楚，可能相較於其他元件放大某些元件的尺寸。此外，適當時，在圖中重複參考標籤來指示相應或相似之元件。

第 1 圖為包括晶片系統（SOC）之多媒體平台的至少一個實施例之簡化區塊圖；

第 2 圖為第 1 圖之多媒體平台的記憶體控制器和記憶體之至少一個實施例的簡化區塊圖；

第 3 圖為第 1 圖之 SOC 的受保護媒體內容流之至少一個實施例的簡化區塊圖；

第 4 圖為用於在 SOC 中建立受保護記憶體區域的方法之至少一個實施例的簡化流程圖；

第 5 圖為用於鑑別 SOC 之硬體週邊的方法之至少一個實施例的簡化流程圖；及

第 6 圖為用於從 SOC 傳遞內容媒體的方法之至少一個實施例的簡化流程圖。

【主要元件符號說明】

- 100：多媒體平台
- 102：晶片系統（SOC）
- 104：平台記憶體
- 110：安全引擎
- 112：受保護記憶體
- 114：記憶體控制器
- 116：處理器核心
- 118：鏈結
- 120：硬體週邊
- 122：解多工器
- 124：視頻預解析器
- 126：視頻解碼器
- 128：顯示處理引擎
- 130：音頻數位信號處理器
- 132：視頻圖形
- 134：音頻/視頻 I/O
- 136：視頻解碼器
- 140：韌體
- 142：密碼鍵
- 150：安全鍵

152 : 安全引擎韌體

154 : 安全記憶體

160 : 未受保護記憶體

162 : 經加密應用鍵

170 : 長期資料貯存

172 : 通訊輸出

174 : 顯示器

176 : 音頻裝置

200 : 受保護記憶體區域

202 : 韌體受保護記憶體區域

204 : 訊框緩衝器受保護記憶體區域

206 : 音頻受保護記憶體區域

208 : 壓縮視頻受保護記憶體區域

210 : 安全引擎至輸送流解多工受保護記憶體區域

212 : 其他受保護記憶體區域

220 : 記憶體介面

300 : 受信賴資料路徑

302 : 主機軟體

304 : 經加密媒體內容

306 : A/V 流

308 : 音頻

310 : 經處理的音頻

312 : 壓縮視頻

314 : 經預解析之壓縮視頻

201340692

316 : 視 頻 畫 素

318 : 視 頻 畫 素

320 : 區 段 資 料

322 : 元 資 料

201340692

發明專利說明書

(本申請書格式、順序，請勿任意更動，※記號部分請勿填寫)

※申請案號：101147203

※申請日：101 年 12 月 13 日

※IPC 分類：H04N 21/4367 (2011.01)

一、發明名稱：(中文／英文)

G06F 21/10 (2013.01)

用以保護並安全地傳遞媒體內容之方法，裝置，及系統

Method, device, and system for protecting and securely delivering media content

二、中文發明摘要：

用以保護並安全地傳遞媒體內容之方法、裝置、及系統包括組態晶片系統(SOC)之記憶體控制器以建立受保護記憶體區域，使用該SOC之安全引擎來鑑別硬體週邊的韌體，並儲存該經鑑別韌體於該受保護記憶體區域中。該安全引擎可藉由鑑別用來加密該韌體之週邊密碼鍵來鑑別該韌體。僅經鑑別硬體週邊可存取該受保護記憶體區域。

201340692

三、英文發明摘要：

A method, device, and system for protecting and securely delivering media content includes configuring a memory controller of a system-on-a-chip (SOC) to establish a protected memory region, authenticating a firmware of a hardware peripheral using a security engine of the SOC, and storing the authenticated firmware in the protected memory region. The security engine may authenticate the firmware by authenticating a peripheral cryptographic key used to encrypt the firmware. Only authenticated hardware peripherals may access the protected memory region.

七、申請專利範圍：

1. 一種晶片系統設備，包含：

具有至少一個受保護區域之記憶體，以儲存至少經解密之媒體內容於其中；及

晶片系統，包含：

耦合到該記憶體之記憶體控制器，以實施該受保護記憶體區域之保護，使得僅許可該晶片系統之經鑑別週邊裝置存取該受保護區域；及

耦合到該記憶體控制器之安全引擎，以鑑別該晶片系統之硬體週邊的韌體來允許該硬體週邊存取該記憶體之該受保護記憶體區域。

2. 如申請專利範圍第 1 項所述之晶片系統設備，其中該安全引擎回應於被該安全引擎鑑別之該韌體而儲存該硬體週邊之該韌體於該受保護記憶體區域中，並允許自該受保護記憶體區域執行該韌體以啟動該硬體週邊。

3. 如申請專利範圍第 1 項所述之晶片系統設備，其中該韌體包含該硬體週邊之經加密韌體，

該安全引擎使用該安全引擎之安全密碼鍵來獲得該硬體週邊之週邊密碼鍵並鑑別該週邊密碼鍵。

4. 如申請專利範圍第 3 項所述之晶片系統設備，其中該安全引擎回應於使用該安全密碼鍵鑑別該週邊密碼鍵而使用該週邊密碼鍵來鑑別該經加密韌體。

5. 如申請專利範圍第 4 項所述之晶片系統設備，其中該安全引擎使用該週邊密碼鍵來解密該經加密韌體。

6. 如申請專利範圍第 5 項所述之晶片系統設備，其中該安全引擎將該經解密韌體儲存於該受保護記憶體區域中。

7. 如申請專利範圍第 1 項所述之晶片系統設備，其中該韌體包含經加密韌體，

該安全引擎使用已由該安全引擎之安全密碼鍵鑑別過的該硬體週邊之週邊密碼鍵來解密該硬體週邊的該經加密韌體。

8. 如申請專利範圍第 1 項所述之晶片系統設備，其中該安全引擎回應於接收傳遞媒體內容之請求而自記憶體擷取經加密應用鍵。

9. 如申請專利範圍第 8 項所述之晶片系統設備，其中該安全引擎以該安全引擎之安全密碼鍵解密該經加密應用鍵並儲存該經解密應用鍵於該受保護記憶體區域中。

10. 如申請專利範圍第 9 項所述之晶片系統設備，其中該安全引擎存取經加密媒體內容並使用該經解密應用鍵來解密該媒體內容。

11. 如申請專利範圍第 10 項所述之晶片系統設備，其中該安全引擎儲存該經解密媒體內容於該受保護記憶體區域中。

12. 如申請專利範圍第 11 項所述之晶片系統設備，其中該經鑑別硬體週邊存取該受保護記憶體區域以擷取該經解密媒體內容。

13. 如申請專利範圍第 11 項所述之晶片系統設備，

進一步包含複數經鑑別硬體週邊以傳遞該經解密媒體到該晶片系統之輸出，使得無未經鑑別硬體週邊存取該經解密媒體內容。

14. 一種方法，包含：

組態晶片系統之記憶體控制器以建立受保護記憶體區域，該受保護記憶體區域僅可被經鑑別硬體週邊存取；

使用該晶片系統之安全引擎來鑑別該晶片系統之硬體週邊的韌體；

回應於由該安全引擎鑑別該韌體而儲存該韌體於該受保護記憶體區域中；及

自該受保護記憶體區域執行該韌體來啟動該硬體週邊。

15. 如申請專利範圍第 14 項所述之方法，其中組態該記憶體控制器包含獲得受保護記憶體區域資訊並使用該經識別資訊來組態該記憶體控制器。

16. 如申請專利範圍第 15 項所述之方法，其中獲得受保護記憶體區域資訊包含獲得該受保護記憶體區域之位址範圍。

17. 如申請專利範圍第 15 項所述之方法，其中獲得受保護記憶體區域資訊包含獲得該受保護記憶體區域之位址範圍、該受保護記憶體區域之類型、及該受保護記憶體區域的至少一個屬性。

18. 如申請專利範圍第 15 項所述之方法，進一步包含使用該晶片系統之該安全引擎來驗證該受保護記憶體區

域資訊。

19. 如申請專利範圍第 14 項所述之方法，其中鑑別該硬體週邊的該韌體包含：

獲得該硬體週邊之週邊密碼鍵及該硬體週邊之經加密韌體，及

使用該安全引擎之安全密碼鍵來鑑別該週邊密碼鍵。

20. 如申請專利範圍第 19 項所述之方法，其中鑑別該韌體包含回應於使用該安全密碼鍵鑑別該週邊密碼鍵而使用該週邊密碼鍵來鑑別該經加密韌體。

21. 如申請專利範圍第 20 項所述之方法，其中鑑別該經加密韌體包含使用該週邊密碼鍵來解密該經加密韌體。

22. 如申請專利範圍第 21 項所述之方法，其中儲存該韌體包含儲存該經解密韌體於該受保護記憶體區域中。

23. 如申請專利範圍第 14 項所述之方法，其中鑑別該硬體週邊的該韌體包含使用已由該安全引擎之安全密碼鍵鑑別過的該硬體週邊之週邊密碼鍵來解密該硬體週邊的該經加密韌體。

24. 如申請專利範圍第 14 項所述之方法，進一步包含回應於接收傳遞媒體內容之請求而使用該安全引擎來自記憶體擷取經加密應用鍵。

25. 如申請專利範圍第 24 項所述之方法，進一步包含以該安全引擎之安全密碼鍵解密該經加密應用鍵並儲存該經解密應用鍵於該受保護記憶體區域中。

26. 如申請專利範圍第 25 項所述之方法，進一步包含存取經加密媒體內容並使用該經解密應用鍵來解密該媒體內容。

27. 如申請專利範圍第 26 項所述之方法，進一步包含儲存該經解密媒體內容於該受保護記憶體區域中。

28. 如申請專利範圍第 27 項所述之方法，進一步包含以經鑑別硬體週邊存取該受保護記憶體區域來擷取經解密媒體內容。

29. 如申請專利範圍第 27 項所述之方法，進一步包含傳遞該經解密媒體到該晶片系統之輸出，使得無未經鑑別硬體週邊存取該經解密媒體內容。

30. 一種媒體平台，包含：

包括複數指令之晶片系統，當執行該些指令時導致該晶片系統履行如申請專利範圍第 14 至 29 項中任一項所述之方法。

31. 一或更多個機器可讀取媒體，包含儲存於其上之複數指令，回應於執行該些指令而導致晶片系統履行如申請專利範圍第 14 至 29 項中任一項所述之方法。

32. 一種方法，包含：

組態晶片系統之記憶體控制器以建立受保護記憶體區域；

以該晶片系統之安全引擎接收硬體週邊之週邊密碼鍵及該硬體週邊之經加密軟體；

使用該安全引擎之安全密碼鍵來鑑別該週邊密碼鍵；

回應於該週邊密碼鍵經鑑別而使用該週邊密碼鍵來鑑別該經加密韌體；

儲存該經解密韌體於該受保護記憶體區域中；及

自該受保護記憶體區域執行該經解密韌體以自重設狀態釋放該硬體週邊。

33. 如申請專利範圍第 32 項所述之方法，進一步包含回應於接收傳遞媒體內容之請求而使用該安全引擎來自記憶體擷取經加密應用鍵。

34. 如申請專利範圍第 33 項所述之方法，進一步包含以該安全引擎之該安全密碼鍵解密該經加密應用鍵並儲存該經解密應用鍵於該受保護記憶體區域中。

35. 如申請專利範圍第 34 項所述之方法，進一步包含存取經加密媒體內容並使用該經解密應用鍵來解密該媒體內容。

36. 如申請專利範圍第 35 項所述之方法，進一步包含儲存該經解密媒體內容於該受保護記憶體區域中。

37. 如申請專利範圍第 36 項所述之方法，進一步包含以經鑑別硬體週邊存取該受保護記憶體區域來擷取經解密媒體內容。

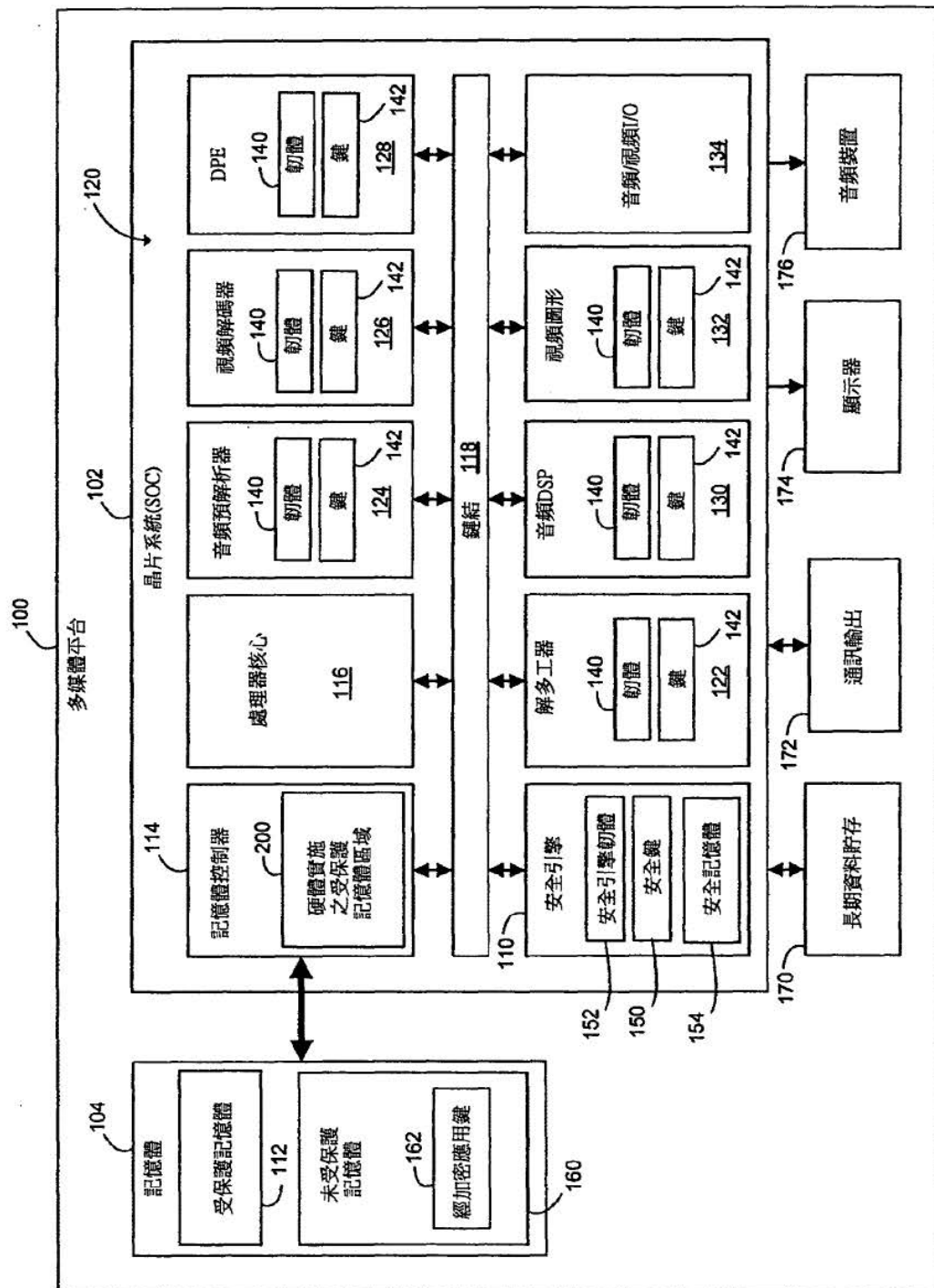
38. 如申請專利範圍第 36 項所述之方法，進一步包含傳遞該經解密媒體到該晶片系統之輸出，使得無未經鑑別硬體週邊存取該經解密媒體內容。

39. 一種媒體平台，包含：

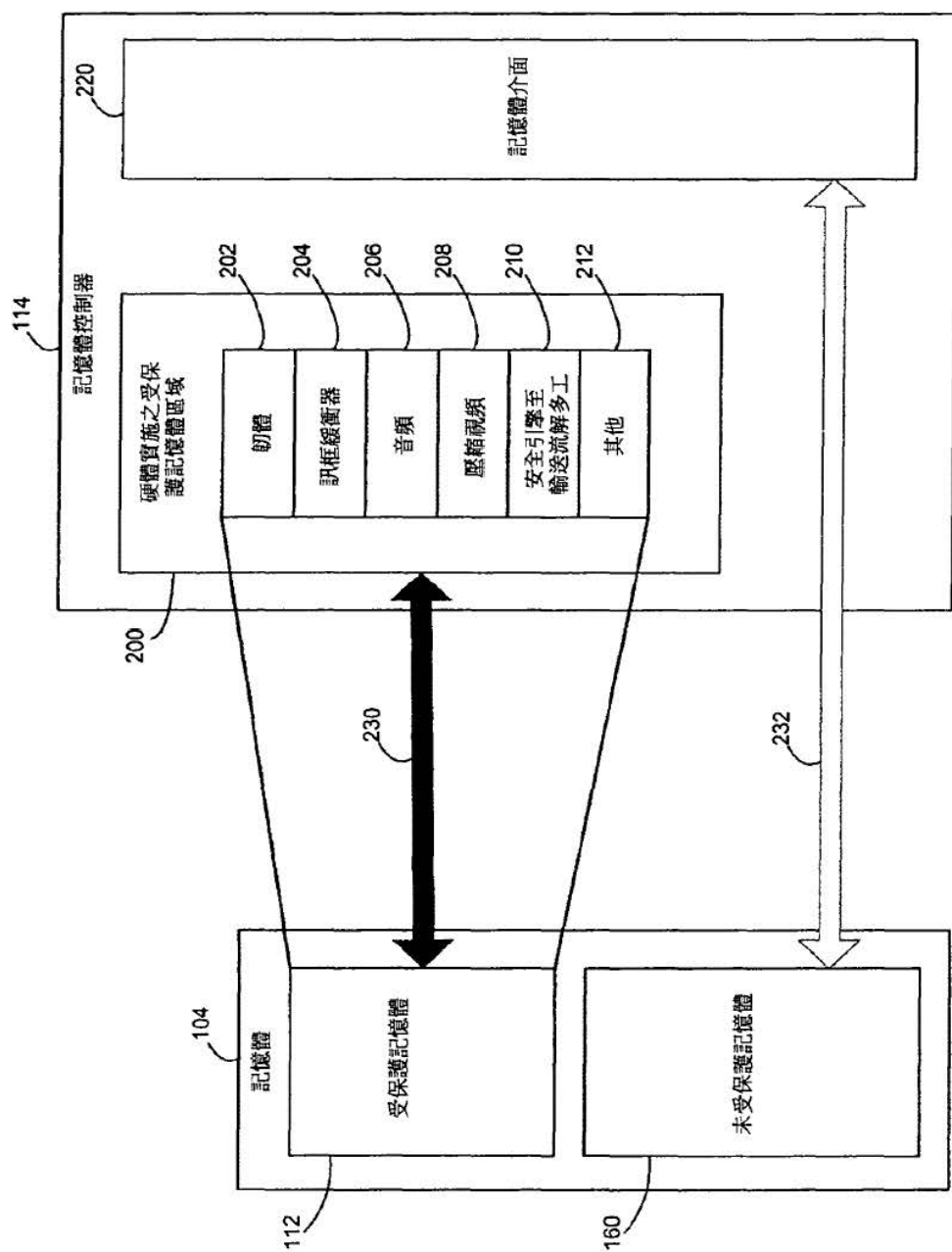
包括複數指令之晶片系統，當執行該些指令時導致該

晶片系統履行如申請專利範圍第 32 至 37 項中任一項所述之方法。

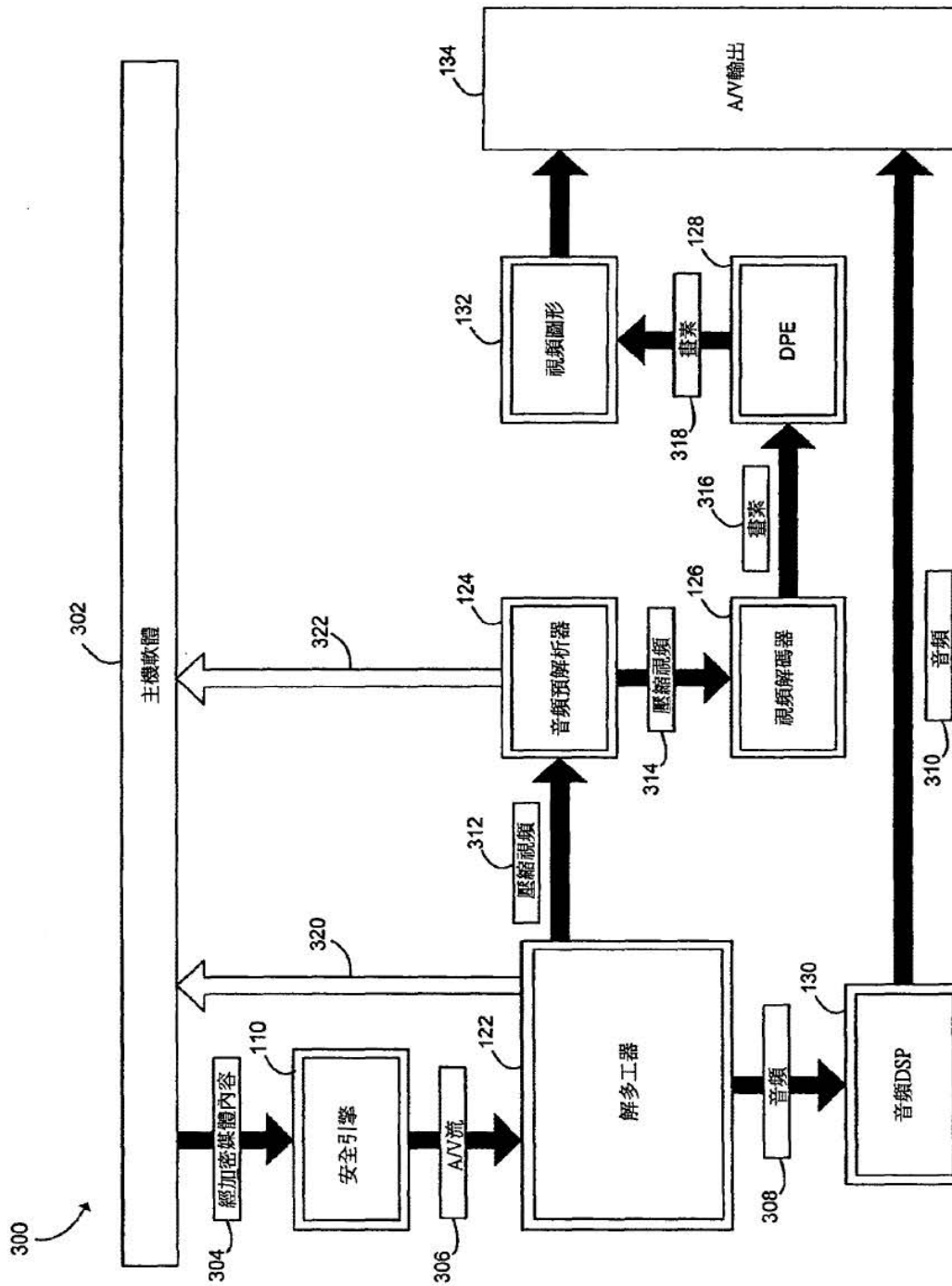
40. 一或更多個機器可讀取媒體，包含儲存於其上之複數指令，回應於執行該些指令而導致晶片系統履行如申請專利範圍第 32 至 37 項中任一項所述之方法。



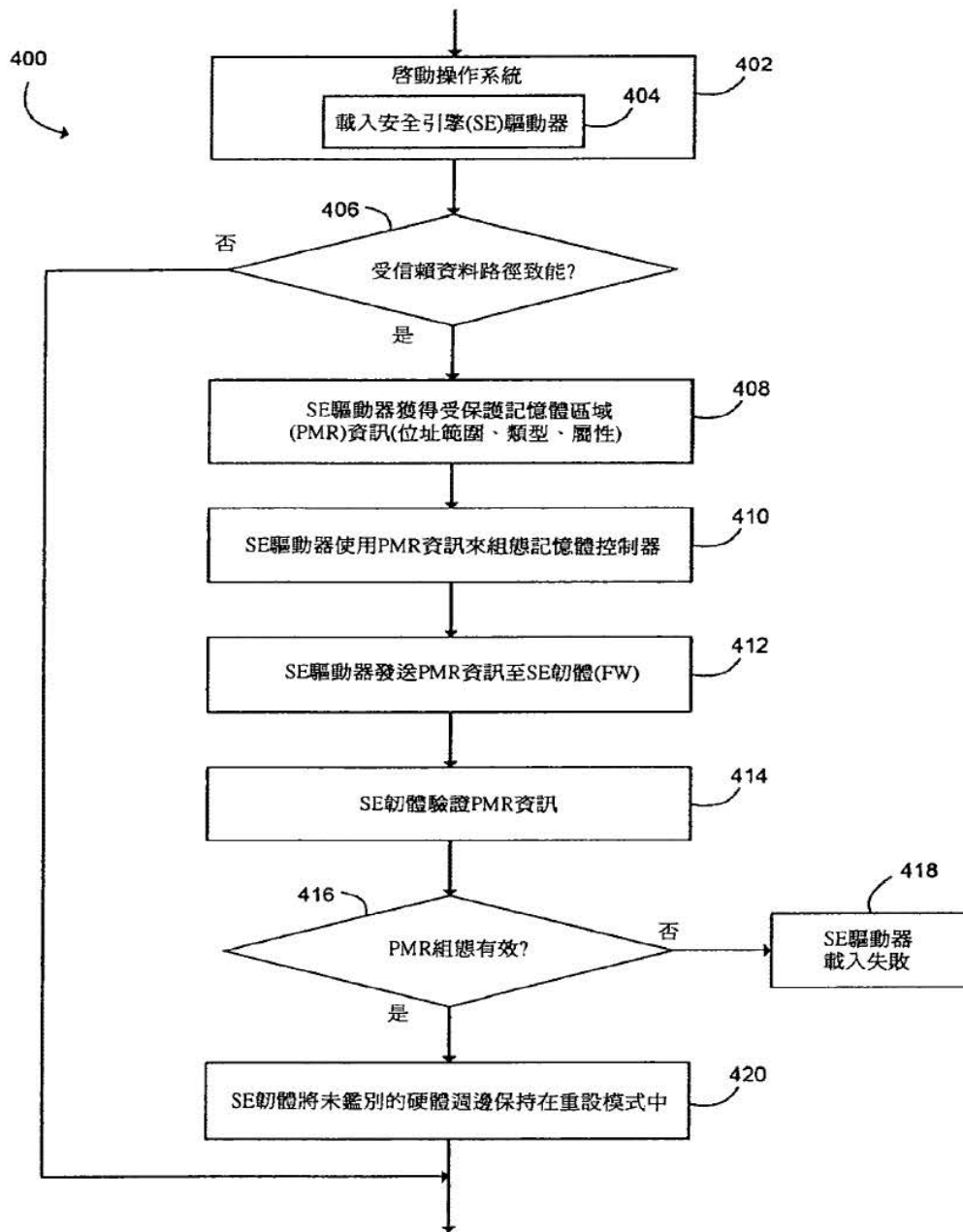
第1圖



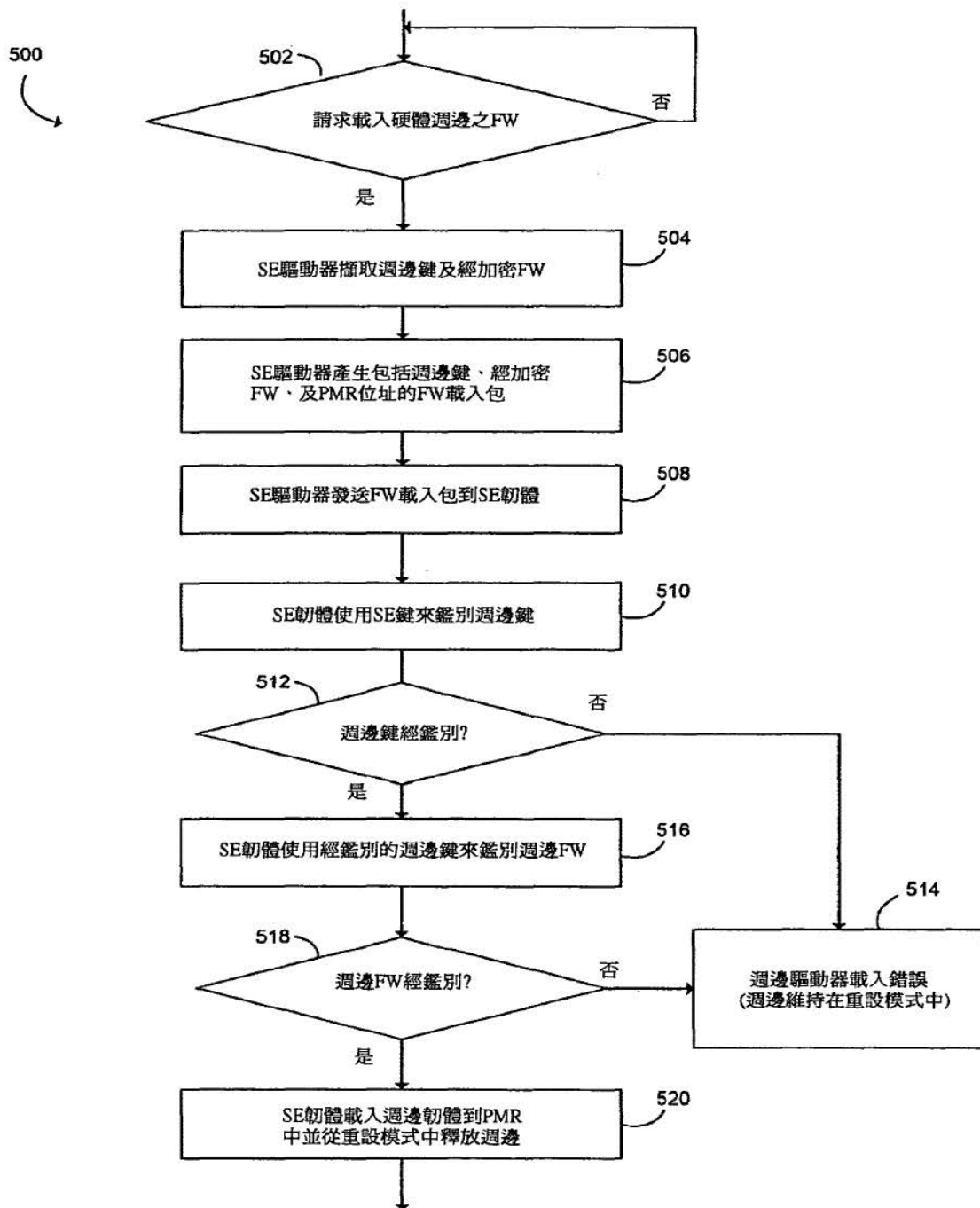
第2圖



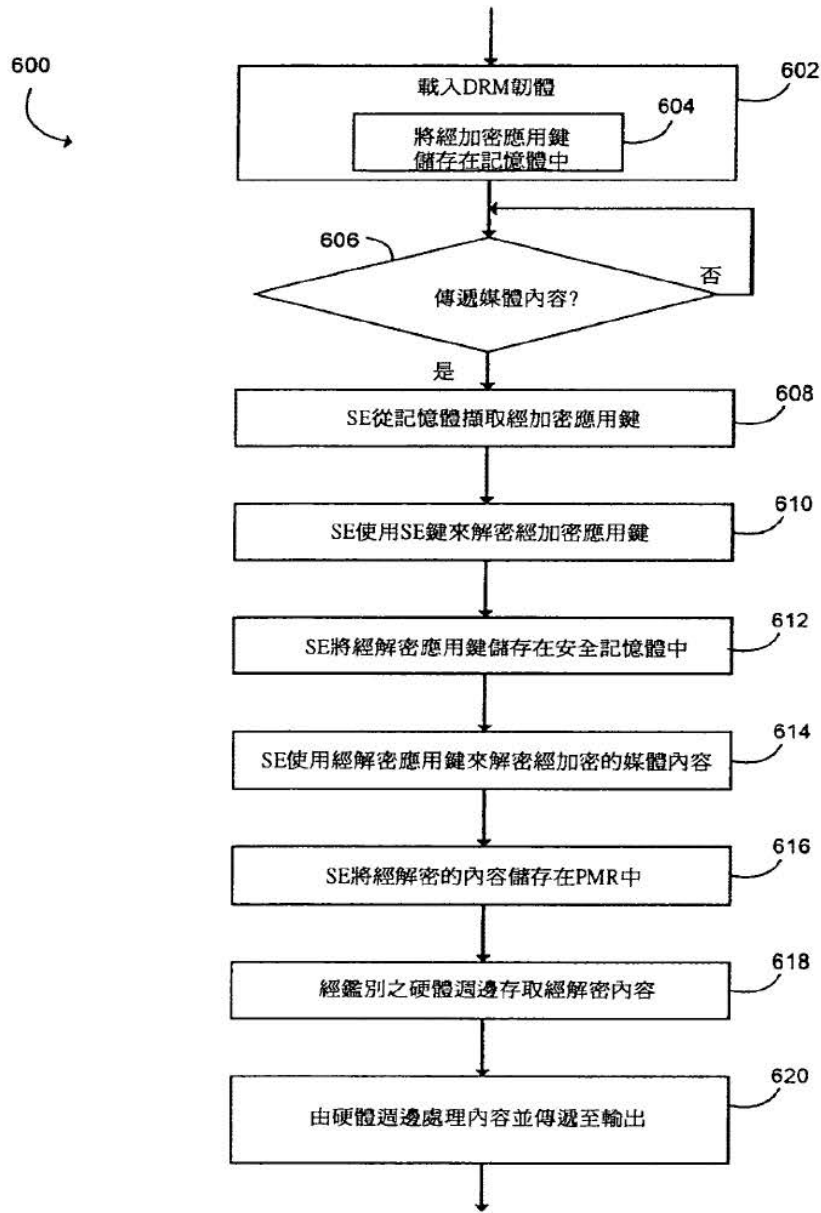
第3圖



第4圖



第5圖



第6圖

四、指定代表圖：

(一) 本案指定代表圖為：第 (1) 圖。

(二) 本代表圖之元件符號簡單說明：

100：多媒體平台
102：晶片系統 (SOC)
104：記憶體
110：安全引擎
112：受保護記憶體
114：記憶體控制器
116：處理器核心
118：鏈結
122：解多工器
124：音頻預解析器
126：視頻解碼器
130：音頻 DSP
132：視頻圖形
134：音頻 / 視頻 I/O
140：韌體
142：鍵
150：安全鍵
152：安全引擎韌體
154：安全記憶體
160：未受保護記憶體
162：經加密應用鍵
170：長期資料貯存
172：通訊輸出
174：顯示器
176：音頻裝置
200：硬體實施之受保護記憶體區域

201340692

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無

Electronic Acknowledgement Receipt	
EFS ID:	19136152
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Christopher A. Singh
Filer Authorized By:	
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	27-MAY-2014
Filing Date:	
Time Stamp:	17:12:25
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P41624US_SupplIDS.pdf	612446 ed2cc37fb7140f85726dd94bad22d1e90fd c73d	no	4

Warnings:

Information:

2	Foreign Reference	FR1.pdf	1293959 2e675262a929587dd0fa9667f25cfa754e55044f	no	37
Warnings:					
Information:					
Total Files Size (in bytes):				1906405	
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41624US/45631-225521		

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1	8645677	B2	2014-02-04	Khosravi et al.			
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1	20110023077	A1	2011-01-27	Simon			
	2	20080177998	A1	2008-07-24	Apsangi et al.			
	3	20060133604	A1	2006-06-22	Buer et al.			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2014074127	WO	A1	2014-05-15	Intel Corporation		☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412
	Filing Date		2013-06-24
	First Named Inventor	Hormuzd M. Khosravi	
	Art Unit	UNK	
	Examiner Name	UNK	
	Attorney Docket Number	P41624US/45631-225521	

If you wish to add additional Foreign Patent Document citation information please click the Add button				Add
NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵	
	1	International Preliminary Report on Patentability received for PCT International Application No. PCT/US2011/065069, mailed June 26, 2014, 8 pages.	☐	
If you wish to add additional non-patent literature document citation information please click the Add button				
EXAMINER SIGNATURE				
Examiner Signature		Date Considered		
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.				
¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.				

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2014-08-18
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

(51) International Patent Classification:
G06F 21/30 (2013.01)(21) International Application Number:
PCT/US2013/000253(22) International Filing Date:
7 November 2013 (07.11.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/694,221 8 November 2012 (08.11.2012) US

(71) Applicant (for all designated States except US): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95054 (US).

(72) Inventors; and

(71) Applicants (for US only): KHOSRAVI, Hormuzd, M. [IN/US]; 4816 NW 166th Ave, Portland, OR 97229 (US). LEE, David, A. [US/US]; 716 NE 28th Avenue, Portland, OR 97232 (US). SRINVASA RAGHAVAN, Raji [IN/US]; 3600 W Ray Rd, Apt #1012, Chandler, AZ 85226 (US).

(74) Agent: CHO, Lawrence, M.; Lawrence Cho, C/o Cpa Global, P.O. Box 52050, Minneapolis, MN 55402 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: AN IMPROVED IMPLEMENTATION OF ROBUST AND SECURE CONTENT PROTECTION IN A SYSTEM-ON-A-CHIP APPARATUS

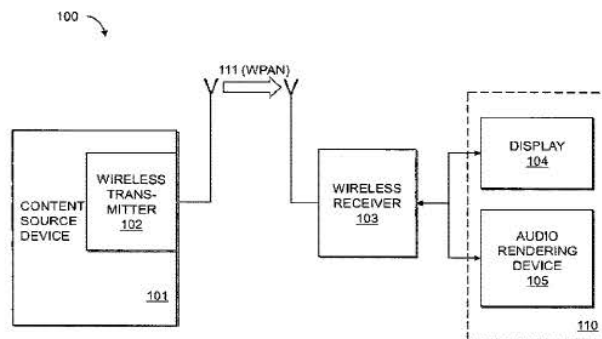


FIG. 1

(57) Abstract: A content processing integrated circuit includes a system-on-a-chip (SoC) that further includes a processor to receive an authentication request from an external device for authenticating if the SoC is permitted to receive encrypted content from the external device, and to receive the encrypted content once the SoC is authenticated. An authentication processor is provided and coupled to the processor to authenticate the SoC to the external device when the processor receives the authentication request, and to generate a decryption key for decrypting the encrypted content. A decryption processor is provided and coupled to the processor and the authentication processor to receive the decryption key from the authentication processor and to decrypt the encrypted content with the decryption key. A wireless display system with such SoC is also described. A method of implementing a secure and robust content protection in a SoC is also described.

AN IMPROVED IMPLEMENTATION OF ROBUST AND SECURE CONTENT
PROTECTION IN A SYSTEM-ON-A-CHIP APPARATUS

TECHNICAL FIELD

5 Embodiments of the present disclosure relate to secure content delivery and display. More specifically, embodiments of the present disclosure relate to an improved implementation of robust and secure content protection in a system-on-a-chip apparatus.

BACKGROUND

10 As is known, media content access by content users is changing from opportunistic access to on-demand access. On-demand media content, as well as some standard media content, is often delivered by streaming the content to a multimedia receiving platform, such as a set-top box, a smart phone, a computer tablet, a laptop computer, or the like, for content display. If the multimedia content is premium content, the multimedia content is often protected in some
15 manner during transmission to the multimedia receiving platform. For example, various Digital Rights Management (DRM) and Conditional Access (CA) technologies may be used to provide protection for the media content from the media source to the multimedia receiving platform. Such technologies generally involve encryption of the content media.

 A system-on-a-chip (SoC) device is an integrated circuit that incorporates various
20 components of electronic systems on a single die or substrate. For example, a SoC integrated circuit may include a processor core, memory, video components, audio components, and/or communication components on a single chip. Due to their relatively small size, SoCs are used in many multimedia receiving platforms.

25 BRIEF DESCRIPTION OF THE DRAWINGS

 The features and advantages of the disclosure are illustrated by way of example and are by no means intended to limit the scope of the disclosure to the particular embodiments shown.

 Figure 1 is an architectural overview of a wireless display system that includes a wireless system-in-a-chip (SoC) receiver according to an exemplary embodiment of the present
30 disclosure.

 Figure 2 illustrates the structure of a wireless SoC receiver of a wireless display system that includes a media engine, an authentication processor, and a decryption processor according to an exemplary embodiment of the present disclosure.

 Figure 3 illustrates the structure of an authentication processor of a wireless SoC receiver
35 of a wireless display system according to an exemplary embodiment of the present disclosure.

Figure 4 illustrates the structure of a decryption processor of a wireless SoC receiver of a wireless display system according to an exemplary embodiment of the present disclosure.

Figure 5 is the overview of a media engine of a wireless SoC receiver of a wireless display system according to an exemplary embodiment of the present disclosure.

5 Figure 6 is a flow chart diagram showing the procedure performed by a media engine of a wireless SoC receiver of a wireless display system for device authentication and content encryption according to an exemplary embodiment of the present disclosure.

10 Figure 7 is a flow chart diagram showing the procedure performed by an authentication processor of a wireless SoC receiver of a wireless display system for device authentication and key decryption according to an exemplary embodiment of the present disclosure.

Figure 8 illustrates the sequence and data flows between a wireless transmitter (without stored master key) and a wireless SoC receiver of a wireless display system during authentication of the receiver according to an exemplary embodiment of the present disclosure.

15 Figure 9 illustrates the sequence and data flows between a wireless transmitter (with stored master key) and a wireless SoC receiver of a wireless display system during authentication of the receiver according to an exemplary embodiment of the present disclosure.

Figure 10 illustrates the sequence and data flows between a wireless transmitter and a wireless SoC receiver of a wireless display system during locality check of the wireless SoC receiver according to an exemplary embodiment of the present disclosure.

20 Figure 11 illustrates the sequence and data flows between a wireless transmitter and a wireless SoC receiver of a wireless display system during session key exchange and decryption according to an exemplary embodiment of the present disclosure.

DESCRIPTION OF THE EMBODIMENTS

25 In the following description, for purposes of explanation, specific nomenclature is set forth to provide a thorough understanding of embodiments of the present disclosure. It will be apparent to one skilled in the art that specific details in the description may not be required to practice the embodiments. In other instances, well-known circuits, devices, and programs are shown in block diagram form to avoid obscuring embodiments of the present disclosure
30 unnecessarily.

