I519990

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I519990 B**

(45)公告日： 中華民國 105 (2016) 年 02 月 01 日

(21)申請案號：097113832 (22)申請日： 中華民國 97 (2008) 年 04 月 16 日

(51)Int. Cl.： *G06F21/30 (2013.01)* *G06F21/70 (2013.01)*

(30)優先權：2007/04/17 美國 11/736,387

(71)申請人：美國博通公司 (美國) BROADCOM CORPORATION (US)
美國

(72)發明人：陳雪敏 XUEMIN (SHERMAN) CHEN (US)

(74)代理人：莊志強

(56)參考文獻：

TW 200410575A US 2006/0107316A1

審查人員：李京叡

申請專利範圍項數：10 項 圖式數：3 共 24 頁

(54)名稱

在通信系統中處理資料的方法和系統

METHOD AND APPARATUS OF SECURE AUTHENTICATION FOR SYSTEM-ON-CHIP (SOC)

(57)摘要

本發明涉及一種在通信系統中處理資料的方法和系統，更具體地，涉及用於認證一個或多個安全功能的接入的 SoC。在 SoC 中生成的密碼對於每個 SoC 示例來說是唯一的，並且對於認證的每次重復來說也是唯一的。SoC 可向試圖接入的外部實體進行問詢，以提供匹配的密碼。可在 SoC 中生成並存儲亂數採樣值。記憶體中還存儲了晶片 ID、加密詞和具有密匙索引的密匙表。將記憶體中存儲的兩個或多個專案傳送到哈希函數以生成密碼。外部實體可生成密碼，並利用每次認證操作中 SoC 傳遞的資訊以及已知的資訊，將該密碼傳送回 SoC。SoC 將返回的密碼與內部生成的密碼進行比較，並授權接入該安全功能。

A SoC may be utilized to authenticate access to one or more secure functions. A password may be generated within the SoC which is unique to each SoC instance and unique to each iteration of authentication. The SoC may challenge external entities attempting access to provide a matching password. A random number sample may be generated within the SoC and stored. A chip ID, secret word and a table of keys with key indices are also stored in memory. Two or more of the stored items may be passed to a hash function to generate the password. The external entity may generate and return the password utilizing information communicated from the SoC during each authentication operation as well as information known a priori. The SoC may compare the returned password with the internally generated password and may grant access to the secure functions.

指定代表圖：

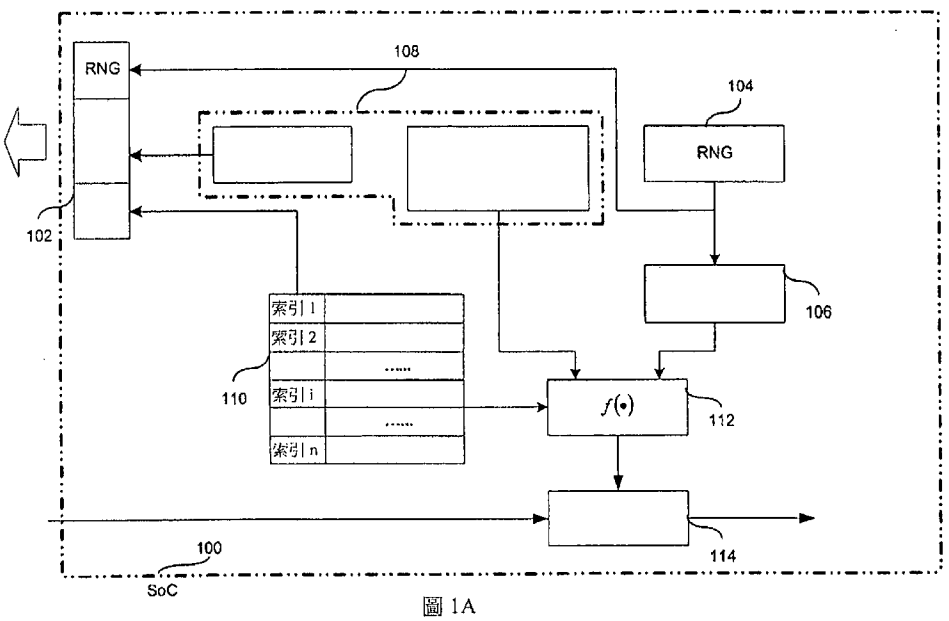

圖 1A

符號簡單說明：

100・・・片上系統 (SoC)

102・・・問詢寄存器 (challenge register)

104・・・亂數生成器 (RNG)

106・・・本地可擦重寫記憶體

108、110・・・本地存儲單元

112・・・加密單元

114・・・數位比較器單元

I519990

公告本

104年10月21日修正替換本

發明摘要

※申請案號：99113832

※申請日：99.4.16　　※IPC分類：G06F 21/30 (2013.01)
G06F 21/70 (2013.01)

【發明名稱】(中文/英文)

在通信系統中處理資料的方法和系統

METHOD AND APPARATUS OF SECURE AUTHENTICATION FOR SYSTEM-ON-CHIP (SoC)

【中文】

本發明涉及一種在通信系統中處理資料的方法和系統，更具體地，涉及用於認證一個或多個安全功能的接入的 SoC。在 SoC 中生成的密碼對於每個 SoC 示例來說是唯一的，並且對於認證的每次重復來說也是唯一的。SoC 可向試圖接入的外部實體進行問詢，以提供匹配的密碼。可在 SoC 中生成並存儲亂數採樣值。記憶體中還存儲了晶片 ID、加密詞和具有密匙索引的密匙表。將記憶體中存儲的兩個或多個專案傳送到哈希函數以生成密碼。外部實體可生成密碼，並利用每次認證操作中 SoC 傳遞的資訊以及已知的資訊，將該密碼傳送回 SoC。SoC 將返回的密碼與內部生成的密碼進行比較，並授權接入該安全功能。

【英文】

A SoC may be utilized to authenticate access to one or more secure functions. A password may be generated within the SoC which is unique to each SoC instance and unique to each iteration of authentication. The SoC may challenge external entities attempting access to provide a matching password. A random number sample may be generated within the SoC and stored. A chip ID, secret word and a table of keys with key indices are also stored in memory. Two or more of the stored items may be passed to a hash function to generate the password. The external entity may generate and return

the password utilizing information communicated from the SoC during each authentication operation as well as information known a priori. The SoC may compare the returned password with the internally generated password and may grant access to the secure functions.

