I517655

(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 I517655 B**

(45)公告日： 中華民國 105 (2016) 年 01 月 11 日

(21)申請案號：102118148 (22)申請日： 中華民國 102 (2013) 年 05 月 23 日

(51)Int. Cl.： ***H04L9/28 (2006.01)*** ***H04L9/06 (2006.01)***

(71)申請人：晨星半導體股份有限公司 (中華民國) MSTAR SEMICONDUCTOR, INC (TW)
新竹縣竹北市台元街 26 號 4 樓之 1

(72)發明人：馬清文 MA, CHING WEN (TW)

(74)代理人：祁明輝；林素華；涂綺玲

(56)參考文獻：

TW	200833054A	TW	201246889A
CN	1423451A	EP	1580934A2
US	2008/0025500A1	US	2012/0084565A1
WO	2000/065426A1	WO	2005/098630A1

審查人員：李仰璧

申請專利範圍項數：20 項 圖式數：14 共 37 頁

(54)名稱

密碼裝置以及密鑰保護方法

CRYPTOGRAPHIC DEVICE AND SECRET KEY PROTECTION METHOD

(57)摘要

本發明揭露一種密碼裝置與一種密鑰保護方法。該密碼裝置於處理一訊息時保護該密碼裝置之一密鑰，包含：一密鑰保護電路，利用一雜湊演算電路依據該訊息及該密鑰產生一防破解訊號；以及一加密處理器，用來依據該防破解訊號處理該訊息及該密鑰，以產生一加密訊息。另外，該密鑰保護方法應用於一密碼裝置，用來於該密碼裝置處理一訊息時保護該密碼裝置之一密鑰，包含：依據該訊息與該密鑰產生一雜湊值；依據該雜湊值產生一防破解訊號；以及依據該防破解訊號處理該訊息及該密鑰，以產生一加密訊息。

The present invention discloses a cryptographic device and a secret key protection method. The cryptographic device protects a secret key of the cryptographic device when processing a message, and comprises: a secret key protection circuit for generating an indecipherable signal according to the message and the secret key with a hash calculation circuit; and a cryptographic processor for processing the message and the secret key with the indecipherable signal to thereby generate an encrypted message. Besides, the secret key protection method is applicable to a cryptographic device for protecting a secret key of the cryptographic device when the cryptographic device processes a message, and comprises: generating a hash value according to the message and the secret key; generating an indecipherable signal according to the hash value; and generating an encrypted message according to the message and the secret key with the indecipherable signal.