Figure 1 illustrates an overall architecture of a wireless display system 100 that includes a content source device 101 with a transmitter 102 and a wireless system-on-a-chip (SoC) receiver 103 that implement a secure and robust content protection scheme according to embodiments of the present disclosure. Figures 2-7 illustrate the structure and operations of various components

of such a SoC receiver integrated circuit as the SoC receiver 103 of Figure 1 and Figures 8-11 show sequences and data flows between devices of the wireless display system 100.

Prior to the wireless display system 100, various Digital Rights Management (DRM) and Conditional Access (CA) technologies have been used to provide protection for the media content from the media source to the media receiving devices. High-bandwidth Digital Content Protection (HDCP) is one such technology offered by Digital Content Protection LLC. The technology is developed to prevent copying of digital audio and video content as the content travels across connections. These connections include Digital Visual Interface (DVI) and High Definition Multimedia Interface (HDMI).

One of the functions of the HDCP protocol is to authenticate receiving devices and generate or exchange decryption keys for the receiving devices during authentication. If the receiving device is authenticated as authorized to receive HDCP-encrypted content, the corresponding transmitter encrypts the content data to prevent eavesdropping as the content data travel to the receiving device. The receiving device then decrypts the encrypted content data using the decryption key generated or exchanged.

One prior way of implementing the HDCP authentication and key exchange functions is in software form running on a processor of the receiving device. One problem associated with this prior approach is that the keys are not secure and easy to be “discovered” or hacked by malware or spyware. This is due to the fact that the keys are stored at software level and need to be accessible to various software codes and the underlying operating system running on the processor, which makes it possible for unauthorized access to these keys via malware or spyware.

Figure 2 illustrates the structure of a SoC receiver integrated circuit 200 that may implement the wireless SoC receiver 103 of Figure 1 to provide secure and robust content protection in accordance with one embodiment of the present disclosure. According to one embodiment of the present disclosure and as will be described in more detail below, the SoC receiver integrated circuit 200 includes an authentication processor 206 and a decryption processor 208 in addition to a media engine 201 that includes a processor 202 and a memory 203. The memory 203 stores software code to be executed on the processor 202. The media engine 201 (i.e., the processor 202) does not perform the device authentication and decryption key generation or exchange functions. It also does not perform the content decryption operation using the decryption key. Instead, these device authentication and decryption key generation or exchange functions are delegated to the authentication processor 206 and the content decryption using the decryption key function is delegated to the decryption processor 208.

In addition, the decryption key, once generated in the authentication processor 206, is not sent to the processor 202 of the media engine 201. Instead, the decryption key is stored in a processor register (i.e., register 207) of the authentication processor 206 and is shared with the decryption processor 208 via backdoor key loading. According to an embodiment of the disclosure, the backdoor key loading technique refers to a procedure where two components or processors securely sharing secret information via hardware level registers that are shared between the two components or processors. In the present embodiment, the authentication processor 206 and the decryption processor 208 “share” processor register (e.g., register 207) of the authentication processor 206, which provides a secure channel for sharing the secret decryption key between the two processors. In other words, the decryption processor 208 has access to the processor register (e.g., the register 207) of the authentication processor 206 that stores the secret and decrypted decryption key.

One advantage of the above described implementation is that by employing the authentication processor 206 (instead of the processor 202), none of the software code running on the processor 202 can have access to the authentication process, thus making the authentication and decryption key exchange process robust and secure.

Another advantage of the above described implementation is that the decryption key is not exposed to any software code running on the processor 202 as the key is not received in the processor 202, thus avoiding the possibility of being hacked or accessed via malware or spyware running in the media engine 202. This provides secure and robust content protection for the SoC receiver integrated circuit 200, as well as the wireless display system 100 of Figure 1. The wireless display system 100 and the SoC receiver integrated circuit 200 (Figure 2) will be described in more detail below, also in conjunction with Figures 1 through 11.

Throughout the specification, the following terms are defined as follows.

The term “content”, “media content”, or “multimedia content” refers to a combination of text, audio, still image, animation, video, and/or interactive content.

The term “wireless”, “wirelessly”, or “wireless communication” refers to the electronic transfer of information between two or more points that are not physically connected.

The term “display” refers to content rendering, and is not limited to visual displaying or rendering. It can refer to displaying of (or visual rendering of) video or audio content. It can also refer to rendering audio content via a speaker or an earphone.

The term “SoC (system-on-a-chip)” refers to an integrated circuit that incorporates various components of electronic systems on a single die or substrate. For example, a SoC may include one or more processors, memories, microprocessors, microcontrollers, video components, audio components, and/or communication components on a single chip.

The term “processor” refers to a data processing circuit that can be a microprocessor, a co-processor, a microcontroller, a microcomputer, a central processing unit, a field programmable gate array (FPGA), a programmable logic circuit, and/or any circuit that manipulates signals (analog or digital) based on operational instructions that are stored in a memory.

5 The term “memory” refers to a storage circuit or multiple storage circuits such as read-only memory, random access memory, volatile memory, non-volatile memory, static memory, dynamic memory, flash memory, cache memory, and/or any circuit that stores digital information.

10 In general, schematic elements used to represent instruction blocks may be implemented using any suitable form of machine-readable instruction, such as software or firmware applications, programs, functions, modules, routines, processes, procedures, plug-ins, applets, widgets, code fragments and/or others, and that each such instruction may be implemented using any suitable programming language, library, application programming interface (API), and/or other software development tools. For example, some embodiments may be implemented using
15 Java, C++, and/or other programming languages. Similarly, schematic elements used to represent data or information may be implemented using any suitable electronic arrangement or structure, such as a register, data store, table, record, array, index, hash, map, tree, list, graph, file (of any file type), folder, directory, database, and/or others.

20 Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to obscure the disclosure. In addition, for ease of illustration, a single connecting
25 element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to effect the communication.

30 Referring to Figure 1, the wireless display system 100 is employed to transmit content from the content source device 101 to a content rendering system 110 of the wireless display system 100 for content rendering. The content can be a combination of text, audio, still image, animation, video, and/or interactive content. The content rendering system 110 is connected to the wireless receiver 103 via wire connection. The content rendering system 110 includes a
35 display 104 and an audio rendering device 105. The display 104 can be a television (TV)

display, a high definition TV (HDTV) display, a computer monitor or display, or a projection display. The audio rendering device 105 can be one or more speakers and/or earphones (including headsets).

The content source device 101 can be a smartphone, a tablet computer, a laptop computer, a desktop computer, a mobile Internet device, a set-top box, or other devices capable of generating or delivering media content. The content source device 101 may include a content generator (such as a DVD player) or may obtain the media content from a remote source on-demand via Internet.

The content source device 101 includes a wireless transmitter 102. The wireless transmitter 102 is used to transmit media content from the content source device 101 to the rendering system 110 via the wireless receiver 103. The wireless transmitter 102 communicates with the wireless receiver 103 using the same wireless communication protocol. The wireless communication technology or protocol employed can be Bluetooth (also known as IEEE 802.15.1 standard), Wi-Fi (also known as IEEE 802.11 standard), HomeRF (Home Radio Frequency standard), Infrared, ZigBee (also known as IEEE 802.15.4 standard). The content source device 101, including the transmitter 102, can be implemented using known means. Thus, their structure and operation will not be described in more detail below.

The wireless receiver 103 may be embodied in a set-top box, a smartphone, a smart display, a tablet computer, a laptop computer, a desktop computer, a mobile Internet device, or other device capable of delivering media content. The wireless receiver 103 may be configured to deliver any type of media content including, for example, movies, pictures, images, songs, audio and/or video recordings, and/or any other type of audio, video, and/or audio and video content.

The wireless network 111 is a wireless personal area network (WPAN) according to one embodiment of the present disclosure. In another embodiment, the wireless network 111 is a wireless local area network. In a further embodiment, the wireless network 111 can be a combination of wired and wireless networks.

Moreover, the wireless display system 100 may include one or more repeaters (not shown in Figure 1). A repeater includes a transmitter circuit like the transmitter 102 and a receiver circuit (like the receiver 103) combined together. It functions as a communication relay station between the transmitter 102 and the receiver 103.

In Figure 1, the wireless display system 100 is shown to have its content source device 101 communicate wirelessly with its wireless receiver 103 through the wireless network 111. This implements one embodiment of the present disclosure. However, the display system 100 is not limited to this wireless implementation. For example, the communication between the content

source device 101 and the receiver 103 can be a wired network or a combination of wired and wireless networks.

In accordance with one embodiment of the present disclosure, the media content transmitted between the transmitter 102 and the receiver 103 is protected or encrypted. One
5 protocol or standard for such content protection or encryption is the High-bandwidth Digital Content Protection (HDCP) standard. The HDCP standard has many versions, including HDCP 1.0 version and HDCP 2.0 version. As described above, HDCP is a content protection protocol that is used to protect media content.

In one embodiment, the HDCP content protection protocol utilizes cryptographic
10 techniques in accordance with the Advanced Encryption Standard (AES) which describes a symmetric encryption technique (also known as Rijndael algorithm) that can encrypt (encipher) and decrypt (decipher) information. A detailed description of the AES can be found in the Federal Information Processing Standards Publication 197 (FIPS PUB 197), dated November 26, 2001. In another embodiment, the HDCP content protection protocol utilizes asymmetric
15 cryptographic techniques.

Many modes of operations may be employed for the AES encryption and decryption operation. Modes of operation include Electronic Code Book (ECB), Cipher-Block Chaining (CBC), Output Feedback (OFB), Counter and Cipher-Feedback (CFB) that provide confidentiality for messages of arbitrary length. Other modes of operation such as Counter with
20 Cipher Block Chaining-Message Authentication Code (CCM), Galois Counter Mode (GCM) and Offset Codebook Mode (OCB) ensure both confidentiality and message integrity.

According to one embodiment of the present disclosure, the SoC circuit implementation of the receiver 103 provides a secure and robust authentication and content decryption for the content transmitted in the wireless display system 100. The structure and operation of the
25 receiver 103 will be described in more detail below, also in conjunction with Figures 2-11.

In Figure 2 and as described above, the wireless SoC receiver integrated circuit 200 may implement the wireless receiver 103 of Figure 1 according to an exemplary embodiment of the present disclosure. As shown in Figure 2, the wireless SoC receiver integrated circuit 200 includes the media engine 201, the authentication processor 206, and the decryption processor
30 208 according to an exemplary embodiment of the present disclosure. The media engine 201 includes the processor 202 and the memory 203. The processor 202 functions as the main processor of the wireless SoC receiver integrated circuit 200 while the memory 203 stores software program codes that are executed on the processor 202. The memory 203 may have a storage area that can be accessed by the authentication processor 206 and/or the decryption
35 processor 208. Other processors of the wireless SoC receiver integrated circuit 200 may function

as co-processors, mini-processors, or microcontrollers of the processor 202. In one embodiment, components of the wireless SoC receiver integrated circuit 200 reside on the same substrate or within the same chip.

In one embodiment, the processor 202 is a central processing unit (CPU) like
5 microprocessor. In another embodiment, the processor 202 is a simple data processing unit. The communication between the processor 202 and other processors like processors 206 and 208 is done using an inter-processor call communication protocol. The structure and function of the processor 202 may be implemented using known technology.

The wireless SoC receiver integrated circuit 200 includes a communication module 205
10 that implements communication protocols to effect the wireless communication of the wireless SoC receiver integrated circuit 200 with external devices. The communication protocols implemented may include TCP/IP (Transmission Control Protocol/Internet Protocol), UDP/IP (User Datagram Protocol/Internet Protocol), RTSP (Real Time Streaming Protocol), RTP (Real-time Transport Protocol), and MPEG-TS (Motion Picture Experts Group-Transport Stream).
15 The wireless communication technology employed can be Bluetooth, Wi-Fi, HomeRF, Infrared, and ZigBee. The structure and functions of the communication module 205 may be implemented using known technologies.

The wireless SoC receiver integrated circuit 200 also includes an audio module 211 and a video module 212. The audio module 211 is employed to process audio content data and send
20 the processed data to an external rendering device. The video module 212 is employed to process video content data and send it to an external rendering device. The structure and functions of these two modules are known and will not be described in more detail below.

All modules, components, or functional blocks within the wireless SoC receiver integrated circuit 200 are connected together via a communication link 204. The communication link 204
25 can be simply referred to as a link 204. In one embodiment, the link 204 is a simple common bus that is provided to pass data, information, and/or instructions among all the modules or components of the wireless SoC receiver integrated circuit 200. In another embodiment, the link 204 collectively represents various dedicated communication links or buses between any two components of the wireless SoC receiver integrated circuit 200. In this case, any pair of
30 components within the wireless SoC receiver integrated circuit 200 has a dedicated communication link or connection and the link 204 represents them all collectively. The link 204 can be implemented using any known bus technology or can simply be electrical connection wires.

According to one embodiment of the present disclosure, the media engine 201 (i.e., the
35 processor 202) does not perform the device authentication and decryption key generation or

exchange functions. It also does not perform the content decryption operation for the content received in the wireless SoC receiver integrated circuit 200. Instead, these device authentication and decryption key generation or exchange functions are delegated to the authentication processor 206 and the content decryption function is delegated to the decryption processor 208.

5 In addition, the decryption key, once generated in the authentication processor 206, is not sent to (or accessible by) the processor 202 of the media engine 201. Instead, the decryption key is stored in a processor register (i.e., register 207) and is shared only by the decryption processor 208 via backdoor key loading. As described above, the backdoor key loading technique refers to a procedure where two components or processors securely sharing secret information via
10 hardware level registers that are shared between the components or processors. In the embodiment of the SoC 200, the authentication processor 206 and the decryption processor 208 “share” processor register (e.g., register 207) of the authentication processor 206, which provides a secure channel for sharing the secret decryption key between the two processors. In other words, the decryption processor 208 has access to the processor register (e.g., the register 207)
15 of the authentication processor 206 that stores the secret and decrypted decryption key. This prevents the decryption key from being exposed to any software code running on the processor 202 as the key is not received by the processor 202. This reduces the possibility of being hacked or accessed via malware or spyware running in the media engine 202. This provides secure and robust content protection for the SoC receiver integrated circuit 200 (and thus the wireless
20 display system 100 of Figure 1).

Figure 3 illustrates the structure of an authentication processor 300 within a SoC integrated circuit according to an exemplary embodiment of the present disclosure. The authentication processor 300 may implement the authentication processor 206 of the SoC integrated circuit 200 of Figure 2. As can be seen from Figure 3, the authentication processor 300 includes a security
25 engine processor 301 and an in-processor memory 303 that stores content protection protocol software 302 and is only accessible by the security engine processor 301. In one embodiment, the content protection protocol software 302 implements the HDCP content protection protocol.

The security engine processor 301 may be embodied as a security co-processor or processing circuitry separate from the main processor of the SoC (e.g., the SoC 200 of Figure 2).
30 In one embodiment, the security engine processor 301 is a co-processor, a microcontroller, a microcomputer, and/or any circuit that manipulates signals (analog or digital) based on operational instructions that are stored in a memory. The security engine processor 301 includes a random number generator (not shown) and a processor register (i.e., the register 207 in Figure 2) that can be employed to store decrypted keys. The structure of the security engine processor
35 301 is known and thus will not be described in more detail below.

Figure 4 illustrates the structure of a decryption processor 400 that may implement the decryption processor 208 of Figure 2 according to an exemplary embodiment of the present disclosure. As can be seen from Figure 4, the decryption processor 400 includes a processor hardware circuit 401 and a memory 402 that stores software program codes 403 and 404 that are executed on the processor hardware circuit 401. The software program code 403 is a transport stream de-multiplexing software program and the software program code 403 implements content decryption function. In other words, the processor 400 performs both the transport stream de-multiplexing function to separate video from audio content and the content decryption function.

The processor hardware circuit 401 can be implemented by any known processor or microcontroller or co-processor and thus will not be described in more detail. The decryption software code 404 is HDCP-based decryption code and the decryption operation is known and will not be described in more detail below.

Figure 5 illustrates the structure of a media engine 500 that may implement the media engine 201 of Figure 2 according to an exemplary embodiment of the present disclosure. As illustrated in Figure 5, the media engine 500 includes processor hardware 501 and an operating system 502 running on the processor hardware 501. On top of the operating system 502, software program codes 503-506 are provided that are run on the operating system 502. The operating system 502 and codes 503-506 are stored in a memory (not shown in Figure 5) of the media engine 500.

Code 503 is an authentication control code that controls interaction and interfacing of the media engine 500 (i.e., the processor hardware 501) with other components (e.g., the authentication processor 206 of Figure 2) of the SoC circuit (i.e., the SoC circuit 200 of Figure 2) during authentication and key exchange. Code 503 implements the HDCP protocol. It may include a HDCP library and a HDCP library API (Application Programming Interface). It may also include security engine processor API and security engine processor driver, as well as HDCP inter-processor call communication protocol code.

Code 505 is a decryption control code that controls interaction and interfacing of the media engine 500 (i.e., the processor hardware 501) with other components (e.g., the decryption processor 208 of Figure 2) of the SoC circuit (i.e., the SoC circuit 200 of Figure 2) during decryption. Figure 6 shows the procedure and operation of the codes 503 and 505, which will be described in more detail below.

Figure 6 illustrates a procedure of device authentication, key decryption, and content decryption according to an exemplary embodiment of the present disclosure. The procedure

shown in Figure 6 may be performed by a processor 202 of Figure 2 and may be implemented by the authentication control code 503 of Figure 5.

The procedure starts at 601 at which the processor receives an AKE_init (Authentication and Key Exchange Initiation) message. The AKE_init message includes a 64 bit random number r_{tx} generated by the transmitter (e.g., the transmitter 102) and a message ID. The transmitter can also be referred to as the requester. The random number r_{tx} serves both as device ID of the transmitter and the authentication request.

At 602, the processor sends back a certificate $Cert_{rx}$ to the transmitter.

At 603, the processor receives an encrypted master key K_m . The master key K_m is generated and encrypted with a receiver public key $K_{pub_{rx}}$ at the transmitter/requester. As described above, this encryption operation is performed with RSA-1024 with RSA OAEP padding.

At 604, the processor sends r_{tx} and the encrypted master key K_m to an authentication processor (e.g., the authentication processor 206 of Figure 2). The master key K_m is then decrypted by the authentication processor (e.g., the processor 206 of Figure 2) with private key values that are in the Chinese Remainder Theorem Format. The decryption is carried out in the authentication processor using Chinese Remainder Theorem calculations. In addition, the authentication processor also calculates H' value (i.e., =HMAC-SHA256 (r_{tx} XOR REPEATER, K_d) after successfully decrypting the master key K_m . The H' value is sent to the transmitter for verifying if the authentication is successful. The processor is not involved in the decryption and H' 's value calculation operation.

In addition and at 604, the processor also sends back to the transmitter the random number r_{rx} . The random number r_{rx} serves as device ID of the receiver and the confirmation that the encrypted master key has been received in the receiver.

At 605, the processor receives confirmation from the transmitter whether the authentication is successful or not. If successful, the processor receives the locality check command r_n from the transmitter.

At 606, the processor causes the authentication processor to perform the locality check operation by sending r_n to the authentication processor. The authentication processor (e.g., the authentication processor 206 of Figure 2) then computes L' values (i.e., =HMAC-SHA256(r_n , k_d XOR r_{rx}). The L' values are then sent to the processor via a shared memory between the two processors. The L' values then sent back to the transmitter for verification with the L values calculated in the transmitter. For the successful completion of authentication and locality check, the computed L' values have to be transmitted to the transmitter within a predetermined time

period. When the transmitter initiates the message for the locality check, it sets up a watchdog timer. The message from the receiver should reach the transmitter within the time specified.

At 607, the processor receives an encrypted session key from the transmitter or requester. The session key is used by the decryption processor (e.g., the decryption processor 208 of Figure 2) to decrypt encrypted content sent by the transmitter. Thus, the session key is the decryption key.

The session key K_s is generated in the transmitter with a 64 bit pseudo-random number r_{iv} . The transmitter then performs key derivation to generate $dkey_2$. The transmitter then encrypts the 128 session key to be $E_{dkey}(K_s)=K_s \text{XOR}(dkey_2 \text{XOR} r_{rx})$. The transmitter then sends the encrypted session key K_s with the 64 bit pseudo-random number r_{iv} to the receiver and received by the processor.

The processor passes the encrypted session key K_s with r_{iv} to the authentication processor to decrypt the session key. The processor is not involved in the session key decryption and does not have access to the decrypted session key. This prevents software code running on the processor from accessing the decrypted session key. This provides secure and robust content protection for the wireless display system such as the system 100 of Figure 1.

At 608, the processor receives encrypted content from the transmitter, sends it to the decryption processor (e.g., the decryption processor 208) for decryption with the decrypted session key directly loaded to the authentication processor to the decryption processor via the backdoor key loading technique.

At 609, the processor receives the decrypted content and performs other content processing functions. The processor then sends the content to the external rendering device (e.g., the content rendering system 110 of Figure 1) for rendering.

Figure 7 illustrates a procedure of device authentication and key decryption according to an exemplary embodiment of the present disclosure. The procedure shown in Figure 7 may be performed by an authentication processor of a wireless SoC receiver of a wireless display system such as the authentication processor 206 of Figure 2.

The procedure starts at 701 at which the authentication processor receives an authentication request r_{tx} from the processor (e.g., the processor 202 of Figure 2). This is done by the software code (e.g., authentication control code 503 of Figure 5) stored in memory (e.g., the memory 203 of Figure 2). The software code writes the authentication request r_{tx} into a memory commonly shared by the processors (e.g., 202 and 206 of Figure 2) and the authentication processor copies r_{tx} into its internal memory through an AKE_init IPC call (i.e., an authentication and key exchange initialization inter-processor call).

At 702, the authentication processor receives an encrypted master key K_m . As described above, the master key K_m is encrypted with a public key $K_{pub_{tx}}$ in the transmitter (e.g., the transmitter 102 of Figure 1).

At 703, the authentication processor generates a random number r_{rx} using its random number generator. The random number r_{rx} is passed to the processor via an inter-processor call command.

At 704, the authentication processor decrypts the master key K_m with a private key $K_{priv_{rx}}$. The private key values used to decrypt the K_m are in the Chinese Remainder Theorem Format. The decryption is carried out in the authentication processor using Chinese Remainder Theorem calculations. In addition, the authentication processor calculates H' value (i.e., =HMAC-SHA256(r_{tx} XOR REPEATER, K_d)). The H' value is used by the transmitter to verify whether the authentication is successful or not. The H' value is then sent back to the processor by writing it in an output payload region of the shared memory between the processor and the authentication processor. The processor then sends the H' value to the transmitter for verification with H value calculated in the transmitter.

At 705, the authentication processor receives the locality check command r_n from the processor. This is done by the authentication control code running on the processor that writes the command in an input payload region of a memory shared by the two processors and then the authentication processor copies that command into its internal memory.

At 706, the authentication processor performs locality check by computing L' values (i.e., =HMAC-SHA256(r_n , k_d XOR r_{rx})). The L' values are then sent to the processor via a shared memory between the two processors. The processor then sends the L' values to the transmitter for verification with L values calculated in the transmitter. For the successful completion of authentication and locality check, the computed L' values have to be transmitted to the transmitter within a predetermined time period for the locality check to be successful.

At 707, the authentication processor receives an encrypted session key K_s and a 64 bit pseudo-random number r_{iv} .

At 708, the authentication processor decrypts the session key. This is done by first performing key derivation to generate $dkey_2$. Then the authentication processor decrypts the 128 bit session key K_s to be $E_{dkey}(K_s)$ XOR($dkey_2$ XOR r_{rx}). The authentication processor also calculates K_s XOR lc_{128} . The decrypted key is then stored in a processor register, waiting to be loaded to the decryption processor (e.g., the decryption processor 208 of Figure 2) via a backdoor key loading. Before the decrypted session key is loaded to the decryption processor, the decrypted session key is not accessible by software codes running on the processor (e.g., the processor 202 of Figure 2).

Figures 6-7 are flow charts illustrating procedures or functions according to embodiments of the present disclosure. The techniques illustrated in these figures may be performed sequentially, in parallel or in an order other than what is described. The techniques may be also be performed once or more times. It should be appreciated that not all of the techniques
5 described are required to be performed, that additional techniques may be added, and that some of the illustrated techniques may be substituted with other techniques.

Figure 8 illustrates the sequence and data flows between a wireless transmitter (e.g., the transmitter 102 of Figure 1) and a wireless SoC receiver (e.g., the receiver 103 of Figure 1) during authentication of the receiver according to an exemplary embodiment of the present
10 disclosure. In this example, the transmitter does not have a stored master key K_m for the receiver. This means that the transmitter and receiver are communicating with each other for the first time. Figure 9 illustrates the sequence and data flows between the transmitter (e.g., the transmitter 102 of Figure 1) and the SoC receiver (e.g., the receiver 103 of Figure 1) during authentication of the receiver according to an exemplary embodiment of the present disclosure.
15 In this example, the transmitter has a stored master key K_m for the receiver. This means that the transmitter and receiver have communicated with each other before. Figure 10 illustrates the sequence and data flows between (e.g., the transmitter 102 of Figure 1) and the SoC receiver (e.g., the receiver 103 of Figure 1) during locality check of the wireless SoC receiver according to an exemplary embodiment of the present disclosure. Locality check refers to determining that
20 the receiver is within a predetermined transmission range of the transmitter. Figure 11 illustrates the sequence and data flows between the transmitter (e.g., the transmitter 102 of Figure 1) and the SoC receiver (e.g., the receiver 103 of Figure 1) during session key exchange and decryption according to an exemplary embodiment of the present disclosure. These sequences and data flows will be described in more detail below.

25 In Figure 8, TX represents the transmitter side and RX represents the receiver side. Arrows indicate the data flow directions. The symbols above the arrow lines indicate data transmitted during authentication and key exchange. As can be seen from Figure 8, the transmitter first sends an AKE_init (Authentication and Key Exchange Initiation) message to the receiver to initiate the authentication operation. The AKE_init message includes a 64 bit random
30 number r_{tx} generated by the transmitter and a message ID. The random number r_{tx} serves both as device ID of the transmitter and the authentication request.

Upon receiving the AKE_init message, the receiver sends back a certificate $Cert_{rx}$. As described above in connection with Figures 2-7, this is done by the processor (e.g., the processor 202 of Figure 2) of the SoC receiver (e.g., the receiver 200). The certificate $Cert_{rx}$ is stored in a
35 flash memory of the receiver. The transmitter then verifies the $Cert_{rx}$, using public key $K_{pub_{dcp}}$.

At this time, the processor of the receiver also passes the random number r_{ix} to the authentication processor (e.g., the authentication processor 206 of Figure 2) to start the authentication and key exchange operation.

After the transmitter has verified the $Cert_{rx}$, the master key K_m is generated and encrypted with a receiver public key $K_{pub_{rx}}$. As described above, this encryption operation is performed with RSA-1024 with RSA OAEP padding.

The master key K_m is then sent to the receiver. The receiver has its authentication processor decrypt the encrypted master key K_m with a private key $K_{priv_{rx}}$. The private key values used to decrypt the K_m are in the Chinese Remainder Theorem Format. The decryption is carried out in the authentication processor (e.g., the processor 206 of Figure 2) using Chinese Remainder Theorem calculations.

The receiver, upon receiving the master key K_m , also generates a receiver random number r_{rx} and sends it to the transmitter. The generation of the random number r_{rx} is performed by a random number generator within the authentication processor of the receiver. The random number r_{rx} serves as device ID of the receiver and the confirmation that the encrypted master key has been received in the receiver.

The authentication processor of the receiver (e.g., the authentication processor 206 of Figure 2) then calculates H' value (i.e., $=HMAC-SHA256(r_{rx} XOR REPEATER, K_d)$). The processor of the receiver then sends the H' value to the transmitter. The transmitter computes H value and verifies whether $H=H'$. If so, the authentication is successful and the transmitter stores the master key K_m and $E(K_m, K_h)$. $E(K_m, K_h)$ is the pairing information which includes the master key K_m and hash of private key K_h of the receiver. If H is not equal to H' , the authentication of the receiver fails.

Referring to Figure 9, the transmitter has created the master key K_m and the sequences and data flows differ from that of Figure 8 in that there is no master key generation. Instead, there is a master key retrieval function to retrieve the stored pairing information $E(K_m, K_h)$ with receiver ID.

Referring to Figure 10, the transmitter (e.g., the transmitter 102 of Figure 1) initiates the locality check by generating and transmitting r_n to the receiver (e.g., the receiver 103 of Figure 1 or the receiver 200 of Figure 2). The authentication processor (e.g., the authentication processor 206 of Figure 2) then computes L' values (i.e., $=HMAC-SHA256(r_n, k_d XOR r_{rx})$). The L' values are then sent to the processor of the receiver (e.g., the processor 202 of Figure 2) via a shared memory between the two processors. The L' values are then sent back to the transmitter for verification with the L values calculated in the transmitter. For the successful completion of authentication and locality check, the computed L' values have to be transmitted to the

transmitter within a predetermined time period (e.g., as shown in Figure 10). When the transmitter initiates the message for the locality check, it sets up a watchdog timer. The message from the receiver should reach the transmitter within the time specified.

In Figure 11, after successful completion of authentication and locality check, the transmitter (e.g., the transmitter 102 of Figure 1) starts the procedure of session key exchange. The session key is used by the decryption processor (e.g., the decryption processor 208 of Figure 2) to decrypt encrypted content sent by the transmitter. Thus, the session key is the decryption key.

As can be seen from Figure 11, the transmitter initiates the procedure by generating the session key K_s and a 64 bit pseudo-random number r_{iv} . The transmitter then performs key derivation to generate $dkey_2$. The transmitter then encrypts the 128 session key to be $E_{dkey}(K_s) = K_s \text{ XOR } (dkey_2 \text{ XOR } r_{rx})$. The transmitter then sends the encrypted session key K_s with the 64 bit pseudo-random number r_{iv} to the receiver.

The authentication processor (e.g., the authentication processor 206 of Figure 2) then receives the encrypted session key K_s with r_{iv} , decrypts the session key. This is done by first performing key derivation to generate $dkey_2$. Then the authentication processor decrypts the 128 bit session key K_s to be $E_{dkey}(K_s) \text{ XOR } (dkey_2 \text{ XOR } r_{rx})$. The authentication processor also calculates $K_s \text{ XOR } lc_{128}$ and sends the decrypted session key to the decryption processor (e.g., the decryption processor 208 of Figure 2) via the backdoor key loading. Before the decrypted session key is loaded to the decryption processor, the decrypted session key is stored in a processor register of the authentication processor and is not accessible by software codes running on the main processor (e.g., the processor 202 of Figure 2). This provides secure and robust content protection for the wireless display system such as the system 100 of Figure 1.

Embodiments of the present disclosure may be provided as a computer program product, or software, that may include an article of manufacture on a machine accessible or machine readable medium having instructions. The instructions on the machine accessible or machine readable medium may be used to program a computer system or other electronic device. The machine-readable medium may include, but is not limited to, floppy diskettes, optical disks, CD-ROMs, and magneto-optical disks or other type of media/machine-readable medium suitable for storing or transmitting electronic instructions. The techniques described herein are not limited to any particular software configuration. They may find applicability in any computing or processing environment. The terms "machine accessible medium" or "machine readable medium" used herein shall include any medium that is capable of storing, or encoding a sequence of instructions for execution by the machine and that cause the machine to perform any one of the methods described herein. Furthermore, it is common in the art to speak of software,

in one form or another (e.g., code, program, procedure, process, application, module, unit, logic, block, and so on) as taking an action or causing a result. Such expressions are merely a shorthand way of stating that the execution of the software by a processing system causes the processor to perform an action to produce a result.

5 The following examples pertain to further embodiments. In one embodiment, a content processing integrated circuit includes a system-on-a-chip (SoC) that further includes a processor to receive an authentication request from an external device for authenticating if the SoC is permitted to receive encrypted content from the external device, and to receive the encrypted content once the SoC is authenticated. An authentication processor is provided and coupled to
10 the processor to authenticate the SoC to the external device when the processor receives the authentication request, and to generate a decryption key for decrypting the encrypted content. A decryption processor is provided and coupled to the processor and the authentication processor to receive the decryption key from the authentication processor and to decrypt the encrypted content with the decryption key.

15 In another embodiment, the authentication processor is a security engine processor separate from the processor and is coupled to the processor via a communication link.

 In yet another embodiment, the security engine processor further comprises a memory within the security engine processor that stores software instructions that, when executed by the security processor, implement a predetermined content protection protocol which is also
20 implemented by the external device.

 In a further embodiment, wherein the predetermined content protection protocol is High-bandwidth Digital Content Protection (HDCP) protocol.

 In a further embodiment, the authentication processor includes a processor register that stores the generated decryption key before the decryption key is sent directly to the decryption
25 processor. The decryption key is not sent to the processor and is not exposed to any software running on the processor.

 In a further embodiment, the decryption processor is separate from the processor and is coupled to the processor via a communication link. The decryption processor further performs a transport stream de-multiplexing function to separate video content from audio content in the
30 encrypted content before the encrypted content is decrypted.

 In a further embodiment, the decryption key is a session-based key that expires after a session is completed.

 In a further embodiment, the above-referenced content processing integrated circuit further comprises a wireless communication module coupled to the processor to receive the
35 authentication request and the encrypted content from the external device wirelessly and to pass

the authentication request and the encrypted content to the processor. The wireless communication module is also coupled to the authentication processor to communicate authentication information between the external device and the authentication processor.

In a further embodiment, a wireless display system includes a content source device to generated and transmit encrypted content wirelessly, a system-on-a-chip (SoC) wireless receiver to receive an authentication request from the content source device for authenticating if the receiver is permitted to receive the encrypted content and to receive the encrypted content once the receiver is authenticated, and a content rendering device coupled to the receiver to receive and display the decrypted content. The SoC wireless receiver further includes a processor coupled to receive the authentication request and the encrypted content, an authentication processor coupled to the processor to (1) authenticate the receiver to the content source device upon the processor receiving the authentication request and (2) generate a decryption key for decrypting the encrypted content, and a decryption processor coupled to receive the decryption key from the authentication processor and to decrypt the encrypted content with the decryption key.

In a further embodiment, the authentication processor is a security engine processor separate from the processor and is coupled to the processor via a communication link. The security engine processor further comprises a memory within the security engine processor that stores software instructions that, when executed by the security processor, implement a predetermined content protection protocol which is also implemented by the content source device to encrypt the encrypted content.

In a further embodiment, the predetermined content protection protocol is High-bandwidth Digital Content Protection (HDCP) protocol.

In a further embodiment, the authentication processor includes a processor register that stores the generated decryption key before the decryption key is sent directly to the decryption processor, wherein the decryption key is not sent to the processor and is not exposed to any software running on the processor.

In a further embodiment, the decryption processor is separate from the processor and is coupled to the processor via a communication link. The decryption processor further performs a transport stream de-multiplexing function to separate video content from audio content in the encrypted content before the encrypted content is decrypted.

In a further embodiment, the decryption key is a session-based key that expires after a session is completed.

In a further embodiment, the wireless display system further includes a wireless communication module coupled to the processor to receive the authentication request and the

encrypted content from the content source device wirelessly and to pass the authentication request and the encrypted content to the processor. The wireless communication module is also coupled to the authentication processor to communicate authentication information between the content source device and the authentication processor.

5 In a further embodiment, a method of providing secure and robust content protection in a system-on-a-chip (SoC) media processing apparatus includes receiving, in a processor of the SoC media processing apparatus, an authentication request from an external device for authenticating if the SoC media processing apparatus is permitted to receive encrypted content from the external device and to receive the encrypted content once the SoC media processing
10 apparatus is authenticated; causing the authentication processor to (1) authenticate the SoC media processing apparatus to the external device in accordance with a pre-determined content protection protocol and (2) generate a decryption key for the encrypted content encrypted according to the pre-determined content protection protocol; and receiving, by the processor, the encrypted content from the external device and sending the encrypted content to a decryption
15 processor of the SoC media processing apparatus to cause the decryption processor to decrypt the encrypted content with the decryption key received directly from the authentication processor once the SoC media processing apparatus is authenticated and the decryption key is generated.

 In a further embodiment, the above-referenced method further includes sending, by the processor, a certificate of the SoC media processing apparatus to the external device upon
20 receiving the authentication request.

 In a further embodiment, the above-referenced method further includes receiving an encrypted master key in the processor from the external device after sending the certificate; sending the encrypted master key to the authentication processor for decryption; receiving confirmation of decryption of the master key in the form of a random generated number from the
25 authentication processor; and sending the random generated number to the external device to confirm decryption and verification of the master key.

 In a further embodiment, the above-referenced method further includes causing the authentication processor to respond to a locality check request from the external device.

 In a further embodiment, wherein causing the authentication processor to generate a
30 decryption key for the encrypted content further includes receiving an encrypted session key from the external device; and sending the encrypted session key to the authentication processor for decryption to become the decryption key.

 In a further embodiment, the above-referenced method further includes causing the decryption processor to receive the decryption key directly from the authentication processor via

backdoor key loading once the SoC media processing apparatus is authenticated and the decryption key is generated and stored in the authentication processor.

In a further embodiment, a computer-readable medium having sequences of instructions, the sequences of instructions including instructions which, when executed, cause a processor to

5 perform device authentication and content decryption, which include receiving an authentication request from an external device for authenticating if the processor is permitted to receive encrypted content from the external device and to receive the encrypted content once the processor is authenticated; causing an external authentication processor separate from the processor to (1) authenticate the processor to the external device in accordance with a pre-

10 determined digital content protection protocol and (2) generate a decryption key for the encrypted content encrypted according to the pre-determined digital content protection protocol; receiving the encrypted content from the external device and causing a decryption processor separate from the processor to receive the decryption key directly from the authentication processor once the processor is authenticated and the decryption key is generated; and sending

15 the encrypted content to the decryption processor for decryption with the decryption key.

In a further embodiment, the decryption key is a decrypted session key encrypted at the external device and sent to the processor.

In a further embodiment, the above-referenced computer-readable medium further includes causing the decryption processor to receive the decrypted session key directly from the

20 authentication processor via backdoor key loading.

In a further embodiment, the above-referenced computer-readable medium further includes sending, by the processor, a certificate of the processor to the external device upon receiving the authentication request; receiving an encrypted master key in the processor from the external device after sending the certificate; sending, by the processor, the encrypted master key to the

25 authentication processor for decryption; receiving confirmation of decryption of the master key in the form of a random generated number from the authentication processor; and sending the random generated number to the external device to confirm decryption and verification of the master key.

In a further embodiment, the above-referenced computer-readable medium further includes

30 causing the authentication processor to respond to a locality check request from the external device.

In a further embodiment, wherein causing the authentication processor to generate a decryption key for the encrypted content further includes receiving an encrypted session key from the external device; and sending the encrypted session key to the authentication processor

35 for decryption to become the decryption key.

While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description are to be regarded as exemplary and not restrictive. It should be understood that only illustrative embodiments of the disclosure have been shown and described and that all changes and modifications consistent with the disclosure
5 and recited claims are intended to be protected.

CLAIMS

What is claimed is:

1. A content processing integrated circuit, comprising:
a system-on-a-chip (SoC) further comprising
5 a processor to receive an authentication request from an external device for authenticating if the SoC is permitted to receive encrypted content from the external device and to receive the encrypted content once the SoC is authenticated;
an authentication processor coupled to the processor to authenticate the SoC to the external device when the processor receives the authentication request, and to
10 generate a decryption key for decrypting the encrypted content once the SoC is authenticated; and
a decryption processor coupled to the processor and the authentication processor to receive the decryption key from the authentication processor and to decrypt the encrypted content with the decryption key.
15
2. The content processing integrated circuit of claim 1, wherein the authentication processor is a security engine processor separate from the processor and is coupled to the processor via a communication link.
- 20 3. The content processing integrated circuit of claim 2, wherein the security engine processor further comprises a memory within the security engine processor that stores software instructions that, when executed by the security processor, implement a predetermined content protection protocol which is also implemented by the external device.
- 25 4. The content processing integrated circuit of claim 3, wherein the predetermined content protection protocol is High-bandwidth Digital Content Protection (HDCP) 2.0 protocol.
5. The content processing integrated circuit of claim 1, wherein the authentication processor includes a processor register that stores the generated decryption key before the
30 decryption key is sent directly to the decryption processor, wherein the decryption key is not sent to the processor and is not exposed to any software running on the processor.
6. The content processing integrated circuit of claim 1, wherein the decryption processor is separate from the processor and is coupled to the processor via a communication
35 link, wherein the decryption processor further performs a transport stream de-multiplexing

function to separate video content from audio content in the encrypted content before the encrypted content is decrypted.

7. The content processing integrated circuit of claim 1, wherein the decryption key is
5 a session-based key that expires after a session is completed.

8. The content processing integrated circuit of claim 1, further comprising a wireless
communication module coupled to the processor to receive the authentication request and the
encrypted content from the external device wirelessly and to pass the authentication request and
10 the encrypted content to the processor, wherein the wireless communication module is also
coupled to the authentication processor to communicate authentication information between the
external device and the authentication processor.

9. A wireless display system, comprising:
15 a content source device to generate and transmit encrypted content wirelessly;
a system-on-a-chip wireless receiver to receive an authentication request from the content
source device for authenticating if the receiver is permitted to receive the encrypted content and
to receive the encrypted content once the receiver is authenticated, further comprising
a processor coupled to receive the authentication request and the encrypted
20 content;
an authentication processor coupled to the processor to (1) authenticate the
receiver to the content source device upon the processor receiving the authentication
request and (2) generate a decryption key for decrypting the encrypted content;
a decryption processor coupled to receive the decryption key from the
25 authentication processor and to decrypt the encrypted content with the decryption key;
and
a content rendering device coupled to the receiver to receive and display the decrypted
content.

10. The wireless display system of claim 9, wherein the authentication processor is a
security engine processor separate from the processor and is coupled to the processor via a
communication link, wherein the security engine processor further comprises a memory within
the security engine processor that stores software instructions that, when executed by the security
processor, implement a predetermined content protection protocol which is also implemented by
35 the content source device to encrypt the encrypted content.

11. The wireless display system of claim 10, wherein the predetermined content protection protocol is High-bandwidth Digital Content Protection (HDCP) 2.0 protocol.

12. The wireless display system of claim 9, wherein the authentication processor includes a processor register that stores the generated decryption key before the decryption key is sent directly to the decryption processor, wherein the decryption key is not sent to the processor and is not exposed to any software running on the processor.