【代表圖】

【本案指定代表圖】：第（1A）圖。

【本代表圖之符號簡單說明】：

片上系統(SoC)・・・100

問詢寄存器(challenge register)・・・102

亂數生成器(RNG)・・・104

本地可擦重寫記憶體・・・106

本地存儲單元・・・108、110

加密單元・・・112

數位比較器單元・・・114

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

104年10月21日修正替換本

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

在通信系統中處理資料的方法和系統

METHOD AND APPARATUS OF SECURE AUTHENTICATION FOR SYSTEM-ON-CHIP (SoC)

【技術領域】

本發明主要涉及安全通信系統，更具體地說，涉及用於片上系統(SoC)安全認證的方法和裝置。

【先前技術】

工業標準爲數位電視或DVD內容的傳送提供了必需的協定和基礎設施。這些數位電視或DVD內容可包括音頻、視頻、和資料信號。可採用寬帶網路、前端設備和終端設備(如機頂盒，STB)以及媒體設備(如DVD)中的多種功能和操作對這些資料流程進行處理。例如，這些功能和操作可包括設備的敏感區的接入(如掃描接入、系統匯流排和系統介面)並且這些功能和操作可從某種安全形式或用戶認證機制中獲益。

密碼是最常用的認證機制。其利用用戶具有的資訊。用戶提供密碼並由安全系統對該密碼進行認證。如果經認證該密碼是與用戶有關的，該用戶的身份通過認證。如果不是，那麼該密碼將被拒絕並且該認證失敗。

密碼具有一個根本性的問題，即其可用於多個設備。如果非授權用戶發現一個設備的密碼，那麼這個密碼可用於進入由同一密碼認證的其他設備。在這種情況下，設備(如STB)不能區別非授權的用戶和合法用戶。

對於許多的應用(如安全下載操作)，非授權用戶可在操作過程中發現密碼，進而將該密碼用於在同一類型的下一操作中得以進入。

爲了確保安全通信，需要在待傳送資料流傳送到設備(如機頂盒)的過程中對其進行保護。一旦接收到該傳送的資料流程，STB中的一個或多個設備需要爲該資料流程提供安全接入。

比較本發明後續將要結合附圖介紹的系統，現有技術的其他局限性和弊端對於本領域的普通技術人員來說是顯而易見的。

【發明內容】

本發明提供了一種片上系統(SoC)安全認證的方法和裝置，結合至少一幅附圖進行了充分的展現和描述，並在權利要求中得到了更完整的闡述。

根據本發明的一個方面，提供了一種在通信系統中處理資料的方法，該方法包括：使用對每個晶片和每次詢問來說唯一的密碼，來認證向一個或多個由晶片控制的安全功能的接入。

優選地，所述方法包括在所述晶片中生成所述對每個晶片和每次詢問來說唯一的密碼。

優選地，所述方法包括在所述晶片中，由亂數生成器(RNG)生成亂數採樣值。

優選地，所述方法包括將所述生成的亂數採樣值存儲到以下中的一個或多個：片上記憶體和片外記憶體。

優選地，所述方法包括在所述晶片上存儲加密詞，其中所述加密詞不能被外部實體獲得。

優選地，所述方法包括在所述晶片上存儲以下中的一個或多個：對所述晶片來說唯一的晶片 ID 和密匙表，其中所述密匙表包括密匙和對應的密匙索引。

優選地，所述方法包括將下列資訊中的兩個或多個傳送到哈希函數：所述加密詞、所述生成的亂數採樣值、和來自所述密匙表的所述密匙。

優選地，所述方法包括在所述晶片內從所述哈希函數生成密碼。

優選地，所述方法包括向試圖接入的外部實體問詢，以回應可與所述哈希函數生成的所述密碼相匹配的密碼。

優選地，所述方法包括在寄存器中存儲下列資訊中的兩個或多個：所述亂數採樣值、對每個晶片來說唯一的所述晶片 ID 和所述密匙索引。

優選地，所述方法包括將所述寄存器中的內容發送到所述試圖接入的外部實體。

優選地，授權的外部記憶體具有關於所述晶片 ID、所述加密詞、具有對應的密匙索引的所述密匙表和哈希函數的消息。

優選地，所述方法包括將所述試圖接入的外部實體生成的回應和所述哈希函數生成的密碼進行比較。

優選地，所述方法包括基於所述比較，授權所述外部實體接入所述一個和多個安全功能。

優選地，所述方法包括在所述晶片中，使用安全加密演算法生成加密詞，其中，基於所述加密詞生成所述密碼。

根據本發明的一個方面，提供了一種在通信系統中處理資料的系統，該系統包括：一個或多個電路，用於使用對每個晶片和每次詢問來說唯一的密碼來認證向一個或多個由晶片控制的安全功能的接入。

優選地，所述一個或多個電路在所述晶片中生成所述對每個晶片和每次詢問來說唯一的密碼。

優選地，所述一個或多個電路在所述晶片中生成亂數採樣值。

優選地，所述一個或多個電路包括片上記憶體和/或片外記憶體，用於存儲生成的亂數採樣值。

優選地，所述一個或多個電路用於存儲加密詞，且所述加密詞不能被外部實體獲得。

優選地，所述一個或多個電路用於存儲一個或多個晶片 ID 和密匙表，其中所述密匙表包括密匙和對應的密匙索引。

優選地，所述一個或多個電路用於將下列資訊中的兩個或多個傳送到所述哈希函數：所述加密詞、所述生成的亂數採樣值、和來自所述密匙表的所述密匙。

優選地，所述一個或多個電路在所述晶片內從所述哈希函數生成所述密碼。

優選地，所述一個或多個電路向試圖接入的外部實體問詢，以回應可與所述哈希函數生成的所述密碼相匹配的密碼。

優選地，所述一個或多個電路包括寄存器，用於存儲下列資訊中的兩個或多個：所述生成的亂數採樣值、對每個晶片來說唯一的所述晶片 ID 和所述密匙索引。

優選地，所述一個或多個電路用於將所述寄存器中的內容發送到所述試圖接入的外部實體。

優選地，授權的外部記憶體具有關於所述晶片 ID、所述加密詞、具有對應的密匙索引的所述密匙表和哈希函數的消息。

優選地，所述一個或多個電路將所述試圖接入的外部實體生成的回應和所述哈希函數生成的密碼進行比較。

優選地，所述一個或多個電路基於所述比較，授權所述外部實體接入所述一個和多個安全功能。

優選地，所述一個或多個電路在所述晶片中，使用安全加密演算法生成加密詞，其中，基於所述加密詞生成所述密碼。

本發明的各種優點、各個方面和創新特徵，以及其中所示例的實施例的細節，將在以下的描述和附圖中進行詳細介紹。

【圖式簡單說明】

圖 1A 是根據本發明實施例的可用於密碼認證的具有內部可擦重寫記憶體的片上系統的典型框圖；

圖 1B 是根據本發明實施例的可用於密碼認證處理的具有外部可擦重寫記憶體的片上系統的典型框圖；

圖 2 是根據本發明實施例的用於生成認證處理密碼的片上系

統的外部實體的典型框圖；

圖 3A 是根據本發明實施例的片上系統中的認證處理的一部分的典型流程圖；

圖 3B 是根據本發明實施例的片上系統的外部實體中的認證處理的一部分的典型流程圖；

圖 3C 是根據本發明實施例的片上系統中的認證處理的一部分的典型流程圖。

【實施方式】

本發明的各個方面涉及用於片上系統(SoC)的安全認證的方法和裝置。本發明的各個方面可包括可用於對試圖獲得某個功能或進入某個系統的外部實體進行認證的 SoC。在認證嘗試之前，該 SoC 和獲得授權的外部實體分別可具有隱藏資料的資訊，並可在該認證過程中進行資料傳送。使用相同的資料，SoC 和外部實體能生成相同的密碼並獲得系統接入。可採用兩種方式使得密碼唯一，例如對每個操作和每個 SoC 設備來說唯一。SoC 上的亂數生成器(RNG)可使得密碼隨著每個認證過程的重復而改變。SoC 的每個實例具有其自身的加密詞(secret word)使得每個設備的密碼都是唯一的。