指定代表圖：

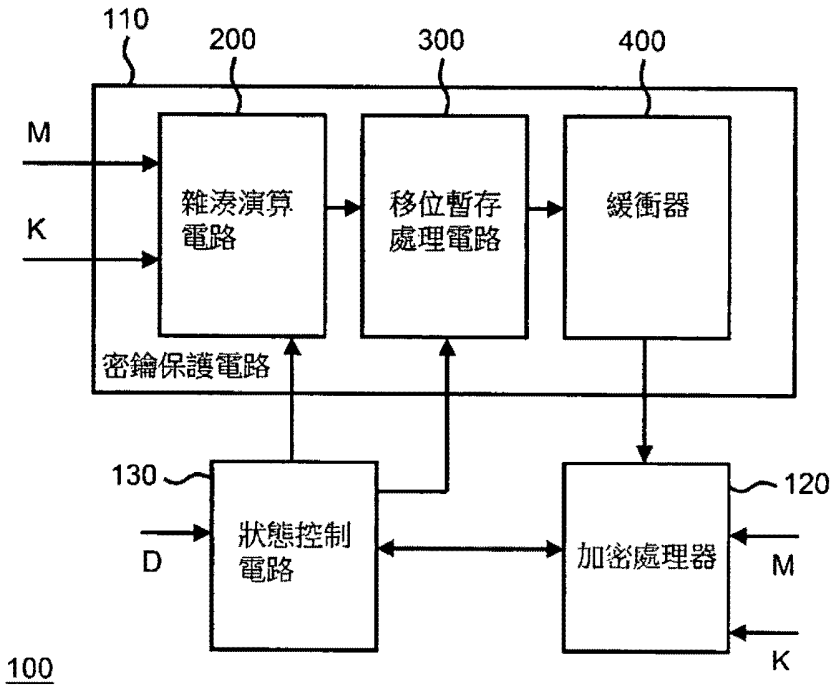

圖 8

符號簡單說明：

100・・・密碼裝置

110・・・密鑰保護電路

120・・・加密處理器

130・・・狀態控制電路

200・・・雜湊演算電路

300・・・移位暫存處理電路

400・・・緩衝器

M・・・訊息

K・・・密鑰

D・・・偵測訊號

發明專利說明書

【發明名稱】(中文/英文)

密碼裝置以及密鑰保護方法

CRYPTOGRAPHIC DEVICE AND SECRET KEY PROTECTION METHOD

【技術領域】

【0001】 本發明是關於密碼裝置以及密鑰保護方法，尤其是關於防破解中防側通道攻擊之密碼裝置以及密鑰保護方法。

【先前技術】

【0002】 時至今日，電子通訊已是主要的通訊方法之一。爲了確保電子通訊的安全性，亦即電子通訊內容的秘密性，通訊內容會先由一金鑰加密後再加以傳輸。以前攻擊者係透過大量運算來取得該金鑰，或利用密碼運算理論上的漏洞來竊取該金鑰，然而由於密碼學理論與應用的進步，攻擊者欲直接破解金鑰變得愈來愈難以實現，因此有攻擊者即透過收集加密通訊裝置（例如 IC 智慧卡（IC Smart Card）、可攜式電子裝置等）運算時所洩露的側通道資訊（Side Channel Information）（例如電力消耗資訊、運算時間資訊、聲音資訊、電磁波資訊等等）來進行統計分析以找出該金鑰，此種攻擊方式被稱之側通道攻擊（Side Channel Attack），當中被視爲相當具有威脅性的是差分能量分析法（Differential Power Analysis, DPA），對於差分能量分析法的防禦之道主要有隱

藏（Hiding）和遮罩（Masking）二種方法，前者是讓所洩露的電力消耗資訊與實際的運算過程儘量無關（例如利用等量電力消耗之設計或額外雜亂電力消耗之設計），後者則是將金鑰或訊息事先與一個遮罩值（Mask Value）進行邏輯運算，再利用該具有遮罩的金鑰或訊息進行加密運算，然而隱藏法需要額外的硬體電路來製造平衡的電力消耗，而遮罩法則需要獨立的亂數來源以避免被破解，二者均有其不足之處。

【發明內容】

【0003】 鑑於先前技術之不足，本發明之一目的在於提供一種密碼裝置以及密鑰保護方法，以解決先前技術的問題。

【0004】 本發明揭露了一種密碼裝置，用來於處理一訊息時保護該密碼裝置之一密鑰。依據本發明之一實施例，該密碼裝置包含：一密鑰保護電路，利用一雜湊演算電路依據該訊息及該密鑰產生一防破解訊號；以及一加密處理器，用來依據該防破解訊號處理該訊息及該密鑰，以產生一加密訊息。本實施例中，該加密處理器係依據該防破解訊號改變處理該密鑰之時間以產生該加密訊息，或依據該防破解訊號分別處理該訊息及該密鑰以分別產生一防破解訊息及一防破解密鑰，再依據該防破解訊息及該防破解密鑰產生該加密訊息。

【0005】 本發明同時揭露一種密鑰保護方法，應用於一密碼裝置，用來於該密碼裝置處理一訊息時保護該密碼裝置之一密鑰。依據本發明之一實施例，該密碼方法包含：依據該訊息與該