13. The wireless display system of claim 9, wherein the decryption processor is separate from the processor and is coupled to the processor via a communication link, wherein the decryption processor further performs a transport stream de-multiplexing function to separate video content from audio content in the encrypted content before the encrypted content is decrypted.

14. The wireless display system of claim 9, wherein the decryption key is a session-based key that expires after a session is completed.

15. The wireless display system of claim 9, further comprising a wireless communication module coupled to the processor to receive the authentication request and the encrypted content from the content source device wirelessly and to pass the authentication request and the encrypted content to the processor, wherein the wireless communication module is also coupled to the authentication processor to communicate authentication information between the content source device and the authentication processor.

16. A method of providing secure and robust content protection in a system-on-a-chip (SoC) media processing apparatus, comprising:

receiving, in a processor of the SoC media processing apparatus, an authentication request from an external device for authenticating if the SoC media processing apparatus is permitted to receive encrypted content from the external device and to receive the encrypted content once the SoC media processing apparatus is authenticated;

causing the authentication processor to (1) authenticate the SoC media processing apparatus to the external device in accordance with a pre-determined content protection protocol and (2) generate a decryption key for the encrypted content encrypted according to the pre-determined content protection protocol; and

receiving, by the processor, the encrypted content from the external device and sending the encrypted content to a decryption processor of the SoC media processing apparatus to cause the decryption processor to decrypt the encrypted content with the decryption key received directly from the authentication processor once the SoC media processing apparatus is
5 authenticated and the decryption key is generated.

17. The method of claim 16, further comprising sending, by the processor, a certificate of the SoC media processing apparatus to the external device upon receiving the authentication request.
10

18. The method of claim 17, further comprising:
receiving an encrypted master key in the processor from the external device after sending the certificate;
sending the encrypted master key to the authentication processor for decryption;
15 receiving confirmation of decryption of the master key in the form of a random generated number from the authentication processor; and
sending the random generated number to the external device to confirm decryption and verification of the master key.

19. The method of claim 16, further comprising causing the authentication processor to respond to a locality check request from the external device.
20

20. The method of claim 16, wherein causing the authentication processor to generate a decryption key for the encrypted content further comprises:
25 receiving an encrypted session key from the external device; and
sending the encrypted session key to the authentication processor for decryption to become the decryption key.

21. The method of claim 16, further comprising causing the decryption processor to receive the decryption key directly from the authentication processor via backdoor key loading once the SoC media processing apparatus is authenticated and the decryption key is generated and stored in the authentication processor.
30

22. A non-transitory computer-readable medium having sequences of instructions, the sequences of instructions including instructions which, when executed, cause a processor to perform device authentication and content decryption, comprising:

receiving an authentication request from an external device for authenticating if the processor is permitted to receive encrypted content from the external device and to receive the encrypted content once the processor is authenticated;

causing an external authentication processor separate from the processor to (1) authenticate the processor to the external device in accordance with a pre-determined digital content protection protocol and (2) generate a decryption key for the encrypted content encrypted according to the pre-determined digital content protection protocol;

receiving the encrypted content from the external device and causing a decryption processor separate from the processor to receive the decryption key directly from the authentication processor once the processor is authenticated and the decryption key is generated; and

sending the encrypted content to the decryption processor for decryption with the decryption key.

23. The non-transitory computer-readable medium of claim 22, wherein the decryption key is a decrypted session key encrypted at the external device and sent to the processor.

24. The non-transitory computer-readable medium of claim 23, further comprising causing the decryption processor to receive the decrypted session key directly from the authentication processor via backdoor key loading.

25. The non-transitory computer-readable medium of claim 22, further comprising: sending, by the processor, a certificate of the processor to the external device upon receiving the authentication request;

receiving an encrypted master key in the processor from the external device after sending the certificate;

sending, by the processor, the encrypted master key to the authentication processor for decryption;

receiving confirmation of decryption of the master key in the form of a random generated number from the authentication processor; and

sending the random generated number to the external device to confirm decryption and verification of the master key.

26. The non-transitory computer-readable medium of claim 22, further comprising
5 causing the authentication processor to respond to a locality check request from the external device.

27. The non-transitory computer-readable medium of claim 22, wherein causing the authentication processor to generate a decryption key for the encrypted content further
10 comprises:

receiving an encrypted session key from the external device; and
sending the encrypted session key to the authentication processor for decryption to become the decryption key.

15

1/11

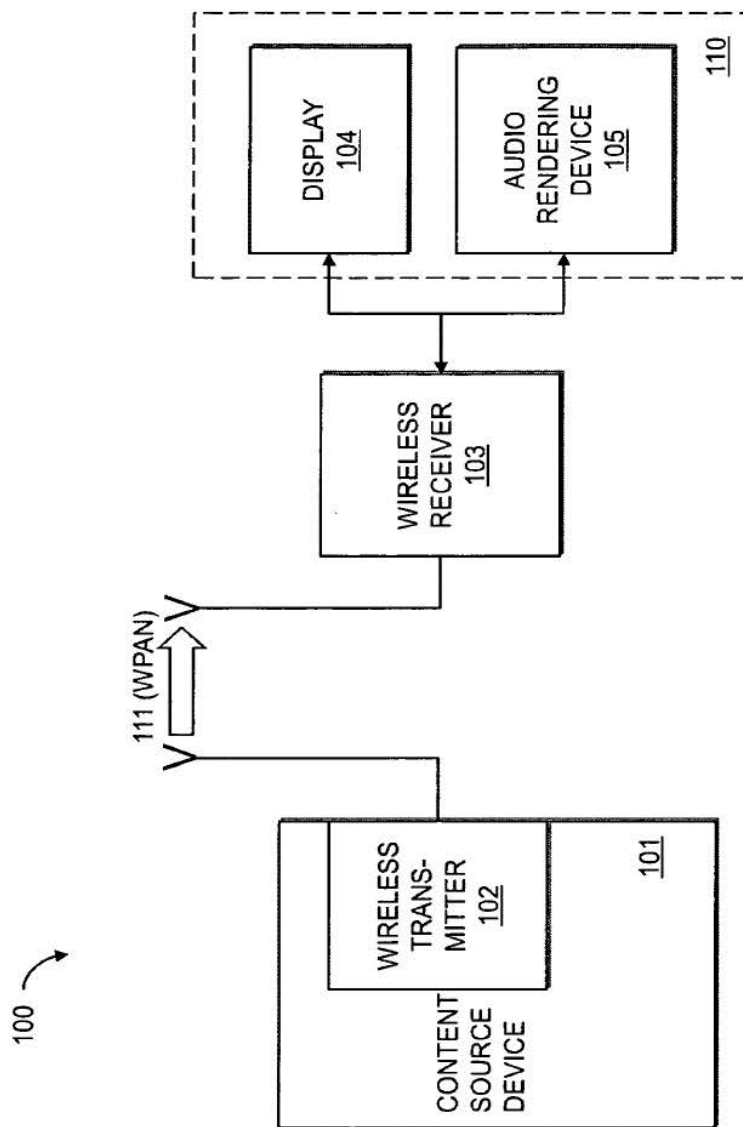


FIG. 1

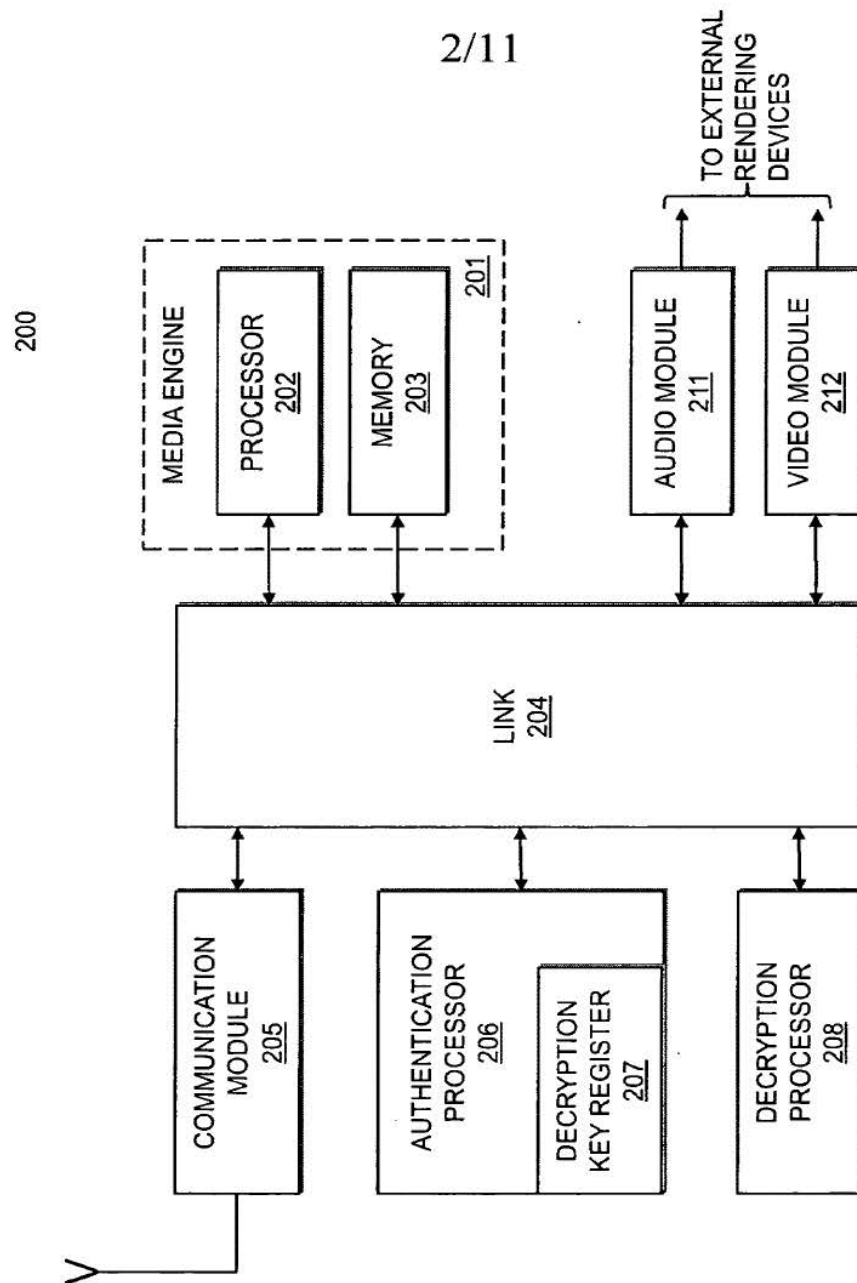


FIG. 2

3/11

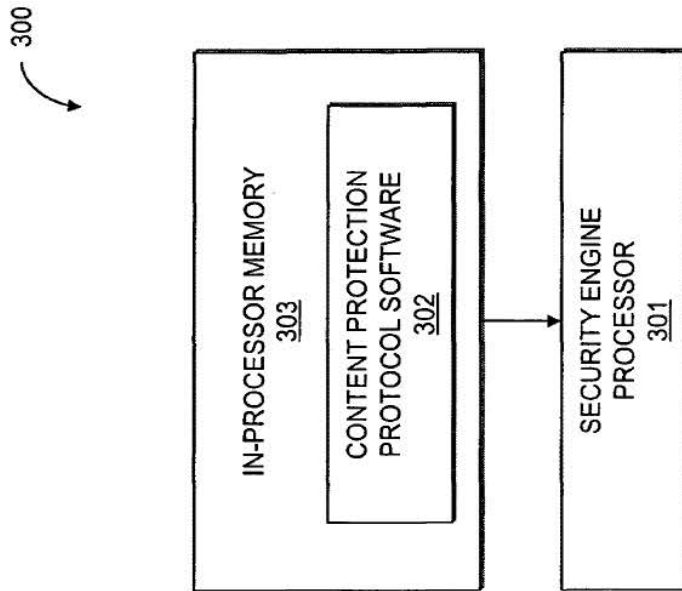


FIG. 3

4/11

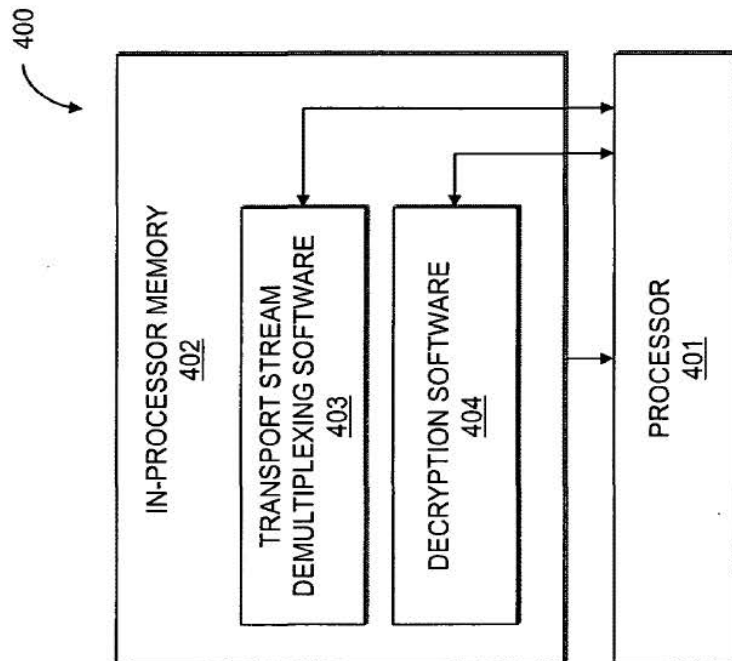


FIG. 4

5/11

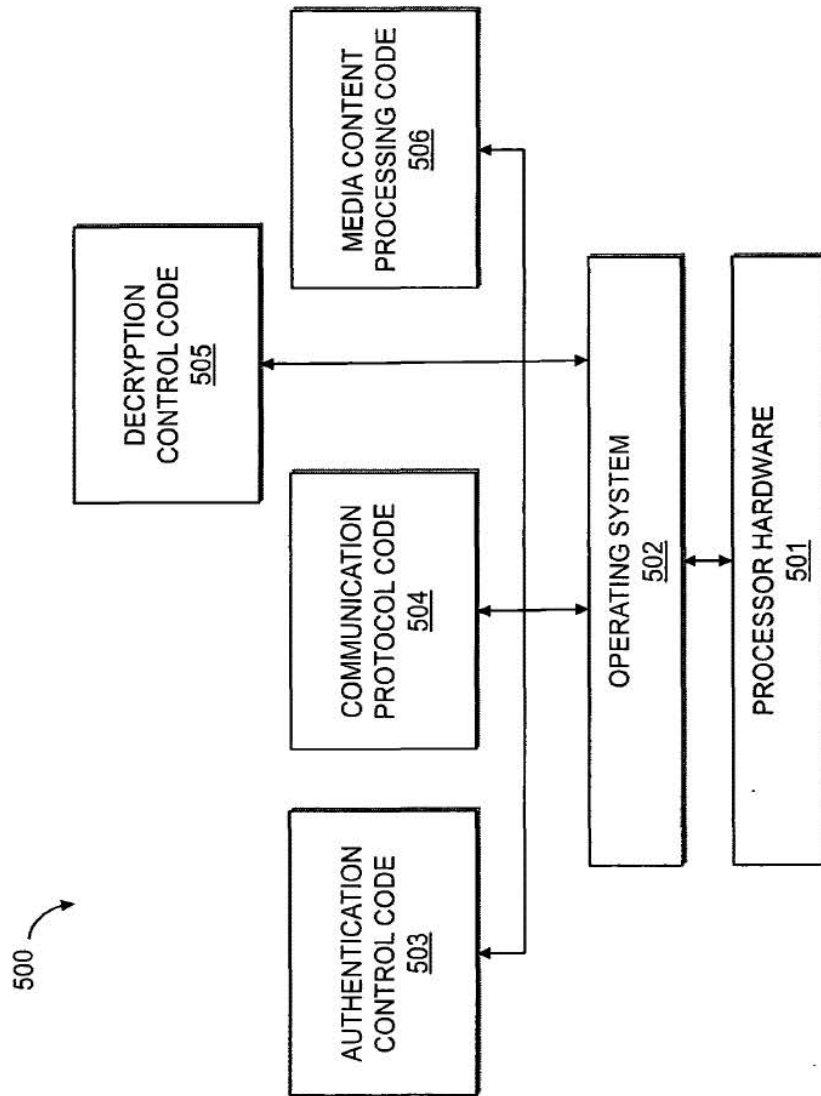


FIG. 5

6/11

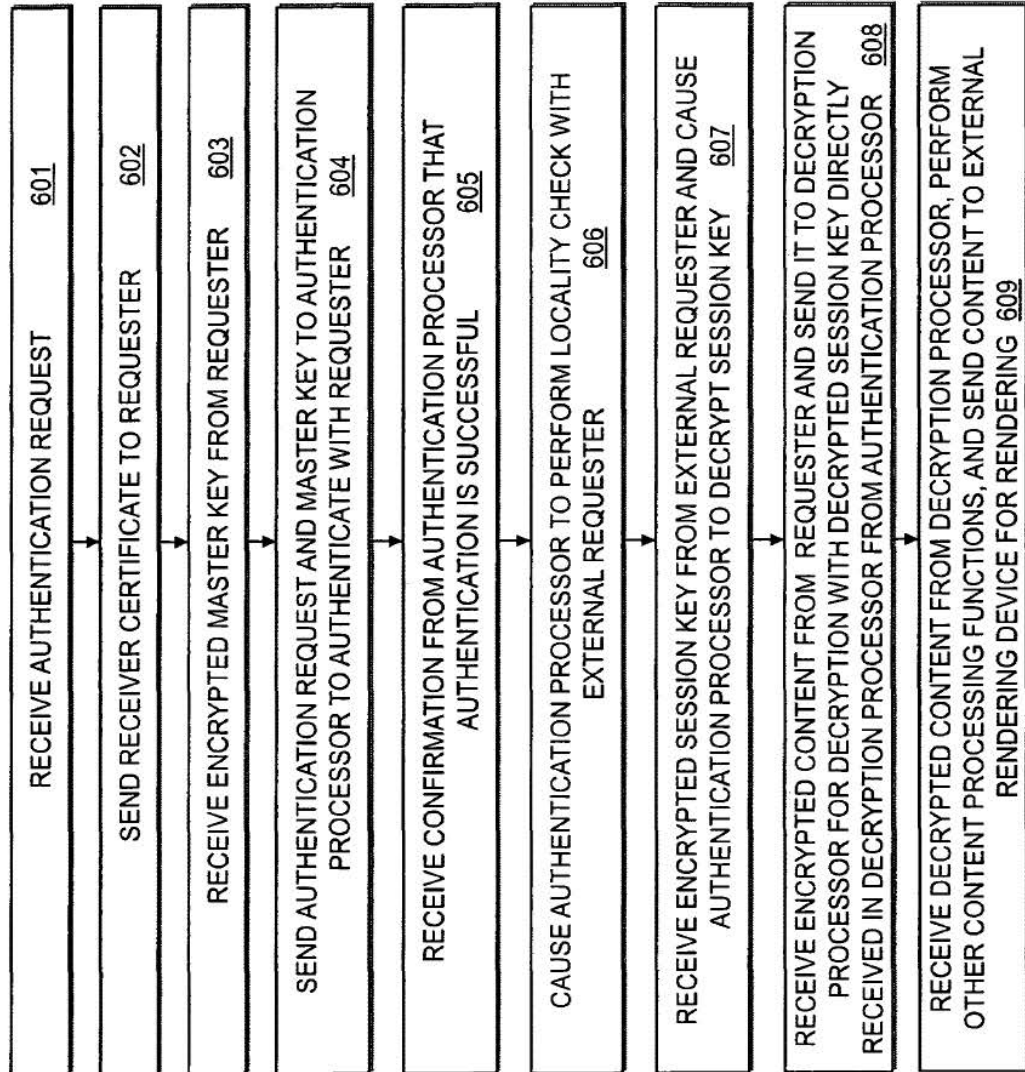


FIG. 6

7/11

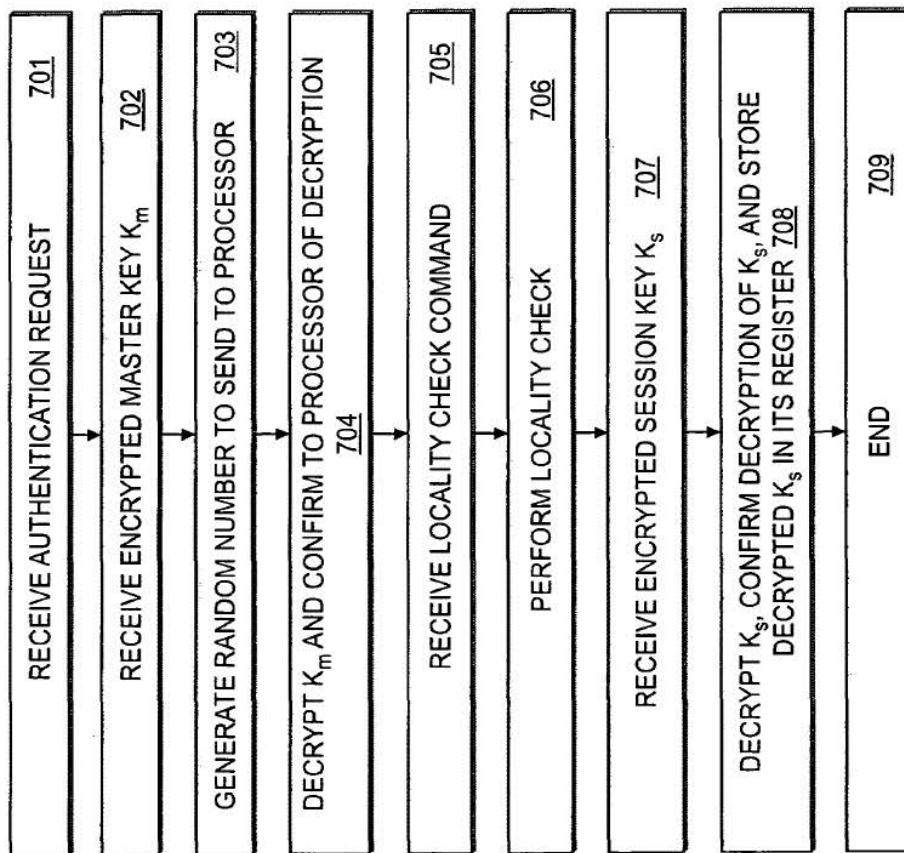


FIG. 7

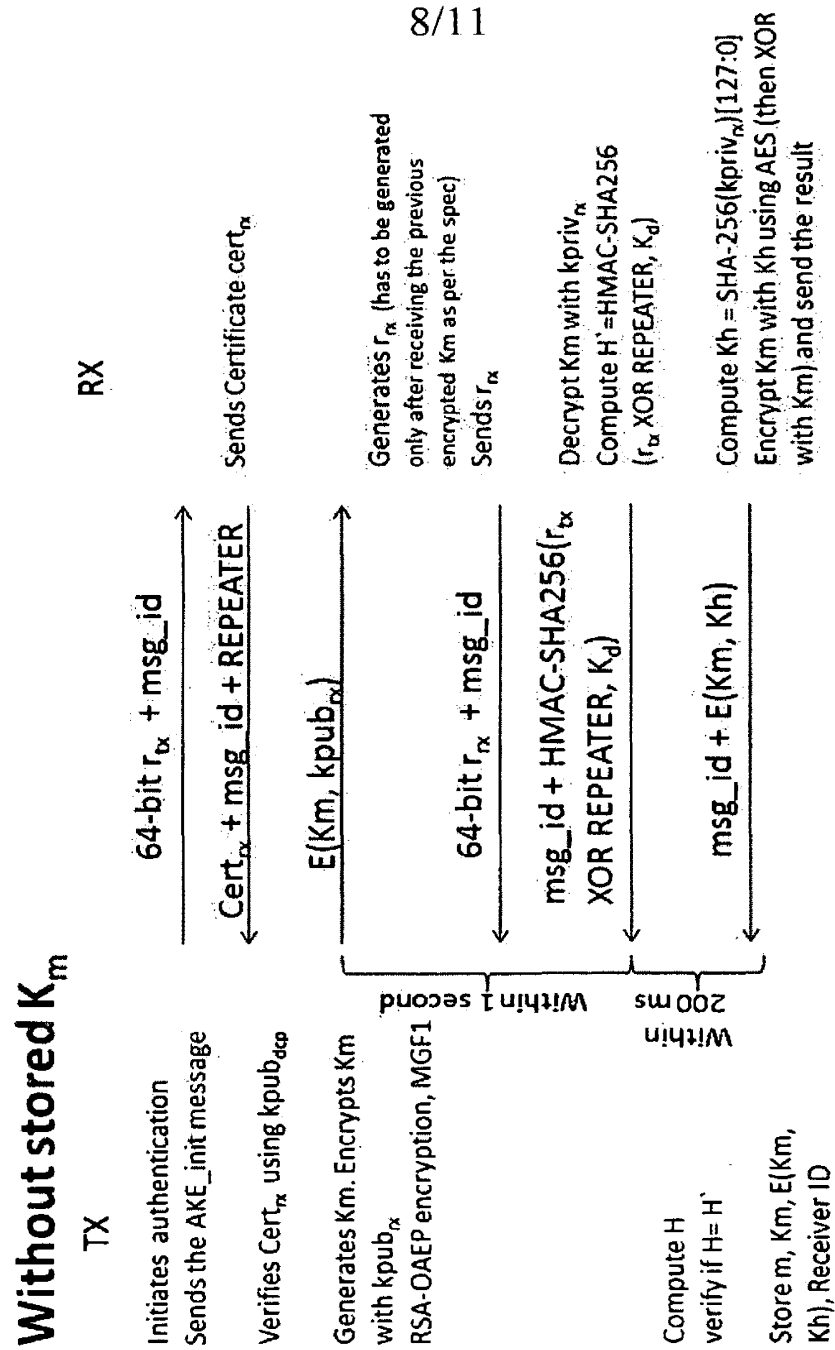


FIG. 8

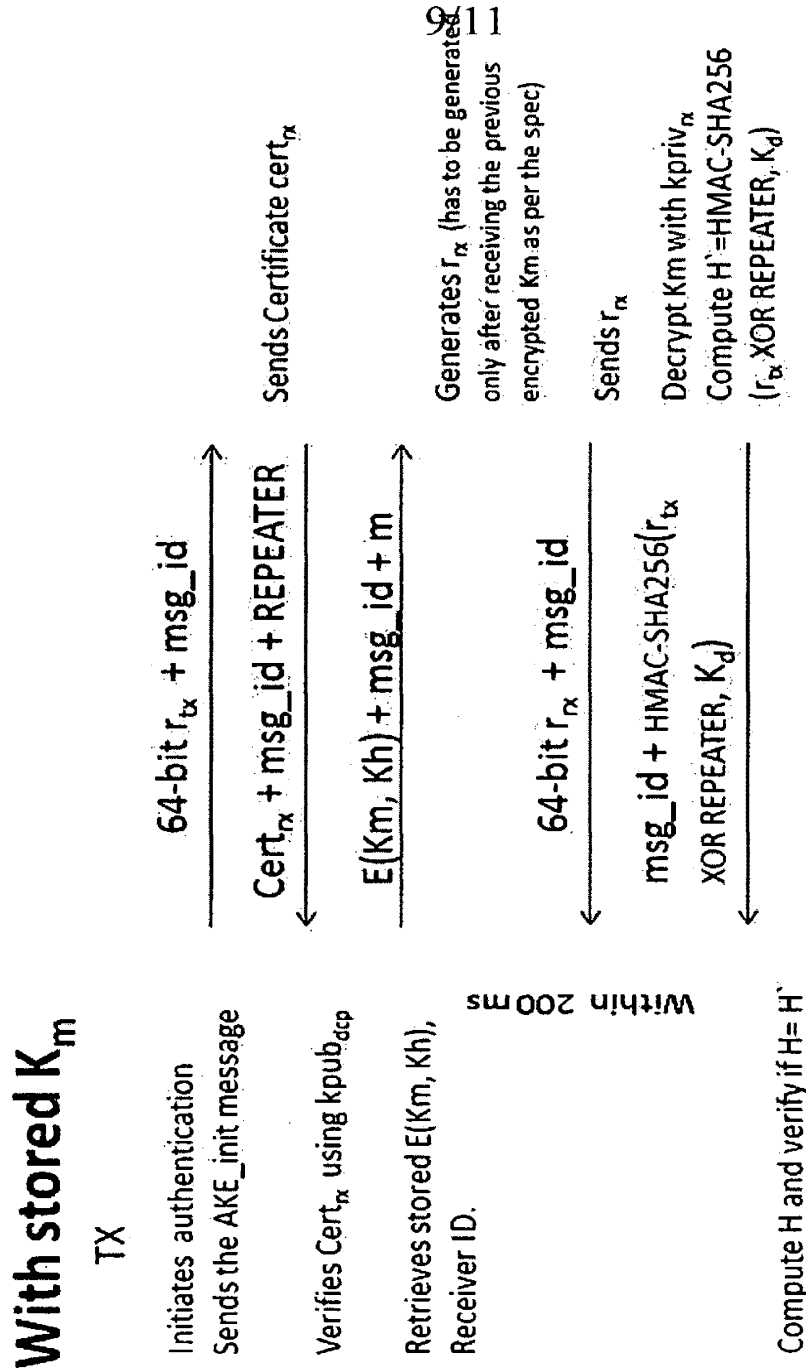


FIG. 9

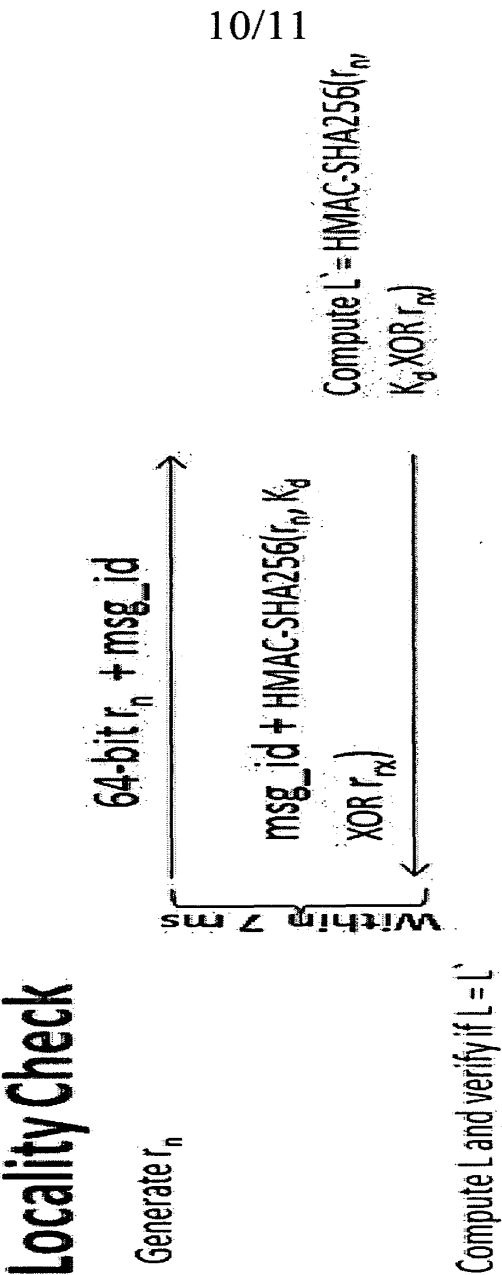


FIG. 10

Session Key Exchange

TX

Generates session key K_s and 64-bit pseudo-random number r_{iv}

Performs key derivation to generate $dkey_2$

Encrypt 128-bit Session Key
 $E_{dkey_1}(k_s) = k_s \text{ XOR } (dkey_2 \text{ XOR } r_{iv})$

Send $E_{dkey_1}(k_s)$ and r_{iv}

RX

$$E_{dkey_1}(k_s) + r_{iv}$$

Performs key derivation to generate $dkey_2$

Decrypt 128-bit Session Key
 $K_s = E_{dkey_1}(k_s) \text{ XOR } (dkey_2 \text{ XOR } r_{iv})$

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2013/000253**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/30(2013.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/30; G06F 12/02; H04K 1/00; G06F 12/14; G06F 13/28; G06F 21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: integrated circuit, SoC (system-on-a-chip), display, secure, encryption, decryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2012-0079287 A1 (MAXIME LECLERCQ) 29 March 2012 see paragraphs [0014], [0016], [0018], [0022], [0051], [0053], [0055], [0061], [0070]-[0079], [0082], [0088]-[0089], [0092]; and figures 1, 3-5, 7-8, 14.	1-16, 22
A		17-21, 23-27
Y	US 2007-0209072 A1 (XUEMIN CHEN) 06 September 2007 see paragraphs [0018]-[0020], [0025]-[0027], [0038], [0047], [0055]-[0058], [0063]-[0064]; and figures 1-2A, 5, 7.	1-16, 22
A	US 8295484 B2 (MARK BUER et al.) 23 October 2012 see column 4, line 25 - column 5, line 2; column 5, line 23 - column 6, line 4; column 6, lines 37-45; and figures 2-4.	1-27
A	US 2002-0163522 A1 (ALLEN J.C. PORTER et al.) 07 November 2002 See paragraphs [0003], [00113], [0017], [0028], [0034], [0040], [0046], [0049]; and figures 1, 2, 4.	1-27

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

27 February 2014 (27.02.2014)

Date of mailing of the international search report

27 February 2014 (27.02.2014)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

LEE, Dong Yun

Telephone No. +82-42-481-8734



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/000253

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2012-0079287 A1	29/03/2012	WO 2011-119985 A2 WO 2011-119985 A3	29/09/2011 29/12/2011
US 2007-0209072 A1	06/09/2007	CN 101031068 A CN 101031068 B EP 1826694 A2 EP 1826694 A3 TW 200802026 A TW I364682 B	05/09/2007 22/06/2011 29/08/2007 14/01/2009 01/01/2008 21/05/2012
US 8295484 B2	23/10/2012	US 2006-133604 A1 US 2013-254542 A1	22/06/2006 26/09/2013
US 2002-0163522 A1	07/11/2002	None	

ADVANCE E-MAIL

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
TRANSMITTAL OF COPY OF INTERNATIONAL
PRELIMINARY REPORT ON PATENTABILITY
(CHAPTER I OF THE PATENT COOPERATION
TREATY)
(PCT Rule 44bis.1(c))

To:

KELLETT, Glen M.
Barnes & Thornburg, LLP
c/o CPA Global
P.O. Box 52050
Minneapolis, Minnesota 55402
ETATS-UNIS D'AMERIQUE

Date of mailing (day/month/year)

26 June 2014 (26.06.2014)

Applicant's or agent's file reference

P41624PCT

IMPORTANT NOTICE

International application No.

PCT/US2011/065069

International filing date (day/month/year)

15 December 2011 (15.12.2011)

Priority date (day/month/year)

Applicant

INTEL CORPORATION et al

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer

Simin Baharlou

Facsimile No. +41 22 338 82 70

e-mail: pt09.pct@wipo.int

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44bis)

Applicant's or agent's file reference P41624PCT	FOR FURTHER ACTION	See item 4 below
International application No. PCT/US2011/065069	International filing date (<i>day/month/year</i>) 15 December 2011 (15.12.2011)	Priority date (<i>day/month/year</i>)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant INTEL CORPORATION		

1.	This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 bis.1(a).																								
2.	This REPORT consists of a total of 7 sheets, including this cover sheet. In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.																								
3.	This report contains indications relating to the following items: <table style="width: 100%; border: none;"> <tr> <td style="width: 5%; text-align: center;">☒</td> <td style="width: 30%;">Box No. I</td> <td style="width: 65%;">Basis of the report</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. II</td> <td>Priority</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. III</td> <td>Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. IV</td> <td>Lack of unity of invention</td> </tr> <tr> <td style="text-align: center;">☒</td> <td>Box No. V</td> <td>Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VI</td> <td>Certain documents cited</td> </tr> <tr> <td style="text-align: center;">☒</td> <td>Box No. VII</td> <td>Certain defects in the international application</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VIII</td> <td>Certain observations on the international application</td> </tr> </table>	☒	Box No. I	Basis of the report	☐	Box No. II	Priority	☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability	☐	Box No. IV	Lack of unity of invention	☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement	☐	Box No. VI	Certain documents cited	☒	Box No. VII	Certain defects in the international application	☐	Box No. VIII	Certain observations on the international application
☒	Box No. I	Basis of the report																							
☐	Box No. II	Priority																							
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability																							
☐	Box No. IV	Lack of unity of invention																							
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement																							
☐	Box No. VI	Certain documents cited																							
☒	Box No. VII	Certain defects in the international application																							
☐	Box No. VIII	Certain observations on the international application																							
4.	The International Bureau will communicate this report to designated Offices in accordance with Rules 44bis.3(c) and 93bis.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44bis .2).																								

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Date of issuance of this report 17 June 2014 (17.06.2014)</td> </tr> <tr> <td style="padding: 5px;"> Authorized officer Simin Baharlou </td> </tr> </table> e-mail: pt09.pct@wipo.int	Date of issuance of this report 17 June 2014 (17.06.2014)	Authorized officer Simin Baharlou
Date of issuance of this report 17 June 2014 (17.06.2014)			
Authorized officer Simin Baharlou			

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

KELLETT GLEN M.

BARNES & THORNBURG, LLP C/O CPA GLOBAL P.O.
BOX 52050 MINNEAPOLIS MN 55402 USA

PCT

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

(PCT Rule 43bis.1)

Date of mailing
(day/month/year) **30 AUGUST 2012 (30.08.2012)**

Applicant's or agent's file reference
P41624PCT

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US2011/065069

International filing date (day/month/year)

15 DECEMBER 2011 (15.12.2011)

Priority date(day/month/year)

International Patent Classification (IPC) or both national classification and IPC

H04L 9/14(2006.01)i, H04L 9/32(2006.01)i

Applicant

INTEL CORPORATION et al

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☒ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon
Metropolitan City, 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140



Date of completion of this opinion

29 AUGUST 2012 (29.08.2012)

Authorized officer

Lee Hyoung Il

Telephone No. 82-42-481-8199



**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/065069

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :
 - ☒ the international application in the language in which it was filed
 - ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:
 - a. a sequence listing filed or furnished
 - ☐ on paper
 - ☐ in electronic form
 - b. time of filing or furnishing
 - ☐ contained in the international application as filed.
 - ☐ filed together with the international application in electronic form.
 - ☐ furnished subsequently to this Authority for the purposes of search.
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065069

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-47	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	33-34,37-47	YES
	Claims	1-32,35-36	NO
Industrial applicability (IA)	Claims	1-47	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2011-0231923 A1 (BOLLAY BENN SAPIN et al.) 22 September 2011
D2: US 2005-0213768 A1 (DAVID DURHAM et al.) 29 September 2005
D3: US 2010-0299525 A1 (SHAH PARAS et al.) 25 November 2010
D4: US 2008-0037793 A1 (BUER MARK) 14 February 2008

1. Novelty and Inventive Step

1.1 Independent Claim 1

D1, which is considered to be the closest prior art to the subject matter of claim 1, discloses an apparatus for a client to generate random number, send client hello message for SSL handshake initiation, perform a server key exchange and a client key exchange, generate a session key based on secret data, store the session in a data store, establish an encrypted session between the server and the client using the session key. Claim 1 differs from D1 in that the apparatus uses the secure memory. However, D2 discloses an apparatus storing the cryptographic key in a secure storage. Accordingly, claim 1 would have been obvious over D1 in view of D2. Therefore, claim 1 lacks an inventive step under PCT Article 33(3).

1.2 Dependent Claims 2-15

Claims 2-15, which are dependent on claim 1, lack an inventive step under PCT Article 33(3), because the additional features of claims 2-15 are merely matters of design option when the general technical knowledge about the state of the art is used.

1.3 Independent Claim 16

Claim 16 relates to a method performing the functions of the apparatus according to claim 1. Claim 16 is considered to lack an inventive step under PCT Article 33(3), because the subject matter of claim 1 is considered to lack an inventive step under PCT Article 33(3).

[Continued on Supplemental Box]

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065069

Box No. VII Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Claims 35-36 and 46-47 do not comply with PCT Rule 6.4(a) because the multiple dependent claims don't refer to other claims in the alternative way.

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065069

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of :

[Box V]

[Box V]

1.4 Dependent Claims 17-32

Claims 17-32, which are dependent on claim 16, lack an inventive step under PCT Article 33(3), because the additional features of claims 17-32 are merely matters of design option when the general technical knowledge about the state of the art is used.

1.5 Dependent Claims 33-34

The additional feature of claim 33 dependent on claim 16 is not disclosed in any of the prior art documents, nor is it obvious to a person skilled in the art by the documents. Accordingly, claim 33 is novel and involves an inventive step under PCT Article 33(2) and (3).

The additional feature of claim 34 dependent on claim 16 is not disclosed in any of the prior art documents, nor is it obvious to a person skilled in the art by the documents. Accordingly, claim 34 is novel and involves an inventive step under PCT Article 33(2) and (3).

1.6 Independent Claim 35

Claim 35 relates to a source device including a plurality of instructions performing the method of claims 16-32. Claim 35 is considered to lack an inventive step under PCT Article 33(3), because the subject matters of claims 16-32 are considered to lack an inventive step under PCT Article 33(3).

1.7 Independent Claim 36

Claim 36 relates to one or more machine readable media comprising a plurality of instructions performing the method of claims 16-32. Claim 36 is considered to lack an inventive step under PCT Article 33(3), because the subject matters of claims 16-32 are considered to lack an inventive step under PCT Article 33(3).

1.8 Claims 37-45

The subject matter of claim 37 differs from these prior art documents in generating a hash code as a function of the session key and sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure. And it is not obvious to a person skilled in the art by the documents, taken alone or in combination. Therefore, claim 37 meets the requirements of PCT Article 33(2) and (3) with respect to novelty and inventive step.

Claims 38-45 are dependent on claim 37 and therefore meet the requirements of PCT Article 33(2) and (3).

1.9 Claims 46-47

Claim 46 relates to a source device including a plurality of instructions performing the method of claims 37-45. Claim 46 is considered to be novel and to involve an inventive step under PCT Article 33(2) and (3), because the subject matters of claim 37-45 are considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

Claim 47 relates to one or more machine readable media comprising a plurality of instructions performing the method of claims 37-45. Claim 47 is considered to be novel and to involve an inventive step under PCT Article 33(2) and (3), because the subject matters of claim 37-45 are considered to be novel and to involve an inventive step under PCT Article 33(2) and (3).