圖 1A 是根據本發明實施例的可用於密碼認證操作的具有內部可擦重寫記憶體的片上系統的典型框圖。參照圖 1A，示出了 SoC 100，所述 SoC 100 包括問詢寄存器(challenge register)102、亂數生成器(RNG)104、多個本地存儲單元 108、110、本地可擦重寫記憶體 106、加密單元 112 和數位比較器單元 114。圖中還示出了 SoC 100 的邊界。

問詢寄存器 102 可包括用於存儲 RNG 104 生成的亂數採樣值的合適記憶體、晶片 ID 和密匙表索引。問詢寄存器 102 可包括合適的邏輯、電路和/或代碼，用於在 SoC 和外部實體(圖 2，200)間交換資訊(請求認證)。該問詢寄存器 102 與 RNG 104、記憶體 108

和 110 通信連接。

RNG 104 可與問詢寄存器 102 和本地可擦重寫記憶體 106 通信連接。RNG 104 可包括合適的邏輯、電路和/或代碼，用於生成亂數採樣值。

記憶體 108 可包括用於存儲晶片 ID 和加密詞的內部記憶體。記憶體 108 可實現加密詞的加密存儲。可使用晶片 ID 和安全加密演算法生成加密詞。記憶體 108 中的安全記憶體可與加密單元 112 通信連接並與其他外部實體解除連接。記憶體 108 可用於存儲晶片 ID，並可與問詢寄存器 102 通信連接。記憶體 108 可採用任何類型的存儲技術，如 PROM、FLASH 和 EEPROM。

本地可擦重寫記憶體 106 可包括用於存儲亂數生成器 104 的輸出的記憶體。該本地可擦重寫記憶體 106 可採用任何類型的存儲技術，如 FLASH 和 EEPROM。該本地可擦重寫記憶體 106 可與 RNG 104 和加密單元 112 通信連接。

記憶體 110 可包括合適的邏輯、電路和/或代碼，用於存儲密匙表和相關密匙索引。該記憶體 110 可用于向加密單元 112 以及問詢寄存器 102 傳送資料。

加密單元 112 可包括合適的邏輯、電路和/或代碼，用於根據多個輸入資料生成密碼。根據本發明的一個方面，加密單元 112 可用於加密來自多個資料源的資料以生成密碼，這些資料包括：來自記憶體 108 的加密詞、來自本地可擦重寫記憶體 106 的亂數採樣值和來自記憶體 110 中的密匙表的密匙。在本發明的另一實施例中，加密單元 112 可包括合適的邏輯、電路和/或代碼，以使用哈希函數，如 SHA1、SHA2 和 HMAC-SHA 生成密碼。在這一點上，可採用來自下列兩個資料源的資料生成密碼：來自記憶體 108 的加密詞和來自本地可擦重寫記憶體 106 的亂數採樣值。

數位比較器 114 可包括合適的邏輯、電路和/或代碼，用於從外部實體接收密碼，該密碼由加密單元 112 生成。數位比較器 114

可包括合適的邏輯、電路和/或代碼，用於比較兩個密碼，並輸出認證通過或失敗的指示。

在運行中，可在 RNG 104 中生成該亂數採樣值。可將 RNG 104 生成的亂數採樣值、來自記憶體 108 的晶片 ID 和來自記憶體 110 的密匙索引傳送到問詢寄存器 102。接著將問詢寄存器 102 中的內容包含在問詢資訊中發送到圖 2 中示出的外部實體 200，這樣外部實體可生成密碼並將在問詢回應中將該密碼回發。可將 RNG 104 中生成的亂數採樣值存儲在本地可擦重寫記憶體 106 中。可將來自記憶體 108 的加密詞、來自本地可擦重寫記憶體 106 的亂數採樣值和來自記憶體 110 中的密匙表的密匙傳送到加密單元 112。加密單元 112 可使用哈希函數生成密碼。數位比較器 114 可接收來自加密單元 112 的密碼和來自外部實體 200 的密碼，並將它們進行比較。SoC 可確定該認證通過或失敗。

圖 1B 是根據本發明實施例的可用於密碼認證操作的具有外部可擦重寫記憶體的片上系統的典型框圖。參照圖 1B，示出了 SoC 100，該 SoC 100 包括問詢寄存器 102、RNG 104、多個本地記憶體 108、110、外部記憶體 120、加密單元 112、數位比較單元 114、標記單元(signing unit)116 和驗證單元 118。該 SoC 110 以及問詢寄存器 102、RNG 104、多個本地記憶體 108、110、加密單元 112、數位比較單元 114 可分別與圖 1A 中的問詢寄存器 102、RNG 104、多個本地記憶體 108、110、加密單元 112、數位比較單元 114 相似。參照圖 1B，示出了一些附加元件，包括外部記憶體 120、標記單元 116 和驗證單元 118。

標記單元 116 可包括合適的邏輯、電路和/或代碼，用於標記 RNG 104 的亂數採樣值輸出。標記單元 116 可使用非對稱演算法(如 RSA、DSA)或對稱演算法(如 HMAC)，採用嵌入標記密匙標記亂數採樣值。該標記單元 116 可包括合適的邏輯、電路和/或代碼，用於與外部記憶體 120 交換資訊，以存儲被標記的亂數採樣值。

根據本發明的另一方面，可加密該標記密匙並存儲在外部記憶體 120 中。

外部記憶體 120 可包括存儲設備，該存儲設備可包括合適的邏輯、電路和/或代碼，用於與 SoC 交換資料。外部記憶體 120 可包括用於存儲來自亂數生成器 104 的輸出的記憶體，該輸出已經在標記單元 116 中進行了標記。例如，外部記憶體 120 可基於快閃記憶體技術。根據本發明的一個方面，該標記和驗證密匙可存儲在外部記憶體 120 中。

該驗證單元 118 可包括合適的邏輯、電路和/或代碼，用於從外部記憶體 120 接收驗證密匙和標記的亂數採樣值，並破譯該標記的亂數採樣值。該驗證單元 118 可包括合適的邏輯、電路和/或代碼，用於與加密單元 112 交換資訊。

在運行中，可在 RNG 104 中生成亂數採樣值。可將來自 RNG 104 的亂數採樣值、來自記憶體 108 的晶片 ID 和來自記憶體 110 的密匙索引傳送到問詢寄存器 102。接著將問詢寄存器 102 中的內容包含在問詢資訊中發送到圖 2 中示出的外部實體 200，這樣外部實體可生成密碼並將在問詢回應中將該密碼回發。可採用標記單元 116 標記 RNG 104 中生成亂數採樣值，並將其存儲到外部記憶體 120 中。可將來自記憶體 108 的加密詞、記憶體 110 中位於定位密匙索引的密匙傳送到加密單元 112。可將存儲在外部記憶體 120 的亂數採樣值回發到 SoC，特別是回發到驗證單元 118，在此可將其向前發送到加密單元 112。加密單元 112 可採用哈希函數生成密碼。數位比較器 114 可從加密單元 112 接收密碼，和來自圖 2 中示出的外部實體 200 的密碼，並對它們進行比較。SoC 可確定該認證通過或失敗。