密鑰產生一雜湊值；依據該雜湊值產生一防破解訊號；以及依據該防破解訊號處理該訊息及該密鑰，以產生一加密訊息。

【0006】 有關本發明的特徵、實作與功效，茲配合圖式作較佳實施例詳細說明如下。

【圖式簡單說明】

〔圖 1〕爲本發明之密碼裝置之一實施例的示意圖；

〔圖 2a〕爲圖 1 之密鑰保護電路之一實施例的示意圖；

〔圖 2b〕爲圖 1 之密鑰保護電路之另一實施例的示意圖；

〔圖 3〕爲圖 1 之密鑰保護電路之另一實施例的示意圖；

〔圖 4〕爲圖 3 之移位暫存電路之一實施例的示意圖；

〔圖 5〕爲圖 3 之移位暫存電路之另一實施例的示意圖；

〔圖 6〕爲圖 4 之移位暫存電路之一虛擬電路的一實施例的示意圖；

〔圖 7〕爲圖 5 之移位暫存電路之一虛擬電路的一實施例的示意圖；

〔圖 8〕爲本發明之密碼裝置之另一實施例的示意圖；

〔圖 9〕爲本發明之密鑰保護裝置之一實施例的示意圖；

〔圖 10〕爲圖 9 之防破解訊號產生電路之一實施例的示意圖；

〔圖 11〕爲本發明之密碼方法之一實施例的流程圖；

〔圖 12〕爲圖 11 之步驟 S110 的一實施例的示意圖；

〔圖 13〕爲本發明之密鑰保護方法之一實施例的流程圖；及

〔圖 14〕爲圖 13 之步驟 S210 之一實施例的示意圖。

【實施方式】

【0007】 以下說明內容之技術用語係參照本技術領域之習慣用語，如本說明書對部分用語有加以說明或定義，該部分用語之解釋係以本說明書之說明或定義爲準。

【0008】 本發明之揭露內容包含密碼（Cryptographic）裝置與方法以及密鑰保護裝置與方法，用來保護一訊息以及一密鑰，該裝置及方法可應用於多種加密通訊裝置例如晶片金融卡、晶片證件、可攜式通訊裝置（如手機、平板裝置、筆記型電腦）及固定式通訊裝置（如桌上型電腦、智慧電視）等，並可防止側通道攻擊之威脅，以達到資訊保護及/或安全通訊之目的。在實施爲可能的前提下，本技術領域具有通常知識者能夠依本說明書之揭露內容來選擇等效之元件或步驟來實現本發明，亦即本發明之實施並不限於後敘之實施例。另外，由於本發明之密碼裝置與密鑰保護裝置所包含之部分元件單獨而言可爲已知元件，因此，在不影響該裝置發明之充分揭露及可實施性的前提下，以下說明對於已知元件的細節將予以節略。再者，本發明之密碼方法以及密鑰保護方法可分別藉由本發明之密碼裝置與密鑰保護裝置來實現，亦可能透過其它已知或新的等效裝置來執行，在不影響該些方法發明之充分揭露及可實施性的前提下，以下方法發明之說明將著重於步驟內容，關於用來執行該方法之硬體則可由本技術領域人士依據本方法發明之揭露來選擇適合之裝置或元件組合。

【0009】 請參閱圖 1，其係本發明之密碼裝置之一實施例的

示意圖。如圖所示，本實施例之密碼裝置 100 包含：一密鑰保護電路 110，用來依據一訊息（簡稱 M）以及一密鑰（簡稱 K）產生一防破解（Indecipherable）訊號，其中該訊息與該密鑰本身係爲受保護之對象，然而視應用與需求之不同，本發明亦可僅依據該訊息及密鑰的其中之一來產生該防破解訊號；以及一加密處理器 120，用來依據該防破解訊號處理上述訊息與密鑰，藉以產生一加密訊號，本實施例中，該加密處理器 120 可利用一已知之處理器來實現。