[Continued on Supplemental Box]

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/065069

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of :

[Box V]

2. Industrial Applicability

Claims 1-47 are industrially applicable under PCT Article 33(4).

Electronic Acknowledgement Receipt	
EFS ID:	19887003
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Christopher A. Singh/Stacy Tebo
Filer Authorized By:	Christopher A. Singh
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	18-AUG-2014
Filing Date:	
Time Stamp:	12:29:58
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	P41624US_SupplIDS.pdf	612385 a2fcaabf3bd9a9bf654610997a6eba4c277b4cd	no	4

Warnings:

Information:

2	Foreign Reference	FR1.pdf	1836210	no	41
			a34b6b8eb01301c62b15862a341138f3426272c5		
Warnings:					
Information:					
3	Non Patent Literature	NPL1.pdf	260581	no	8
			a372ced5356b790fba386cd61954003cc76a0d3		
Warnings:					
Information:					
Total Files Size (in bytes):			2709176		
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					



UNITED STATES PATENT AND TRADEMARK OFFICE

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

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
13/997,412	Hormuzd M. Khosravi	P41624US
73486 Barnes & Thornburg LLP (Intel) c/o CPA Global P.O. Box 52050 Minneapolis, MN 55402		INTERNATIONAL APPLICATION NO. PCT/US11/65069
		L.A. FILING DATE 12/15/2011
		PRIORITY DATE

CONFIRMATION NO. 1045
371 ACCEPTANCE LETTER



Date Mailed: 10/28/2014

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office, in its capacity as a Designated / Elected Office (37 CFR 1.495), has ACCEPTED the above identified international application for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

04/03/2014
DATE OF RECEIPT OF 35 U.S.C. 371(c)(1),
(c)(2) and (c)(4) REQUIREMENTS

04/03/2014
DATE OF COMPLETION OF ALL
35 U.S.C. 371 REQUIREMENTS

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1), (c)(2) and (c)(4) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE.** The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363).

The following items have been received:

- Copy of the International Application filed on 06/24/2013
- Copy of the International Search Report filed on 06/24/2013
- Preliminary Amendments filed on 06/24/2013
- Information Disclosure Statements filed on 07/26/2013
- Inventor's Oath or Declaration filed on 04/03/2014
- Request for Immediate Examination filed on 04/03/2014
- U.S. Basic National Fees filed on 06/24/2013
- Authorization to Permit Access filed on 06/24/2013

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

BRIAN A HARDEN

Telephone: (703) 756-1815



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
13/997,412	04/03/2014		1800	P41624US	24	3

CONFIRMATION NO. 1045

73486

Barnes & Thornburg LLP (Intel)
c/o CPA Global
P.O. Box 52050
Minneapolis, MN 55402

FILING RECEIPT



OC000000071507631

Date Mailed: 10/28/2014

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Hormuzd M. Khosravi, Portland, OR;
Edward C. Epp, Portland, OR;
Farhana Kabir, Camas, WA;

Applicant(s)

Hormuzd M. Khosravi, Portland, OR;
Edward C. Epp, Portland, OR;
Farhana Kabir, Camas, WA;

Power of Attorney: The patent practitioners associated with Customer Number 73486

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/US11/65069 12/15/2011

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 10/23/2014

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/997,412**

Projected Publication Date: 02/05/2015

Non-Publication Request: No

Early Publication Request: No

Title

METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A
HARDWARE SECURITY ENGINE

Preliminary Class

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number 13/997,412	
APPLICATION AS FILED - PART I						
(Column 1)		(Column 2)		SMALL ENTITY		OR
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)	OTHER THAN SMALL ENTITY	
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A		N/A	280
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A		N/A	480
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A		N/A	720
TOTAL CLAIMS (37 CFR 1.16(i))	24	minus 20 = * 4			OR	x 80 = 320
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *			OR	x 420 = 0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))						0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL		TOTAL	1800
APPLICATION AS AMENDED - PART II						
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	OTHER THAN SMALL ENTITY
	Total (37 CFR 1.16(i))	* Minus **	=	x =		OR
	Independent (37 CFR 1.16(h))	* Minus ***	=	x =		OR
	Application Size Fee (37 CFR 1.16(s))					OR
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR
TOTAL ADD'L FEE					TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)	OTHER THAN SMALL ENTITY
	Total (37 CFR 1.16(i))	* Minus **	=	x =		OR
	Independent (37 CFR 1.16(h))	* Minus ***	=	x =		OR
	Application Size Fee (37 CFR 1.16(s))					OR
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR
TOTAL ADD'L FEE					TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.						



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US

CONFIRMATION NO. 1045

73486

Barnes & Thornburg LLP (Intel)
c/o CPA Global
P.O. Box 52050
Minneapolis, MN 55402

PUBLICATION NOTICE



OC000000073236526

Title:METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

Publication No.US-2015-0039890-A1

Publication Date:02/05/2015

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101



UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/997,412	04/03/2014	Hormuzd M. Khosravi	P41624US	1045
73486 7590 11/16/2015 Barnes & Thornburg LLP (Intel) c/o CPA Global P.O. Box 52050 Minneapolis, MN 55402			EXAMINER LE, THANH T	
			ART UNIT 2495	PAPER NUMBER
			NOTIFICATION DATE 11/16/2015	DELIVERY MODE ELECTRONIC

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

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

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

INDocket@btlaw.com
inteldocket@btlaw.com
inteldocs_docketing@cpaglobal.com

Office Action Summary	Application No. 13/997,412	Applicant(s) KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	AIA (First Inventor to File) Status No

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

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

Status

- 1) ☒ Responsive to communication(s) filed on 06/24/2013.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

- 5) ☒ Claim(s) 48-71 is/are pending in the application.
5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 48-71 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 06/24/2013 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

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

Certified copies:

- a) ☐ All b) ☐ Some** c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

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

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date 07/26/2013, 09/20/2013, 05/27/2014 and 08/18/2014.
- 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 4) ☐ Other: ____.

DETAILED ACTIONS

Notice of Pre-AIA status

1. The present application is being examined under the pre-AIA first to invent provisions.

Priority

2. Acknowledgement is made of applicant's claim of 371 of PCT /US11/65069 12/15/2011.

Information Disclosure Statement

3. The information disclosure statements (IDS) submitted on 07/26/2013, 09/20/2013, 05/27/2014 and 08/18/2014 have been considered by the examiner.

Drawing Objection

4. Fig. 2 recites: "RSA Key Exchange" which should be a typo.
Appropriate correction is required.

Claim Rejections- 35 U.S.C. § 112 Second Paragraph

5. The following is a quotation of 35 U.S.C. 112 (pre-AIA), second paragraph:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 2 recites the limitations "the response message". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 U.S.C. § 101

6. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 64-71 are rejected under 35 U.S.C. §101.

Regarding claim 64, it recites "One or more machine-readable storage media comprising..." which can be interpreted as a signal or a carrier wave. This does not fall under one of the four statutory categories. Applicant can overcome this rejection by instead reciting a "***non-transitory*** machine-readable storage media ", which would explicitly exclude signals per se.

- Claims 65-71 depend on claim 71 and they do not limit independent claim 64 or themselves to statutory subject matter; therefore, they are also rejected under 35 USC 101.

Claim Rejections - 35 U.S.C. § 103

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

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

8. Claims 48-50, 56-58 and 64-66 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646) hereinafter "Chou", in view of Goss (US application No. 2005/0213766) hereinafter "Goss".

Regarding claim 48, Chou discloses system-on-a-chip apparatus comprising:

[a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, the security engine to]:

generate a random nonce for initiating a request for a secure communication session with a server over a network using the nonce (Fig. 1 and associated text: Client hello message 150 is sent from first network device-client- to second network device-server. Fig. 2A and associated text: Client hello message 150 includes first random number-random nonce. Chou discloses that a random number is generated internally within the second device (Col. 6, line 67 and Col.7, line1 and claim 7). Therefore, it is obvious to apply this feature of generating random number internally within a device so that the first device can generate its own random number);

perform a cryptographic key exchange with the server (Fig. 1, step 180 and associated text: client key exchange message is sent to second network device-server) to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session (Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120);

store the session key in the [secure memory] (Chou does not explicitly disclose about storing the session key; however, in order for using the key to communicate between the two device in a period of time-a session of communication-, it is obvious that the key must be stored), [the system-on-a-chip] to establish the secure communication session with the server over the network using the session key (Col. 4, lines 60-63: Client Hello message 150 is a message that provides second network device 120 with information that is used to establish secured communications between network devices 110 and 120. Col. 5, lines 63-67: a Master key can be produced prior to completion of the SSL/TLS authentication procedure. The Master key is now used as a symmetric key for supporting encrypted communications between the network devices 110 and 120).

Chou does not explicitly disclose a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine.

However, in the field of cryptography, Goss discloses a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine (Abstract: a system-on-a-chip (SoC) has a secure execution environment (SEE) comprising secure memory containing cryptographic key. Fig. 1 and associated text: SoC comprises secure memory. The system on the chip can be interpreted as a security engine).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou's invention of establishing a secure communication session with the server over the network using a session key with a

system on a chip that contains a secure memory to store session key as taught by Goss. The motivation to do so would be to achieve a higher encryption or decryption throughput in SoC than uses a cryptographic accelerator without compromising key or process security as taught by Goss (paragraphs [0006-0008]).

Regarding claim 49, Chou and Goss disclose the system-on-a-chip apparatus of claim 48, wherein the security engine to receive a server nonce from the server in response to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory (Figs. 1, 2B and associated text: server hello message 160-response message- includes random number 260. Chou does not explicitly disclose that the server nonce is stored. However, it is known in the art and is the designer's choice to store data for later retrieving. Combining with Goss' teaching of secure memory as in claim 48 above, it is obvious to have the server's nonce stored in the secure memory to protect the nonce from being compromised).

Regarding claim 50, Chou and Goss disclose the system-on-a-chip apparatus of claim 48, wherein the security engine to generate a pre-master key, encrypt the pre-master key using a security key of the security engine, and send the encrypted pre-master key to the server (Chou, Col. 5, lines 50-57: first network device generates Pre-Master key and pre-master key is encrypted with the public key of second network device. Goss, Abstract: secure memory stores cryptographic key. The combination of Chou and Goss' teaching makes it obvious that the server's public key could be stored

Art Unit: 2495

in the secure memory; therefore, the server's public key is a security key of the security engine).

Claims 56-58 and 64-66 are s 48-50 respectively.

9. Claims 51, 52, 59-61 and 67-69 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Goss (US application No. 2005/0213766), hereinafter "Goss", and further in view of Weisman et al. (US application No. 2009/0280905), hereinafter "Weisman".

Regarding claim 51, Chou and Goss disclose the system-on-a-chip apparatus of claim 50, wherein the security engine to wrap the pre-master key using a server public key (Chou, Col. 5, lines 50-57: first network device generates Pre-Master key and pre-master key is encrypted with the public key of second network device. Goss, Abstract: secure memory stores cryptographic key).

Chou and Goss do not **explicitly** disclose the **wrapped** pre-master key is stored in the secure storage.

However, in the field of system-on-the-chip, Weisman discloses encrypted key is stored in secure memory (paragraph [0076]: system-on-the-chip product comprises CPU 300. Paragraph [0078]: data stored in `secure` memory may instead be encrypted such that a key known to the CPU 300 is used to decrypted the information strictly inside of registers of CPU 300").

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Goss' invention of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to store session key and with Weisman's invention of storing encrypted key in secure memory. The motivation to do so would be to provide extra protection to the key.

Regarding claim 52, Chou, Goss, and Weisman disclose the system-on-a-chip apparatus of claim 50. Chou further discloses wherein the security engine to:

generate the session key as a function of the pre-master key (Col. 5, lines 61-65: a master key is produced from the pre-master key); and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

Claims 59 and 67 are rejected because they disclose similar subject matter to claim 48.

Claims 60-61 and 68-69 are rejected because they disclose similar subject matter to claim 52.

10. Claims 53, 54, 62-63, and 70-71 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Goss (US application No. 2005/0213766), hereinafter "Goss", and further in view of Jin-Meng Ho (US application No. 2010/0042839), hereinafter "Ho".

Regarding claim 53, Chou and Goss disclose the system-on-a-chip apparatus of claim 48. Chou further discloses that client hello message includes list of cryptographic algorithms supported by first network device 110 such as Ephemeral Diffie-Hellman (DHE). Chou also discloses data is encrypted with server's private key before being sent to the server (Chou, Col. 5, lines 50-57: pre-master key is encrypted with the public key of second network device-server).

Chou and Goss do not explicitly disclose wherein the security engine to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the server.

However, in the field of data communication and security, Ho discloses the security engine to generate a public Diffie-Hellman client key and a private Diffie-

Hellman client key (Fig. 3, step 0a and associated text: a secret (private) key is chosen and a public key is computed. Paragraph [0038]: public key generated initiating device A-client- is used for Diffie-Hellman key exchange), sign the public Diffie-Hellman client key using a security key of the security engine (it is obvious to apply Chou's teaching of encrypting-signing- data before sending as stated above), and send the signed public Diffie-Hellman key to the server (Fig. 3, Step 2a and associated text: Public key PKa is sent to device B-server).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Goss' invention of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to store session key and with Ho's invention of using Diffie-Hellman for generating key. The motivation to do so would be to allow two parties to exchange information over an insecure channel to establish a shared secret as taught by Ho (paragraph [0022]).

Regarding claim 54, Chou, Goss, and Ho disclose the system-on-a-chip apparatus of claim 53. Ho further discloses wherein the security engine to receive a public Diffie-Hellman server key from the server (Fig. 3, step 4b and associated text: Public key of device B-server- is sent to device A) and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key (step 5a and associated text: DHkey-session key- is computed based on Private key of device A –client- and public key of Device B-server).

Claims 62 and 70 are rejected because they disclose similar subject matter to the combination of claims 53 and 54.

Regarding claim 63, Chou and Goss disclose the method of claim 56 (claim 56 is rejected for disclosing similar subject matter to claim 48, as stated in section 8 above). Chou further disclose:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server (Col. 3, lines 27-29: The completion of a TLS handshake includes a hash of all the frames sent and received by each peer. Col. 7, lines 11-17: According to one embodiment of the invention, each hash value is a result produced by performing one-way hash operations on authentication messages during the SSL/TLS Handshake. These hash operations may be in accordance with MD5, SHA-1 or other hash algorithms that are performed in an iterative to produce a single hash value or in any other selected manner. The hash value is used by the CP processing element to continue the remaining portion of the SSL/TLS Handshake. Therefore, it is obvious that the designer can calculate hash function on his/her choices of values which could be random numbers from client and server).

signing the hash code using a security key stored in a secure memory of the security engine (Chou discloses data is encrypted with server's private key before being sent to the server (Chou, Col. 5, lines 50-57: pre-master key is encrypted with the public key of second network device-server. Goss, Abstract: secure memory stores cryptographic key. The combination of Chou and Goss' teaching makes it obvious that

the server's public key could be stored in the secure memory; therefore, the server's public key is a security key of the security engine and it is obvious that the hash code could be signed using a security key stored in a secure memory of the security engine).

Chou and Goss do not explicitly disclose sending a client certificate verification message to the server, the client certificate verification message including the signed hash code.

However, in the field of data communication and security, Ho discloses sending a hash client certificate verification message to the server, the client certificate verification message including the signed hash code (Fig. 3, steps 5a and 7a and associated text: Verification Va1 is computed and sent to device B-server. With Chou's teaching of signing data before sending as above, the client certificate verification message including the signed hash code is sent to the server).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Goss' invention of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to store session key and with Ho's invention of using hash code for verification message. The motivation to do so would be to ensure secure communication for involved parties.

Claim 71 is rejected because it discloses similar subject matter to claim 63.

11. Claim 55 is rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Chou et al. (US Patent No. 7,966,646), hereinafter "Chou", in view of Goss

(US application No. 2005/0213766), hereinafter "Goss", in view of Jin-Meng Ho (US application No. 2010/0042839), hereinafter "Ho", and further in view of Peyravian et al (US application No. 2004/0158715), hereinafter "Peyravian".

Regarding claim 55, Chou and Goss disclose the system-on-a-chip apparatus of claim 48. Chou also discloses the secure memory stores cryptographic key as stated in claim 48.

Chou and Goss do not explicitly disclose wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server.

However, in the field of data communication and security, Ho discloses the security engine to receive Diffie-Hellman [global values] and a public Diffie-Hellman server key from the server (Fig. 3, step 4b and associated text: Public key of device B-server- is sent to device A-client).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou and Goss' invention of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to store session key and with Ho's invention of using Diffie-Hellman for generating key. The motivation to do so would be to allow two parties to exchange information over an insecure channel to establish a shared secret as taught by Ho (paragraph [0022]).

Chou, Goss, and Ho do not explicitly disclose the security engine to receive Diffie-Hellman global values.

However, in the field of data security, Peyravian discloses a prime modulus-global Diffie-Hellman value- is sent to a device (paragraph [0011]: prime modulus is sent to server, so that the server can use this prime modulus as one of parameters to generate Diffie-Hellman symmetric secret key-session key. It is obvious that the client and server can switch roles. In other words, the server can be the sender instead of receiver of the prime modulus).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Chou, Goss, and Ho' inventions of establishing a secure communication session with the server over the network using a session key with a system on a chip that contains a secure memory to store session key with using Diffie-Hellman for generating key and with Peyravian's invention of sending a global value. The motivation to do so would be to provide an improved way to distribute and authenticate public cryptographic keys as taught by Peyravian (paragraph [0010].

The combination of Chou and Ho's references discloses store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage (Chou, Abstract: secure memory stores cryptographic key. Ho, Fig. 3, step 4b and associated text: Public key of device B-server- is sent to device A-client).

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to THANH LE whose telephone number is (571)270-0279. The examiner can normally be reached on M-F 6:00 am- 2:30pm.

Art Unit: 2495

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Farid Homayounmehr can be reached on 571-272-3739. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

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

/THANH T. LE/

Examiner, Art Unit 2495

/FARID HOMAYOUNMEHR/

Supervisory Patent Examiner, Art Unit 2495

Application/Control Number: 13/997,412
Art Unit: 2495

Page 16

Notice of References Cited	Application/Control No. 13/997,412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-5,657,390 A	08-1997	Elgamal; Taher	H04L29/06	713/151
*	B	US-2005/0005093 A1	01-2005	Bartels, Andrew	G06F21/606	713/150
*	C	US-2005/0213766 A1	09-2005	Goss, Steven C.	G06F21/72	380/277
*	D	US-2005/0289343 A1	12-2005	Tahan, Thomas	G06F21/72	713/169
*	E	US-2006/0041938 A1	02-2006	Ali; Asad Mahboob	G06Q20/341	726/14
*	F	US-7,069,352 B2	06-2006	Pezzini; Saverio	G06F13/385	710/3
*	G	US-7,096,352 B2	08-2006	Kang; Kyoung Jin	H04L67/04	380/270
*	H	US-2009/0280905 A1	11-2009	Weisman; Jordan K.	A63F13/08	463/40
*	I	US-2010/0042839 A1	02-2010	Ho; Jin-Meng	H04L9/3226	713/169
*	J	US-2010/0205443 A1	08-2010	Zhao; Yunlei	H04L9/3218	713/171
*	K	US-7,966,646 B2	06-2011	Chou; Randy	H04L63/166	726/2
*	L	US-2011/0235806 A1	09-2011	Fukuda; Naohiro	H04L9/0825	380/282
*	M	US-2011/0231923 A1	09-2011	Bollay; Benn Sapin	H04L63/166	726/9

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Notice of References Cited	Application/Control No. 13/997,412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.	
	Examiner THANH T. LE	Art Unit 2495	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-8,615,787 B2	12-2013	Murray; Bruce	H04L63/0853	380/281
*	B	US-8,627,440 B2	01-2014	Mowers; David R.	H04L63/0807	380/279
*	C	US-2014/0270166 A1	09-2014	Avanzi; Roberto	H04L9/0822	380/201
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

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

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

Receipt date: 08/18/2014

13997412 - GAU: 2495

Doc code: IDS

PTO/SB/08a (01-10)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41624US/45631-225521		

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
/T.L./	1	8645677	B2	2014-02-04	Khosravi et al.			
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
/T.L./	1	20110023077	A1	2011-01-27	Simon			
/T.L./	2	20080177998	A1	2008-07-24	Apsangi et al.			
/T.L./	3	20060133604	A1	2006-06-22	Buer et al.			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
/T.L./	1	2014074127	WO	A1	2014-05-15	Intel Corporation		☐

Receipt date: 08/18/2014

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd M. Khosravi
Art Unit	UNK
Examiner Name	UNK
Attorney Docket Number	P41624US/45631-225521

If you wish to add additional Foreign Patent Document citation information please click the Add button				Add
NON-PATENT LITERATURE DOCUMENTS				Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵	
/T.L./	1	International Preliminary Report on Patentability received for PCT International Application No. PCT/US2011/065069, mailed June 26, 2014, 8 pages.	☐	
If you wish to add additional non-patent literature document citation information please click the Add button				
EXAMINER SIGNATURE				
Examiner Signature	/Thanh Le/		Date Considered	08/20/2015
*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.				
¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.				

Receipt date: 08/18/2014

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd M. Khosravi
Art Unit	UNK
Examiner Name	UNK
Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

- ☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

- ☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2014-08-18
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	34	("20100299525" "20020163522" "20130275769" "20060133604" "20120079287" "20080177998" "20110231923" "8295484" "20050213768" "20130297936" "20140129827" "8645677" "20080037793" "20070209072" "20110023077").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 06:04
S2	1	13/997412	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 06:42
S3	22	((("8205238") or ("7813822") or ("6324288") or ("20120137137") or ("20110154061") or ("20130080764")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/08/14 06:54
S4	2	13/694221	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 08:50
S5	0	((hormuzd near2 khosravi) (edward near2 epp) (farhana near2 kabir)).in. and (generat\$3 with random with nonce with key with exchang\$3 with session with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:12
S6	0	((hormuzd near2 khosravi) (edward near2 epp) (farhana near2 kabir)).in. and (generat\$3 with random with nonce with key with exchang\$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:12
S7	0	(intel).as. and (generat\$3 with random with nonce with key with exchang\$3 with session with key).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:13

S8	0	(intel).as. and (generat\$3 with random with nonce with key with exchange\$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:13
S9	1	(generat\$3 with random with nonce with key with exchange\$3 with session with key).clm. and (H04L63/61 H04L9/0861 H04L9/0841 H04L9/0838).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:14
S10	2	(generat\$3 with random with nonce with key with exchange\$3 with session with key) and (H04L63/61 H04L9/0861 H04L9/0841 H04L9/0838).cpc.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:19
S11	1	S10 not S9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:19
S12	1	(generat\$3 with random with nonce with key with exchange\$3 with session with key).clm. and (713/171).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:21
S13	4	(generat\$3 with random with nonce with key with exchange\$3 with session with key) and (713/171).ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:23
S14	3	S13 not S12	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/14 11:23
S17	5	((("20080077809") or ("20110161645"))).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/08/21 08:17
S18	3	("20080037793").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO;	OR	OFF	2015/08/21 11:30

			DERWENT; IBM_TDB			
S19	15	(generat\$3 with random with nonce with key with exchang\$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:35
S20	19	(random with nonce with key with exchang\$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:53
S21	4	S20 not S19	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:53
S22	94	(nonce with key with exchang\$3 with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:59
S23	75	S22 not (S19 S20)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 11:59
S24	763	(diffie-hellman with session with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 13:02
S25	41	(diffie-hellman with session with key) and (nonce with key with exchang\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 13:02
S26	34	((@pd<"20111215" @ad<"20111215") and (diffie-hellman with session with key) and (nonce with key with exchang\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/21 13:05
S27	29	((("20060041938") or ("8627440") or ("8006090") or ("8392968") or ("5657390") or ("5825890") or	US-PGPUB; USPAT; USOCR;	OR	OFF	2015/08/24 11:28

		("7966646").PN.	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S28	11	S27 and (random nonce (key with exchang\$3) (session adj key))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 11:58
S29	11	S27 and (random nonce (key with exchang\$3) (session adj key) hash diffie- hellman)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 12:00
S30	75	((@pd<"20111215" @ad<"20111215") and (diffie-hellman with generat\$3 with key) and ((random nonce) with key with exchang\$3) and (hash with (random nonce)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 13:30
S31	9	((@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and ((TLS (transport adj layer adj security)) with (handshak\$3 hello) with (random nonce)) and (key with exchang\$3) and ((secret session) with key) and (hash with (nonce random)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 14:39
S32	0	((@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and ((system-on-a- chip SOC) with secure with communication))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:45
S33	1596	((@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and (system-on-a- chip SOC))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:45
S34	26	((@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and ((system-on-a- chip SOC) with (TLS (transport adj layer adj security))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:46
S35	26	((@pd<"20111215" @ad<"20111215") and (TLS (transport adj layer adj security)).ti,bsum,ab. and ((system-on- chip SOC) with (TLS (transport adj layer adj security))))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:48
S36	8	((@pd<"20111215" @ad<"20111215") and	US-PGPUB;	OR	ON	2015/08/24

		((SSL (secure adj socket adj layer)).ti, bsum, ab. and ((system-on-chip SOC) with (SSL (secure adj socket adj layer)))	USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB			15:50
S37	155	((@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag\$3))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:53
S38	23	((@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag\$3) with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 15:53
S39	168	((@pd<"20111215" @ad<"20111215") and (diffie-hellman with (generat\$3 exchang\$3) with key with stor\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 16:43
S40	48	((@pd<"20111215" @ad<"20111215") and (SSL (secure adj socket adj layer) TLS (transport adj layer adj security)) and (diffie-hellman with (generat\$3 exchang\$3) with key with stor\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/24 16:45
S41	2	("8788805").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/08/24 17:34
S42	30	("20010020274" "6367009" "20030120948" "20050074126" "6643774" "20050074126" "20030126464" "6081900" "20030005286" "20010020274" "5923756" "6633979" "6205482" "7096352").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/08/26 11:41
S43	5	((("20080077809") or ("20110161645")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/11/02 08:37
S44	1	"13997406"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT;	OR	ON	2015/11/02 09:06

			IBM_TDB			
S45	38	(US-20080037793-\$ or US-20140129827-\$ or US-20130297936-\$ or US-20130275769-\$ or US-20120079287-\$ or US-20110231923-\$ or US-20110023077-\$ or US-20100299525-\$ or US-20080177998-\$ or US-20070209072-\$ or US-20060133604-\$ or US-20050213768-\$ or US-20020163522-\$ or US-20130080764-\$ or US-20120137137-\$ or US-20110154061-\$).did. or (US-8205238-\$ or US-7813822-\$ or US-6324288-\$).did. or (KR-20140129827-\$ or KR-20120079287-\$ or KR-20110023077-\$ or KR-20080037793-\$ or KR-20060133604-\$).did. or (US-20140129827-\$ or WO-2013089726-\$ or WO-2013089728-\$ or US-20130080764-\$ or WO-2011116342-\$ or WO-2011109780-\$ or US-20100299525-\$ or WO-2009073925-\$ or US-20080177998-\$ or EP-1826694-\$ or US-20060133604-\$ or US-20050213768-\$ or EP-1484890-\$ or US-20020163522-\$).did.	US-PGPUB; USPAT; FPRS; DERWENT	OR	ON	2015/11/02 09:16
S46	30	S45 and (system-on-a-chip (random adj nonce) (key with exchang\$3) (session adj key) (stor\$3) hash Diffie-Hellman (Diffie near2 Hellman) d-h)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/02 09:16
S47	3	("7096352").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/11/02 12:56
S48	41	((("20050213766") or ("8615787") or ("20100299525") or ("7069352") or ("20050005093") or ("20110235806") or ("20080037793") or ("20140270166") or ("8627440") or ("20050289343") or ("20110231923") or ("7966646") or ("20100042839") or ("20110161645") or ("20080077809") or ("20060041938")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/11/03 07:56
S51	16	(US-20150039890-\$ or US-20050005093-\$ or US-20100205443-\$ or US-20060041938-\$ or US-20100042839-\$ or US-20050289343-\$ or US-20050213766-\$ or US-20110235806-\$ or US-20140270166-\$ or US-20110231923-\$).did. or (US-8627440-\$ or US-7966646-\$ or US-5657390-\$ or US-7096352-\$ or US-8615787-\$ or US-7069352-\$).did.	US-PGPUB; USPAT	OR	ON	2015/11/04 08:56
S52	16	S51 and (hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric sign verification)	US-PGPUB; USPAT	OR	ON	2015/11/04 09:01
S53	16	S51 and (sign\$3 hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric sign verification)	US-PGPUB; USPAT	OR	ON	2015/11/04 13:01

S54	16	S51 and (sign\$3 hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric sign verification verif\$3)	US-PGPUB; USPAT	OR	ON	2015/11/04 13:06
S55	37	((@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag\$3)) and (cryptograph\$3 with key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/04 13:37
S56	232	((@pd<"20111215" @ad<"20111215") and (diffie-hellman with session with key) and ((global near3 value) prime primitive)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/04 13:40
S57	31	((@pd<"20111215" @ad<"20111215") and (diffie-hellman with session with key) same ((global near3 value) prime primitive)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/04 13:40
S58	16	(US-20150039890-\$ or US-20050005093-\$ or US-20100205443-\$ or US-20060041938-\$ or US-20100042839-\$ or US-20050289343-\$ or US-20050213766-\$ or US-20110235806-\$ or US-20140270166-\$ or US-20110231923-\$).did. or (US-8627440-\$ or US-7966646-\$ or US-5657390-\$ or US-7096352-\$ or US-8615787-\$ or US-7069352-\$).did.	US-PGPUB; USPAT	OR	ON	2015/11/05 09:06
S59	16	S58 and (sign\$3 hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric stor\$3 verification verif\$4)	US-PGPUB; USPAT	OR	ON	2015/11/05 09:06
S60	16	S58 and (sign\$3 hash diffie-hellman d-h system-on-a-chip random nonce session pre-master symmetric stor\$3 verification verif\$4 encrypt\$3 master)	US-PGPUB; USPAT	OR	ON	2015/11/05 09:08
S61	3291	((@pd<"20111215" @ad<"20111215") and ((encrypted adj key) with stor\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 09:51
S62	5	((@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag\$3)) and ((encrypted adj key) with stor\$3)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 09:53
S63	11	S58 and (Diffie-Hellman global prime primitive adj root)	US-PGPUB; USPAT	OR	ON	2015/11/05 12:24
S64	3	S58 and (Diffie-Hellman with (global prime primitive adj root))	US-PGPUB; USPAT	OR	ON	2015/11/05 12:24

EAST Search History

S65	0	((@pd<"20111215" @ad<"20111215") and ((system-on-chip SOC) with secure with (memory storag\$3)) and (Diffie-Hellman with (global prime primitive adj root))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 12:26
S66	409	((@pd<"20111215" @ad<"20111215") and (Diffie-Hellman with (global prime primitive adj root))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 12:26
S67	28	((@pd<"20111215" @ad<"20111215") and ((send\$3 transmit\$3) with (Diffie-Hellman with (global prime primitive adj root)))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2015/11/05 12:27

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S15	3	(generat\$3 with random with nonce with key with exchang\$3 with session with key).clm.	US-PGPUB; USPAT	OR	ON	2015/08/14 11:29
S16	4	"8209533"	US-PGPUB; USPAT	OR	ON	2015/08/14 11:52

11/ 5/ 2015 2:29:05 PM

C:\Users\tle22\Documents\EAST\Workspaces\13997412.wsp

Receipt date: 05/27/2014

13997412 - GAU: 2495

Doc code: IDS

PTO/SB/08a (01-10)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41621US/45631-225520		

U.S. PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
/T.L./	1	8295484	B2	2012-10-23	Buer et al.	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S. PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
/T.L./	1	20140129827	A1	2014-05-08	Khosravi et al.	
/T.L./	2	20130297936	A1	2013-11-07	Khosravi et al.	
/T.L./	3	20130275769	A1	2013-10-17	Khosravi et al.	US equivalent of TW 201340692 below.
/T.L./	4	20120079287	A1	2012-03-29	Leclercq	
/T.L./	5	20070209072	A1	2007-09-06	Chen	

Receipt date: 05/27/2014

13997412 - GAU: 2495

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd M. Khosravi
Art Unit	UNK
Examiner Name	UNK
Attorney Docket Number	P41621US/45631-225520

/T.L./	6	20020163522	A1	2002-11-07	Porter et al.	
--------	---	-------------	----	------------	---------------	--

If you wish to add additional U.S. Published Application citation information please click the Add button. **Add**

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
/T.L./	1	201340692	TW	A	2013-10-01	Intel Corporation	Taiwanese equivalent of US 20130275769 above.	☒

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Thanh Le/	Date Considered	08/20/2015
--------------------	------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd M. Khosravi
Art Unit	UNK
Examiner Name	UNK
Attorney Docket Number	P41621US/45631-225520

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

- ☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

- ☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2014-05-27
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Receipt date: 07/26/2013

13997412 - GAU: 2495

Doc code: IDS

PTO/SB/08a (01-10)

Doc description: Information Disclosure Statement (IDS) Filed

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41624US/45631-225521		

U.S. PATENTS							Remove	
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
	1							
If you wish to add additional U.S. Patent citation information please click the Add button.							Add	
U.S. PATENT APPLICATION PUBLICATIONS							Remove	
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear		
/T.L./	1	20110231923	A1	2011-09-22	Bollay et al.			
/T.L./	2	20100299525	A1	2010-11-25	Shah et al.			
/T.L./	3	20080037793	A1	2008-02-14	Buer			
/T.L./	4	20050213768	A1	2005-09-29	Durham et al.			
If you wish to add additional U.S. Published Application citation information please click the Add button.							Add	
FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41624US/45631-225521		

	1	2013089725	WO	A1	2013-06-20	Intel Corporation		☐
--	---	------------	----	----	------------	-------------------	--	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/T.L./	1	International Search Report and Written Opinion received for International Application No. PCT/US2011/065069, mailed August 30, 2012, 11 pages.	☐
/T.L./	2	"Transport Layer Security," Wikipedia, The Free Encyclopedia, available: [http://en.wikipedia.org/w/index.php?title=Transport_Layer_Security&oldid=464220022], edited December 5, 2011, 19 pages.	☐
/T.L./	3	"HTTP Secure," Wikipedia, The Free Encyclopedia, available: [http://en.wikipedia.org/w/index.php?title=HTTP_Secure&oldid=465003157], edited December 9, 2011, 6 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Thanh Le/	Date Considered	08/20/2015
--------------------	------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd M. Khosravi
Art Unit	UNK
Examiner Name	UNK
Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

- ☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

- ☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- ☐ See attached certification statement.
- ☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- ☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2013-07-26
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



UNITED STATES PATENT AND TRADEMARK OFFICE

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

BIB DATA SHEET

CONFIRMATION NO. 1045

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
13/997,412	04/03/2014 RULE	713	2495	P41624US		
APPLICANTS INVENTORS Hormuzd M. Khosravi, Portland, OR; Edward C. Epp, Portland, OR; Farhana Kabir, Camas, WA; ** CONTINUING DATA ***** This application is a 371 of PCT/US11/65069 12/15/2011 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 10/23/2014						
Foreign Priority claimed ☒ Yes ☐ No 35 USC 119(a-d) conditions met ☒ Yes ☐ No Verified and Acknowledged <u>/THANH T. LE/</u> Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY OR	SHEETS DRAWINGS 4	TOTAL CLAIMS 24	INDEPENDENT CLAIMS 3
ADDRESS Barnes & Thornburg LLP (Intel) c/o CPA Global P.O. Box 52050 Minneapolis, MN 55402 UNITED STATES						
TITLE METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE						
FILING FEE RECEIVED 1800	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit		

Search Notes 	Application/Control No. 13997412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.
	Examiner THANH T LE	Art Unit 2495

CPC- SEARCHED		
Symbol	Date	Examiner
H04L9/0838 H04L9/0841 H04L9/0861 with text	8/14/2015	T.L

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and assignee search with text	8/14/2015	T.L
Interference search with text	8/14/2015	T.L
International and foreign search	8/14/2015	T.L
713/171 with text	8/14/2015	T.L
text based search of claim keywords and synonyms	8/14/2015	T.L
NPL search in IP.com	8/14/2015	T.L

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

--	--

<i>Index of Claims</i> 	Application/Control No. 13997412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.
	Examiner THANH T LE	Art Unit 2495

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

☐ Claims renumbered in the same order as presented by applicant			☐ CPA			☐ T.D.			☐ R.1.47		
CLAIM		DATE									
Final	Original	11/05/2015									
	1	-									
	2	-									
	3	-									
	4	-									
	5	-									
	6	-									
	7	-									
	8	-									
	9	-									
	10	-									
	11	-									
	12	-									
	13	-									
	14	-									
	15	-									
	16	-									
	17	-									
	18	-									
	19	-									
	20	-									
	21	-									
	22	-									
	23	-									
	24	-									
	25	-									
	26	-									
	27	-									
	28	-									
	29	-									
	30	-									
	31	-									
	32	-									
	33	-									
	34	-									
	35	-									
	36	-									

<i>Index of Claims</i> 	Application/Control No. 13997412	Applicant(s)/Patent Under Reexamination KHOSRAVI ET AL.
	Examiner THANH T LE	Art Unit 2495

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

☐ Claims renumbered in the same order as presented by applicant			☐ CPA			☐ T.D.			☐ R.1.47		
CLAIM		DATE									
Final	Original	11/05/2015									
	37	-									
	38	-									
	39	-									
	40	-									
	41	-									
	42	-									
	43	-									
	44	-									
	45	-									
	46	-									
	47	-									
	48	✓									
	49	✓									
	50	✓									
	51	✓									
	52	✓									
	53	✓									
	54	✓									
	55	✓									
	56	✓									
	57	✓									
	58	✓									
	59	✓									
	60	✓									
	61	✓									
	62	✓									
	63	✓									
	64	✓									
	65	✓									
	66	✓									
	67	✓									
	68	✓									
	69	✓									
	70	✓									
	71	✓									

Receipt date: 09/20/2013

13997412 - GAU: 2495

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (01-10)

Approved for use through 07/31/2012. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412	
	Filing Date		2013-06-24	
	First Named Inventor	Hormuzd M. Khosravi		
	Art Unit	UNK		
	Examiner Name	UNK		
	Attorney Docket Number	P41624US/45631-225521		

U.S.PATENTS						
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.L./	1	8205238	B2	2012-06-19	Blumenthal et al.	
/T.L./	2	7813822	B1	2010-10-12	Hoffberg	
/T.L./	3	6324288	B1	2001-11-27	Hoffman	
If you wish to add additional U.S. Patent citation information please click the Add button.						
U.S.PATENT APPLICATION PUBLICATIONS						
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/T.L./	1	20130080764	A1	2013-03-28	Khosravi et al.	
/T.L./	2	20120137137	A1	2012-05-31	Brickell et al.	
/T.L./	3	20110154061	A1	2011-06-23	Chilukuri et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41624US/45631-225521

/T.L./	4	20080229104	A1	2008-09-18	Ju et al.	
/T.L./	5	20080148061	A1	2008-06-19	Jin et al.	
/T.L./	6	20080022395	A1	2008-01-24	Holtzman et al.	
/T.L./	7	20070156987	A1	2007-07-05	Chen	
/T.L./	8	20050114687	A1	2005-05-26	Zimmer et al.	
/T.L./	9	20040243823	A1	2004-12-02	Moyer et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
/T.L./	1	2013089728	WO	A1	2013-06-20	Intel Corporation		☐
/T.L./	2	2013089726	WO	A1	2013-06-20	Intel Corporation		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41624US/45631-225521

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/T.L./	1	BAJIKAR, "Trusted Platform Module (TPM) based Security on Notebook PCs," White Paper, June 20, 2002, 20 pages.	☐
/T.L./	2	INTEL CORP., "Product Brief: Intel® Atom™ Processor CE4100," 2009, 4 pages.	☐
/T.L./	3	"Diffie-Hellman key exchange," Wikipedia, The Free Encyclopedia, available: <http://en.wikipedia.org/w/index.php?title=Diffie%E2%80%93Hellman_key_exchange&oldid=464229141>, accessed December 8, 2011, 9 pages.	☐
/T.L./	4	"Elliptic curve cryptography," Wikipedia, The Free Encyclopedia, available: <http://en.wikipedia.org/w/index.php?title=Elliptic_curve_cryptography&oldid=464634149>, accessed December 8, 2011, 8 pages.	☐
/T.L./	5	"Scrambler," Wikipedia, The Free Encyclopedia, available: <http://en.wikipedia.org/w/index.php?title=Scrambler&oldid=460036487>, accessed December 8, 2011, 4 pages.	☐
/T.L./	6	U.S. Patent Application Serial No. 13/694,221, filed November 8, 2012, 50 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Thanh Le/	Date Considered	08/20/2015
--------------------	------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd M. Khosravi
	Art Unit	UNK
	Examiner Name	UNK
	Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/CHRISTOPHER A. SINGH/	Date (YYYY-MM-DD)	2013-09-20
Name/Print	CHRISTOPHER A. SINGH	Registration Number	61236

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

BARNES & THORNBURG LLP

11 South Meridian Street
Indianapolis, Indiana 46204

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 13/997,412
Confirmation No.: 1045
Art Unit: 2495
Examiner: Le, Thanh T.
Application Title: METHOD AND DEVICE FOR
SECURE COMMUNICATIONS
OVER A NETWORK USING A
HARDWARE SECURITY ENGINE
First Named Inventor: Hormuzd M. Khosravi
Filed: April 3, 2014
Attorney Docket: P41624US/45631-225521

**ELECTRONICALLY
SUBMITTED ON:**

FEBRUARY 15, 2016

RESPONSE TO OFFICE ACTION

MAIL STOP AMENDMENT

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

Sir:

In response to the Office Action dated November 16, 2015, please consider the following:

Amendments to the Claims, which begin on page **2**; and
Remarks, which begin on page **9**.

AMENDMENTS TO THE CLAIMS

1-47. (Canceled)

48. (Currently Amended) A system-on-a-chip apparatus comprising:

a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to:

generate a random nonce for initiating a request for a secure communication session with a server over a network using the nonce;

perform a cryptographic key exchange with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;

encrypt the session key based on the security key; and

store the encrypted session key in the secure memory,

the system-on-a-chip to establish the secure communication session with the server over the network using the session key.

49. (Currently Amended) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive a server nonce from the server in a response message to the request for the secure communication session, the response message including a server nonce and store the server nonce in the secure memory.

50. (Currently Amended) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a pre-master key, encrypt the pre-master key using [[a]] the security key of the security engine, and send the encrypted pre-master key to the server.