圖 2 是根據本發明一個實施例的與 SoC 100 相關的用於進行安全認證操作的外部實體 200 的典型框圖。參照圖 2，示出了外部實體 200，其包括：多個記憶體 206 和 210、加密單元 212。圖中

還示出了該外部實體 200 的邊界。

記憶體 206 可包括內部記憶體，用於存儲晶片 ID，還可包括合適的邏輯、電路和/或代碼，用於與圖 1A 和 1B 中示出的 SoC 100 交換資料。記憶體 206 可包括用於存儲加密詞的記憶體。記憶體 206 可用於將接收到的晶片 ID 與其存儲的加密詞相關聯。可基於晶片 ID 和安全加密演算法生成加密詞。該記憶體 206 可與加密單元 212 通信連接。

記憶體 210 可包括合適的邏輯、電路和/或代碼，用於存儲密匙表和相關密匙索引。該記憶體 210 可用于向加密單元 212 傳送資料。

加密單元 212 可包括合適的邏輯、電路和/或代碼，用於根據多個輸入資料生成密碼。根據本發明的一個方面，該加密單元 212 可用於加密來自三個資料源的資料以生成密碼，這些資料包括：來自記憶體 206 的加密詞、來自圖 1A 和圖 1B 中的 SoC 100 的問詢寄存器 102 的亂數採樣值和來自記憶體 110 的密匙。在本發明的另一實施例中，加密單元 212 可包括合適的邏輯、電路和/或代碼，以使用哈希函數，如 SHA1、SHA2 和 HMAC-SHA。在這一點上，可採用來自下列兩個資料源的資料生成密碼：來自記憶體 206 的加密詞和來來自圖 1A 和圖 1B 中的 SoC 100 的問詢寄存器 102 的亂數採樣值。

在運行中，可在問詢寄存器 102 中重獲亂數採樣值、晶片 ID 和密匙索引。晶片 ID 存儲在記憶體 206 中，並和對應密匙相關。可基於接收到晶片 ID 生成加密詞，並在認證過程之前存儲加密詞。來自問詢寄存器 102 的密匙索引可用於在記憶體 210 中查找對應的密匙。接著將來自記憶體 206 的加密詞、來自記憶體 210 的密匙和來自問詢寄存器 102 的亂數採樣值傳送到加密單元 212。該加密單元 212 可使用哈希函數生成密碼。可在問詢回應中將擺密碼發送到圖 1A 和圖 1B 中示出的 SoC 100。

參照圖 3A，示出了流程圖，其中步驟 300 涉及在圖 1A 和 1B 中示出的 SoC 100 上的認證操作的開始。在步驟 302 中，將來自記憶體 108 的晶片 ID 發送到問詢寄存器 102。在步驟 304 中，將來自記憶體 110 的密匙索引發送到問詢寄存器 102。在步驟 306 中，亂數生成器(RNG) 104 生成亂數採樣值。在步驟 308 中，將亂數採樣值發送到問詢寄存器 102。在步驟 310 中，將問詢寄存器 102 中的內容從 SoC 100 發送到圖 2 中示出的外部實體 200。步驟 312 指示該流程圖向圖 3B 和 3C 延續。

圖 3B 是根據本發明實施例的片上系統的外部實體中的認證處理的一部分的典型流程圖。參照圖 3B，示出了流程圖，其中步驟 312 是圖 3A 的延續。在步驟 314 中，圖 2 中示出的外部實體 200 從 SoC 上的問詢寄存器 102 接收亂數採樣值、晶片 ID 和密匙索引。在步驟 316 中，可將亂數採樣值發送到加密單元 212 中的哈希函數。在步驟 318 中，將從問詢寄存器 102 中接收到的晶片 ID 用於生或查找加密詞。接著可將記憶體 206 中的加密詞發送到加密單元 212 中的哈希函數。在步驟 320 中，將從問詢寄存器 102 中接收到的密匙索引用於在密匙表中查找密匙。可將該密匙發送到加密單元 212 中的哈希函數。在步驟 322 中，加密單元 212 生成密碼。在步驟 324 中，在問詢回應中將密碼從外部實體 200 發送到 SoC 100。步驟 326 指示流程圖向圖 3C 延續。

圖 3C 是根據本發明實施例的片上系統中的認證處理的一部分的典型流程圖。參照圖 3C，示出了流程圖，其中步驟 312 是圖 3A 的延續。在步驟 328，當晶片具有如圖 1A 中的內部可擦重寫記憶體，該過程可進行到步驟 330。在步驟 330 中，可將來自 RNG 104 的亂數採樣值存儲到本地可擦重寫記憶體 106 中。在步驟 332 中，將來自於記憶體 108 的加密密匙發送到加密單元 112 中的哈希函數。在步驟 334 中，將密匙索引用於在記憶體 110 中查找密匙，並將該密匙發送到加密單元 112。在步驟 336 中，將存儲在內

部可擦重寫記憶體 106 中的亂數採樣值發送到加密單元 112 的哈希函數。在步驟 338 中，可從加密單元 112 中的哈希函數中生成密碼。在步驟 340 中，由數位比較器 114 分別接收來自加密單元 112 中的 SoC 密碼和來自圖 2 中示出的外部實體 200 的密碼。在步驟 342 中，當這些密碼相同時。該方法可前進到步驟 344，並在最後步驟中通過認證。在步驟 342 中，當這些密碼不相同時。該方法可前進到步驟 346，並在最後步驟中認證失敗。

在步驟 328 中，當 SoC 100 不具有內部可擦重寫記憶體 106 時，該方法可前進到步驟 348。在步驟 348 中，在標記單元 116 中標記來自 RNG 104 中的亂數採樣值。在步驟 350 中，可將亂數採樣值以及其標記存儲在外部可擦重寫記憶體 120 中。在步驟 352 中，可將亂數採樣值以及其標記回發到 SoC 100，並在驗證單元 118 中進行驗證。在步驟 356 中，當亂數採樣值以及標記在驗證單元 118 中沒有通過驗證時，該過程可進行到步驟 358 並在最後步驟中認證失敗。在步驟 356 中，當亂數採樣值以及標記在驗證單元 118 中通過驗證時，該過程可進行到步驟 336 並在最後步驟中通過認證。

圖 1A、1B 和 2 中示出的系統可用於實現對一個或多個安全功能的接入的認證。可由圖 1A 和 1B 中示出的 SoC 100 控制認證，也可使用以兩種方式的唯一的密碼：對每個執行認證的 SoC 來說唯一，以及對驗證過程的每次重復來說唯一。