51. (Currently Amended) The system-on-a-chip apparatus of claim 50, wherein the security engine is further to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure ~~storage~~ memory.

52. (Currently Amended) The system-on-a-chip apparatus of claim 50, wherein the security engine is further to:

generate the session key as a function of the pre-master key; and

calculate a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

53. (Currently Amended) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using [[a]] the security key of the security engine, and send the signed public Diffie-Hellman key to the server.

54. (Currently Amended) The system-on-a-chip apparatus of claim 53, wherein the security engine is further to receive a public Diffie-Hellman server key from the server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

55. (Currently Amended) The system-on-a-chip apparatus of claim 48, wherein the security engine is further to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure ~~storage~~ memory.

56. (Currently Amended) A method comprising:
generating a random nonce in a security engine of a system-on-a-chip of a client device;

initiating, using the client device, a request for a secure communication session with a server over a network, the request including the random nonce;

performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;

encrypting the session key based on a security key that was encoded in a secure memory of the security engine during a manufacturing process of the system-on-a-chip;

storing the encrypted session key in [[a]] the secure memory of the security engine of the system-on-a-chip; and

establishing, using the client device, the secure communication session with the server using the session key.

57. (Previously Presented) The method of claim 56, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the server; and further comprising:

receiving a ServerHello message from the server, the ServerHello message including a server nonce; and

storing the server nonce in the secure memory of the security engine of the system-on-a-chip.

58. (Currently Amended) The method of claim 56, wherein performing the cryptographic key exchange with the server comprises:

generating a pre-master key in the security engine;

encrypting the pre-master key using [[a]] the security key of the security engine;

and

sending the encrypted pre-master key to the server.

59. (Currently Amended) The method of claim 58, further comprising:

wrapping the pre-master key in the security engine of the system-on-a-chip using a server public key, and

storing the wrapped pre-master key in the secure ~~storage~~ memory of the security engine of the system-on-a-chip.

60. (Previously Presented) The method of claim 58, wherein performing the cryptographic key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

61. (Previously Presented) The method of claim 60, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

62. (Currently Amended) The method of claim 56, wherein performing the cryptographic key exchange with the server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

signing the public Diffie-Hellman client key using ~~[[a]]~~ the security key of the security engine of the system-on-a-chip;

sending the signed public Diffie-Hellman key to the server;

receiving a public Diffie-Hellman server key from the server; and

generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

63. (Currently Amended) The method of claim 56, further comprising:

generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server;

signing the hash code using ~~[[a]]~~ the security key stored in ~~[[a]]~~ the secure memory of the security engine; and

sending a client certificate verification message to the server, the client certificate verification message including the signed hash code.

64. (Currently Amended) One or more non-transitory machine-readable storage media comprising a plurality of instructions stored thereon that, in response to execution by a computing device, cause the computing device to:

generate a random nonce in a security engine of a system-on-a-chip of the computing device;

initiate a request for a secure communication session with a server over a network, the request including the random nonce;

perform a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;

encrypt the session key based on a security key that was encoded in a secure memory of the security engine during a manufacturing process of the system-on-a-chip;

store the session key in [[a]] the secure memory of the security engine of the system-on-a-chip; and

establish the secure communication session with the server using the session key.

65. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 64, wherein to initiate a request for a secure communication session comprises to send a ClientHello message, including the nonce, to the server; and

wherein the plurality of instructions further cause the computing device to:
receive a ServerHello message from the server, the ServerHello message including a server nonce; and

store the server nonce in the secure memory of the security engine of the system-on-a-chip.

66. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the server comprises to:

generate a pre-master key in the security engine;

encrypt the pre-master key using [[a]] the security key of the security engine; and

send the encrypted pre-master key to the server.

67. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 66, wherein the plurality of instructions further cause the computing device to:

wrap the pre-master key in the security engine of the system-on-a-chip with a server public key, and

store the wrapped pre-master key in the secure ~~storage~~ memory of the security engine of the system-on-a-chip.

68. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 66, wherein to perform the cryptographic key exchange with the server comprises to generate the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

69. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 68, wherein to generate the session key in the security engine comprises to calculate, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

70. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 64, wherein to perform the cryptographic key exchange with the server comprises to:

generate, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

sign the public Diffie-Hellman client key using [[a]] the security key of the security engine of the system-on-a-chip;

send the signed public Diffie-Hellman key to the server;

receive a public Diffie-Hellman server key from the server; and

generate, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

71. (Currently Amended) The one or more non-transitory machine-readable storage media of claim 64, wherein the plurality of instructions further cause the computing device to:

generate, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server;

sign the hash code using [[a]] the security key stored in [[a]] the secure memory of the security engine; and

send a client certificate verification message to the server, the client certificate verification message including the signed hash code.

REMARKS

Applicants thank the Examiner for consideration of the present application. Applicants have carefully reviewed the Office Action dated November 16, 2015 (hereinafter “the Office Action”). Claims 1-47 are pending in this application. In the present Response, Applicants have amended claims 48-56, 58, 59, and 62-71 without prejudice or disclaimer of subject matter. Applicants respectfully request reconsideration of the present application in light of the above amendments and the remarks presented below.

I. DRAWING OBJECTION

The Office Action objected to FIG. 2, stating that FIG. 2 recites “RSA Key **Exxcange**” rather than “RSA Key **Exchange**”. A replacement drawing is submitted herewith to address the typographical error. Accordingly, Applicants respectfully request withdrawal of the objection to the drawings.

II. CLAIM REJECTION – 35 U.S.C. § 112, Second Paragraph

The Office Action rejected claim 49 under 35 U.S.C. 112, Second Paragraph stating that there is insufficient antecedent basis for “the response message”. Claim 49 has been amended to address the rejection. More specifically, claim 49 has been amended to recite “to receive a server nonce from the server in a response message . . . the response message including . . .” For at least this reason, Applicants respectfully request withdrawal of the Section 112, Second Paragraph rejection of claim 49.

I. 35 U.S.C. § 101 REJECTIONS

The Office Action rejected each of claims 64-71 as being directed to non-statutory subject matter. Specifically, the Office Action found that the metes and bounds of those claims to not positively limit the invention to non-transitory media. In the interest of expediting prosecution of the present application, Applicants have amended each of claims 64-71 to recite “one or more non-transitory machine-readable storage media.” In so doing, Applicants respectfully submit that the term “non-transitory” excludes only the subject matter of a transitory signal *per se* in accordance with *In re Nuijten*, 500 F. 3d 1346 (Fed. Cir. 2007), and specifically includes machine-readable devices wherein data is stored in a temporary manner, such as volatile

memory devices or RAM. As such, Applicants respectfully submit that those amendments overcome the present Section 101 rejections.

II. 35 U.S.C. § 103(a) REJECTIONS

Each of claims 48-50, 56-58, and 64-66 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,966,646 of Chou et al. (hereinafter “Chou”) in view of U.S. Patent Application Publication No. 2005/0213766 of Goss (hereinafter “Goss”). Additionally, each of claims 51, 52, 59-61, and 67-69 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chou in view of Goss and U.S. Patent Application Publication No. 2009/0280905 to Weisman et al. (hereinafter “Weisman”). Further, each of claims 53, 54, 62, 63, 70, and 71 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chou in view of Goss and U.S. Patent Application No. 2010/0042839 of Ho (hereinafter “Ho”). Additionally, claim 55 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Chou in view of Goss and Ho, in further view of U.S. Patent Application Publication No. 2004/0158715 of Peyravian et al. (hereinafter “Peyravian”). It is well settled that the analysis required under 35 U.S.C. § 103(a) must be resolved on the basis of the factual inquiries outlined in *Graham v. John Deere, Co.*, 383 U.S. 1, 148 USPQ 459 (1966); see *KSR v. Teleflex*, 127 S.Ct. at 1740. The *Graham* Court stated that as part of any analysis under Section 103,

the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined.

148 USPQ at 467. The analysis of obviousness therefore requires an inquiry into the scope and content of the prior art and, more particularly, an inquiry into whether the prior art discloses all of the elements of the claimed invention.

A. Independent Claim 48

In support of the 35 U.S.C. § 103(a) rejection of independent claim 48, the Office Action asserts that Chou in view of Goss describes or suggests every feature of independent claim 48. Applicants disagree. However, in order to expedite prosecution of the present application, Applicants have amended independent claim 48 to recite that the secure memory includes a

security key that was encoded in the secure memory when the system-on-a-chip was manufactured and that the security key is used by the security engine to encrypt a session key. More specifically, claim 1 has been amended to recite: “a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, wherein the secure memory includes a security key that was encoded in the secure memory during a manufacturing process of the system-on-a-chip, the security engine to . . . encrypt the session key based on the security key....”

No combination of Chou and Goss describes or suggests a system-on-a-chip that includes a security engine in which a secure memory of the security engine includes a security key that was encoded in the secure memory when the system-on-a-chip was manufactured. Further, no combination of Chou and Goss describes using such a security key to encrypt a session key. The Office Action acknowledges, on page 5, that Chou does not disclose a system-on-a-chip that includes a security engine. Rather, the Office Action cites Goss at the Abstract and FIG. 1 as allegedly describing a system-on-a-chip having a security engine that includes a secure memory that is accessible only by the security engine. In Goss, a cryptographic accelerator is used to perform encryption functions. The cryptographic accelerator has a key register that receives a key from a secure execution environment (“SEE”) and performs cryptographic functions on behalf of the SEE. As described at paragraph [0024], the key in Goss is stored in RAM, which is a type of volatile memory. In other words, the key is unlike the security key recited in claim 48, which was encoded in the secure memory when the system-on-a-chip was manufactured. Accordingly, in Goss, any cryptographic functions are performed by a cryptographic accelerator that receives a temporary key into a key register from RAM, rather than using a security key that (i) was permanently encoded into a secure memory of a system-on-a-chip when the system-on-a-chip was manufactured and (ii) is accessible only to a security engine residing on the system-on-a-chip. For at least the reasons discussed above, Applicants respectfully submit that the proposed combination of Chou and Goss does not render claim 48 obvious and Applicants respectfully request withdrawal of the Section 103(a) rejection of claim 48.

B. Independent Claim 56

The Office Action also rejected claim 56 under Section 103(a) as being rendered obvious by Chou and Goss, using similar rational as set forth in the rejection of claim 48. Although Applicants respectfully disagree, Applicants have amended independent claim 56 in a manner similar to amended independent claim 48, in order to expedite prosecution. As such, all of the arguments presented above with regard to amended independent claim 48 apply with equal force to the rejection of amended claim 56 and are incorporated into this section by reference. Accordingly, Applicants submit that the proposed combination of Chou and Goss does not render claim 56 obvious and Applicants respectfully request withdrawal of the Section 103(a) rejection of claim 56.

C. Independent Claim 64

The Office Action also rejected claim 64 under Section 103(a) as being rendered obvious by Chou and Goss, using similar rational as set forth in the rejection of claim 48. Although Applicants respectfully disagree, Applicants have amended independent claim 64 in a manner similar to amended independent claim 48, in order to expedite prosecution. As such, all of the arguments presented above with regard to amended independent claim 48 apply with equal force to the rejection of amended claim 64 and are incorporated into this section by reference. Accordingly, Applicants submit that the proposed combination of Chou and Goss does not render claim 64 obvious and Applicants respectfully request withdrawal of the Section 103(a) rejection of claim 64.

D. Dependent Claims 49-55, 57-63, and 65-71

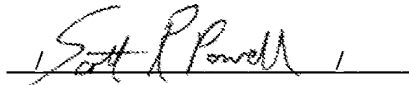
Each of claims 49-55 includes independent claim 48 as a base claim; each of claims 57-63 includes independent claim 56 as a base claim; and each of claims 65-71 includes independent claim 64 as a base claim. Weisman, Ho, and Peyravian do not cure the deficiencies of Chou and Goss with respect to independent claims 48, 56, and 64. Accordingly, Applicants respectfully request withdrawal of the Section 103(a) rejection of claims 49-55, 57-63, and 65-71. Any arguments specific to claims 49-55, 57-63, and 65-71 are held in abeyance without prejudice or admission to any assertion made in the Office Action in order to expedite prosecution.

III. CONCLUSION

In view of the foregoing, it is submitted that this application is in a condition for allowance. Action to that end is hereby solicited. If there are any questions or comments that would expedite prosecution of this application, the Examiner is invited to call the undersigned at (317) 231-7307.

It is respectfully requested that, if necessary to effect a timely response, this paper be considered as a Petition for an Extension of Time sufficient to effect a timely response. The Commissioner is hereby authorized to charge the fee for such Petition, if needed, and any shortage of fees, and credit any overpayment of fees, to the Account of Barnes & Thornburg, Deposit Account No. 10-0435 with reference to file P41624US/45631-225521.

Respectfully submitted,

A handwritten signature in dark ink, appearing to read "Scott R. Powell", is written over a horizontal line.

Scott R. Powell
Registration No. 58,378
Barnes & Thornburg
11 South Meridian Street
Indianapolis, Indiana 46204-3535
Telephone: (317) 231-7307

REPLACEMENT SHEET

200

LEVEL 0	PROTECTION OF CLIENT PRIVATE DEVICE KEY USED FOR SIGNING & VERIFICATION	
LEVEL 1	PROTECTION OF SESSION KEYS USED FOR DATA ENCRYPTION	
	RSA KEY EXCHANGE	DIFFIE-HELLMAN KEY EXCHANGE
	PROTECTION OF PRE-MASTER KEY	PROTECTION OF CLIENT PRIVATE DH KEY
LEVEL 2	PROTECTION OF APPLICATION DATA	

FIG. 2

Electronic Acknowledgement Receipt	
EFS ID:	24912659
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Scott Rylan Powell/Priscilla York
Filer Authorized By:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	15-FEB-2016
Filing Date:	03-APR-2014
Time Stamp:	15:58:02
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	225521_Response_To_Office_Action.pdf	65979 85170e9b87fb3740145b3fbaf1f04bdb68398964	no	13

Warnings:

Information:

2	Drawings-only black and white line drawings	Replacement_FIG_2.pdf	19847 5527689954fa726d154890c6d5eb8237c8c34f07	no	1
Warnings:					
Information:					
Total Files Size (in bytes):				85826	
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

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

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 13/997,412		Filing Date 04/03/2014		☐ To be Mailed	
ENTITY: ☒ LARGE ☐ SMALL ☐ MICRO									
APPLICATION AS FILED – PART I									
(Column 1)		(Column 2)							
FOR		NUMBER FILED		NUMBER EXTRA		RATE (\$)		FEE (\$)	
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A		N/A		N/A			
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))		N/A		N/A		N/A			
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A		N/A		N/A			
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 = *				X \$ =			
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 = *				X \$ =			
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).							
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))									
* If the difference in column 1 is less than zero, enter "0" in column 2.						TOTAL			
APPLICATION AS AMENDED – PART II									
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT	02/15/2016	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	* 24	Minus	** 24	= 0	X \$80 =		0	
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	X \$420 =		0	
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE		0	
(Column 1)		(Column 2)		(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)	
	Total (37 CFR 1.16(i))	*	Minus	**	=	X \$ =			
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =			
	☐ Application Size Fee (37 CFR 1.16(s))								
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))								
						TOTAL ADD'L FEE			
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.									

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

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

Doc code: IDS

Doc description: Information Disclosure Statement (IDS) Filed

PTO/SB/08a (03-15)

Approved for use through 07/31/2016. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

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

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd Khosravi
	Art Unit	2495
	Examiner Name	Le, Thanh T.
	Attorney Docket Number	P41624US/45631-225521

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	8014530		2011-09-06	Ernest Brickell	
	2	7802085		2010-09-21	Gary L. Graunke	
	3	7747862		2010-06-29	Shlomo Ovadia	
	4	7350083		2008-03-25	Steven E. Wells	
	5	6948065		2005-09-20	David W. Grawrock	
	6	7600132		2009-10-06	Fadi A. Mahmoud	
	7	6401208		2002-06-04	DEREK L DAVIS	
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		13997412
Filing Date		2013-06-24
First Named Inventor	Hormuzd Khosravi	
Art Unit	2495	
Examiner Name	Le, Thanh T.	
Attorney Docket Number	P41624US/45631-225521	

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20080244267		2008-10-02	Vincent J. Zimmer	
	2	20070138229		2007-06-21	Yasuyuki Fujimoto	
	3	20110154023		2011-06-23	Ned M. Smith	
	4	20060005011		2006-01-05	Masakazu Satoh	
	5	20070240200		2007-10-11	Hee-chul Han	
	6	20130297936		2013-11-07	Hormuzd M. Khosravi	
	7	20050144436		2005-06-30	Tse-Min Chen	
	8	20030236970		2003-12-25	Rodney Wendell Palmer	
	9	20090319804		2009-12-24	Zheng Qi	
	10	20080256363		2008-10-16	Boris Balacheff	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	13997412
Filing Date	2013-06-24
First Named Inventor	Hormuzd Khosravi
Art Unit	2495
Examiner Name	Le, Thanh T.
Attorney Docket Number	P41624US/45631-225521

11	20070192611	2007-08-16	Shamanna M. Datta
12	20020112161	2002-08-15	Fred C. Thomas
13	20080077809	2008-03-27	Don L. Hayler
14	20110161645	2011-06-30	Jiang Zhang
15	20050213766	2005-09-29	Steven C. Goss
16	20080005586	2008-01-03	Peter Munguia

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2011119985	WO		2011-09-29	Maxlinear, Inc.		
	2	2013089725	WO		2013-06-20	Intel Corporation		

If you wish to add additional Foreign Patent Document citation information please click the Add button.

Add

NON-PATENT LITERATURE DOCUMENTS

Remove

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		13997412
	Filing Date		2013-06-24
	First Named Inventor	Hormuzd Khosravi	
	Art Unit	2495	
	Examiner Name	Le, Thanh T.	
	Attorney Docket Number	P41624US/45631-225521	

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	Taiwanese Office Action issued in connection with Taiwanese Application No. 101147203, completed December 29, 2014, 11 pages	×
	2	International Preliminary Report on Patentability received for PCT International Application No. PCT/US2011/065072, mailed June 26, 2014, 6 pages.	☐
	3	International Search Report and Written Opinion received for International Application No. PCT/US2011/065072, Mailed July 18, 2012, 10 Pages	☐
	4	Platform Independent Overall Security architecture in multi-processor system-on-chip integrated circuits for use in mobile phones and handheld devices. Ashkenazi et al. EISevier (2007)	☐
	5	Data Security Architure using Embedded Chip. Thomas et al. IJCSNS (May 2011)	☐
	6	Scalable Architectural Support for Trusted Software. Champagne et al. IEEE (2009)	☐
	7	Secure Memory Accesses on Networks-on Chip. Fiorin et al. IEEE (2009)	☐
	8	Extended European Search Report issued in connection with European Application No. 11877254.0 - 1853, dated July 17, 2015, 8 pages	☐
	9	HITACHI, Ltd., "Digital Transmission Content Protection Specification Revision 1.7," December 14, 2011, Retrieved from the Internet: URL: http://www.dtcp.com/documents/dtcp/info-20111214-dtcp-v1-rev-1-p-7.pdf (retrieved on 2014-07-21), Chapter 4: Full Authentication and Chapter 6: Content Channel Management and Protection.	☐
	10	Intel Corp., Product Brief: Intel Atom Processor CE4100, 2009, Pg. 1-4	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd Khosravi
	Art Unit	2495
	Examiner Name	Le, Thanh T.
	Attorney Docket Number	P41624US/45631-225521

11	Digital Transmission License Administrator, Digital Transmission Content Protection Specification, March 19, 2010, Volume 1, Pg. 11, 26-29, and 36-38	☐
12	Broadcom, August 24, 2011, What is BCM7309 - Single-Chip Back-End Set-Top Decoder, http:// Web.archive.org/web/20110824145230/http://www.broadcom.com/products/Cable/Cable-Set-Top-Box-Solutions/BCM7309	☐

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	13997412
	Filing Date	2013-06-24
	First Named Inventor	Hormuzd Khosravi
	Art Unit	2495
	Examiner Name	Le, Thanh T.
	Attorney Docket Number	P41624US/45631-225521

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Scott R. Powell/	Date (YYYY-MM-DD)	2015-02-17
Name/Print	Scott R. Powell	Registration Number	58378

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:		13997412		
Filing Date:		03-Apr-2014		
Title of Invention:		METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE		
First Named Inventor/Applicant Name:		Hormuzd M. Khosravi		
Filer:		Scott Rylan Powell/Priscilla York		
Attorney Docket Number:		P41624US/45631-225521		
Filed as Large Entity				
Filing Fees for U.S. National Stage under 35 USC 371				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				180

Electronic Acknowledgement Receipt	
EFS ID:	24924828
Application Number:	13997412
International Application Number:	
Confirmation Number:	1045
Title of Invention:	METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE
First Named Inventor/Applicant Name:	Hormuzd M. Khosravi
Customer Number:	73486
Filer:	Scott Rylan Powell/Priscilla York
Filer Authorized By:	Scott Rylan Powell
Attorney Docket Number:	P41624US/45631-225521
Receipt Date:	17-FEB-2016
Filing Date:	03-APR-2014
Time Stamp:	09:57:14
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$180
RAM confirmation Number	9706
Deposit Account	100435
Authorized User	KELLETT, GLEN M.
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 CFR 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 CFR 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 CFR 1.19 (Document supply fees)					
Charge any Additional Fees required under 37 CFR 1.20 (Post Issuance fees)					
Charge any Additional Fees required under 37 CFR 1.21 (Miscellaneous fees and charges)					
Charge any Additional Fees required under 37 CFR 1.492(a) (basic national fee only)					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	Ashkenazi_et_al.pdf	1470181 a9b1ae7e71836fe43265cd392774bb3fcc16b506	no	18
Warnings:					
Information:					
2	Non Patent Literature	Broadcom_What_is_BCM7309.pdf	365745 927c5b686958457482bfcc54784bfab28c5d4cade	no	1
Warnings:					
Information:					
3	Non Patent Literature	Champagne_et_al.pdf	1610561 3319cc40bb0c84575d40eeda083b659bc3a7196f	no	12
Warnings:					
Information:					
4	Non Patent Literature	Digital_Transmission_Content_Protection_Specification.pdf	2841835 6dc677d1a1c8d112a26331a7c4cfa79e120a6adf5	no	80
Warnings:					
Information:					
5	Non Patent Literature	European_Search_Report_11877254.pdf	305438 46306862870a2731e23d492a9b2d1d6e51fd08e7	no	8
Warnings:					
Information:					
6	Non Patent Literature	Fiorin_et_al.pdf	1593557 f257cd29dafaebc5125dea9a60e43fd700acfd0b4	no	14
Warnings:					
Information:					
7	Non Patent Literature	Hitachi_LTD.pdf	3941756 27f5799303e0cc8919104fbd0f5afc81bd28ad06	no	84
Warnings:					
Information:					

8	Non Patent Literature	Intel_Atom_Processor_CE4100.pdf	1164799	no	4
			7c06ea629f1ea46d529e3368d77285d3242ed809		
Warnings:					
Information:					
9	Non Patent Literature	International_Preliminary_Report_PCT_US2011065072.pdf	235859	no	6
			f7bbd856b95a790b9740a5089057cbc3c0dd23d1		
Warnings:					
Information:					
10	Non Patent Literature	International_Search_Report_PCT_US2011_065072.pdf	388711	no	10
			5e8f35baab524fbc0e0cec9c973d36e24f12f1bf		
Warnings:					
Information:					
11	Non Patent Literature	Taiwanese_Office_Action_English.pdf	365280	no	8
			864838175e7f570442033979da8308c20fedee7d		
Warnings:					
Information:					
12	Non Patent Literature	Thomas_et_al.pdf	821404	no	9
			d4d7074816e7b39aa0b00bc9d44713cf02d10ac9		
Warnings:					
Information:					
13	Foreign Reference	WO2013089725.pdf	21808301	no	37
			86c2667e033dd19e8048f6f403339466f58a21e2		
Warnings:					
Information:					
14	Foreign Reference	WO2011119985.pdf	2226295	no	49
			2eba21c77ce10c42773db5e5629fac7fd763d94dd		
Warnings:					
Information:					
15	Non Patent Literature	Taiwanese_Office_Action.pdf	501058	no	11
			b9d7da779446721e7f036827741309c0b53b4f5c		
Warnings:					
Information:					
16	Information Disclosure Statement (IDS) Form (SB08)	P41624US_IDS.pdf	1037066	no	7
			210fb502e06058c3c5727e7fad70da4c13e5771d		
Warnings:					
Information:					

17	Fee Worksheet (SB06)	fee-info.pdf	31299 b5817d56414b65f8aea409666e4ae835b1206d5c	no	2
Warnings:					
Information:					
Total Files Size (in bytes):				40709145	
This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503. <u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application. <u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course. <u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.					

ADVANCE E-MAIL

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
TRANSMITTAL OF COPY OF INTERNATIONAL
PRELIMINARY REPORT ON PATENTABILITY
(CHAPTER I OF THE PATENT COOPERATION
TREATY)
(PCT Rule 44bis.1(c))

To:

KELLETT, Glen M.
Barnes & Thornburg, LLP
C/O CPA Global
PO Box 52050
Minneapolis, Minnesota 55402
ETATS-UNIS D'AMERIQUE

Date of mailing (<i>day/month/year</i>) 26 June 2014 (26.06.2014)		
Applicant's or agent's file reference P41620PCT		IMPORTANT NOTICE
International application No. PCT/US2011/065072	International filing date (<i>day/month/year</i>) 15 December 2011 (15.12.2011)	
Priority date (<i>day/month/year</i>)		
Applicant INTEL CORPORATION et al		

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Simin Baharlou
Facsimile No. +41 22 338 82 70	e-mail: pt09.pct@wipo.int

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44bis)

Applicant's or agent's file reference P41620PCT	FOR FURTHER ACTION	See item 4 below
International application No. PCT/US2011/065072	International filing date (<i>day/month/year</i>) 15 December 2011 (15.12.2011)	Priority date (<i>day/month/year</i>)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant INTEL CORPORATION		

1.	This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 bis.1(a).																								
2.	This REPORT consists of a total of 5 sheets, including this cover sheet. In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.																								
3.	This report contains indications relating to the following items: <table style="width: 100%; border: none;"> <tr> <td style="width: 5%; text-align: center;">☒</td> <td style="width: 30%;">Box No. I</td> <td style="width: 65%;">Basis of the report</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. II</td> <td>Priority</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. III</td> <td>Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. IV</td> <td>Lack of unity of invention</td> </tr> <tr> <td style="text-align: center;">☒</td> <td>Box No. V</td> <td>Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VI</td> <td>Certain documents cited</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VII</td> <td>Certain defects in the international application</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VIII</td> <td>Certain observations on the international application</td> </tr> </table>	☒	Box No. I	Basis of the report	☐	Box No. II	Priority	☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability	☐	Box No. IV	Lack of unity of invention	☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement	☐	Box No. VI	Certain documents cited	☐	Box No. VII	Certain defects in the international application	☐	Box No. VIII	Certain observations on the international application
☒	Box No. I	Basis of the report																							
☐	Box No. II	Priority																							
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability																							
☐	Box No. IV	Lack of unity of invention																							
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement																							
☐	Box No. VI	Certain documents cited																							
☐	Box No. VII	Certain defects in the international application																							
☐	Box No. VIII	Certain observations on the international application																							
4.	The International Bureau will communicate this report to designated Offices in accordance with Rules 44bis.3(c) and 93bis.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44bis .2).																								

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Date of issuance of this report 17 June 2014 (17.06.2014)</td> </tr> <tr> <td style="padding: 2px;"> Authorized officer Simin Baharlou </td> </tr> </table> e-mail: pt09.pct@wipo.int	Date of issuance of this report 17 June 2014 (17.06.2014)	Authorized officer Simin Baharlou
Date of issuance of this report 17 June 2014 (17.06.2014)			
Authorized officer Simin Baharlou			

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

KELLETT GLEN M.

BARNES & THORNBURG, LLP C/O CPA GLOBAL PO
BOX 52050 MINNEAPOLIS MN 55402 USA

PCT

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

(PCT Rule 43bis.1)

Date of mailing
(day/month/year) **18 JULY 2012 (18.07.2012)**

Applicant's or agent's file reference
P41620PCT

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US2011/065072

International filing date (day/month/year)

15 DECEMBER 2011 (15.12.2011)

Priority date(day/month/year)

International Patent Classification (IPC) or both national classification and IPC

G06F 21/20(2006.01)i, G06F 21/22(2006.01)i

Applicant

INTEL CORPORATION et al

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon
Metropolitan City, 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140



Date of completion of this opinion

31 MAY 2012 (31.05.2012)

Authorized officer

UHM, In Kwon

Telephone No. 82-42-481-5712



**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/065072

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :
 - ☒ the international application in the language in which it was filed
 - ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis* 1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:
 - a. a sequence listing filed or furnished
 - ☐ on paper
 - ☐ in electronic form
 - b. time of filing or furnishing
 - ☐ contained in the international application as filed.
 - ☐ filed together with the international application in electronic form.
 - ☐ furnished subsequently to this Authority for the purposes of search.
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065072

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-40	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	3-13,15-29,32-40	YES
	Claims	1-2,14,30-31	NO
Industrial applicability (IA)	Claims	1-40	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2004-0243823 A1 (MOYER WILLIAM C. et al.) 02 December 2004
D2: US 2005-0114687 A1 (VINCENT ZIMMER et al.) 26 May 2005
D3: US 2007-0156987 A1 (IUE-SHUENN CHEN et al.) 05 July 2007
D4: US 2008-0022395 A1 (MICHAEL HOLTZMAN et al.) 24 January 2008

1. NOVELTY AND INVENTIVE STEP

1-1. claim 1, 14, 30-31

D1, which are closest to claims 1, discloses a system-on-a-chip apparatus comprising:

a memory having at least one protected region to store at least decrypted media content therein(Par.[0017]: the processor reads the data stored in the storage area to be subject to encryption processing based on the information acquired from the processing up to the execution of the encryption application processing(S40));

a system-on-a-chip comprising(Par.[0011]: the processor reads the data stored in the storage area to be subject to encryption processing based on the information acquired from the processing up to the execution of the encryption application processing(S40));

a memory controller coupled to the memory to enforce protection of the protected memory region such that access to the protected memory region is permitted only to authenticated peripheral devices of the system-on-a-chip(Par.[0014]: the processor reads the data stored in the storage area to be subject to encryption processing based on the information acquired from the processing up to the execution of the encryption application processing(S40)).

a security engine coupled to the memory controller to authenticate a firmware of a hardware peripheral of the system-on-a-chip to allow the hardware peripheral access to the protected memory region of the memory(Par.[0022]: Master 12 access protection field 70 includes master 12 read access protection field 72 which indicates whether master 12 is allowed to perform read accesses to non-volatile memory 36 and master 12 write access protection field 74 which indicates whether master 12 is allowed to perform write accesses to non-volatile memory 36)

Continued on Supplemental Box

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065072

Supplemental Box

In case **the space in any of the preceding boxes is not sufficient.**

Continuation of :

Box V

Although D1 doesn't manifest the protected memory region of claim 1, it is disclosed in D2(FIG.1: If the memory access request is an access to the protected firmware resources 106; Par.[0064]: the memory access request is checked to determine if it is an access request to firmware data (block 706). If the memory request access is an access request to firmware data, another check is made to determine if the memory access request was made by firmware code (block 708). If the memory access request was made by firmware code, the memory access is allowed (block 710)).

Thus, claim 1 is considered to lack an inventive step over the combination of D1 and D2.

Also, claims 14, 30, 31 are considered to lack an inventive step over the combination of D1 and D2 because they share the same technical features as those of claim 1.

1-2. claim 2-13, 15-29

The additional feature of claim 2 is disclosed in D2(Par.[0048],[0062]-[0067]: Fig.4,7). Thus, claim 2 is considered to lack an inventive step over the combination of D1 and D2.

None of the prior art documents reveal the additional features of claims 3-13, and 15-29. Thus claims 3-13, and 15-29 are considered to meet the requirement according to PCT Article 33(3) and (2).

1-3. claim 32-40

None of the prior art documents reveal the step of authenticating the peripheral cryptographic key using a security cryptographic key of the security engine of claim 32. Thus claim 32 is considered to meet the requirement according to PCT Article 33(3) and (2).

Also, claims 33-40 are considered to meet the requirement according to PCT Article 33(3) and (2) because they are dependent on claim 32.

2. INDUSTRIAL APPLICABILITY

Claims 1-40 are industrially applicable under PCT Article 33(4).

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:

KELLETT GLEN M.

BARNES & THORNBURG, LLP C/O CPA GLOBAL PO
BOX 52050 MINNEAPOLIS MN 55402 USA**PCT****NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT AND
THE WRITTEN OPINION OF THE INTERNATIONAL
SEARCHING AUTHORITY, OR THE DECLARATION**

(PCT Rule 44.1)

Date of mailing
(day/month/year) 18 JULY 2012 (18.07.2012)

Applicant's or agent's file reference

P41620PCT

FOR FURTHER ACTION See paragraphs 1 and 4 below

International application No.

PCT/US2011/065072International filing date
(day/month/year)**15 DECEMBER 2011 (15.12.2011)**

Applicant

INTEL CORPORATION et al

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the international search report.**Where?** Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: +41 22 338 82 70**For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004, 9.011.**

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:
☐ the protest together with the decision thereon has been transmitted to the International Bureau together with any request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.**4. Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before the completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the PCT Applicant's Guide, National Chapters.

Name and mailing address of the ISA/KR



Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

COMMISSIONER

Telephone No. 82-42-481-8754



Form PCT/ISA/220 (July 2010)

*** Attention**

Copies of the documents cited in the international search report can be searched in the following Korean Intellectual Property Office English website for three months from the date of mailing of the international search report.

<http://www.kipo.go.kr/en/> => PCT Services => PCT Services

ID : PCT international application number

PW : **Z2KU63Q7**

Inquiries related to PCT International Search Report or Written Opinion prepared by KIPO as an International Searching Authority can be answered not only by KIPO but also through IPKC (Intellectual Property Korea Center), located in Vienna, VA, which functions as a PCT Help Desk for PCT applicants.

Homepage: <http://www.ipkcenter.com>

Email: ipkc@ipkcenter.com

Phone: +1 703 388 1066

Fax: +1 703 388 1084

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference P41620PCT	FOR FURTHER ACTION see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US2011/065072	International filing date (<i>day/month/year</i>) 15 DECEMBER 2011 (15.12.2011)	(Earliest) Priority Date (<i>day/month/year</i>)
Applicant INTEL CORPORATION et al		

This International search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

☐ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

- ☒ the international application in the language in which it was filed
☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

- b. ☐ This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).
c. ☐ With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. ☐ **Certain claims were found unsearchable** (See Box No. II)

3. ☐ **Unity of invention is lacking** (See Box No. III)

4. With regard to the **title**,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

- ☒ the text is approved as submitted by the applicant.
☐ the text has been established, according to Rule 38.2, by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. With regard to the **drawings**,

- a. the figure of the **drawings** to be published with the abstract is Figure No. 1
☒ as suggested by the applicant.
☐ as selected by this Authority, because the applicant failed to suggest a figure.
☐ as selected by this Authority, because this figure better characterizes the invention.
b. ☐ none of the figure is to be published with the abstract.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/065072**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/20(2006.01)i, G06F 21/22(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/20; G06F 12/14; H04L 9/32; H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords:

(SOC*,systemonchip*,systemonachip*,embed*,embedded*+)(peripheral*,demux*,video*,preparser*,DPE*,DSP*,audio*+)(firmwar*,softwar* applicat* PROGRAM* SW* DRIVER*+)(authentica* access* VALIDATION* CERTIE*+)(protect* secur* hidden* lock* shield

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 2004-0243823 A1 (MOYER WILLIAM C. et al.) 02 December 2004 See abstract, paragraphs [0011],[0014],[0017],[0022] and figures 1-3	1,2,14,30,31 3-13,15-29,32-40
Y A	US 2005-0114687 A1 (VINCENT ZIMMER et al.) 26 May 2005 See abstract, paragraphs [0048],[0062]-[0067] and figure 4,7	1,2,14,30,31 3-13,15-29,32-40
A	US 2007-0156987 A1 (IUE-SHUENN CHEN et al.) 05 July 2007 See abstract, paragraphs [0038]-[0039] and figure 5	1-40
A	US 2008-0022395 A1 (MICHAEL HOLTZMAN et al.) 24 January 2008 See abstract, paragraphs [0064], [0066] and figure 2	1-40



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents.	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier application or patent but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

31 MAY 2012 (31.05.2012)

Date of mailing of the international search report

18 JULY 2012 (18.07.2012)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

UHM, In Kwon

Telephone No. 82-42-481-5712



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/065072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004-0243823 A1	02.12.2004	CN 1799030 A	05.07.2006
		CN 1799030 C0	27.02.2008
		JP 2007-501477 A	25.01.2007
		JP 2007-501477 T	25.01.2007
		KR 10-1010801 B1	25.01.2011
		KR20060032954A	18.04.2006
		US 7444668 B2	28.10.2008
		WO 2004-107176 A1	09.12.2004
US 2005-0114687 A1	26.05.2005	None	
US 2007-0156987 A1	05.07.2007	None	
US 2008-0022395 A1	24.01.2008	CN 101484903 A	15.07.2009
		CN 101484904 A	15.07.2009
		CN 101490687 A	22.07.2009
		CN 101490688 A	22.07.2009
		CN 101490689 A	22.07.2009
		EP 2038799 A2	25.03.2009
		EP 2038800 A2	25.03.2009
		EP 2038802 A2	25.03.2009
		EP 2038803 A2	25.03.2009
		EP 2038804 A2	25.03.2009
		JP 2009-543207 A	03.12.2009
		JP 2009-543208 A	03.12.2009
		JP 2009-543210 A	03.12.2009
		JP 2009-543211 A	03.12.2009
		JP 2009-543212 A	03.12.2009
		KR 10-2009-0026357 A	12.03.2009
		KR 10-2009-0028806 A	19.03.2009
		KR 10-2009-0033191 A	01.04.2009
		KR 10-2009-0034332 A	07.04.2009
		KR 10-2009-0052321 A	25.05.2009
		TW 200821837 A	16.05.2008
		TW 200822669 A	16.05.2008
		TW 200822670 A	16.05.2008
		TW 200823715 A	01.06.2008
		US 2008-0010449 A1	10.01.2008
		US 2008-0010450 A1	10.01.2008
		US 2008-0010451 A1	10.01.2008
		US 2008-0010452 A1	10.01.2008
		US 2008-0010455 A1	10.01.2008
		US 2008-0010458 A1	10.01.2008
		US 2008-0010685 A1	10.01.2008
		US 2008-0022413 A1	24.01.2008
		US 2008-0034440 A1	07.02.2008
		US 2010-0138652 A1	03.06.2010
		US 8140843 B2	20.03.2012
		WO 2008-008243 A2	17.01.2008

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2011/065072

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		WO 2008-008243 A3	17.01.2008
		WO 2008-008244 A2	17.01.2008
		WO 2008-008244 A3	17.01.2008
		WO 2008-008245 A2	17.01.2008
		WO 2008-008245 A3	17.01.2008
		WO 2008-013655 A2	31.01.2008
		WO 2008-013655 A3	31.01.2008
		WO 2008-013656 A2	31.01.2008
		WO 2008-013656 A3	31.01.2008
		WO 2011-075281 A1	23.06.2011

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

KELLETT GLEN M.

BARNES & THORNBURG, LLP C/O CPA GLOBAL PO
BOX 52050 MINNEAPOLIS MN 55402 USA

PCT

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

(PCT Rule 43bis.1)

Date of mailing
(day/month/year) **18 JULY 2012 (18.07.2012)**

Applicant's or agent's file reference

P41620PCT

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US2011/065072

International filing date (day/month/year)

15 DECEMBER 2011 (15.12.2011)

Priority date(day/month/year)

International Patent Classification (IPC) or both national classification and IPC

G06F 21/20(2006.01)i, G06F 21/22(2006.01)i

Applicant

INTEL CORPORATION et al

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon
Metropolitan City, 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140



Date of completion of this opinion

31 MAY 2012 (31.05.2012)

Authorized officer

UHM, In Kwon

Telephone No.82-42-481-5712



Form PCT/ISA/237 (cover sheet) (July 2011)

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065072

Box No. 1 Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - ☒ the international application in the language in which it was filed
 - ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:
 - a. a sequence listing filed or furnished
 - ☐ on paper
 - ☐ in electronic form
 - b. time of filing or furnishing
 - ☐ contained in the international application as filed.
 - ☐ filed together with the international application in electronic form.
 - ☐ furnished subsequently to this Authority for the purposes of search.
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065072

**Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability;
citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-40	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	3-13,15-29,32-40	YES
	Claims	1-2,14,30-31	NO
Industrial applicability (IA)	Claims	1-40	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2004-0243823 A1 (MOYER WILLIAM C. et al.) 02 December 2004
D2: US 2005-0114687 A1 (VINCENT ZIMMER et al.) 26 May 2005
D3: US 2007-0156987 A1 (IUE-SHUENN CHEN et al.) 05 July 2007
D4: US 2008-0022395 A1 (MICHAEL HOLTZMAN et al.) 24 January 2008

1. NOVELTY AND INVENTIVE STEP

1-1. claim 1, 14, 30-31

D1, which are closest to claims 1, discloses a system-on-a-chip apparatus comprising:

a memory having at least one protected region to store at least decrypted media content therein(Par.[0017]: the processor reads the data stored in the storage area to be subject to encryption processing based on the information acquired from the processing up to the execution of the encryption application processing(S40));

a system-on-a-chip comprising(Par.[0011]: the processor reads the data stored in the storage area to be subject to encryption processing based on the information acquired from the processing up to the execution of the encryption application processing(S40));

a memory controller coupled to the memory to enforce protection of the protected memory region such that access to the protected memory region is permitted only to authenticated peripheral devices of the system-on-a-chip(Par.[0014]: the processor reads the data stored in the storage area to be subject to encryption processing based on the information acquired from the processing up to the execution of the encryption application processing(S40)).

a security engine coupled to the memory controller to authenticate a firmware of a hardware peripheral of the system-on-a-chip to allow the hardware peripheral access to the protected memory region of the memory(Par.[0022]: Master 12 access protection field 70 includes master 12 read access protection field 72 which indicates whether master 12 is allowed to perform read accesses to non-volatile memory 36 and master 12 write access protection field 74 which indicates whether master 12 is allowed to perform write accesses to non-volatile memory 36)

Continued on Supplemental Box

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/065072

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of :

Box V

Although D1 doesn't manifest the protected memory region of claim 1, it is disclosed in D2 (FIG. 1: If the memory access request is an access to the protected firmware resources 106; Par. [0064]: the memory access request is checked to determine if it is an access request to firmware data (block 706). If the memory request access is an access request to firmware data, another check is made to determine if the memory access request was made by firmware code (block 708). If the memory access request was made by firmware code, the memory access is allowed (block 710)).