該認證方法可包括在 SoC 100 中生成所述密碼或在圖 2 中示出的外部實體 200 中生成所述密碼。該認證過程可始於在 SoC 100 的亂數生成器(RNG) 104 中生成亂數採樣值。可將該亂數採樣值存儲在圖 1A 的片上系統 106 或圖 1B 的片外記憶體 120 中。可將加密詞存儲在記憶體 108 中，並使其不能被試圖接入的外部實體獲得。該方法至少包括下列條件中的一個：將對 SoC 100 來說唯一的晶片 ID 存儲到記憶體 108 中、將密匙表存儲到記憶體 110 中。

該密匙表包括一個密匙和對應的密匙索引。

可將下列資訊中的兩個或多個發送到加密單元 112 中的哈希函數：來自記憶體單元 108 中的加密詞、來自圖 1A 中的記憶體 106 或來自圖 1B 中的記憶體 120 的亂數採樣值、來自記憶體 110 中的密匙表的密匙。該哈希函數可生成密碼。圖 1A 和 1B 中示出的 SoC 100 可向圖 2 中示出的外部實體 200 發送詢問，以生成並回發密碼。可在問詢寄存器 102 中存儲下列資訊中的至少兩個：對於 SoC 100 來說唯一的晶片 ID 和密匙索引，接著可將這些資訊發送到外部實體 200。授權的外部實體可提前瞭解晶片 ID、加密詞、具有對應密匙索引的密匙表和哈希函數。授權的外部實體能根據接收到的晶片 ID 和安全加密演算法生成加密詞。當密碼從外部實體 200 返回時，在數位比較器 114 中將返回的密碼與在加密單元 112 中生成密碼進行比較。如果密碼相互匹配，授權接入一個和多個功能。

本發明的又一實施例可提供一種機器可讀存儲。其內存儲的電腦程式包括至少一個代碼段，用於在網路中傳送資訊，所示至少一個代碼段由機器執行而使得所述機器執行上述步驟。

因此，本發明可以通過硬體、軟體，或者軟、硬體結合來實現。本發明可以在至少一個電腦系統中以集中方式實現，或者由分佈在幾個互連的電腦系統中的不同部分以分散方式實現。任何可以實現方法的電腦系統或其他設備都是可適用的。常用軟硬體的結合可以是安裝有電腦程式的通用電腦系統，通過安裝和執行程式控制電腦系統，使其按方法運行。

本發明的一個實施可作爲主板級產品，如單晶片、特定用途積體電路(ASIC)和具有與作爲單獨元件的系統的其他部分的不同集成程度的單晶片。系統的集成程度首要由速度和成本考慮確定。由於現代處理器的複雜性，可使用商業可用的處理器，該處理器可與現有系統的 ASIC 執行外接。可選地，如果處理器可用(如

ASIC 核心和邏輯模組)，那麼商業可用的處理器可爲作爲固件執行的具有不同功能的 ASIC 設備的一部分。

本發明還可以通過電腦程式產品進行實施，套裝程式含能夠實現本發明方法的全部特徵，當其安裝到電腦系統中時，可以實現本發明的方法。本文件中的電腦程式所指的是：可以採用任何程式語言、代碼或符號編寫的一組指令的任何運算式，該指令組使系統具有資訊處理能力，以直接實現特定功能，或在進行下述一個或兩個步驟之後實現特定功能：a)轉換成其他語言、編碼或符號；b)以不同的格式再現。

雖然本發明是通過具體實施例進行說明的，本領域技術人員應當明白，在不脫離本發明範圍的情況下，還可以對本發明進行各種變換及等同替代。另外，針對特定情形或材料，可以對本發明做各種修改，而不脫離本發明的範圍。因此，本發明不局限於所公開的具體實施例，而應當包括落入本發明權利要求範圍內的全部實施方式。

【符號說明】

片上系統(SoC)・・・100

問詢寄存器(challenge register)・・・102

亂數生成器(RNG)・・・104

本地可擦重寫記憶體・・・106

本地存儲單元・・・108、110

加密單元・・・112

數位比較器單元・・・114

標記單元(signing unit)・・・116

驗證單元・・・118

外部記憶體・・・120

外部實體・・・200

記憶體・・・206、210

加密單元・・・212

104 年 10 月 21 日修正替換本

申請專利範圍

1.一種在通信系統中認證裝置的方法，其特徵在於，所述方法包括：

在一晶片中根據對所述晶片來說唯一及對從所述晶片向一外部實體發送的一詢問來說唯一的資料生成一密碼，其中該資料係來自一資料源；

發送所述詢問至所述外部實體，其中所述詢問包括可供所述外部實體再生成所述密碼的資訊；以及

根據由所述外部實體回應所述詢問再生成的所述密碼，在所述晶片中認證向一個或多個由晶片控制的安全功能的接入。

2.如申請專利範圍第 1 項所述的方法，其中，所述方法包括在所述晶片中生成所述對所述晶片來說唯一和對從所述晶片發送的每次詢問來說唯一的密碼。

3.如申請專利範圍第 2 項所述的方法，其中，所述方法包括在所述晶片中，由亂數生成器中生成亂數採樣值。

4.如申請專利範圍第 3 項所述的方法，其中，所述方法包括將所述生成的亂數採樣值存儲到以下中的一個或多個：片上記憶體和片外記憶體。

5.如申請專利範圍第 4 項所述的方法，其中，在所述晶片上存儲加密詞，其中所述加密詞不能被外部實體獲得。

6.根如申請專利範圍第 5 項所述的方法，其中，所述方法包括在所述晶片上存儲以下中的一個或多個：對所述晶片來說唯一的晶片 ID 和密匙表，其中所述密匙表包括密匙和對應的密匙索引。

7.一種在通信系統中認證裝置的系統，其特徵在於，所述系統包括：

一個或多個電路，用以：

在一晶片中根據對所述晶片來說唯一及對從所述晶片向一外部實體發送的一詢問來說唯一的資料生成一密碼，其中該資料係來自一資料源；

發送所述詢問至所述外部實體，其中所述詢問包括可供所述外部實體再生成所述密碼的資訊；以及

根據由所述外部實體回應所述詢問再生成的所述密碼，在所述晶片中認證向一個或多個由晶片控制的安全功能的接入。

8.如申請專利範圍第 7 項所述的系統，其中，所述一個或多個電路在所述晶片中生成所述對所述晶片來說唯一和對從所述晶片發送的每次詢問來說唯一的密碼。

9.如申請專利範圍第 8 項所述的系統，其中，所述一個或多個電路在所述晶片中生成亂數採樣值。

10.如申請專利範圍第 9 項所述的系統，其中，所述一個或多個電路包括片上記憶體和片外記憶體中的一種或兩種，用於存儲生成的亂數採樣值。

104年10月21日修正替換本

十一、圖式：

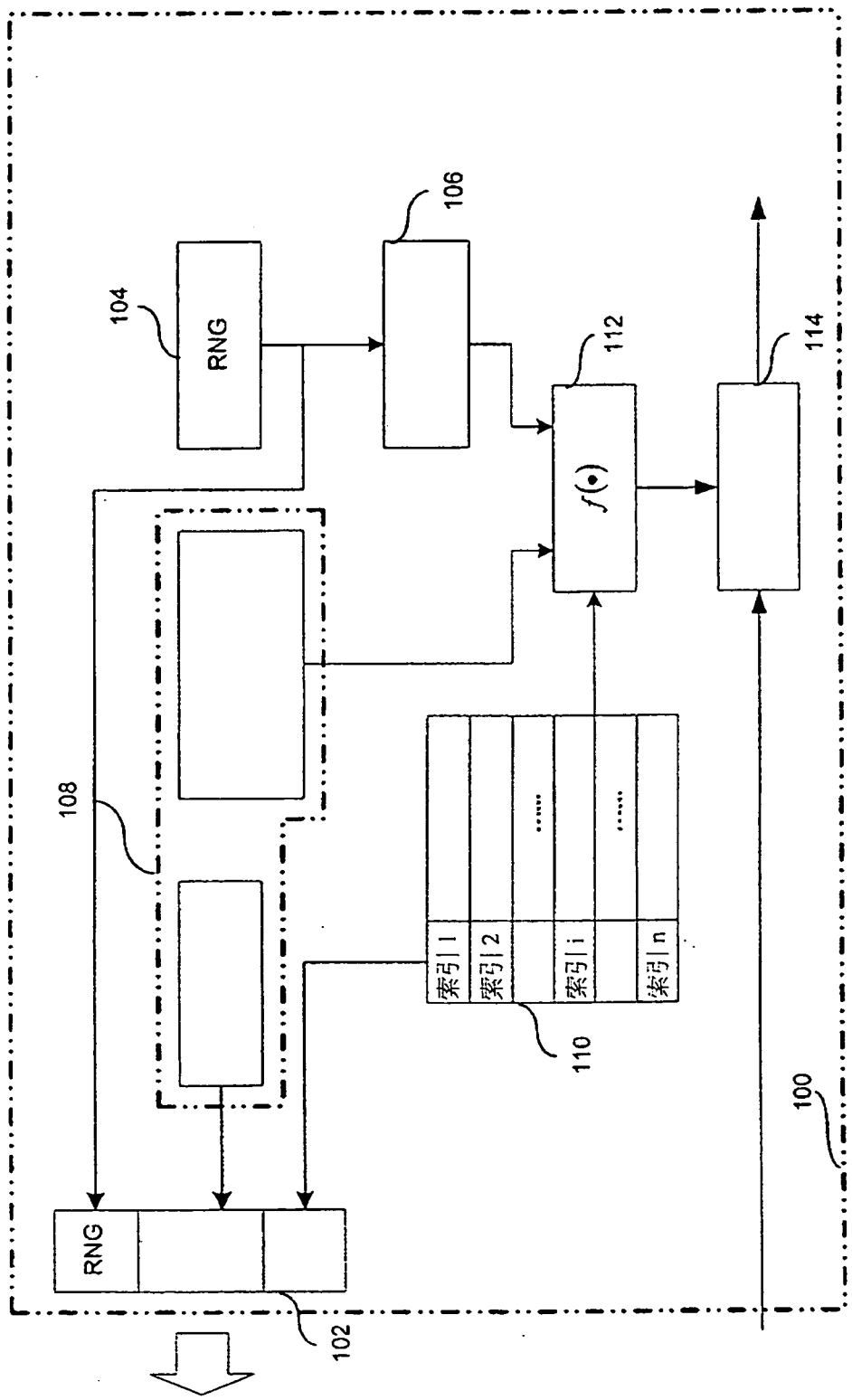

圖 1A

104年10月21日修正替換本

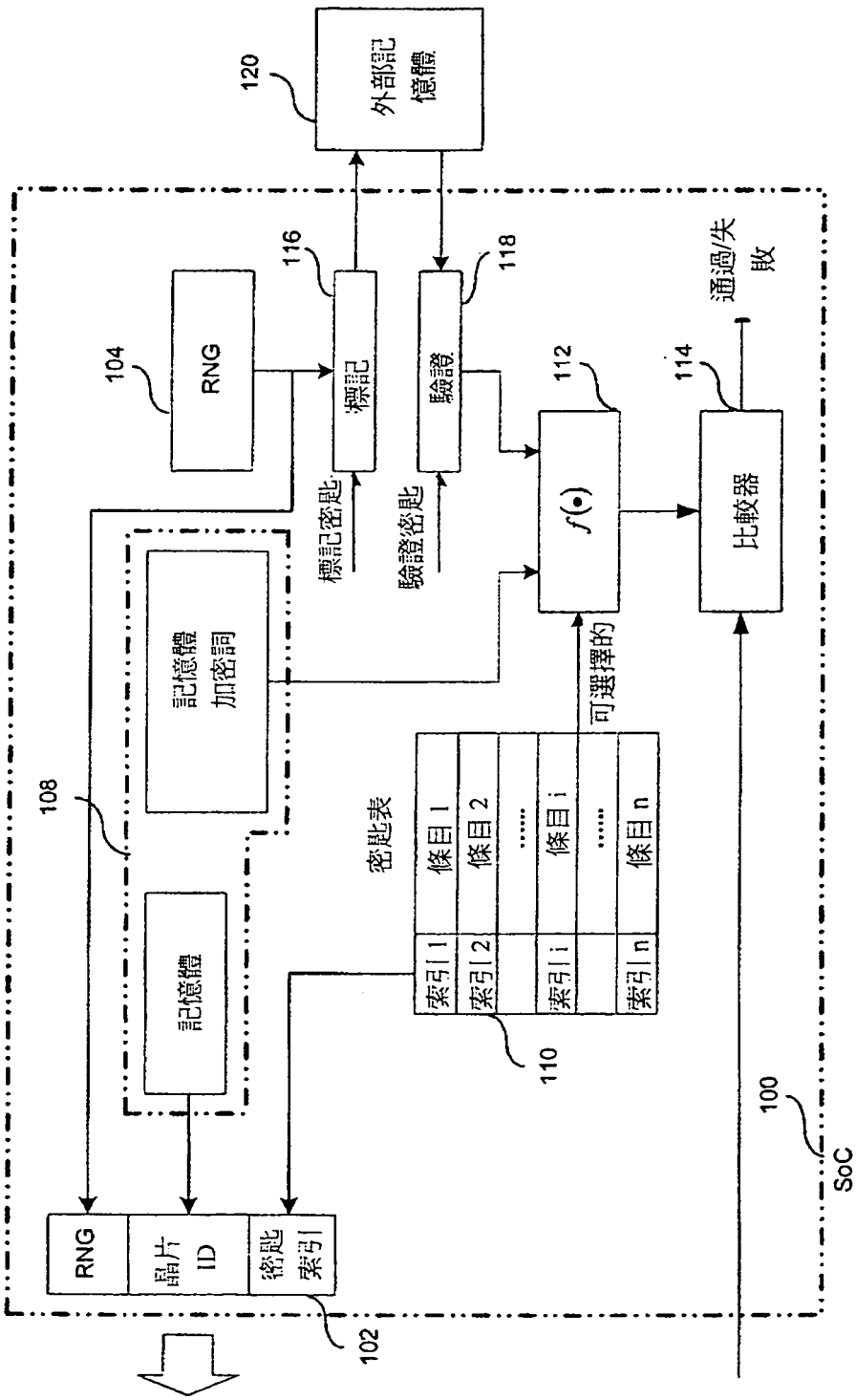

圖 1B

104年10月21日修正替換本

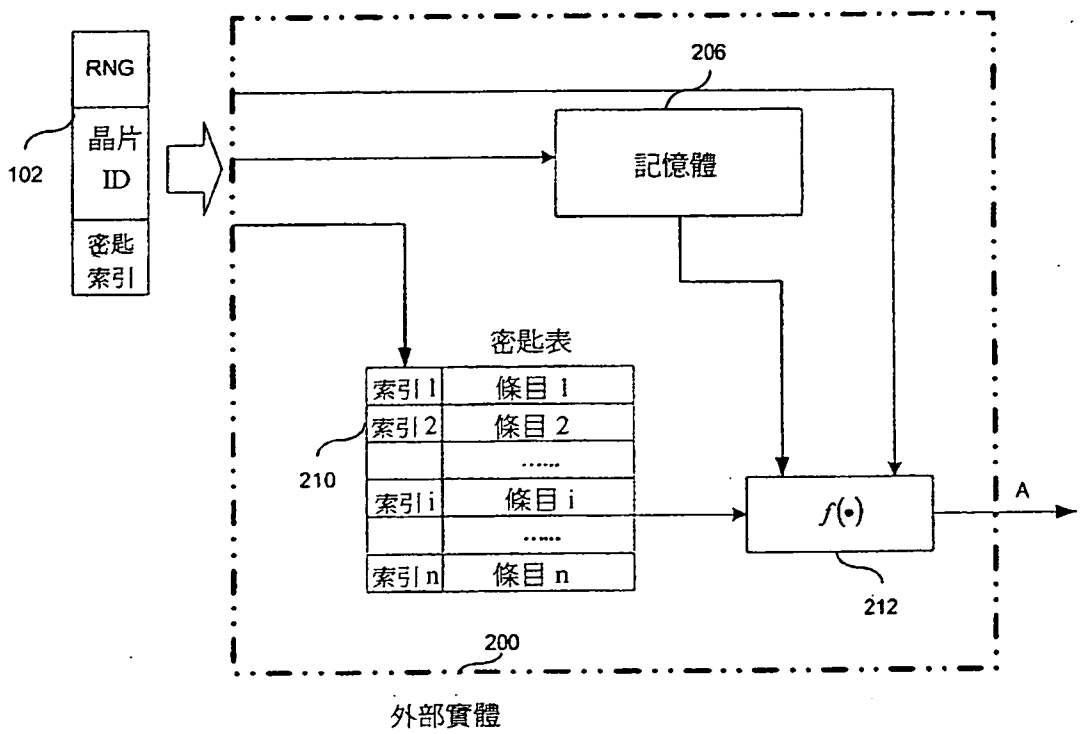

圖 2

104年10月21日修正替換本