Thus, claim 1 is considered to lack an inventive step over the combination of D1 and D2.

Also, claims 14, 30, 31 are considered to lack an inventive step over the combination of D1 and D2 because they share the same technical features as those of claim 1.

1-2. claim 2-13, 15-29

The additional feature of claim 2 is disclosed in D2 (Par. [0048], [0062]-[0067]; Fig. 4, 7). Thus, claim 2 is considered to lack an inventive step over the combination of D1 and D2.

None of the prior art documents reveal the additional features of claims 3-13, and 15-29. Thus claims 3-13, and 15-29 are considered to meet the requirement according to PCT Article 33(3) and (2).

1-3. claim 32-40

None of the prior art documents reveal the step of authenticating the peripheral cryptographic key using a security cryptographic key of the security engine of claim 32. Thus claim 32 is considered to meet the requirement according to PCT Article 33(3) and (2).

Also, claims 33-40 are considered to meet the requirement according to PCT Article 33(3) and (2) because they are dependent on claim 32.

2. INDUSTRIAL APPLICABILITY

Claims 1-40 are industrially applicable under PCT Article 33(4).

PATENT COOPERATION TREATY

PCT/US2011/065072

ADVANCE E-MAIL

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
TRANSMITTAL OF COPY OF INTERNATIONAL
PRELIMINARY REPORT ON PATENTABILITY
(CHAPTER I OF THE PATENT COOPERATION
TREATY)

(PCT Rule 44bis.1(c))

To:

KELLETT, Glen M.
Barnes & Thornburg, LLP
C/O CPA Global
PO Box 52050
Minneapolis, Minnesota 55402
ETATS-UNIS D'AMERIQUE

Date of mailing (day/month/year)

26 June 2014 (26.06.2014)

Applicant's or agent's file reference

P41620PCT

IMPORTANT NOTICE

International application No.

PCT/US2011/065072

International filing date (day/month/year)

15 December 2011 (15.12.2011)

Priority date (day/month/year)

Applicant

INTEL CORPORATION et al

The International Bureau transmits herewith a copy of the international preliminary report on patentability (Chapter I of the Patent Cooperation Treaty)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer

Simin Baharlou

Facsimile No. +41 22 338 82 70

e-mail: pct@wipo.int

Form PCT/IB/326 (January 2004)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY (Chapter I of the Patent Cooperation Treaty)

(PCT Rule 44bis)

Applicant's or agent's file reference P41620PCT	FOR FURTHER ACTION	See item 4 below
International application No. PCT/US2011/065072	International filing date (<i>day/month/year</i>) 15 December 2011 (15.12.2011)	Priority date (<i>day/month/year</i>)
International Patent Classification (8th edition unless older edition indicated) See relevant information in Form PCT/ISA/237		
Applicant INTEL CORPORATION		

1.	This international preliminary report on patentability (Chapter I) is issued by the International Bureau on behalf of the International Searching Authority under Rule 44 bis.1(a).																								
2.	This REPORT consists of a total of 5 sheets, including this cover sheet. In the attached sheets, any reference to the written opinion of the International Searching Authority should be read as a reference to the international preliminary report on patentability (Chapter I) instead.																								
3.	This report contains indications relating to the following items: <table style="width: 100%; border: none;"> <tr> <td style="width: 5%; text-align: center;">☒</td> <td style="width: 25%;">Box No. I</td> <td style="width: 70%;">Basis of the report</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. II</td> <td>Priority</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. III</td> <td>Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. IV</td> <td>Lack of unity of invention</td> </tr> <tr> <td style="text-align: center;">☒</td> <td>Box No. V</td> <td>Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VI</td> <td>Certain documents cited</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VII</td> <td>Certain defects in the international application</td> </tr> <tr> <td style="text-align: center;">☐</td> <td>Box No. VIII</td> <td>Certain observations on the international application</td> </tr> </table>	☒	Box No. I	Basis of the report	☐	Box No. II	Priority	☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability	☐	Box No. IV	Lack of unity of invention	☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement	☐	Box No. VI	Certain documents cited	☐	Box No. VII	Certain defects in the international application	☐	Box No. VIII	Certain observations on the international application
☒	Box No. I	Basis of the report																							
☐	Box No. II	Priority																							
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability																							
☐	Box No. IV	Lack of unity of invention																							
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement																							
☐	Box No. VI	Certain documents cited																							
☐	Box No. VII	Certain defects in the international application																							
☐	Box No. VIII	Certain observations on the international application																							
4.	The International Bureau will communicate this report to designated Offices in accordance with Rules 44bis.3(c) and 93bis.1 but not, except where the applicant makes an express request under Article 23(2), before the expiration of 30 months from the priority date (Rule 44bis .2).																								

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. +41 22 338 82 70	Date of issuance of this report 17 June 2014 (17.06.2014) Authorized officer Simin Baharlou e-mail: pt09.pct@wipo.int
--	--

Form PCT/IB/373 (January 2004)

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

KELLETT GLEN M.

BARNES & THORNBURG, LLP C/O CPA GLOBAL PO
BOX 52050 MINNEAPOLIS MN 55402 USA

PCT

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

(PCT Rule 43bis.1)

Date of mailing
(day/month/year) **18 JULY 2012 (18.07.2012)**

Applicant's or agent's file reference
P41620PCT

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US2011/065072

International filing date (day/month/year)

15 DECEMBER 2011 (15.12.2011)

Priority date (day/month/year)

International Patent Classification (IPC) or both national classification and IPC

G06F 21/20(2006.01)i, G06F 21/22(2006.01)i

Applicant

INTEL CORPORATION et al

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

Name and mailing address of the ISA/KR
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon
Metropolitan City, 302-701,
Republic of Korea
Facsimile No. 82-42-472-7140

Date of completion of this opinion

31 MAY 2012 (31.05.2012)

Authorized officer

UHM, In Kwon

Telephone No 82-42-481-5712



**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US2011/065072

Box No. I Basis of this opinion

1. With regard to the **language**, this opinion has been established on the basis of :
 - ☒ the international application in the language in which it was filed
 - ☐ a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43*bis*.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of:
 - a. a sequence listing filed or furnished
 - ☐ on paper
 - ☐ in electronic form
 - b. time of filing or furnishing
 - ☐ contained in the international application as filed.
 - ☐ filed together with the international application in electronic form.
 - ☐ furnished subsequently to this Authority for the purposes of search.
4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065072

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-40	YES
	Claims	NONE	NO
Inventive step (IS)	Claims	3-13,15-29,32-40	YES
	Claims	1-2,14,30-31	NO
Industrial applicability (IA)	Claims	1-40	YES
	Claims	NONE	NO

2. Citations and explanations :

Reference is made to the following documents:

D1: US 2004-0243823 A1 (MOYER WILLIAM C. et al.) 02 December 2004
D2: US 2005-0114687 A1 (VINCENT ZIMMER et al.) 26 May 2005
D3: US 2007-0156987 A1 (IUE-SHUENN CHEN et al.) 05 July 2007
D4: US 2008-0022395 A1 (MICHAEL HOLTZMAN et al.) 24 January 2008

1. NOVELTY AND INVENTIVE STEP

1-1, claim 1, 14, 30-31

D1, which are closest to claims 1, discloses a system-on-a-chip apparatus comprising:

a memory having at least one protected region to store at least decrypted media content therein(Par.[0017]: the processor reads the data stored in the storage area to be subject to encryption processing based on the information acquired from the processing up to the execution of the encryption application processing(S40));

a system-on-a-chip comprising(Par.[0011]: the processor reads the data stored in the storage area to be subject to encryption processing based on the information acquired from the processing up to the execution of the encryption application processing(S40));

a memory controller coupled to the memory to enforce protection of the protected memory region such that access to the protected memory region is permitted only to authenticated peripheral devices of the system-on-a-chip(Par.[0014]: the processor reads the data stored in the storage area to be subject to encryption processing based on the information acquired from the processing up to the execution of the encryption application processing(S40)).

a security engine coupled to the memory controller to authenticate a firmware of a hardware peripheral of the system-on-a-chip to allow the hardware peripheral access to the protected memory region of the memory(Par.[0022]: Master 12 access protection field 70 includes master 12 read access protection field 72 which indicates whether master 12 is allowed to perform read accesses to non-volatile memory 36 and master 12 write access protection field 74 which indicates whether master 12 is allowed to perform write accesses to non-volatile memory 36)

Continued on Supplemental Box

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/065072

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of :

Box V

Although D1 doesn't manifest the protected memory region of claim 1, it is disclosed in D2 (FIG. 1: If the memory access request is an access to the protected firmware resources 106; Par. [0064]: the memory access request is checked to determine if it is an access request to firmware data (block 706). If the memory request access is an access request to firmware data, another check is made to determine if the memory access request was made by firmware code (block 708). If the memory access request was made by firmware code, the memory access is allowed (block 710)).

Thus, claim 1 is considered to lack an inventive step over the combination of D1 and D2.

Also, claims 14, 30, 31 are considered to lack an inventive step over the combination of D1 and D2 because they share the same technical features as those of claim 1.

1-2. claim 2-13, 15-29

The additional feature of claim 2 is disclosed in D2 (Par. [0048], [0062]-[0067]; Fig. 4.7). Thus, claim 2 is considered to lack an inventive step over the combination of D1 and D2.

None of the prior art documents reveal the additional features of claims 3-13, and 15-29. Thus claims 3-13, and 15-29 are considered to meet the requirement according to PCT Article 33(3) and (2).

1-3. claim 32-40

None of the prior art documents reveal the step of authenticating the peripheral cryptographic key using a security cryptographic key of the security engine of claim 32. Thus claim 32 is considered to meet the requirement according to PCT Article 33(3) and (2).

Also, claims 33-40 are considered to meet the requirement according to PCT Article 33(3) and (2) because they are dependent on claim 32.

2. INDUSTRIAL APPLICABILITY

Claims 1-40 are industrially applicable under PCT Article 33(4).

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
20 June 2013 (20.06.2013)



(10) International Publication Number
WO 2013/089725 A1

- (51) International Patent Classification:
H04L 9/14 (2006.01) *H04L 9/32* (2006.01)
- (21) International Application Number:
PCT/US2011/065069
- (22) International Filing Date:
15 December 2011 (15.12.2011)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (for all designated States except US): **INTEL CORPORATION** [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95052 (US).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **KHOSRAVI, Hormuzd M.** [IN/US]; 4816 NW 166th Avenue, Portland, Oregon 97229 (US). **EPP, Edward C.** [US/US]; 2111 NE 25th Avenue, Hillsboro, Oregon 97124 (US). **KABIR, Farhana** [US/US]; 20021 SE 3rd Circle, Camas, Washington 98607 (US).
- (74) Agent: **KELLETT, Glen M.**; Barnes & Thornburg, LLP, c/o CPA Global, P.O. Box 52050, Minneapolis, Minnesota 55402 (US).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD AND DEVICE FOR SECURE COMMUNICATIONS OVER A NETWORK USING A HARDWARE SECURITY ENGINE

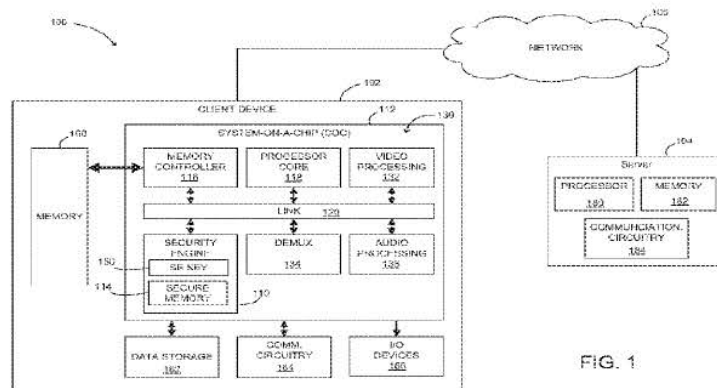


FIG. 1

(57) Abstract: A method, device, and system for establishing a secure communication session with a server includes initiating a request for a secure communication session, such as a Secure Sockets Layer (SSL) communication session with a server using a nonce value generated in a security engine of a system-on-a-chip (SOC) of a client device. Additionally, a cryptographic key exchange is performed between the client and the server to generate a symmetric session key, which is stored in a secure storage of the security engine. The cryptographic key exchange may be, for example, a Rivest-Shamir-Adleman (RSA) key exchange or a Diffie-Hellman key exchange. Private keys and other data generated during the cryptographic key exchange may be generated and/or stored in the security engine.

WO 2013/089725 A1

**METHOD AND DEVICE FOR SECURE COMMUNICATIONS
OVER A NETWORK USING A HARDWARE SECURITY ENGINE**

BACKGROUND

5 Cryptographic communication protocols are used to establish a secure communication session between computing devices over an untrusted network or communication link. One commonly used cryptographic communication protocol is the Secure Sockets Layer (SSL) protocol. The SSL protocol, and the related Transport Layer Security (TLS) protocol, is used for many different types of secure communication sessions including, for example, secure web-browsing, ecommerce, secure upgrades, and other secure communication sessions between two computing devices on an untrusted network such as the Internet. Other communication protocols may utilize the SSL/TLS protocol to provide the underlying security. For example, the Hypertext Transfer Protocol Secure (HTTPS) uses SSL/TLS for encryption of messages between devices. Typically, the cryptographic security offered by the SSL/TLS protocols is done so in-band and performed at the software application level.

15 Some computing and electronic devices utilize system-on-a-chip (SOC) designs due to their relatively small footprint. SOC devices are integrated circuits that incorporate various components, in addition to the processing core, of electronic systems on a single die. For example, an SOC may include a processor core, memory controller, video components, audio components, and/or communication components on a single chip.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention described herein is illustrated by way of example and not by way of limitation in the accompanying figures. For simplicity and clarity of illustration, elements illustrated in the figures are not necessarily drawn to scale. For example, the dimensions of some elements may be exaggerated relative to other elements for clarity. Further, where considered appropriate, reference labels have been repeated among the figures to indicate corresponding or analogous elements.

25 FIG. 1 is a simplified block diagram of at least one embodiment of a system for establishing a secure communication session between a client device having a system-on-a-chip (SOC) and a server over a network;

30 FIG. 2 is a block diagram of at least one embodiment of a security scheme for the system of FIG. 1;

FIG. 3 is a simplified sequence diagram of at least one embodiment of a communication sequence of the client device and server of FIG. 1 to establish a secure communication session; and

5 FIG. 4 is a simplified flow diagram of at least one embodiment of a method for establishing a secure communication session executed by the client device of FIG. 1.

DETAILED DESCRIPTION OF THE DRAWINGS

While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific exemplary embodiments thereof have been shown by way of example in the drawings and will herein be described in detail. It should be understood,
10 however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives consistent with the present disclosure and the appended claims.

In the following description, numerous specific details such as logic implementations, opcodes, means to specify operands, resource partitioning/sharing/duplication implementations, types and interrelationships of system components, and logic partitioning/integration choices are set forth in order to provide a more thorough understanding of the present disclosure. It will be appreciated, however, by one skilled in the art that embodiments of the disclosure may be practiced without such specific details.
15 In other instances, control structures, gate level circuits and full software instruction sequences have not been shown in detail in order not to obscure the invention. Those of ordinary skill in the art, with the included descriptions, will be able to implement appropriate functionality without undue experimentation.

References in the specification to “one embodiment,” “an embodiment,” “an example embodiment,” etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may not necessarily include the particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is
25 within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described.

Embodiments of the invention may be implemented in hardware, firmware, software, or any combination thereof. Embodiments of the invention implemented in a computer

system may include one or more bus-based interconnects between components and/or one or more point-to-point interconnects between components. Embodiments of the invention may also be implemented as instructions carried by or stored on a machine-readable medium, which may be read and executed by one or more processors. A machine-readable
5 medium may be embodied as any device, mechanism, or physical structure for storing or transmitting information in a form readable by a machine (e.g., a computing device). For example, a machine-readable medium may be embodied as read only memory (ROM); random access memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; mini- or micro-SD cards, memory sticks, electrical signals, and others.

10 In the drawings, specific arrangements or orderings of schematic elements, such as those representing devices, modules, instruction blocks and data elements, may be shown for ease of description. However, it should be understood by those skilled in the art that the specific ordering or arrangement of the schematic elements in the drawings is not meant to imply that a particular order or sequence of processing, or separation of processes, is
15 required. Further, the inclusion of a schematic element in a drawing is not meant to imply that such element is required in all embodiments or that the features represented by such element may not be included in or combined with other elements in some embodiments.

In general, schematic elements used to represent instruction blocks may be implemented using any suitable form of machine-readable instruction, such as software or firmware
20 applications, programs, functions, modules, routines, processes, procedures, plug-ins, applets, widgets, code fragments and/or others, and that each such instruction may be implemented using any suitable programming language, library, application programming interface (API), and/or other software development tools. For example, some embodiments may be implemented using Java, C++, and/or other programming languages.

25 Similarly, schematic elements used to represent data or information may be implemented using any suitable electronic arrangement or structure, such as a register, data store, table, record, array, index, hash, map, tree, list, graph, file (of any file type), folder, directory, database, and/or others.

30 Further, in the drawings, where connecting elements, such as solid or dashed lines or arrows, are used to illustrate a connection, relationship or association between or among two or more other schematic elements, the absence of any such connecting elements is not meant to imply that no connection, relationship or association can exist. In other words, some connections, relationships or associations between elements may not be shown in the drawings so as not to obscure the disclosure. In addition, for ease of illustration, a single

connecting element may be used to represent multiple connections, relationships or associations between elements. For example, where a connecting element represents a communication of signals, data or instructions, it should be understood by those skilled in the art that such element may represent one or multiple signal paths (e.g., a bus), as may be needed, to effect the communication.

Referring now to FIG. 1, a system 100 for establishing a secure communication session includes a client device 102, a server 104, and a network 106. In operation, the client device 102 initiates a request for a secure communication session with the server 104 over the network 106. To establish the secure communication session, the client device 102 and the server 104 perform a cryptographic key exchange, such as a Diffie-Hellman or a Rivest-Shamir-Adleman (RSA) key exchange, to generate a secret symmetric session key. The secret symmetric session key may then be used to encrypt and decrypt messages between the client device 102 and the server 104. To ensure a secure communication session, the various keys and other cryptographic functions generated by the client device 102 are done so within a security engine 110 of a system-on-a chip (SOC) 112 of the client device 102. The client device 102 maintains the keys in secrecy within a secure memory 114 of the security engine 110. For example, the security engine 110 may include a security key 150, as discussed below, used to sign and/or otherwise encrypt other keys and messages. In this way, the client device 102 and server 104 may establish a secure communication session across the network 106 using out-of-band (i.e., not application level), hardware security features of the client device 102. In the illustrative embodiments described herein, the secure communication session is a Secure Sockets Layer (SSL) communication session, but the system 100 and features described herein may be used to establish other types of secure communication sessions in other embodiments.

The client device 102 may be embodied as any type of computing device capable of communicating with the server 104 over the network 106. For example, the client device 102 may be embodied as a set-top box, a digital television, a smartphone, a tablet computer, a laptop computer, a mobile internet device (MID), a desktop computer, or other device capable of communicating with the server 104.

As discussed above, the client device 102 includes the SOC 112, which may be embodied as any type of system-on-a-chip device having various components and structures. In the illustrative embodiment of FIG. 1, the SOC 112 includes the security engine 110, a memory controller 116, a processor core 118, and a plurality of hardware peripherals 130, which are communicatively coupled to each other via a link 120. The link 120 may be

embodied as any type of interconnect such as a bus, point-to-point, or other interconnect capable of facilitating communication between the various components of the SOC 112. The hardware peripherals 130 may include any type of hardware peripheral component depending upon the intended functionality of the SOC 112. For example, in the illustrative embodiment, the hardware peripherals 130 include a demux 132 to separate audio and video content streams, video processing component(s) 134 to process video content, and audio processing component(s) 136 to process audio content. Of course, it should be appreciated that the hardware peripherals 130 of the SOC 112 have been simplified in the illustrative embodiment of FIG. 1 and that the SOC 112 may include additional, different, and/or greater detailed hardware peripherals 130, which are not illustrated in FIG. 1 for clarity of the disclosure.

The security engine 110 may be embodied as a security co-processor or processing circuitry separate from the processor core 118. The security engine 110 includes the security key 150 and the secure memory 114, which is accessible only by the security engine 110. The security engine 110 stores the security key 150, and other cryptographic keys as discussed below, in the secure memory 114. In the illustrative embodiment, the security key 150 is provisioned during the manufacturing of the SOC 112, but may be generated by the SOC 112 during operation in other embodiments. For example, in some embodiments, the security key 150 is based on blown fuses within the security engine 110 itself. Additionally or alternatively, the security engine 110 may include a key-generating module, such as a trusted platform module (TPM), to generate the security key 150. During use, the security engine 110 may use any number of security keys 150, which may be identical or different from each other.

In some embodiments, the client device 102 may include additional components and structures other than the SOC 112 depending on the type and intended use of the client device 102. For example, in the illustrative embodiment of FIG. 1, the client device 102 includes a system memory 160, a data storage 162, a communications output 164, and one or more input/output devices 166. The system memory 160 may be embodied as any type of main memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices.

5 The data storage 162 may be embodied as any type of device or devices configured for the short-term or long-term storage of data such as, for example, memory devices and circuits, memory cards, hard disk drives, solid-state drives, or other data storage devices. The communications output 164 may be embodied as a simplified output or as various circuits and/or devices to facilitate, for example, communications with the server 104. For example, the communications output 164 (and/or communication circuitry within the SOC 112) may use any suitable communication protocol such as Ethernet (i.e. the IEEE 802.3 standard) or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards. Additionally, the input/output devices 166 may be embodied as any type of I/O device for interacting with the client device 102. For example, the I/O devices 166 may include output devices such as a display for displaying data on the client device 102, speakers for generating audio, and/or input devices such as a remote control receiver, a keyboard, a mouse, and/or the like.

15 The server 104 may be embodied as any type of data server capable of establishing a secure communication session with the client device 102. As such, the server 104 may include various hardware and software components typically found in a server for communicating, maintaining, and transferring data over a network. For example, the illustrative server 104 includes a processor 180, a memory 182, and communication circuitry 184, which may be similar to such components found in other data servers. For example, the processor 180 may be embodied as any type of processor capable of executing software/firmware, such as a microprocessor, digital signal processor, microcontroller, or the like, and may include one or more processing cores. The memory 182 may be embodied as any type of memory or data storage locations including, for example, dynamic random access memory devices (DRAM), synchronous dynamic random access memory devices (SDRAM), double-data rate synchronous dynamic random access memory device (DDR SDRAM), mask read-only memory (ROM) devices, erasable programmable ROM (EPROM), electrically erasable programmable ROM (EEPROM) devices, flash memory devices, and/or other volatile and/or non-volatile memory devices. The communication circuitry 184 may be embodied any type of circuitry and/or device to facilitate, for example, communications with the client device 102. For example, the communication circuitry 184 may support communication protocols such as Ethernet (i.e. the IEEE 802.3 standard) and/or Wi-Fi® (i.e., the IEEE 802.11 standard), and/or other communication protocols or standards.

The network 106 may be embodied as any number of various wired and/or wireless networks. For example, the network 106 may be embodied as or otherwise include a local area network (LAN), a wide area network (WAN), and/or a publicly accessible, global network such as the Internet. Additionally, the network 106 may include any number of additional devices to facilitate communication between the client device 102 and the server 104. As discussed above, in the illustrative embodiment, the client device 102 and the server 104 establish a SSL communication session over the network 106. However, other types of secure communication sessions may be established in other embodiments.

Referring now to FIG. 2, as discussed in more detail below, the use of the security engine 110 of the client device 102 to perform the cryptographic functions and store keying data associated with the establishment of the secure communication session allows the system 100 to offer several different levels of security. The particular level of security used in the system 100 may depend upon various criteria such as the nature of the network 106, the importance of the data being transferred between the client device 102 and the server 104, and/or the like. For example, one illustrative security scheme 200 includes three different levels of security as shown in FIG. 2. At level 0 security, the client device 102 is configured to protect the client private device key (i.e., the security key 150), which is used for encrypting, signing, and verification functions as discussed in more detail below.

At level 1 security, the client device 102 is configured to protect the session keys and related keys used for data encryption. For example, if an RSA key exchange is performed, the pre-master key and the master key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Additionally, in some embodiments as discussed below, the master key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150). In embodiments in which a Diffie-Hellman key exchange is used, the private Diffie-Hellman client key and/or shared secret key (i.e., the session key) may be stored in the secure memory 114 of the security engine 110 of the SOC 112. Again, in some embodiments, the private Diffie-Hellman client key and/or session key may be stored in an encrypted or wrapped form (e.g., encrypted using the security key 150).

Additionally, at level 2 security, the client device 102 may be configured to protect the data of the host application. For example, if the host application is being used to perform an e-commerce transaction, the bank account information used in such transaction may be encrypted using the security key 150 and stored in the secure memory 114. In this way, the bank account information is not available to the host application. Of course, it should

be appreciated that, in other embodiments, security schemes having more or fewer security levels may be used.

Referring now to FIG. 3, in operation, the client device 102 and the server 104 establish a secure communication session using the security engine 110 of the client device 102 to perform various cryptographic functions and store keying data therein. To do so, the client device 102 and server 104 may perform a handshake session as shown in the communication sequence 300 of FIG. 3. To establish the secure communication session, a security engine driver 302 of the security engine 110 communicates with a firmware of the security engine 110 and a client secure communication application 304 executed on the client device 102. The client secure communication application 304 also communicates with a corresponding server secure communication application 306 executed on the server 104.

The communication sequence 300 begins with block 310 in which the client secure communication application 304 sends a ClientHello message to the server secure communication application 306 to request the initiation of a secure communication session. As discussed above, the secure communication session is a SSL session in the illustrative embodiment. To facilitate the request, the security engine driver 302 communicates with security engine 110 of the SOC 112 to request a random nonce from the security engine 110 in block 312. The security engine 110 may use any suitable random number-generating algorithm to generate the random nonce in block 312. The nonce is embodied as random or pseudo-random number intended to be used only once in cryptographic functions to thwart, for example, replay attacked. In the illustrative embodiment, the random nonce includes a 32-bit timestamp and a 28-byte random number. Of course, other numeric formats for the random nonce may be used in other embodiments. Regardless, it should be appreciated that because the random nonce is generated in the security engine 110, the generation and storage of the random nonce is protected compared to generation of the nonce at, for example, the application level.

The random nonce generated in block 312 is included in the ClientHello message sent to the server secure communication application 306 in block 310. Additionally, the ClientHello message may include a list of cipher suites, compression methods, and other cryptographic protocols or algorithms from which the server 104 may make a selection for use in establishing the secure communication session. In response to the secure communication session request, the server secure communication application 306 sends a ServerHello message in block 314. The ServerHello message may be substantially similar

to the ClientHello message. For example, in the illustrative embodiment, the ServerHello message includes a server random nonce generated by the server 104. Additionally, the ServerHello message includes the selection(s) of the cryptographic protocols and/or other options made by the server 104 from the list included in the ClientHello message. The ServerHello message completes the session initiation phase (Phase 1) of the illustrative handshake session.

In block 316, the server secure communication application 306 sends a server certificate to the client secure communication application 304. The server certificate, like the client certificate discussed below, is typically generated by a certification authority organization, which acts as a third-party verifier of the authentication of the server 104. The server certificate may include unique identifier or number assigned to the server 104 by the certification authority organization to verify the server 104 to other devices on the network 106. As such, in block 318, the client device 102 may verify the server certificate. In some embodiments, the client device 102 verifies the server certificate using a public certificate key issued by the certification authority organization. In such embodiments, the security engine 110 may store the public certificate key in the secure memory 114 in an unencrypted or encrypted state (e.g., using the security key 150).

To establish the secure communication session, the client device 102 and the server 104 perform a key exchange to establish a shared secret key (i.e., a master or session key) in each of the client device 102 and server 104. The client device 102 and the server 104 may use any appropriate key exchange algorithm to effect the establishment of the shared secret. In the illustrative embodiment, the key exchange may be embodied as an RSA key exchange or a Diffie-Hellman key exchange. In embodiments wherein a RSA key exchange is used, the server secure communication application 306 performs a server RSA key exchange in block 320. In such embodiments, the server 104 may generate a temporary RSA public/private key pair and send the RSA public key to the client device 102 in block 320. Such message may be signed by the server 104 and verified by the client device 102 using a public server key, which may be stored in the secure memory 114 as discussed above.

Alternatively, the server secure communication application 306 may perform a server Diffie-Hellman key exchange in block 320. In such embodiments, the server 104 selects or otherwise generates the Diffie-Hellman global values (e.g., a prime number and a primitive root of the prime number), generates a private and public Diffie-Hellman server key, and sends the Diffie-Hellman global values and public Diffie-Hellman server key to the client

device 102 in block 320. Again, such message may be signed by the server 104 and verified by the client device 102 using a public server key.

5 In some embodiments, the sever secure communication application 306 may send a client certification request in block 322. If so, the request may specify the types of certificates accepted by the server 104 (e.g., the public key algorithm used), acceptable certificate authorities, and/or other certificate parameters. Subsequently, in block 324, the server secure communication application 306 sends a server completion message (a "ServerHelloDone" message) to the client secure communication application 304 to indicate that the server 104 has completed this phase of the handshake session. In the
10 illustrative embodiment, no parameters or other data are required for the server completion message. The ServerHelloDone message completes the server authentication and key exchange phase (Phase 2) of the illustrative handshake session.

After receiving the server completion message, the client secure communication application 304 initiates the client authentication and key exchange phase (Phase 3) of the
15 handshake session by sending the client certificate in block 326. As discussed above, the client certificate is typically generated by the certification authority organization and may include a unique identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. In some embodiments, the client certificate may be stored in the secure memory 114 of the
20 security engine 110 of the SOC 112 in an unencrypted or encrypted state. Additionally, the client device 102 may use a private device key issued by the certification authority organization to sign the certificate prior to sending it to the server 104.

In block 328, the client secure communication application 304 performs a client key exchange. Again, the client device 102 and the server 104 may use any appropriate key
25 exchange algorithm to effect the establishment of the shared secret as discussed above. In embodiments wherein an RSA key exchange is used, the security engine 110 of the SOC 112 of the client device 102 generates a random pre-master key in block 330. Illustratively, the pre-master key is embodied as a 48-byte random number, but other numeric formats may be used in other embodiments. In block 332, the pre-master key generated in block 330 is encrypted or otherwise wrapped using the server public key
30 provided by the server in server authentication and key exchange phase (Phase 2). The encrypted pre-master key may be stored in the secure memory 114 of the security engine 110 of the SOC 112 and sent to the server 104 in block 328.

Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates, in block 334, a private Diffie-Hellman client key and a public Diffie-Hellman client key using the Diffie-Hellman global values received from the server 104 in block 320. The private Diffie-Hellman client key may be embodied as a random value generated by the security engine 110, while the public Diffie-Hellman client key is generated by the security engine 110 using the Diffie-Hellman global values received from the server 104. The private Diffie-Hellman client key may be stored in the secure memory 114 of the security engine 110. Of course, in some embodiments, the client device 102 may generate the Diffie-Hellman global values in block 334 and send such global values to the server 104 in block 328 to allow the server 104 to generate the public Diffie-Hellman server key based thereon. Regardless, in block 336, the security engine 110 of the SOC 112 signs the public Diffie-Hellman client key (and Diffie-Hellman global values if generated by the client device 102) in block 336 using the security key 150 or other private client key of the security engine 110. The signed Diffie-Hellman parameters may be further encrypted using the public server key and sent to the server 104 in block 328.

In some embodiments, the client secure communication application 304 may send a client certification verification message to the sever secure communication application 306 in block 338. To do so, the security engine 110 generates a hash code based on the preceding message and signs the hash code using the security key 150 of the security engine 110 in block 340. The client device 102 sends the signed hash code to the server 104 in block 338 as verification of the preceding message. It should be appreciated that such client certification verification messages may be used subsequent to any message sent to the server 104 from the client device 102 to provide an added level of security and verification to the secure communication session. The client certification verification message in block 338 completes the client authentication and key exchange phase (Phase 3) of the illustrative handshake session.

In block 342, the client secure communication application 304 sends a change cipher specification message to the server secure communication application 306 to inform the server 104 that subsequent communications will use the agreed-upon cipher (e.g., the generated session key). In block 344, the security engine 110 of the client device 102 generates a session key (i.e., the "master" key). In embodiments wherein an RSA key exchange is used, the security engine 110 generates the session key as a function of the pre-master key generated in block 330. To do so, the security engine 110 calculates a hash

function of the pre-master key, the client random nonce generated in block 312, and the server random nonce received in block 314. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. As discussed above, the session key is stored in the secure memory 114 of the security engine 110.

In block 346, the security engine 110 generates a hash code of the session key, which may include additional padding depending on the type of hash function used. The hash code of the session key is sent to the server 104 for verification in a client-finished message in block 348. The hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above.

In response to the client-finished message, the server 104 sends a change cipher specification message that acknowledges the use of the agreed-upon cipher (e.g., the session key) in block 350. The server 104 also sends a server-finished message in block 352 that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages. Again, it should be appreciated that the security engine 110 of the SOC 112 of the client device 102 is used for all cryptographic functions and storage of sensitive keying data to provide hardware-based protection of the cryptographic keys and certificate keys used during the communication sequence 300.

Referring now to FIG. 4, in use, the client device 102 may execute a method 400 to establish a secure communication session with the server 104. The method 400 begins with block 402 in which the security engine 110 of the SOC 112 of the client device 102 is provisioned. To do so, in one embodiment, the security engine 110 receives a client device certificate, a private client device key, and a public certification key. The client device certificate, the private client device key, and the public certification key are typically generated by the certification authority organization, which acts as a third-party verifier of the authentication of the client device 102 as discussed above. The client device certificate may include a unique device identifier or number assigned to the client device 102 by the certification authority organization to verify the client device 102 to other devices on the network 106. The private client device key may be used by the client device 102 to sign the client device certificate so as to authenticate the client device 102 to other devices as

discussed in more detail below. Conversely, the public certification key may be used by the client device 102 to verify certification of other devices on the network 106 by the certification authority organization.

The security engine 110 encrypts the private client device key using the security key 150 and stores the encrypted private client device key in the secure memory 114. The security engine 110 may also store the client device certificate and/or the public certification key in the secure memory 114. Additionally, in some embodiments, the security engine 110 may encrypt the client device certificate and/or the public certification key using the security key 150 stored in the security engine 110.

After the security engine 110 has been provisioned in block 402, the client device 102 determines whether to establish a secure communication session (e.g., an SSL session) with the server 104 in block 404. If so, in block 406, the security engine 110 generates a random nonce value. As discussed above, the security engine 110 may use any suitable random number-generating algorithm to generate the random nonce. In block 408, the client device 102 sends a request (a ClientHello message) to initiate the secure communication session to the server 104. The request includes the random nonce generated in block 406 along with a list of cipher protocols, compression methods, and/or other cryptographic choices from which the server 104 may select.

In block 410, the client device 102 completes the server authentication and server key exchange. In so doing, the client device 102 may receive a corresponding ServerHello message including a server random nonce, the server's 104 public key, and the server's 104 selection of cryptographic choices presented in the ClientHello message. As discussed above, the server random nonce, along with the client random nonce, is used to generate the session key. As such, the security engine 110 may store the server random nonce in the secure memory 114. Additionally, in some embodiments, the security engine 110 may store the server certificate and/or other keying data in the secure memory 114. For example, in embodiments wherein an RSA key exchange is used, the security engine 110 may store the public RSA key received from the server in the secure memory 114. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 may store the Diffie-Hellman global values and/or public Diffie-Hellman server key in the secure memory 114.

In block 414, the client 104 determines whether the server 104 is successfully authenticated. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104.

However, if the server 104 is successfully authenticated, the method 400 advances to block 416 in which the client device 102 sends the server 104 the client certificate. If the client certificate has been encrypted (e.g., using the secure key 150), the security engine 110 decrypts the client certificate and signs the client certificate using the private client device

5

key. In block 418, the client 104 completes the client key exchange using the security engine 110 to maintain the security of the keying functions. For example, if a RSA key exchange was selected, the security engine 110 generates the pre-master key and encrypts the pre-master key using the server public key received in block 410 prior to sending the encrypted pre-master key to the server 104 in block 420. Alternatively, if a Diffie-Hellman key exchange was selected, the security engine 110 generates the public and private Diffie-Hellman client keys using the Diffie-Hellman global values received from the server 104 in block 410. The security engine 110 may sign the public Diffie-Hellman client key using the security key 150 or the public client device key provisioned in block 402. The client device 102 sends the signed public Diffie-Hellman client key to the server 104 in block 422. The keys and related keying data generated during the client key exchange may be stored in the secure memory 114 in an encrypted state (using the security key 150) or an unencrypted state.

10

15

20

25

30

In block 424, the client device 102 determines whether the client device 102 has been successfully authenticated by the server 104. If not, the method 400 loops back to block 404 in which the client device 102 may reattempt to establish a secure communication session with the server 104. However, if the client device 102 is successfully authenticated, the method 400 advances to block 426 in which the client device 102 confirms the cipher suite with the server 104 by informing the server 104 that subsequent messages will use the agreed-upon cryptographic protocols. In so doing, the security engine 110 may generate the master or session key. To do so, in embodiments wherein an RSA key exchange is used, the security engine 110 calculates a hash function of the pre-master key, the client random nonce generated in block 406, and the server random nonce received in block 410. Alternatively, in embodiments wherein a Diffie-Hellman key exchange is used, the security engine 110 generates the session key as a function of the Diffie-Hellman global values, the public Diffie-Hellman server key, and the private Diffie-Hellman client key. Once generated, the security engine 110 of the SOC 112 may store the session key in the secure memory 114 of the security engine 110. In some embodiments,

the session key may be encrypted using the security key 150 while stored in the secure memory 114.

5 In block 428, the security engine 110 generates a hash function of the session key, which is sent to the server 104 for verification in a client finished message. Again, the hash code of the session key may be encrypted by the security engine 110 using the public server key as discussed above. In response, the server 104 confirms the cipher suite with the client device 102 to acknowledge the agreed-upon cipher (e.g., the session key). The server 104 also sends a server finished message that includes a similar hash code of the session key for verification by the client device 102. Assuming that the client device 102 and the server 104 verify the hash code of the session key, the handshake session is complete and each of the client device 102 and server 104 have a shared secret session key that is used to encrypt and decrypt subsequent messages.

10 While the disclosure has been illustrated and described in detail in the drawings and foregoing description, such an illustration and description is to be considered as exemplary and not restrictive in character, it being understood that only illustrative embodiments have been shown and described and that all changes and modifications consistent with the disclosure and recited claims are desired to be protected.

CLAIMS:

1. A system-on-a-chip apparatus comprising:
a system-on-a-chip comprising a security engine having a secure memory accessible only by the security engine, the security engine to:
5 generate a random nonce for initiating a request for a secure communication session with a server over a network using the nonce;
perform a cryptographic key exchange with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;
10 store the session key in the secure memory,
the system-on-a-chip to establish the secure communication session with the server over the network using the session key.
2. The system-on-a-chip apparatus of claim 1, wherein the system-on-a-chip
15 to establish a Secure Sockets Layer communication session with the server over the network using the session key.
3. The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server nonce from the server in response to the request for the secure communication
20 session, the response message including a server nonce and store the server nonce in the secure memory.
4. The system-on-a-chip apparatus of claim 1, wherein the security engine to receive a server certificate from the server and store the server certificate in the secure memory.
25
5. The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Rivest-Shamir-Adleman key exchange with the server to generate the symmetric session key.
- 30 6. The system-on-a-chip apparatus of claim 5, wherein the security engine to generate a pre-master key, encrypt the pre-master key using a security key of the security engine, and send the encrypted pre-master key to the server.

7. The system-on-a-chip apparatus of claim 6, wherein the security engine to wrap the pre-master key using a server public key and store the wrapped pre-master key in the secure storage.
- 5 8. The system-on-a-chip apparatus of claim 6, wherein the security engine to generate the session key as a function of the pre-master key.
9. The system-on-a-chip apparatus of claim 8, wherein the security engine to calculate a hash function as a function of the random nonce generated by the security engine and
10 a nonce received from the server.
10. The system-on-a-chip apparatus of claim 5, wherein the security engine to receive a public Rivest-Shamir-Adleman server key from the server and store the public Rivest-Shamir-Adleman server key in the secure memory.
15
11. The system-on-a-chip apparatus of claim 1, wherein the security engine to perform a Diffie-Hellman key exchange with the server to generate the symmetric session key.
12. The system-on-a-chip apparatus of claim 11, wherein the security engine
20 to generate a public Diffie-Hellman client key and a private Diffie-Hellman client key, sign the public Diffie-Hellman client key using a security key of the security engine, and send the signed public Diffie-Hellman key to the server.
13. The system-on-a-chip apparatus of claim 12, wherein the security engine
25 to receive a public Diffie-Hellman server key from the server and generate the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.
14. The system-on-a-chip apparatus of claim 13, wherein the security engine
30 to use the session key to encrypt a subsequent message sent from the client device to the server.
15. The system-on-a-chip apparatus of claim 11, wherein the security engine to receive Diffie-Hellman global values and a public Diffie-Hellman server key from the server and store at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage.

16. A method comprising:
generating a random nonce in a security engine of a system-on-a-chip of a client device;
initiating, using the client device, a request for a secure communication session with a server over a network, the request including the random nonce;
performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the secure communication session;
storing the session key in a secure memory of the security engine of the system-on-a-chip; and
establishing, using the client device, the secure communication session with the server using the session key.
17. The method of claim 16, wherein initiating a request for a secure communication session comprises initiating a request for a Secure Sockets Layer communication session.
18. The method of claim 16, further comprising:
receiving a response message from the server in response to the request for a secure communication session, the response message including a server nonce, and
storing the server nonce in the secure memory of the security engine of the system-on-a-chip.
19. The method of claim 16, wherein initiating a request for a secure communication session comprises sending a ClientHello message, including the nonce, to the server; and further comprising:
receiving a ServerHello message from the server, the ServerHello message including a server nonce; and
storing the server nonce in the secure memory of the security engine of the system-on-a-chip.