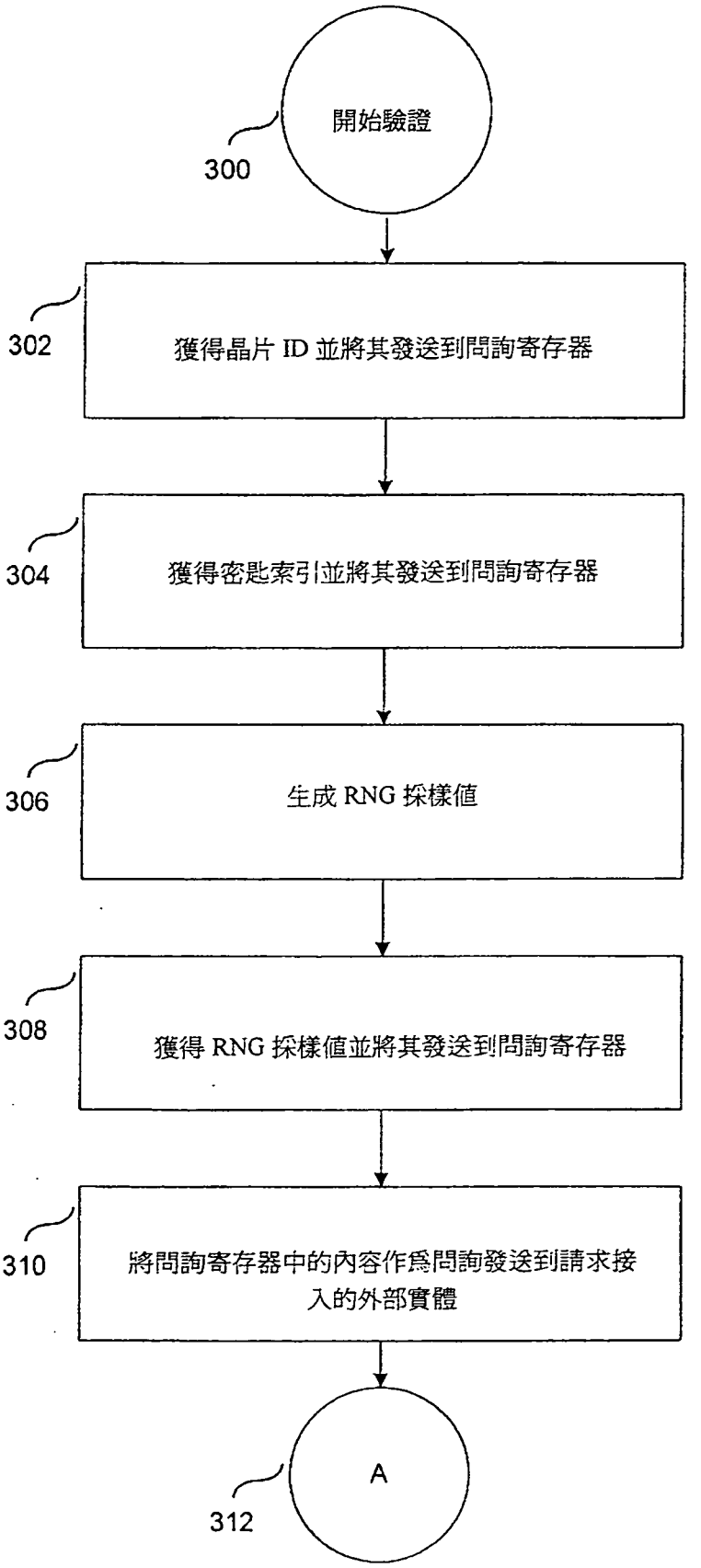

圖 3A

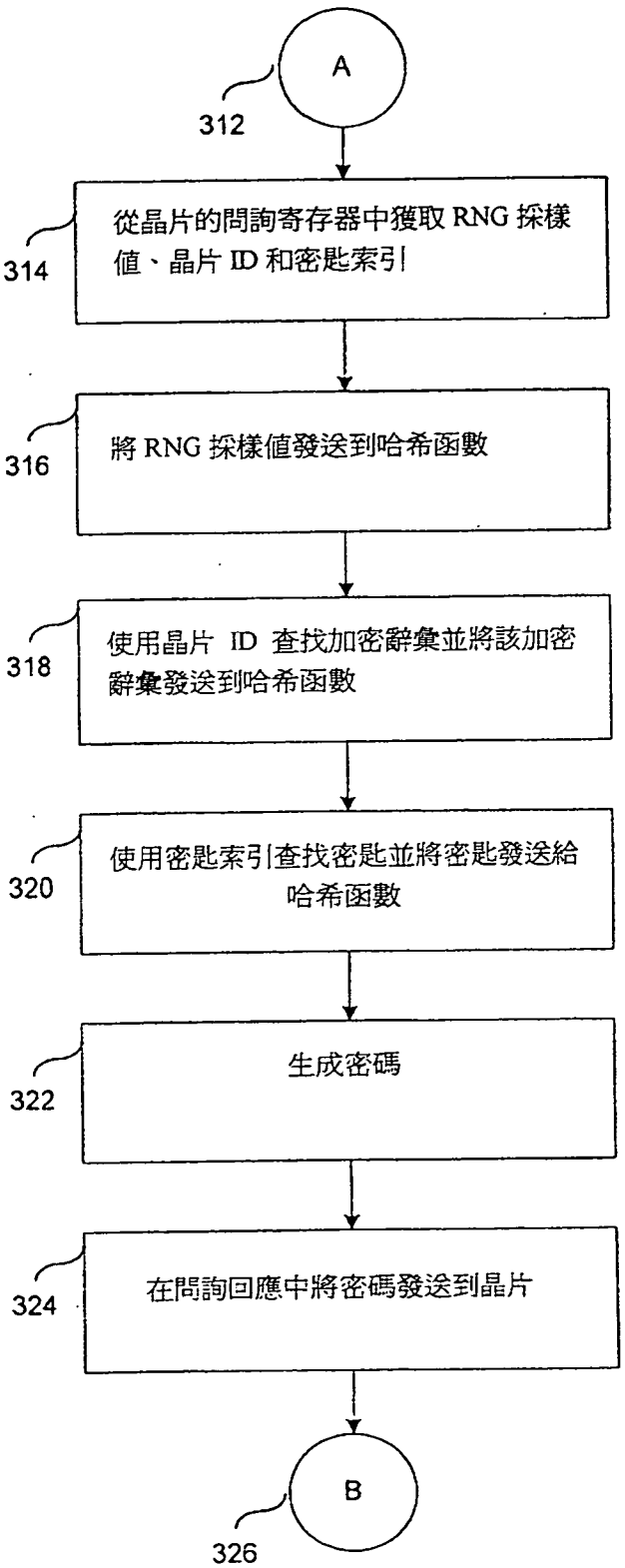
A
312
從晶片的問詢寄存器中獲取 RNG 採樣值、晶片 ID 和密匙索引
314
將 RNG 採樣值發送到哈希函數
316
使用晶片 ID 查找加密辭彙並將該加密辭彙發送到哈希函數
318
使用密匙索引查找密匙並將密匙發送給哈希函數
320
生成密碼
322
在問詢回應中將密碼發送到晶片
324
B
326

圖 3B

104年10月21日修正替換本

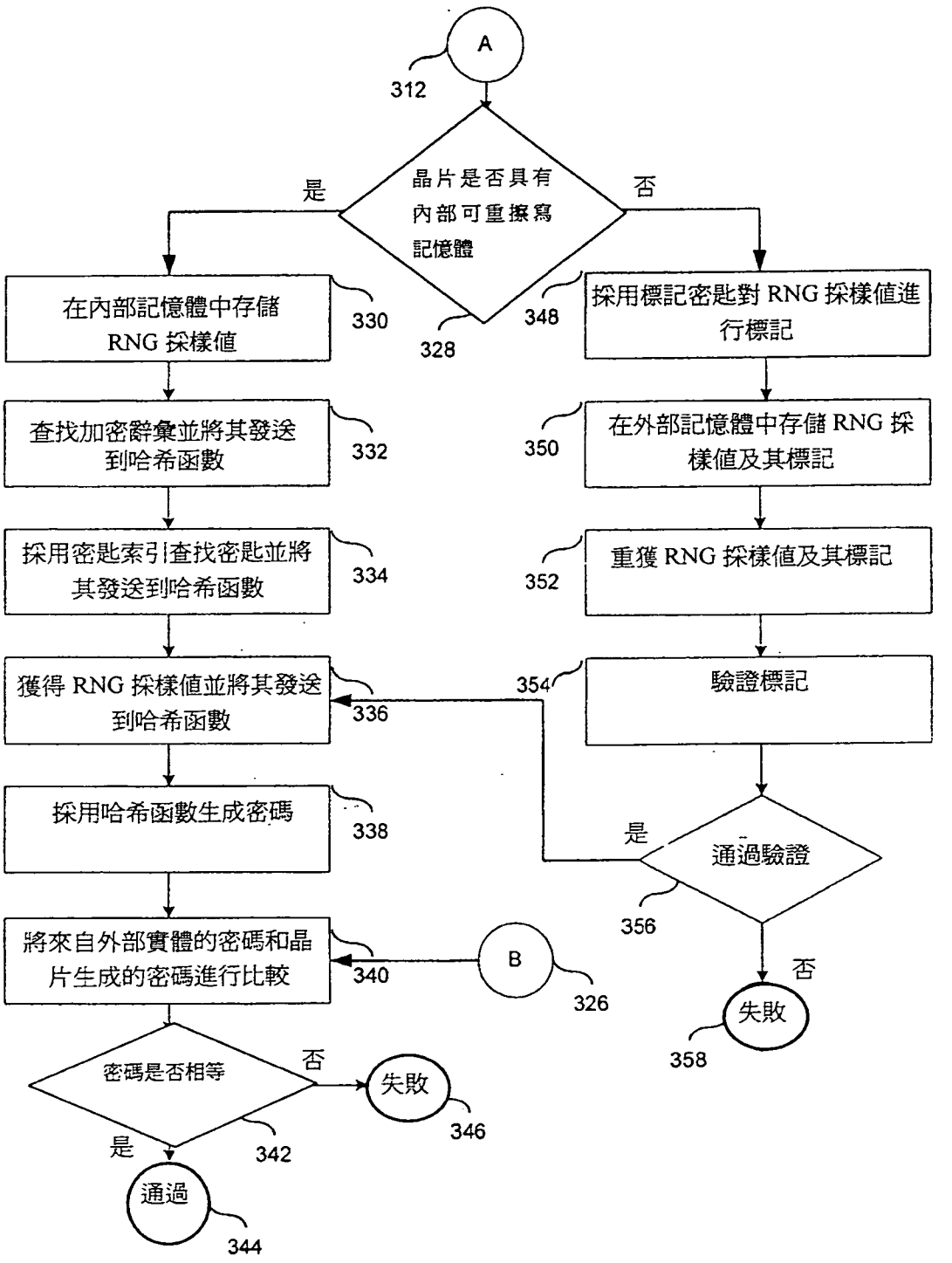

圖 3C