20. The method of claim 16, further comprising receiving a server certificate from the server and storing the server certificate in the secure memory of the security engine of the system-on-a-chip of the client device.
- 5 21. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.
22. The method of claim 21, wherein performing the Rivest-Shamir-Adleman
10 key exchange with the server comprises:
generating a pre-master key in the security engine;
encrypting the pre-master key using a security key of the security engine; and
sending the encrypted pre-master key to the server.
- 15 23. The method of claim 22, further comprising:
wrapping the pre-master key in the security engine of the system-on-a-chip using a server public key, and
storing the wrapped pre-master key in the secure storage of the security engine of the system-on-a-chip.
- 20 24. The method of claim 22, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.
- 25 25. The method of claim 24, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.
- 30 26. The method of claim 21, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:
receiving a public Rivest-Shamir-Adleman server key from the server; and
storing the public Rivest-Shamir-Adleman server key in the secure memory of the security engine of the system-on-a-chip.

27. The method of claim 16, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

5

28. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;

10 signing the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

29. The method of claim 28, wherein performing a Diffie-Hellman key exchange with the server comprises:

15

receiving a public Diffie-Hellman server key from the server;

generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

20

30. The method of claim 29, wherein performing a Diffie-Hellman key exchange with the server comprises using the session key to encrypt a subsequent message sent from the client device to the server.

31. The method of claim 27, wherein performing a Diffie-Hellman key exchange with the server comprises:

receiving Diffie-Hellman global values and a public Diffie-Hellman server key from the server, and

5 storing at least one of the Diffie-Hellman global values and the public Diffie-Hellman server key in the secure storage of the security engine of the system-on-a-chip.

32. The method of claim 16, further comprising:

retrieving a client certificate stored on the client device;

10 signing a client certificate using a security key stored in a secure memory of the security engine of the system-on-a-chip; and

sending the client certificate to the server.

33. The method of claim 16, further comprising:

15 generating, in the security engine of the system-on-a-chip, a hash code of a preceding message sent from the client to the server;

signing the hash code using a security key stored in a secure memory of the security engine; and

20 sending a client certificate verification message to the server, the client certificate verification message including the signed hash code.

34. The method of claim 16, wherein establishing the secure communication session comprises:

generating, in the security engine, a hash code as a function of the session key;

and

5 sending a client completion message that includes the hash code to the server to indicate the client has completed an initial handshake procedure.

35. A source device comprising:

10 a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 16-34.

36. One or more machine readable media comprising a plurality of instructions that in response to being executed by a client device result in the client device
15 performing the method of claims 16-34.

37. A method comprising:

generating a random nonce in a security engine of a system-on-a-chip of a client device;

20 initiating, using the client device, a request for a Secure Sockets Layer communication session with a server over a network, the request including the random nonce;

performing a cryptographic key exchange, using the security engine of the system-on-a-chip, with the server to generate a symmetric session key to encrypt messages sent to the server and decrypt messages received from the server during the Secure Sockets Layer
25 communication session;

storing the session key in a secure memory of the security engine of the system-on-a-chip; and

generating, in the security engine, a hash code as a function of the session key;

and

30 sending a client completion message to the server that includes the hash code to indicate the client has completed an initial handshake procedure.

38. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Rivest-Shamir-Adleman key exchange, using the security engine of the system-on-a-chip, with the server.

5 39. The method of claim 38, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises:

generating a pre-master key in the security engine;
encrypting the pre-master key using a security key of the security engine; and
10 sending the encrypted pre-master key to the server.

40. The method of claim 39, further comprising:
wrapping the pre-master key in the security engine using a server public key, and
storing the wrapped pre-master key in the secure storage of the security engine of
15 the system-on-a-chip.

41. The method of claim 39, wherein performing the Rivest-Shamir-Adleman key exchange with the server comprises generating the session key in the security engine of the system-on-a-chip as a function of the pre-master key.

20 42. The method of claim 41, wherein generating the session key in the security engine comprises calculating, using the security engine of the system-on-a-chip, a hash function as a function of the random nonce generated by the security engine and a nonce received from the server.

25 43. The method of claim 37, wherein performing the cryptographic key exchange with the server comprises performing a Diffie-Hellman key exchange, using the security engine of the system-on-a-chip, with the server.

30 44. The method of claim 43, wherein performing a Diffie-Hellman key exchange with the server comprises:

generating, in the security engine of the system-on-a-chip, a public Diffie-Hellman client key and a private Diffie-Hellman client key;
signing the public Diffie-Hellman client key using a security key of the security engine of the system-on-a-chip; and

sending the signed public Diffie-Hellman key to the server.

45. The method of claim 44, wherein performing a Diffie-Hellman key exchange with the server comprises:

- 5 receiving a public Diffie-Hellman server key from the server;
 generating, in the security engine of the system-on-a-chip, the session key as a function of the private Diffie-Hellman client key and the public Diffie-Hellman server key.

46. A source device comprising:
10 a system-on-a-chip having a security engine, the system-on-a-chip including a plurality of instructions that when executed results in the system-on-a-chip performing the method of claim 37-45.

47. One or more machine readable media comprising a plurality of
15 instructions that in response to being executed by a client device result in the client device performing the method of claims 37-45.

1/4

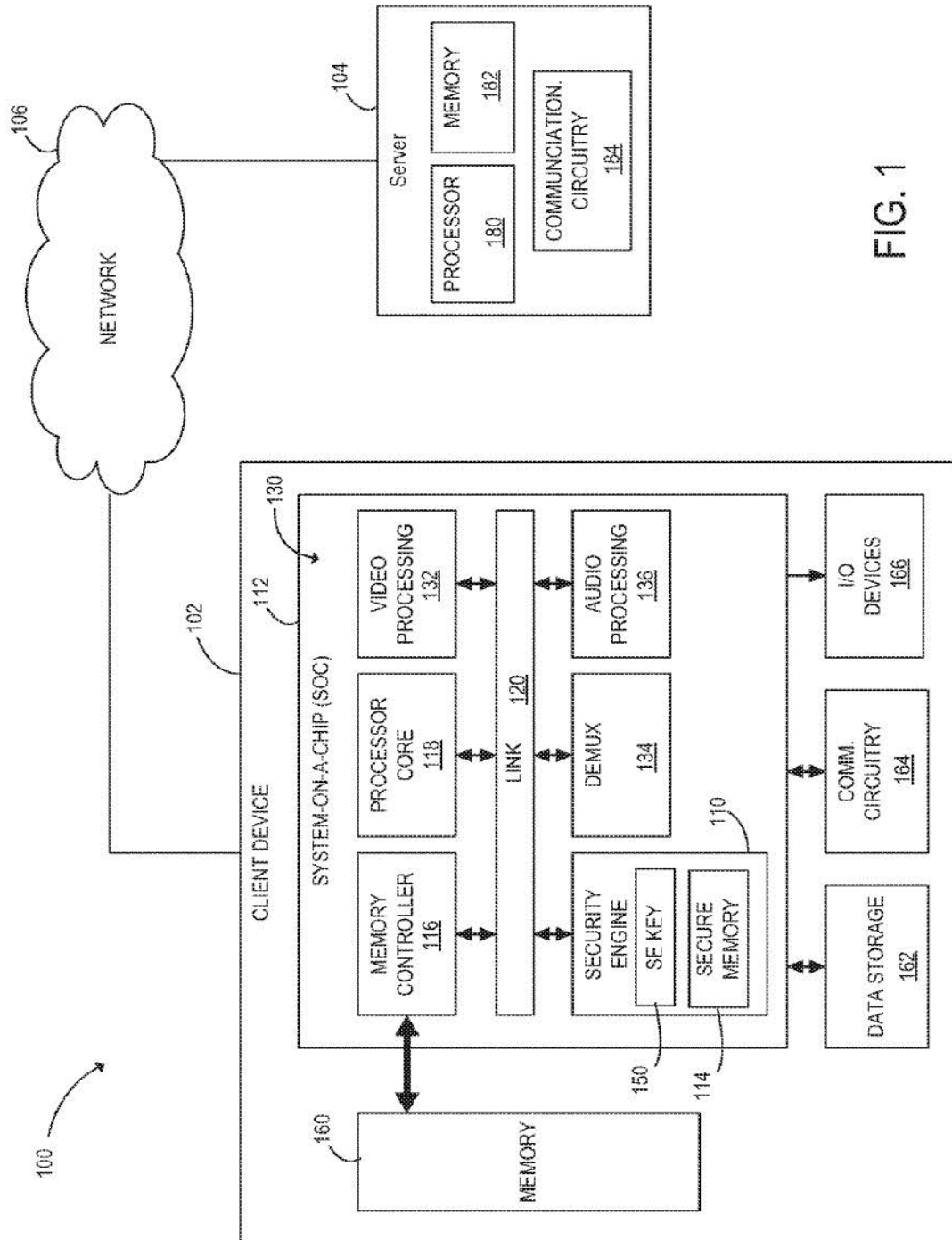


FIG. 1

2/4

200

LEVEL 0	PROTECTION OF CLIENT PRIVATE DEVICE KEY USED FOR SIGNING & VERIFICATION	
LEVEL 1	PROTECTION OF SESSION KEYS USED FOR DATA ENCRYPTION	
	RSA KEY EXCHANGE	DIFFIE-HELLMAN KEY EXCHANGE
	PROTECTION OF PRE-MASTER KEY	PROTECTION OF CLIENT PRIVATE DH KEY
LEVEL 2	PROTECTION OF APPLICATION DATA	

FIG. 2

3/4

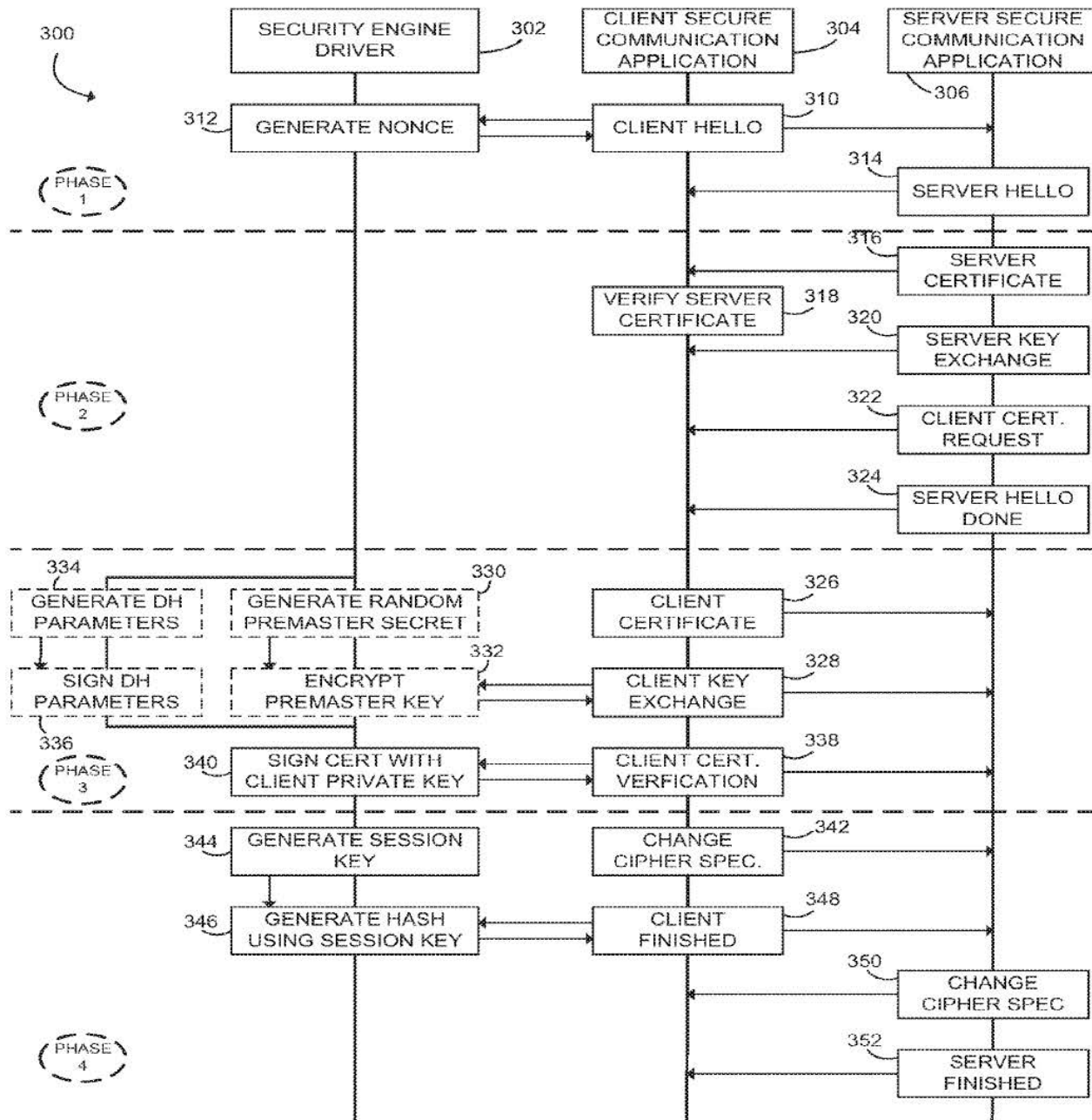


FIG. 3

4/4

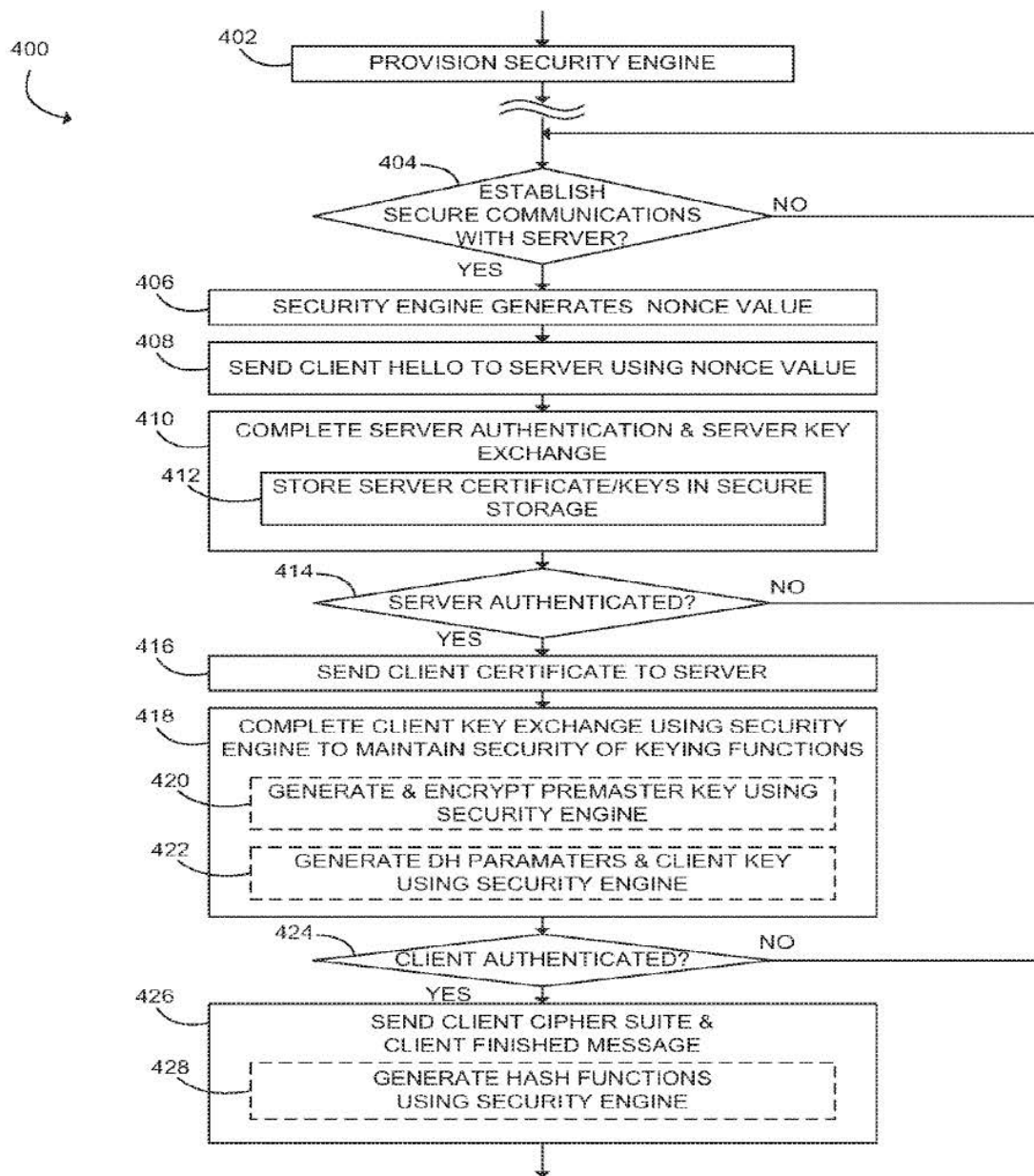


FIG. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/065069**A. CLASSIFICATION OF SUBJECT MATTER***H04L 9/14(2006.01); H04L 9/32(2006.01);*

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 9/14; H04L 9/08; H04L 9/32; H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) & Keywords: secure communication, secure socket layer, SSL, transport layer security, IPSec, random nonce, handshake initiate, key exchange, session key, secure memory, hash code, handshake completion

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011-0231923 A1 (BOLLAY BENN SAPIN et al.) 22 September 2011 See Claims 1,6; Paragraphs [27],[63],[70],[89]-[93],[95],[123]-[126]; Figures 2,5,8	1-32,35-36
A		33-34,37-47
Y	US 2005-0213768 A1 (DAVID DURHAM et al.) 29 September 2005 See Claims 1-4; Paragraphs [14],[15],[17],[20],[21],[26],[28],[33],[45],[49],[53],[54]; Figures 1,2,5	1-32,35-36
A		33-34,37-47
A	US 2010-0239525 A1 (SHAH PARAS et al.) 25 November 2010 See Claims 1,8; Paragraphs [47],[50],[54]-[56],[59],[60]; Figures 2,3	1-17
A	US 2008-0037793 A1 (BUER MARK) 14 February 2008 See Claims 11-17; Paragraphs [35],[39]-[43]; Figures 4,7-9	1-47

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 AUGUST 2012 (29.08.2012)

Date of mailing of the international search report

30 AUGUST 2012 (30.08.2012)

Name and mailing address of the ISA/KR


 Korean Intellectual Property Office
 189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan
 City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Lee Hyoung Ji

Telephone No. 82-42-481-8199



INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2011/065069

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0231923 A1	22.09.2011	CN 102195878 A US 2011-231649 A1 US 2011-231651 A1 US 2011-231652 A1 US 2011-231653 A1 US 2011-231655 A1 WO 2011-116342 A2 WO 2011-116342 A3	21.09.2011 22.09.2011 22.09.2011 22.09.2011 22.09.2011 22.09.2011 22.09.2011 22.12.2011
US 2005-0213768 A1	29.09.2005	CN 1926837 A CN 1926837 B CP 1728376 A1 EP 1728376 B1 JP 04-579969 B2 JP 2007-525913 A JP 4579969 B2 KR 10-0831437 B1 KR 10-2006-0127229 A WO 2005-101794 A1	07.03.2007 06.04.2011 06.12.2006 15.07.2009 03.09.2010 06.09.2007 10.11.2010 21.05.2008 11.12.2006 27.10.2005
US 2010-0299525 A1	25.11.2010	AU 2006-280301 A1 CN 101292233 A0 EP 1904931 A2 JP 2009-505493 A US 2007-0038853 A1 US 2009-0119504 A1 WO 2007-021483 A2	22.02.2007 22.10.2008 02.04.2008 05.02.2009 15.02.2007 07.05.2009 22.02.2007
US 2008-0037793 A1	14.02.2008	EP 1484890 A2 EP 1484890 A3 EP 1484913 A2 EP 1484913 A3 US 2004-0247131 A1 US 2005-0041802 A1 US 2010-0296573 A1 US 6724335 B1 US 7289632 B2 US 7768434 B2 US 8111183 B2	08.12.2004 11.07.2012 08.12.2004 15.04.2009 09.12.2004 24.02.2005 25.11.2010 20.04.2004 30.10.2007 03.08.2010 07.02.2012

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
29 September 2011 (29.09.2011)

PCT

(10) International Publication Number
WO 2011/119985 A2

(51) International Patent Classification:
G06F 21/00 (2006.01)

(21) International Application Number:
PCT/US2011/030033

(22) International Filing Date:
25 March 2011 (25.03.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/318,220 26 March 2010 (26.03.2010) US
61/318,744 29 March 2010 (29.03.2010) US
61/319,198 30 March 2010 (30.03.2010) US
61/372,390 10 August 2010 (10.08.2010) US

(71) Applicant (for all designated States except US): **MAX-LINEAR, INC.** [US/US]; 2051 Palomar Airport Road, Suite 100, Carlsbad, California 92011-1462 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **LECLERCQ, Maxime** [FR/US]; 1232 Hygeia Avenue, Encinitas, California 92024 (US).

(74) Agents: **TABIBI, Ardeshir** et al.; Kilpatrick Townsend & Stockton LLP, Two Embarcadero Center, Eighth Floor, San Francisco, California 94111-3834 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report (Rule 48.2(g))

(54) Title: FIRMWARE AUTHENTICATION AND DECIPHERING FOR SECURE TV RECEIVER

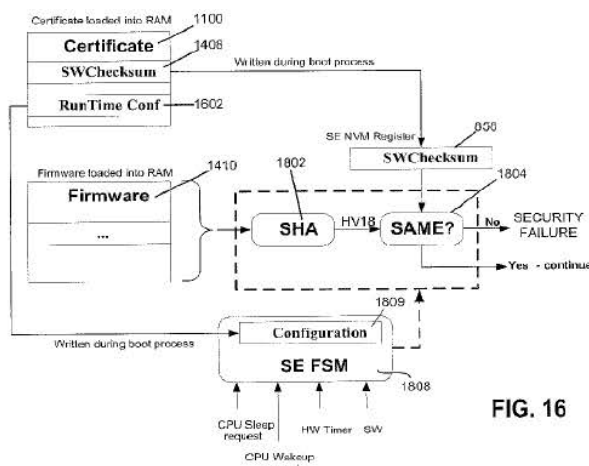


FIG. 16

(57) Abstract: A method for authenticating and deciphering an encrypted program file for execution by a secure element includes receiving the program file and a digital certificate that is associated with the program file from an external device. The method stores the program file and the associated certificate in a secure random access memory disposed in the secure element and hashes the program file to obtain a hash. The method authenticates the program file by comparing the obtained hash with a checksum that is stored in the certificate. Additionally, the method writes runtime configuration information stored in the certificate to corresponding configuration registers disposed in the secure element. The method further generates an encryption key using a seed value stored in the certificate and a unique identifier disposed in the secure element and deciphers the program file using the generated encryption key.

WO 2011/119985 A2

FIRMWARE AUTHENTICATION AND DECIPHERING FOR SECURE TV RECEIVER

CROSS-REFERENCES TO RELATED APPLICATIONS

5

[0001] The present application claims benefit under 35 USC 119(e) of the following US applications, the contents of all of which are incorporated herein by reference in their entirety:

- U.S. application number 61/318,220, filed March 26, 2010, entitled “Firmware Authentication and Deciphering for Secure TV Receiver”;
- U.S. application number 61/318,744, filed March 29, 2010, entitled “Generation of SW Encryption Key During Silicon Manufacturing Process”;
- U.S. application number 61/319,198, filed March 30, 2010, entitled “Control Word Obfuscation in Secure TV Receiver”; and
- U.S. application number 61/372,390, filed August 10, 2010, entitled “Control Word Obfuscation in Secure TV Receiver”.

15

[0002] The present application is related to and incorporates by reference the entire contents of the following US applications:

- U.S. application number 13/021,178, filed February 04, 2011, entitled “Conditional Access Integration in a SOC for Mobile TV Applications”;
- U.S. application number 13/026,000, filed February 11, 2011, entitled “RAM Based Security Element for Embedded Applications”; and
- U.S. application number 13/041,256, filed March 04, 2011, entitled “Code Download and Firewall for Embedded Secure Application”.

20

25

BACKGROUND OF THE INVENTION

[0003] The present invention relates to information processing, and more particularly, to an integrated circuit device and method for authenticating and deciphering an encrypted program file that may be used to provide conditional access to protected information data such as pay TV and others.

30

[0004] There are several well-known digital radio and digital TV broadcast standards. In Europe, the digital radio broadcast is the DAB (Digital Audio Broadcasting) adopted by the ITU-R standardization body and by ETSI. The digital TV standard is DVB (Digital Video Broadcasting) in Europe, ATSC (Advanced Television Systems Committee) in the U.S., and ISDB (Integrated Services Digital Broadcasting) in Japan and South America. In addition to these standards, there are also mobile TV standards which relate to the reception of TV on handheld devices such as mobile phones or the like. Some well-known mobile TV standards are DVB-H (Digital Video Broadcasting-Handheld), CMMB (China), DMB (Digital Multimedia Broadcasting), and Mediaflo.

[0005] In most digital TV broadcasting services, the service providers scramble and encrypt the transmitted data streams to protect the broadcasted content and require their customers or users to install "security protection" mechanisms to decrypt and descramble the content. Security protection mechanisms such as digital rights management enable users to store content. Conditional access systems are other security protection mechanisms that allow users to access and view content but may or may not record the viewed content.

[0006] In a typical pay-TV system, the conditional access software runs on a dedicated secure element implementing robust mechanisms so as to prevent a malicious entity ("hacker") from gaining access to the broadcast system secret to decipher the TV content. The CA instruction code and keys provisioned by the CA provider adapted to ensure security are typically stored in a non-volatile memory, such as an EEPROM or Flash, which are relatively expensive and require a specifically tuned CMOS process and additional process steps for fabrication and testing.

[0007] Figure 1 is a block diagram of a conventional TV receiver 100 performing conditional access (CA) functions. Receiver 100 includes a TV demodulator 110 coupled to a suitable antenna 105 for receiving broadcast content. Demodulator 110 is connected to a secure element 120. The connection can be a proprietary interface or a standard interface. Secure element 120 may be provided by the service provider and controls access to a broadcast service by descrambling an encrypted broadcast transmission. Secure element 120 may also hold service entitlement information controlled by the service provider. The service provider may communicate with the secure element using encrypted messages that carry descrambling keys and other service management information. Secure element 120 descrambles encrypted data streams received from the TV demodulator and provides the descrambled data streams to a video and audio decoder 130. A display 140 coupled to the video and audio decoder displays the decoded video and audio data streams. In general,

secure element 120 may be provided in several forms and in multiple packaging options. For example, the secure element may be a dedicated surface mount device mounted on the receiver, a SIM card, a secure SD card, or a module. The secure element typically includes a crypto processor, a secure CPU, read-only memory (ROM), and electrical erasable and programmable ROM (EEPROM) or Flash, as shown in Figure 1.

[0008] Figure 2 is a block diagram of a conventional secure element 200 showing components incorporated in the secure element 120 of Figure 1. Secure element 200 includes a demodulator interface 210 that establishes a physical and electrical connection with the demodulator 110. Typically, the physical and electrical connection is a proprietary hardware interface that enables a user to plug the secure element to the TV demodulator. Secure element 200 also includes a secure CPU 220 that is configured to decrypt messages or data streams that are transmitted by the service providers. Secure element 200 further includes a plurality of hardware accelerators 230-1, 230-2, ..., 230-n that assist the secure CPU for descrambling data streams and decode specific messages from the service provider. Secure element 200 additionally includes read-only memory 240 (ROM) and EEPROM/Flash memory 250. The ROM and EEPROM/Flash memory are programmed by the conditional access (CA) provider and contain CA firmware and decryption keys. When enabled by the user, CPU 220 executes program code stored in ROM and EEPROM/Flash memory and starts processing data streams received through the demodulator interface 210.

[0009] As shown in Figure 1, the secure element 120 may include two physical interfaces, one for receiving encrypted data streams and the other one for sending decrypted data streams back to the demodulator. Other physical interfaces may exist for facilitating communication between the secure element and the demodulator.

[0010] It can be seen that the conventional secure element has a hardware architecture that is inflexible and adds costs to service providers. Furthermore, conventional techniques do not appear to address the concerns of service providers, CA operators, and content owners, namely, to provide security to the operation of their devices.

BRIEF SUMMARY OF THE INVENTION

[0011] Embodiments of the present invention provide an integrated circuit that integrates functions (secure element) required to achieve security in a monolithic silicon device formed on the same substrate using a conventional CMOS process, e.g., a CMOS system-on-a-chip (SOC). In an embodiment, the integrated circuit includes a demodulator having an interface

unit for receiving a program file and a certificate that is associated with program file from an external memory device. The integrated circuit also includes a secure element that is communicatively and electrically coupled to the demodulator and configured to authenticate the received program file and the certificate. The secure element includes a non-volatile
5 memory register that contains a unique identifier of the integrated circuit, a read-only access memory (ROM) having a boot code, a static random access memory (RAM) for storing the received program file, and a processing unit that is coupled to the read-only memory and the static random access memory. In an embodiment, the secure element is locked after the program file and the certificate are stored in the random access memory, thereby preventing
10 the demodulator from accessing the secure element.

[0012] The processing unit is configured to authenticate the program file and the certificate by executing the boot code, wherein the authentication of the certificate includes computing a first hash value of a portion of the certificate and comparing the first hash value with the unique identifier. In a specific embodiment, the unique identifier is burned or blown during
15 the integrated circuit manufacturing process. In an embodiment, the external memory device may include a Flash memory. In an embodiment, the boot code may include computer readable and executable instruction code that performs multiple security validations on the certificate and on the program file. In an embodiment, the portion of the certificate includes information data associated with a secure state of the program file to ensure that the program
20 file is authentic and has not been modified. In an embodiment, the information data may include a software vendor key, a software distribution key, and/or a software personalization key that are referred to as public keys, and each of the public keys is associated with a signature that is also included in the certificate. In an embodiment, the secure element may perform an encryption algorithm (e.g., an RSA encryption) on the signature to obtain an
25 encryption key and compare the obtained encryption key with the associated public key. In the event that the encryption key with regard to its signature does not match the associated public key, the secure element may disable or remove the program file stored in the random access memory.

[0013] In an embodiment, the secure element performs a series of validations for
30 authenticating the program file. The series of validations may include a chain of trust verification, a boot certificate validation, a certificate binding validation, and a firmware image validation that are performed in sequence.

[0014] In an embodiment, the secure element further deciphers the program file using an encryption key that is generated using the unique identifier (HUK) upon a successful

authentication. In a specific embodiment, the unique identifier is burned or blown during the integrated circuit manufacturing process.

- 5 [0015] In an embodiment, a device includes a unique identifier, a processing unit and a random access memory and a read-only memory, both memories are coupled to the processing unit. The read-only memory includes instruction codes that cause the processing unit to read in a firmware image and a certificate associated with the firmware image, and stores the firmware image and the certificate into the random access memory. The instruction codes also cause the processing unit to simultaneously authenticate the certificate and the firmware image. In an embodiment, the simultaneously authentication of the
- 10 firmware image and the certificate includes generating an encryption key using a seed number disposed in the certificate and the unique identifier, encrypting or decrypting the firmware image using the generated encryption key, hashing the encrypted or decrypted firmware image to obtain a hash, encrypting the public key using the obtained hash, and comparing the encrypted public key with a digital signature disposed in the certificate.
- 15 [0016] Embodiments of the present invention also disclose a method for authenticating a program code for execution by an information processing apparatus. The method includes receiving the program code and a certificate that is associated with the program code from an external device. The method also includes storing the received program code and the certificate in a secure random access memory disposed in the information processing
- 20 apparatus and hashing a portion of the certificate to obtain a first hash value. The method authenticates the certificate by comparing the first hash value with a unique identifier stored in a non-volatile memory register of the information processing apparatus. The method further includes disabling or removing the stored program code if the hash value does not match the unique identifier.
- 25 [0017] In an embodiment, the portion of the certificate may include information data associated with a secure state of the program code. The information data may include a public key and a signature, both the public key and the signature may be associated with a vendor or a service provider. In an embodiment, the method may further hash the program code to obtain a second hash value and perform an encryption algorithm on a crypto public
- 30 key public key to obtain an encryption key and authenticates the certificate based on a result of comparison between the encryption key and a signature disposed in the certificate.

[0018] A specific embodiment of the present invention provides a method for authenticating a firmware image for execution by a secure element at runtime. The method

includes receiving the firmware image and a digital certificate that is associated with a secure state of the firmware image, and storing the firmware image and the certificate in a random access memory disposed in the secure element. The method also includes hashing the firmware image to obtain a hash value and authenticating the firmware image based on a comparison result between the hash value and a checksum disposed in the digital certificate. In addition, the method includes writing runtime configuration data disposed in the digital certificate to associated configuration registers in the secure element.

[0019] In an embodiment, the authentication of the program may be triggered by software, a hardware timer, or when the secure element enters or exits a sleep period.

[0020] Other embodiments, features and advantages of the present invention may be more apparent upon review of the specification and the claims to follow.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] Preferred embodiments of the present invention are described below, by way of example only, with reference to the accompanying drawings, in which

[0022] Figure 1 is a block diagram of a conventional TV receiver 100 performing conditional access (CA) functions;

[0023] Figure 2 is a block diagram of a conventional secure element 200 used in pay-TV applications;

[0024] Figure 3 is a simplified block diagram of an integrated conditional access subsystem in an SOC according to an embodiment of the present invention;

[0025] Figure 4 is a simplified block diagram of an integrated secure element disposed in a demodulator SOC according to an embodiment of the present invention;

[0026] Figure 5 is a simplified block diagram of an integrated secure element disposed in a demodulator SOC according to another embodiment of the present invention;

[0027] Figure 6 is an exemplary process for generating an encryption key according to an embodiment of the present invention;

[0028] Figure 7 is a simplified timing diagram illustrating a startup operation of a demodulator SOC according to an embodiment of the present invention;

[0029] Figure 8 is an exemplary demodulator SOC that executes a data download operation from an external memory according to an embodiment of the present invention;

[0030] Figure 9 is a simplified flow chart diagram illustrating a boot loader process according to an embodiment of the present invention;

5 [0031] Figure 10 is an exemplary diagram illustrating a chain of trust validation having four-layer RSA public/private keys according to an embodiment of the present invention;

[0032] Figure 11 is a simplified diagram illustrating a boot certificate validation according to an embodiment of the present invention;

10 [0033] Figure 12 is a simplified diagram illustrating a certificate binding validation according to an embodiment of the present invention;

[0034] Figure 13 is a simplified diagram illustrating a firmware image validation according to an embodiment of the present invention;

[0035] Figure 14A is a simplified diagram illustrating a firmware image decryption (deciphering) according to an embodiment of the present invention;

15 [0036] Figure 14B is a simplified diagram illustrating a firmware image decryption (deciphering) according to an alternative embodiment of the present invention;

[0037] Figure 15 is a simplified diagram illustrating a one-step firmware decryption and authentication process according to an embodiment of the present invention;

20 [0038] Figure 16 is a simplified diagram illustrating a firmware run-time authentication using hardware facilities provided by the secure element according to an embodiment of the present invention; and

[0039] Figure 17 is an exemplary process of decrypting or deciphering a firmware stored in the secure RAM according to an embodiment of the present invention.

25 DETAILED DESCRIPTION OF THE INVENTION

[0040] Conditional access is used by TV broadcasters to generate revenue. To achieve this, security guidelines are used to protect the keys provisioned to the user and to guarantee that no hacker or malicious entity can crack the system and watch contents for free. These guidelines, also referred to as security requirements, define methods adapted to prevent
30 misuse of the SOC (system-on-chip) device and its associated firmware, and furthermore to

inhibit unauthorized access to secrets, such as keys, operating modes, etc. The SOC security framework described herein defines hardware (HW), software (SW), or a combination thereof (i.e., firmware) to achieve these objectives.

[0041] Figure 3 is a simplified block diagram of a receiver system on a chip (SOC) 300 configured to perform tuning, demodulating, CA security, and the like, in accordance with an embodiment of the present invention. Receiver system 300 includes a digital broadcast receiver 310 that may be capable of receiving signals in a number of different frequency bands of interest and/or in a number of different formats. By way of example, receiver system 300 may be capable of receiving any one or more of the standards mentioned above or other suitable standards. In an exemplary embodiment, receiver system 300 also includes a conditional access security (CAS) sub-system 350.

[0042] Digital broadcast receiver 310 includes a tuner 312 that is connected to an antenna 311. Although an antenna is shown, tuner 312 may be connected to a number of antennas that is configured to suit different frequency bands of interest. The tuner frequency translates received signals and provide them to a demodulator 314, which may demodulate the frequency translated signals into multiple data streams (audio, video, text, and others). Receiver 310 also includes a descrambler 316 that descrambles the data streams (indicated as encrypted TS) and provides clear (i.e., descrambled) data streams (indicated as clear TS in Figure 3) to a host via a host interface unit 318. Receiver 310 further includes a control processor 320 and a memory unit 322 that contains software (program code) to enable a user to select a service and to program the tuner to a desired frequency. In an embodiment, the memory 322 may include dynamic random memory and/or permanent memory such as read-only memory (ROM).

[0043] Receiver 310 also includes a control interface unit 324 that connects the digital broadcast receiver 310 with the conditional access security sub-system 350. As described in section above, control access is a protection of content required by content owners or service providers. Conventional access approaches use dedicated surface mount devices such as Smartcard, SIM card, secure SD card or the like. In conventional approaches, CA instruction code and keys provisioned by CA providers adapted to ensure security are typically stored in a non-volatile memory, such as an EEPROM or Flash, which are relatively expensive and cannot be easily and cost effectively integrated using standard CMOS fabrication processes. A novel conditional access security (CAS) sub-system according to an embodiment of the present invention will be described in detail below.

[0044] Referring to Figure 3, CAS sub-system 350 includes a secure processor 352 coupled to a memory unit 354. The secure CPU may be a RISC CPU configured to process various processing operations. CAS sub-system 350 further includes a crypto hardware 356 that, in an embodiment, includes suitable crypto logic, circuitry (e.g., hardware) for performing cryptographic operations. In a specific embodiment, crypto hardware 356 may be a crypto processor configured to perform cryptographic functions such as processing digital signature, key management, identifying public keys and others due to the secure access requirements. During the manufacturing process, cryptographic hardware may generate a unique crypto ID (identity) for the receiver SOC 300 and a unique encryption key. CAS sub-system also includes a fuse bank 360. In an embodiment, fuse bank 360 may include electrically programmable fuses on the chip. In an embodiment, the fuse bank may contain an array of electrically programmable registers, each having a number of bits. The bits can be programmed during the manufacturing process or later by the service provider as the device is shipped to the user. In an embodiment, corresponding bits of the fuse bank are burned or blown according to the value of the unique device ID and a certificate key. In a specific embodiment, memory unit 354 includes random access memory and read-only memory. In contrast to conventional techniques, memory unit 354 does not include EEPROM and/or Flash memory to facilitate the integration process and to minimize cost by using conventional (i.e., standard) CMOS process.

[0045] In an embodiment, the receiver SOC 300 includes an external memory interface 368 configured to interface with an external memory. Although the external memory interface 368 is shown to be located in the CAS sub-system 350, it can be located in any part of the receiver SOC as further disclosed below. In an embodiment, the external memory interface 368 can include a SD memory card slot, a multimedia card (MMC), a micro SD card slot, a mini SDHC, a microSDHC, a Memory Stick slot, a PCMCIA interface, a USB interface, a serial or a parallel interface, and others. The external memory can be a commercial off-the-shelf Flash memory in a specific embodiment.

[0046] In accordance with embodiments of the present invention, the conditional access (CA) software code is stored in a random access memory (RAM). The CA software is dynamically downloaded from an external non-volatile flash memory via the external memory interface 368 to the RAM during the power cycle of the security sub-system. However, because the external flash storing the CA software is outside the security perimeter it must first be authenticated and checked for any malicious alteration (such as bypass of the security function that could be inserted by a hacker). The secure sub-system implements a

protocol to authenticate the firmware using a public key algorithm and digital certificate provisioned during manufacturing.

[0047] Figure 4 is a block diagram of a demodulator SOC 400 including a demodulation logic 410 coupled to a remote memory device 480 (e.g., Flash memory) and an integrated secure element 450 according to an embodiment of the present invention. Demodulation logic 410 may have a similar configuration of the receiver 310 shown in Figure 3. For example, demodulation logic 410 may include a demodulator, a descrambler, a control CPU, a memory unit that comprises RAM and/or ROM, a host interface, and a control interface unit; the functions of those elements have been described in details in the sections above and won't be repeated herein for brevity. The demodulator logic 410 may further include system-on-a chip infrastructure such as registers, IO ports, an host interface, an external memory interface link 420, which may be similar to the external memory interface port 368 shown in Figure 3 and described above. In an embodiment, remote or external Flash memory 480 may be coupled to the demodulator SOC 400 through the interface link 420. The coupling can be by means of a physical connection such as a SD card connector or a USB connector. In another embodiment, the coupling can be by means of an optical (e.g., infrared) or radio wave (e.g., Bluetooth, wireless LAN IEEE802.11, or the like) communication link.

[0048] In an embodiment, integrated secure element 450 includes a secure CPU 452, a boot read-only memory (ROM) 453, a secure random access memory (RAM) 455, multiple non-volatile memory registers (or fuse banks) 460. CPU 452 may include an adder and logic for executing arithmetic operations or comparative decisions. In an embodiment, the non-volatile memory registers are implemented using fuse cells that can be fabricated using standard CMOS processes. In an embodiment, the non-volatile memory registers are programmed (burned or blown) during the silicon manufacturing process to store information such as the device ID, the root public key, and others. Integrated secure element 450 also includes multiple hardware accelerators 456 that can be one or more crypto processors as described above in association with crypto hardware 356 of Figure 3.

[0049] In order to minimize cost, the CA software code is stored in the secure RAM 455 according to an embodiment of the present invention. CA software is understood as instructions, one or more sets of instructions, data files, or executable applications that are provided to the secure CPU 452 for execution. CA software is dynamically downloaded from the remote (external) flash memory 480 to the RAM 455 ("RAM-ware") during the power cycle of the integrated secure element 450. Because CA software is downloaded from the external Flash memory, it must be first authenticated by the integrated secure element

450. In an embodiment, the secure element operates a protocol to authenticate the RAM-ware using a public key algorithm and a digital certificate (e.g., a unique device ID) that is provided during the manufacturing of the demodulator SOC. In an embodiment, the authentication process can be assisted and accelerated using hardware accelerators 456.

5 **[0050]** In an embodiment, CA software is received by the demodulator logic from the external memory and transferred to the secure RAM 455 via a demodulator interface circuit 466. In contrast to conventional secure elements that store the CA software code in EEPROM and/or Flash memory, embodiments of the present invention provides a RAM-ware architecture that can be updated securely and easily, e.g., by downloading firmware
10 (i.e., software, program codes, data files) stored in external memories. The downloaded firmware is authenticated by the secure element running boot authenticate programs from the boot ROM 453. Because the RAM-ware architecture does not require EEPROM and/or Flash memory that requires among other things a double poly process or a tunnel oxide process and expensive testing equipment and procedures, the RAM-based architecture of the present
15 invention can be cost effectively produced using standard CMOS processes.

[0051] In an embodiment, the integrated secure element produces an attribute based on a digital certificate contained in the received software (now RAM-ware because it is now stored in the secure RAM) and provides the attribute to the demodulator logic for descrambling the received data streams (not shown). In some embodiments, the attribute can
20 be a secure bit pattern or a secure codeword to enable the descrambling process in the demodulator logic 410.

[0052] In an embodiment, the integrated secure element 450 is activated when the TV application is enabled by the user. When the TV application is enabled, the demodulator logic causes the boot ROM to execute the boot instructions and activate the integrated secure
25 element. During the boot process, the conditional access (CA) firmware stored in the external flash memory is downloaded to the RAM disposed in the secure element, so that the CPU starts operating.

[0053] As described above, the remote Flash memory contains conditional access (CA) executable applications or data files that are dynamically loaded to the RAM 455 disposed in
30 the integrated secure element. In an embodiment, the external memory contains a digital certificate that is generated by the CA vendor or the demodulator SOC device manufacturer and signed with the root private key or a derivative of the root key using public key infrastructure (PKI). In an embodiment, the digital certificate may be unique to each

demodulator SOC device and contains a device identification (ID) code. In an embodiment, the same identification code may also be stored in one or more of the non-volatile registers 460. In an embodiment, the non-volatile registers 460 may also store a digital signature of the CA software or CA firmware. In an embodiment, the boot ROM authenticates the CA
5 firmware by means of the digital certificate.

[0054] In an embodiment, the secure boot ROM may process the digital certificate as follows: (i) verify that the certificate is authentic and the certificate has been signed by a trusted delegate of the root key owner; (ii) verify that the certificate is intended for the given device by comparing the device ID stored in the secure element NVM (non-volatile memory) registers and the code stored in the certificate to ensure that they match; and (iii) authenticate
10 the firmware by regenerating its signature with the root public key and comparing the result with the value stored in the certificate. Only when the above three steps are successful, the SW that has been downloaded to the secure element RAM is verified and considered to be trustworthy. In an embodiment, the SW code in the external memory may be encrypted. In
15 this case, it is first deciphered by the boot ROM. The SW encryption key (or a derivative) is stored in the secure element NVM registers and used directly by the ROM code.

[0055] Figure 5 is a simplified block diagram of an integrated secure element disposed in a demodulator SOC 500 according to an embodiment of the present invention. Demodulator SOC 500 includes a demodulation logic 510 that may have a similar configuration of the receiver 310 shown in Figure 3. For example, demodulation logic 510 may include a tuner, a
20 demodulator, a descrambler, a control CPU, a memory unit that comprises RAM and/or ROM, a host interface, and a control interface unit; the functions of those elements have been described in details in the sections above and won't be repeated herein for brevity reason. The demodulator logic 510 may further include system-on-a chip infrastructure such as
25 registers, IO ports, one or more direct memory access controllers for interfacing with external storage devices, and other hardware and firmware. In an embodiment, a remote or external Flash memory 580 may be coupled to the demodulator SOC 500 through the demodulator logic 510 by means of a direct memory access controller (DMA) via a communication link 520..

[0056] Demodulator SOC 500 also includes an integrated secure element 550 that is coupled to the demodulation logic 510 by means of a demodulator interface 566. In an embodiment, integrated secure element 550 includes a secure CPU 552, a boot read-only memory (ROM) 553 containing a boot code that causes the secure CPU to download a
30 firmware disposed in the external memory 580 and stores the firmware in a secure random

access memory (RAM) 555. Integrated secure element 550 also includes a plurality of non-volatile memory registers 560 that are implemented using fuse cells that can be fabricated using standard CMOS processes, i.e., without the additional processing steps required for making EEPROM or Flash memory units of conventional secure elements. For example, the non-volatile memory registers are programmed (burned or blown) during the silicon manufacturing process to store information such as the device ID, the root public key, and others. Integrated secure element 550 further includes multiple hardware accelerators 556 that can be one or more crypto processors as described above in association with crypto hardware 356 of Figure 3.

10 [0057] In accordance with some embodiments of the present invention, CA software, i.e., one or more sets of instructions provided to the secure CPU for execution, is stored in the secure RAM 555 to reduce hardware implementation cost. The CA software is dynamically downloaded from the remote (external) flash memory 580 to the RAM 555 ("RAM-ware") during the power cycle of the integrated secure element 550. Because the CA software is
15 downloaded from the external Flash memory, it must be first authenticated by the integrated secure element 550. In an embodiment, the secure element operates a protocol to authenticate the RAM-ware using a public key algorithm and a digital certificate that is provided during the manufacturing of the demodulator SOC. In an embodiment, the authentication process can be assisted and accelerated using one or more hardware
20 accelerators 556.

[0058] In an embodiment, CA software (used alternatively for firmware herein) is received by the demodulator logic from the external memory and transferred to the secure RAM 555 via a demodulator interface circuit 566. In contrast to conventional secure elements that store the CA software code in on-chip EEPROM and/or Flash memory, embodiments of the
25 present invention provides a RAM-ware architecture that can be updated easily and securely (e.g., by reading in software codes stored in external memories). Because the RAM-ware architecture does not require EEPROM and/or Flash memory, it can be cost effectively produced using standard CMOS processes.

[0059] In an embodiment, the integrated secure element produces an attribute based on a
30 digital certificate contained in the received software (now RAM-ware because it is now stored in the secure RAM) and provides the attribute to the demodulator logic for descrambling the received data streams (not shown). In some embodiments, the attribute can be a secure bit pattern or a secure codeword to enable the descrambling process in the demodulator logic 510.

[0060] In an embodiment, the integrated secure element 550 is activated when a TV application is enabled by the user. When the TV application is enabled, the demodulator logic 510 causes the boot ROM to execute the boot instructions and activate the integrated secure element. During the boot process, the conditional access (CA) firmware stored in the external flash memory is downloaded to the secure RAM disposed in the secure element 550.

[0061] As described above, the remote Flash memory contains conditional access (CA) software or firmware that is dynamically loaded to the RAM 555 disposed in the integrated secure element. In an embodiment, the external memory contains a digital certificate that is generated by the CA vendor or the demodulator SOC device manufacturer and signed with the root private key or a derivative of the root key using public key infrastructure (PKI). In an embodiment, the digital certificate may be unique to each demodulator SOC device and contains a device identification (ID) code. In an embodiment, the same identification code may also be stored in one or more of the non-volatile memory registers 560. In an embodiment, the non-volatile memory registers 560 may also store a digital signature of the CA software or CA firmware. In an embodiment, the boot ROM authenticates the firmware using the digital certificate.

[0062] In accordance with some embodiments of the present invention, as shown in Figure 5, external flash memory 580 is used to back up (copy) the data stored in the secure RAM during the execution of the CA software. The backup operation may be triggered in response to any number of events, such as (i) when recurring timers force a periodic backup; (ii) when a specific data set is modified, based, for example, on the secure firmware state-machine and key provisioning; or (iii) upon a power-off cycle when an off condition is detected or requested by the host. In other embodiments, the backup operation can be dynamically user driven or based on other criteria.

[0063] Referring to Figure 5, integrated secure element 550 includes a direct memory access (DMA) controller 570 coupled to secure RAM 555. DMA controller 570 is a hardware feature that enables movement of blocks of data from peripheral to memory, memory to peripheral, or memory to memory with minimal involving of the secure CPU. In an embodiment, the DMA controller can also be used to move data in parallel with the CPU. In some embodiments, the DMA controller retrieves the clear data stored in the secure RAM and writes it to an external memory port that can reside in the integrated secure element (shown as external memory interface 368 in Figure 3, memory port interface 420 in Figure 4, or communication link 520 in Figure 5). The DMA controller manages the flow of data in

and out of the secure element 550. In some embodiments, the DMA controller operations can be performed by secure CPU 552.

5 [0064] In an embodiment, the clear data stored in the secure RAM is encrypted using an encryption key before being backing up. The encryption key can be from a private key security system, where the integrated secure element 550 and the external memory 580 share a “private” key for encrypting and decrypting data passing between them. In an embodiment, the encryption key can be from a public key system, where the secure element has a key pair that consists of a private key and a public key, wherein both keys are used to encrypt and decrypt data, and the private key is only known to the integrated secure element, and the
10 public key is available to many other devices.

[0065] Figure 6 is an exemplary process 600 for generating an encryption key and for outputting encrypted data to an external memory according to an embodiment of the present invention. At step S610, a hardware unique key (HUK) that is stored in one of the non-volatile memory registers is provided to a first AES unit. The AES unit can be one of the
15 HW accelerators 556 performing known encryption algorithms, such as AES, DES/3DES, RSA algorithms, and others. At step S620, the first AES unit processes the HW unique key with a SEED value (i.e., binary data), which may be a preset value or it can be a random number set by the secure CPU or by a on-chip random number generating unit. The seed value or the random number, can be generated from an on-chip random number generator
20 (e.g., one of the HW accelerators) in an embodiment of the present invention. An encryption key is then generated and provided to a second AES unit. The second AES unit processes the clear data stored in the secure RAM with the encryption key at step S630 according to an encryption algorithm and produces encrypted data. In an embodiment, the first AES and second AES units can be a same AES unit. In another embodiment, they may be individual
25 units. At step S640, the encrypted data is written to the external memory in a backup event. The backup event may be triggered by a user, by software, in the event of an overvoltage or under voltage supply, light emitting sensors, periodically set by a timer, and others. In an embodiment, the seed value (random number) is also written to the external memory at a predetermined location (step S650).

30 [0066] Figure 7 is a simplified timing diagram illustrating a startup operation 700 of a demodulator SOC according to an embodiment of the present invention. The timing diagram is described with respect to Figure 4. The startup sequence begins with the application of system power at a time period before t1 where the demodulator SOC remains in a reset mode. When all voltages reach acceptable operating levels, the power supply may send a power-

good signal to the demodulator SOC. Upon completion of a power-on-reset at time t1, the secure element is in the default secure mode, and the host interface is disabled. The secure CPU updates the working registers with values stored in associated non-volatile memory registers (indicated as OTP sensing in Figure 7). The integrated secure element is in the secure mode (the default mode) while the secure CPU updates its working registers. At time t2, the power-on-reset deassertion of the secure element takes place to set the demodulator in action (indicated by going high at "D-CPU action") and initiates the data wipe off of the secure RAM (indicated as 'Data Wipe Off'). At time t3, upon the wipe-off (erasure) of the secure memory (i.e., setting the RAM content to all "0" or "1"), the secure element signals to the demodulator that the secure memory is ready for data (firmware) download (at time t3), the host interface is also enabled at that time, the secure element signals its readiness by outputting an SE_READY_OUT (indicated as going high at time t4). The download process (i.e., fetching of CAS firmware from external memory) may start and the firewall, if present, is open to allow firmware download from an external memory. Upon the download completion, the secure CPU can start the boot-up process at time t5, the secure element is now locked, the firewall, if present, is locked, and the host interface is disabled while the secure element initiates the boot process by means of the boot ROM (this boot process is indicated in the last row in Figure 7). This diagram is merely an example, which should not unduly limit the scope of the claims. One of ordinary skill in the art would recognize many variations, alternatives, and modifications. For example, Figure 7 shows that the demodulator D-CPU reads data of the remote (external) Flash memory and writes to the on-chip secure memory (indicated as a box 710). In an alternative embodiment, the secure CPU may reads data from the remote Flash memory and writes the data to the secure memory. In any event, the secure element is locked to prevent the demodulator from accessing the secure random access memory and the read-only memory. If the data stored in the random access memory is deemed to be authentic or valid in the boot process, the secure element will executes the data upon completion of the boot process. If the data is deemed to be not authentic, then the secure element may remove the data from the random access memory. Details of the validation and authentication will be described in detail below.

[0067] Figure 8 illustrates a demodulator SOC 800 performing a firmware image download operation from an external memory according to an embodiment of the present invention. Demodulator SOC 800 comprises a demodulator logic 810 and an integrated secure element 850. Demodulator logic 810 may include a tuner, a demodulator, a descrambler, control CPU, a memory unit, a host interface as shown in Figure 3. The demodulator logic may

include SOC infrastructure having one or more IO ports, a memory interface unit, and others. In an exemplary embodiment, the SOC infrastructure may include an interface unit 812 such as a USB, a peripheral computer interface (PCI), a SD (secure digital) interface, or a communication link for interfacing with an off-chip non-volatile memory 880. In a specific
5 embodiment, the interface unit 812 may establish a connection to the remote memory via a short distance physical connection by means of a USB connector, an SD connector, or the like. In another embodiment, the interface unit 812 may coupled to the remote memory 880 via a local area network, a personal area network (Bluetooth) or a wireless area network according to the IEEE802.11 standard or the like (the local, personal, or wireless area
10 network is indicated as a cloud 870).

[0068] The integrated secure element includes a secure CPU 852 that together with a boot ROM 854 initiates the integrated secure element at power up. The secure element further includes a secure static random access memory (S-RAM) 856, one or more hardware accelerators 858, one or more non-volatile memory (NVM) registers or fuses (one-time
15 programmable) 860, and a slave demodulator interface circuit 862 that couples the integrated secure element 850 with the demodulator logic 810.

[0069] The secure element may include a firewall 864 that allows for the secure CPU to initiate a connection to the remote memory 880 and download firmware (i.e., data files, executable applications) 882 from the remote memory to the secure S-RAM 856, but does not
20 allows the remote memory to initiate a connection in the reverse direction.

[0070] Upon wiping off the content of the secure S-RAM at time t3 (Figurer 7), the demodulator SOC initiates a download of the firmware. The download process can be performed by the demodulator CPU D-CPU by means of the hardware master port to fetch a firmware from remote flash memory 880 and write the fetched firmware to the secure S-
25 RAM using the slave port interface 862. However, this read-and-write of the CA firmware from the remote flash memory cannot be considered as secure because the demodulator logic 810 and the remote flash memory 880 are outside of the secure element boundary. Therefore, the downloaded firmware in the secure S-RAM must be authenticated to protect the firmware from modification. Once the firmware download is complete, the secure element locks the
30 slave interface firewall to prevent any subsequent access from the non-trusted demodulator interface (indicated as "SE LOCKED" in Figure 7) and the secure S-CPU may start executing from the boot ROM (indicated as "Boot process (from ROM)" in the last row "S-CPU Activity" of Figure 7). It is noted that the demodulator logic cannot access the secure

element through the master-slave demodulator interface 862 once the security element is locked.

[0071] The timing diagram of Figure 7 is summarized as follows: Prior to time t1, the demodulator SOC is in a power-on reset mode. At time t1, all required voltage supplies reach
5 their operating levels. Between time interval t2 and t3, the secure element updates registers with data from their associated non-voltage memory registers ("OTP sensing"). The content of the secure static RAM is erased during that time ("Data Wipe off"). During time interval between t4 and t5 (indicated by box 710), the firmware image of the remote flash device 880 is downloaded to the secure static RAM. Upon the download completion, the secure element
10 is in a locked mode so that no communication between the demodulator logic 810 and the secure element 850 is possible. The secure element executes the boot process including the authentication of the firmware image during time interval between t5 and t6. Upon a successful authentication of the firmware image, the secure element may now initiate the firmware and a normal operation may start at time t6. If the authentication process is not
15 successful, the secure element may disable or remove the firmware stored in the static random access memory.

[0072] Figure 9 is a simplified flow chart diagram illustrating a boot loader process 900 according to an embodiment of the present invention. Boot loader process 900 includes a
20 multiple-step sequence and may be implemented in multiple phases. This diagram is merely an example, which should not unduly limit the scope of the claims. One of ordinary skill in the art would recognize many variations, alternatives, and modifications. In a specific embodiment, the boot loader process begins at start (step 910) with the application of supply voltages to the demodulator SOC and the subsequent removal of power-on-reset of the various hardware reset configurations as described with regard with the startup operation
25 shown in Figure 7. The boot ROM as shown in Figure 8 includes a boot loader so that the secure CPU 852 can subsequently perform a boot sequence on its own once the firmware image is written into the secure RAM. As described above, the firmware image can be downloaded using the interface unit 812 that may include asynchronous or synchronous memory interface such as SRAM, PSRAM, or DRAM interface. In an embodiment, the
30 asynchronous or synchronous memory interface may couple with a variety of peripherals, such as Ethernet, SD (secure digital) card or MMC (multimedia card), a USB or a wireless connection. Upon the completion of the downloading of the firmware from the remote memory 880 to the secure memory 856, the integrated secure element starts a series of validations that includes a chain of trust validation at step 920, a boot certificate validation

(step 930), a certificate binding validation (step 940), a firmware image validation (step 950), and a firmware image decryption (960) if the firmware image is encrypted. In the event that the secure element completes the series of validations successfully, the firmware is considered valid, the secure element will switch execution control to the secure S-RAM 856 and begins the executable applications stored in the S-RAM (step 970). In the event that the validation is unsuccessful, the content of the secure S-RAM may be flushed and the operation is terminated (indicated by the “no” in each validation shown in Figure 9). Each of the validations is described in detail below.

[0073] In an alternative embodiment, the boot loader process may authenticate the firmware image from the external memory prior to writing the firmware image to the secure S-RAM. The authentication may be performed using a public key infrastructure (PKI) and a digital certificate. The boot process authenticates the digital certificate and binds the public key to the device. The boot process may also decipher the firmware image if it is encrypted.

[0074] Figure 10 is an exemplary diagram illustrating a chain of trust validation 1000 having four-layer RSA public/private keys according to an embodiment of the present invention. In an embodiment, a certificate 1100 that is to be loaded to the secure S-RAM includes a root public key 1102. The secure element performs a hash algorithm 1104 on the root public key to obtain a hash value HV and compare (1105) the obtained hash value HV with a digest root public key (or full key) 1108 that is stored in a non-volatile memory register (shown as NVM block 860 in Figure 8). If the validation is negative, the secure element will stop the chain of trust validation (1107). If the comparison is positive, the chain of trust validation continue to a first RSA operation 1114. First RSA operation 1114 performs a first RSA algorithm on the root public key RPK 1102 and a software vendor public key signature SVPbK_SIG 1112 to obtain a first RSA value EK1 and compares (operation 1115) the RSA value EK1 with a software vendor key SVPbK 1116. If the comparison is negative (1117), the secure element stops the validation operation. If the comparison 1115 is positive, the secure element will continue a second RSA operation 1124. Second RSA operation 1124 performs a second RSA algorithm 1124 on the software distribution public key SVPbK 1116 and a software distribution public key signature SDPbK_SIG 1122 to obtain a second RSA value EK2 and compares (operation 1125) the second RSA value EK2 with a software distribution public key SDPbK 1126. If the comparison is negative (1127), the secure element stops the validation operation. If the comparison 1125 is positive, the secure element continues to perform a third RSA operation 1134. Third RSA operation 1134 perform a third RSA algorithm 1134 on the software

distribution public key SDPbK 1126 and a software personalization site key signature SPPbK_SIG 1132 to obtain a third RSA value EK3 and compares the third RSA value EK3 with a software personalization public key SPPbK 1136. If the result of the comparison is negative (1137), the secure element stops the chain of trust validation. If the result of the comparison is positive, the secure element will continue to the boot certificate validation. It is appreciated that the RSA operation means a public key cryptographic operation.

[0075] For the purposes of the present invention, root public key RPK 1102 is at the highest level in the boot loader process. All other keys are derived and signed from the root public key. The digest of the root public key DRPK or full key 1108 is stored in the OTP (one time programmable memory, i.e., the non-volatile memory register 860 of Figure 8) or hardcoded in hardware. Software vendor key SVPbK 1116 is a dedicated CAS software vendor key, where vendor may refer to a service provider, a network operator, a device manufacturer, or other entity that may want to use the demodulator SOC. Software distribution key SDPbK 1126 is a sub-key offered for flexibility of the software signing process to further discriminate the distribution channels (e.g., by region, by customers, by volume, etc.). Software personalization site SPPbK 1136 is a sub-key to identify the physical personalization site or machine used to package the main certificates and firmware. Each sub-key is associated with a digital signature that is the corresponding public key encrypted with the higher level private key (e.g., SVPbK_SIG is the RSA result of SVPbK and RPK). It is understood that the certificate 1100 and the root public key 1102, software vendor public key code (or signature) 1112, software public key 1116, software distribution public key code 1122, software distribution public key 1126, software personalization site code 1132, and software personalization public key 1136 are part of the data and executable codes or applications that need to be loaded to the secure S-RAM.

[0076] The chain of trust validation provides numerous security benefits such as verifying that all sub-keys can be verified against the digest root public key (or full key) stored in the non-volatile memory or tamper-proof register of the demodulator SOC device. The other benefits include establishing a root of trust between the software personalization site public key in the certificate and the device: The certificate loaded in the secure memory belongs to the same chain of trust as the hardware device itself.

[0077] Figure 11 is a diagram illustrating a boot certificate validation 1100 according to an embodiment of the present invention. Boot certificate validation 1100 verifies that the certificate content can be trusted and has not been altered and establishes a legitimate relationship between the content and the software personalization site public key. Boot

certificate validation 1100 comprises hashing (1152) the certificate 1100 including the software personalization site private key SPPvK 1156 to obtain a hash value HV1 and performing an RSA function (1154) on the HV1 and the software personalization private key SPPvK 1156 to generate an RSA value EK5. Boot certificate validation 1100 further includes validating the certificate content by comparing (1176) the RSA value EK5 with a certificate signature CERT_SIG 1166. If the comparison is negative (1177), the secure element stops the boot loader process. If the comparison 1175 is positive, the secure element continues to step 940 of the boot loader process, which is the certificate binding validation.

[0078] Figure 12 is a diagram illustrating a certificate binding validation 1200 according to an embodiment of the present invention. Certificate binding validation 1200 verifies that the loaded certificate is intended for the given device and has not been duplicated or copied on another hardware platform. Certificate binding validation 1200 includes comparing the device identification DVID 1208 stored in the OTP or tamper-proof register (NVM register 860 of Figure 8) with a value 1202 stored in the digital certificate 1100 that has been verified for authenticity in previously validations. If the result of the comparison is negative (1207), the secure element stops the boot loader process. If the comparison 1205 is positive, the secure element continues to step 950 of the boot loader process, which is the firmware image validation.

[0079] Figure 13 is a diagram illustrating a firmware image validation 1300 according to an embodiment of the present invention. Firmware image validation 1300 verifies that the entire firmware image has not been altered and is issued from the same chain of trust as the boot certificate. Firmware image validation 1300 executes a hash algorithm 1304 on the firmware image 1310 and obtains a hash value HV3. An RSA operation is further performed on the obtained hash value HV3 and the software personalization site PPPbk 1156 to generate an RSA value EK13. The generated RSA value EK13 is then compared (1355) with the obtained hash value HV3. If the result of the comparison is negative, the secure element will stop the boot loader process (1357). If the result of the comparison is positive, the secure element may continue the boot loader process at step 960, which is a firmware image decryption.

[0080] In some embodiments, firmware may be encrypted for confidentiality requirements. The secure element may use one of the following encryption/decryption methods for deciphering firmware: 1) using a symmetric encryption of a software encryption key that is generated from the hardware unique key, which is stored in one of the NVM registers, or 2) and using an asymmetric encryption of a software encryption key with a private/public key

pair for which the private key is stored in one of the NVM registers and the public key is used for encryption of the software encryption key that is stored in the digital certificate.

[0081] Figure 14A is a diagram illustrating a firmware image decryption (deciphering) 1400A according to an embodiment of the present invention. The secure element performs a symmetric key encryption 1404 on a software encoded seed value 1402 (which is disposed in the digital certificate 1100) and a hardware unique key 1406 (which is stored in one of the fuse banks, NVM or OTP registers 860 of Figure 8). The generated encryption key EK14 is used in a second encryption process 1414 for decrypting firmware image 1410 if it has been previously encrypted. The decrypted firmware image 1415 is then stored in the secure memory. The decrypted firmware image is further provided to a hash process 1418 to obtain a hash value HV14 that is compared with a software checksum 1408 embedded in the certificate 1100. If the result of the comparison 1420 is negative, the secure element will abort the boot loader process. If the result of the comparison is positive, the secure element starts the applications at step 970.

[0082] Figure 14B is a diagram illustrating a firmware image decryption (deciphering) 1400B according to an alternative embodiment of the present invention. The secure element performs a first encryption operation 1454 on the software key SWkey1452 and a private key CSPvK 1456 stored in the NVM or OTP register. The generated software encrypted key EK15 is then used in a second encryption operation 1464 to decrypt the firmware image 1410. The decrypted firmware is stored in the secure S-RAM and also provided to a hash operator 1468 to obtain a hash value HV15. The obtained hash value HV15 is compared with the software checksum 1408. If the result of the comparison 1470 is negative, the secure element will abort the boot loader process. If the result of the comparison is positive, the secure element starts the applications at step 970.

[0083] The foregoing description of the code download and boot loader process is not intended to be exhaustive and to limit the scope of the invention to the precise disclosed order and form. For example, although the boot loader process has been described having several sequential steps of validations and firmware image decryption as the last step after the validation. The boot loader process may begins with decryption of the firmware in an embodiment. The boot loader process may also perform in parallel instead of sequentially.

[0084] Figure 15 is a diagram illustrating a one-step firmware decryption and authentication process 1500 according to an embodiment of the present invention. The one-step firmware decryption and authentication process includes a first encryption process 1502

that can be performed for example by one of the hardware accelerators 858. First encryption process 1502 generates an encryption key EK14 from a SWENC_SEED 1402 disposed in the certificate 1100 and the unique identifier HUK 1406 disposed in the NVM register. Software encryption key EK14 is then provided to a second encryption process 1503 that uses the encryption key EK14 to decipher the firmware image 1410. The deciphered or decrypted firmware image is then hashed to obtain a hash value HV15. An encryption engine RSA 1554 (e.g., one of the hardware accelerators 858) operates on the hash value HV15 and a software personalization site key SPPbK 1156 to produce an encryption value EK20 that is compared with a software signature SW_SIG 1366. In the event that the comparison 1555 produces a match, the secure element starts the applications (the firmware image). In the event that the comparison is negative, the secure element stops the authentication process and may flush the firmware image 1410 (data and applications files) stored in the secure memory. Note that the firmware image and the certificate can be authenticated in one validation step.

[0085] Figure 16 is a diagram illustrating a firmware run-time authentication using hardware facilities provided by the secure element according to an embodiment of the present invention. The firmware run-time authentication provides an efficient way to mitigate the risk of running malicious code at run time. The firmware run-time authentication verifies and authenticates software within power cycles to protect hardware intrusive attacks and fault injection. In an embodiment, the hardware facilities of the secure element writes (programs by burning or blowing fuses) a software checksum SWChecksum 1408 to one or more of the NVM registers 858 during the boot process and writes runtime configuration parameter to corresponding configuration registers of the secure element finite state machine 1808, which controls the cryptographic hash function 1802 and the comparator 1804. Cryptographic hash function 1802 produces a hash value HV18 from firmware 1410 and compares (1804) the hash value HV18 with the SWChecksum stored in one of the NVM registers 858. In the event that there is a match (indicated as “Yes”), the secure element continues its operation. In the event there is no match (indicated as “No”), i.e., the firmware may have been modified or compromised, the secure element disables the firmware execution. In some embodiments, the firmware run-time authentication can be triggered from different sources that may include, but is not limited to: 1) software driven by requesting an authentication through a control register in the security element; 2) hardware timer as a recurring event driven by a hardware counter set during the boot process; 3) when the secure S-CPU enters or exits a sleep period; or 4) when the secure S-CPU receives a wakeup request.

[0086] In an embodiment, the hash value of the decrypted firmware is stored in the boot certificate and is programmed into one of the NVM (one-time- programmable) registers in the secure element during the boot process so that it cannot be modified or altered. It is important to note that this process cannot be performed by the RAM-ware itself because the RAM-ware can be tampered with. Thus, the process has to be performed entirely in hardware or using code stored in ROM that cannot be modified. The SWchecksum written into a write-once memory register can be reset on power-on/off of the secure element. In addition, the secure element includes control parameters that define the source and recurrence of the run-time check.

[0087] In an embodiment, digital certificate 1100 may include runtime configuration data 1602 that is written into associated configuration registers 1809 of the secure element during the boot process. Configuration data 1602 may configure or customize the finite state machine (FSM) so that the secure element operates in a manner that is desired by a vendor or a service provider.

[0088] Figure 17 is an exemplary process of decrypting or deciphering a firmware stored in the secure RAM according to an embodiment of the present invention. The decryption process is optional and is only needed when the stored firmware has been previously received in an encrypted form. To decipher the encrypted firmware 1730, the secure element first retrieves a SEED 1750 disposed in a boot certificate 1710 that has been validated and thus considered to be authentic and encrypts the SEED using a unique device key 1760 (Hardware unique key that is unique and private per device and stored in a non-volatile memory register). The thus generated software encryption key 1770 at step S1720 is then used to decipher the encrypted software 1730 at step S1725.

[0089] While the advantages and embodiments of the present invention have been depicted and described, there are many more possible embodiments, applications and advantages without deviating from the spirit of the inventive ideas described herein. It will be apparent to those skilled in the art that many modifications and variations in construction and widely differing embodiments and applications of the present invention will suggest themselves without departing from the spirit and scope of the invention. For example, the hardware accelerators may include one or more AES units to generate an encryption key and/or perform data encryption. Other alternatives for firmware image validations can also be provided where steps are added, one of more steps are removed, or one or more steps are provided in a different sequence without departing from the scope of the claims herein.

[0090] It is understood that the above embodiments of the present invention are illustrative and not limitative. Various alternatives and equivalents are possible. The invention is not limited by the type of integrated circuits in which the present disclosure may be disposed. Other additions, subtractions or modifications are obvious in view of the present invention and are intended to fall within the scope of the appended claims.

5

WHAT IS CLAIMED IS:

- 1 1. An integrated circuit comprising:
2 a demodulator having an interface unit configured to receive a program file
3 and a certificate associated with the program file from an external memory device; and
4 a secure element communicatively coupled to the demodulator, the secure
5 element comprising:
6 a non-volatile register containing a unique identifier;
7 a read-only memory comprising a boot code;
8 a random access memory configured to store the received program file
9 and the associated certificate; and
10 a processing unit coupled to the read-only memory and the random
11 access memory and being configured to execute the boot code for authenticating the
12 certificate stored in the random access memory;
13 wherein the secure element is locked after the program file and the certificate
14 are stored in the random access memory, thereby preventing the demodulator from accessing
15 the secure element.
- 1 2. The integrated circuit of claim 1, wherein the authenticating the
2 certificate stored in the random access memory comprises:
3 comparing a value of the certificate with the unique identifier.
- 1 3. The integrated circuit of claim 2, wherein the value of the certificate
2 includes a first hash value of a portion of the certificate and the unique identifier includes a
3 digest root public key.
- 1 4. The integrated circuit of claim 2, wherein the unique identifier includes
2 a device identifier of the integrated circuit and the value of the certificate includes the unique
3 device identifier of the integrated circuit.
- 1 5. The integrated circuit of claim 2, wherein the value of the certificate
2 comprises a root public key.
- 1 6. The integrated circuit of claim 1, wherein the secure element disables
2 or removes the program file from the random access memory in the event that the first hash
3 value and the unique identifier do not match.

1 7. The integrated circuit of claim 1, wherein the certificate comprises
2 information data associated with a secure state of the program file.

1 8. The integrated circuit of claim 7, wherein the information data
2 comprises a public key and a digital signature associated with the program file.

1 9. The integrated circuit of claim 8, wherein the secure element
2 authenticates the programs file by hashing the program file to obtain a second hash value,
3 encrypting the second hash value with the public key to obtain an encrypted second hash
4 value, and comparing the encrypted second hash value with the digital signature.

1 10. The integrated circuit of claim 9, wherein the secure element disables
2 or removes the program file stored in the random access memory if the encrypted second
3 hash value and the digital signature do not match.

1 11. The integrated circuit of claim 1, wherein the secure element performs
2 a series of validations in the event that the first hash value matches the unique identifier.

1 12. The integrated circuit of claim 11, wherein the series of validations
2 comprises one of a chain of trust verification, a boot certificate validation, a certificate
3 binding validation, and a firmware image validation.

1 13. The integrated circuit of claim 12, wherein the chain of trust
2 verification comprises a plurality layers of public key validations.

1 14. The integrated circuit of claim 1, wherein the secure element decrypts
2 or deciphers the program file using an encryption key that is derived from the unique
3 identifier and from a seed value stored in the certificate if the program file stored in the
4 random access memory has been encrypted.

1 15. The integrated circuit of claim 14 further comprising a logic unit
2 configured to encrypt the decrypted program file in the random access memory and writes the
3 encrypted program file to the external memory device in response to a backup event.

1 16. The integrated circuit of claim 1, wherein the secure element
2 authenticates the program file prior to initiating the program file.

1 17. A device comprising:

2 a unique identifier;
3 a processing unit;
4 a random access memory coupled to the processing unit;
5 a read-only memory coupled to the processing unit and having instruction
6 codes that, when executed by the processing unit, causes the processing unit to:
7 read in a firmware image and a certificate associated with the firmware
8 image, the certificate including a seed number, a public key, and a digital signature;
9 store the firmware image and the associated certificate into the random
10 access memory; and
11 simultaneously authenticate the certificate and the firmware image.

1 18. The device of claim 17, wherein the simultaneous authentication of the
2 certificate and the firmware image comprises:
3 generating an encryption key using the seed number and the unique identifier;
4 encrypting or decrypting the firmware image using the generated encryption
5 key;
6 hashing the encrypted or decrypted firmware image to obtain a hash;
7 encrypting the public key using the obtained hash; and
8 comparing the encrypted public key with the digital signature.

1 19. A method for authenticating program code to be executed by an
2 information processing apparatus, the method comprising:
3 receiving the program code and a certificate associated with the program code
4 from an external device;
5 storing the received program code and the associated certificate in a secure
6 random access memory disposed in the information processing apparatus;
7 hashing a portion of the certificate to obtain a first hash value; and
8 comparing the first hash value with a unique identifier disposed in the
9 information processing apparatus.

1 20. The method of claim 19 further comprising disabling or removing the
2 stored program code in the event that the first hash value does not match the unique
3 identifier.

1 21. The method of claim 19, wherein the portion of the certificate
2 comprises information data associated with a secure state of the program code.

1 22. The method of claim 21, wherein the information data comprises a root
2 public key, a public key associated with a manufacturer of the information processing
3 apparatus or a service provider, and a signature associated with the public key.

1 23. The method of claim 22 further comprising:
2 encrypting the signature using the root public key to obtain a first encryption
3 key; and
4 authenticating the program code by comparing the first encryption key with
5 the public key.

1 24. The method of claim 19 further comprising decrypting the program
2 code in the event that the comparison returns a positive result, wherein the decrypting
3 comprising:
4 generating a second encryption key by performing a first encryption
5 algorithm on a seed value disposed in the certificate and the unique identifier; and
6 decrypting the program code using the second encryption key.

1 25. The method of claim 24 further comprising:
2 hashing the decrypted program to obtain a second hash value; and
3 verifying the decrypted program by comparing the second hash value with a
4 checksum stored in the portion of the certificate.

1 26. The method of claim 19 further comprising decrypting the program
2 code, wherein the decrypting comprises:
3 generating a third encryption key by performing a second encryption
4 algorithm on a crypto public key disposed in the certificate and the unique identifier; and
5 deciphering the program code using the third encryption key.

1 27. The method of claim 26 further comprising:
2 hashing the deciphered program code to obtain a third hash value; and
3 comparing the deciphered program code by comparing the third hash value
4 with a checksum stored in the portion of the certificate.

1 28. A method for authenticating a firmware image by a receiver having a
2 secure random access memory, the method comprising:
3 receiving the firmware image and a digital certificate associated with the
4 firmware image from an external device;

5 storing the firmware image and the digital certificate in the secure random
6 access memory;
7 hashing the firmware image to obtain a hash;
8 authenticating the firmware image by comparing the hash with a checksum
9 stored in the digital certificate.

1 29. The method of claim 28 further comprising writing runtime
2 configuration information stored in the digital certificate to associated registers in the
3 receiver.

1 30. The method of claim 28, wherein the authenticating is triggered by
2 software, periodically by a timer, by a wakeup event, or when the receiver enters or exits a
3 sleep period.

1 31. The method of claim 28 further comprising:
2 generating an encryption key using a seed value stored in the digital certificate
3 and a unique identifier disposed in the receiver;
4 decrypting the firmware image using the generated encryption key; and
5 storing the decrypted firmware in the secure random access memory.

1 32. The method of claim 31 further comprising:
2 encrypting the decrypted firmware stored in the secure random access
3 memory; and
4 writing the encrypted firmware to an external memory device in response to a
5 backup event.

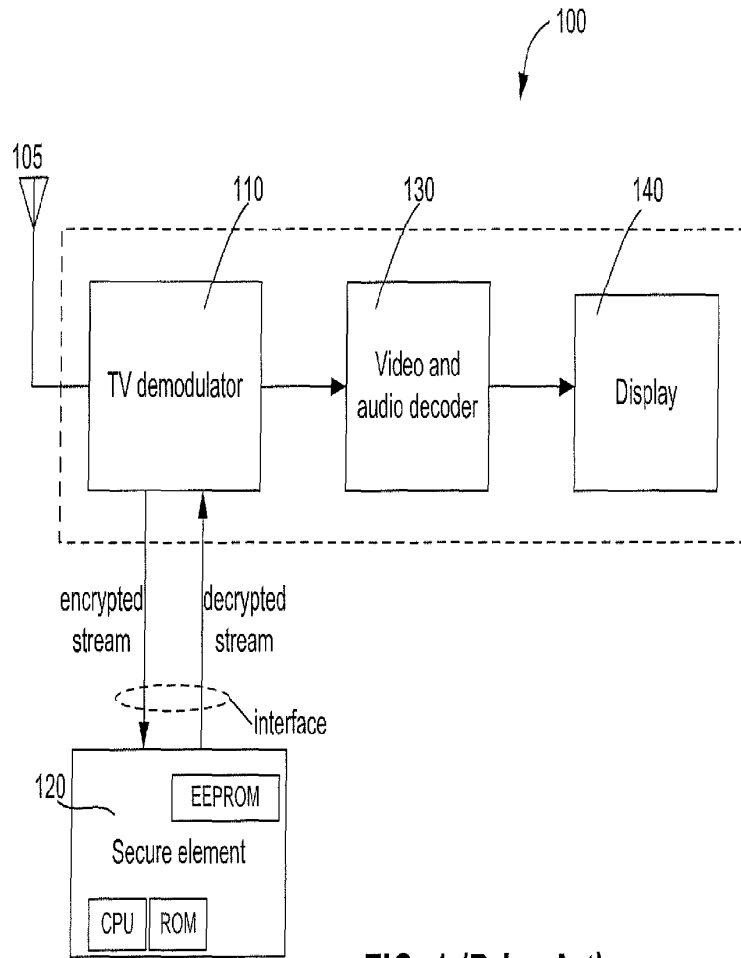


FIG. 1 (Prior Art)

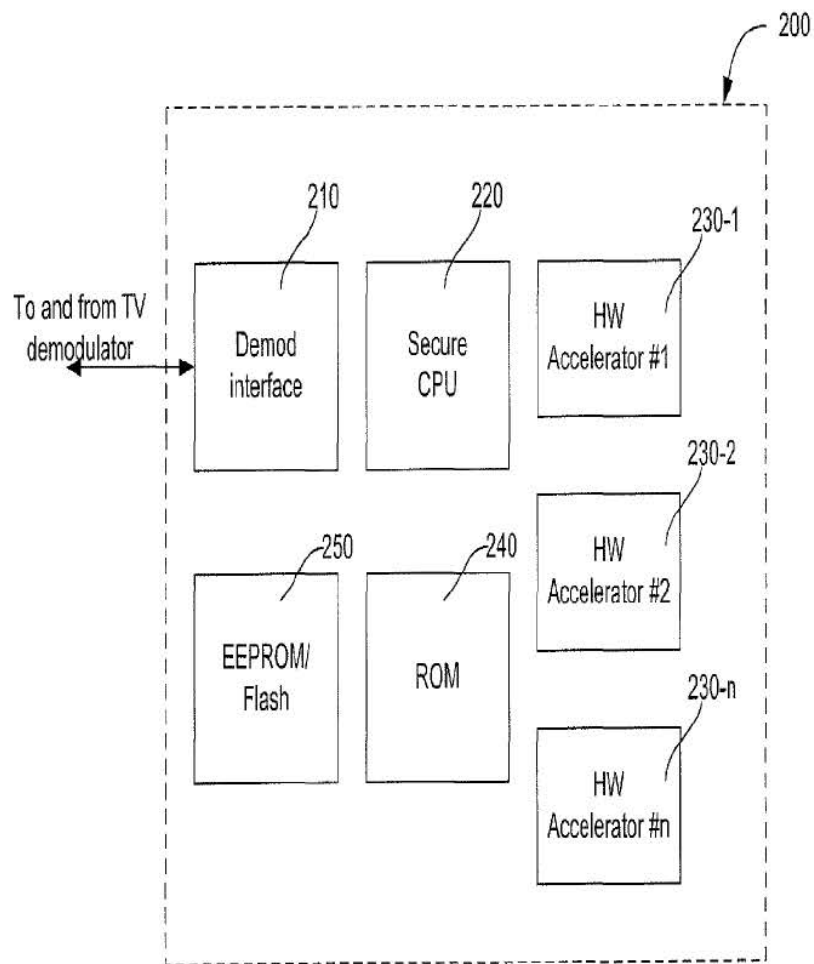


FIG. 2 (Prior Art)