【0010】 承上所述，該加密處理器 120 係依據該防破解訊號改變處理該密鑰之時間以利用該密鑰加密該訊息，據以產生該加密訊號，或依據該防破解訊號分別處理該訊息及該密鑰以分別產生一防破解訊息及一防破解密鑰，再依據該防破解訊息及該防破解密鑰產生該加密訊號。舉例來說，基於該防破解訊號之特性，該加密處理器 120 能夠依據該防破解訊號以非固定週期、非特定時間點、非與特定參數相關或類隨機之方式來處理該密鑰，以達到隱藏（Hiding）處理該密鑰之時間點的效果；或者該加密處理器 120 依據該防破解訊號對該訊息及該密鑰分別執行一遮罩（Masking）運算（例如一互斥或（Exclusive OR）運算或其它邏輯運算）以產生該防破解訊息及該防破解密鑰，再利用該防破解密鑰對該防破解訊息進行處理以得到該加密訊號。

【0011】 請參閱圖 2a 與圖 2b，爲了能產生適當之防破解訊號以供加密處理器 120 使用，本發明之密鑰保護電路 110 之一實

施例包含：一雜湊（Hash）演算電路 200，用來依據前述訊息以及密鑰產生至少一雜湊值，該至少一雜湊值用來產生或作爲該防破解訊號。本實施例中，該雜湊演算電路 200 包含一雜湊演算單元 210 以及一雜湊演算單元 220，如圖 2a 所示，該雜湊演算單元 210 可用來依據該訊息產生該至少一雜湊值之一部分，該雜湊演算單元 220 則可用來依據該密鑰產生該至少一雜湊值之另一部分，藉此構成該至少一雜湊值；或者如圖 2b 所示，該雜湊演算單元 210 可用來依據該訊息產生一初始雜湊值，而該雜湊演算單元 220 則用來於該雜湊演算單元 210 依據該訊息產生該初始雜湊值時，依據該密鑰及該初始雜湊值產生該至少一雜湊值；或用來於該雜湊演算單元 210 依據該密鑰產生該初始雜湊值時，依據該訊息及該初始雜湊值產生該至少一雜湊值（未繪示）。然而，視應用及需求之不同，本技術領域具有通常知識者亦可使用一個或二個以上之雜湊演算單元來產生該至少一雜湊值，藉此簡化設計或增加安全性。

【0012】 請參閱圖 3，爲了確保該防破解訊號之內容不重複以針對每一訊息增加保護程度，該密鑰保護電路 110 可進一步包含：一移位暫存處理電路 300（例如一線性回饋移位暫存器（Linear Feedback Shift Register, LFSR）），用來依據該至少一雜湊值產生該防破解訊號；以及一緩衝器 400，用來接收並儲存該移位暫存處理電路 300 所輸出之防破解訊號，並將該防破解訊號輸出至該密碼處理器 120。舉例來說，請參閱圖 4，該移位暫存處理電路

300 可包含：複數個暫存單元（簡稱 R）310，該些暫存單元 310 包含至少一輸入暫存單元（例如該些暫存單元 310 中的第一個暫存單元），用來接收該至少一雜湊值，該些暫存單元 310 另包含至少一輸出暫存單元（例如該些暫存單元 310 中的最後一個暫存單元），用來輸出該防破解訊號；以及至少一邏輯運算單元（簡稱 L）320（例如複數個加法器），用來依據該至少一雜湊值或其衍生值產生一邏輯運算值，該邏輯運算值與該至少一雜湊值或其衍生值用來產生該防破解訊號。請注意，圖 4 之移位暫存處理電路 300 之架構僅係舉例，其它架構如圖 5 所示亦得爲本發明所採用，由於相關架構變化可由本技術領域具有通常知識者依本發明之揭露及本領域之公知技術來實現，因此在不影響本發明之揭露要求及可實施性的前提下，冗餘之說明在此予以節略。另請注意，在適當設計下或某些應用情形下，若該移位暫存處理電路 300 可提供足夠之防破解保護，該移位暫存處理電路 300 亦可直接取代前述雜湊演算電路 200（此時該雜湊演算電路 200 即非必要），以直接依據該訊息及該密鑰來產生該防破解訊號，更精確地說，此時複數個輸入暫存單元用來分別接收該訊息與密鑰，而該至少一邏輯運算單元 320 則用來依據該訊息與密鑰或其衍生值來產生該邏輯運算值，該邏輯運算值再用來與該訊息及密鑰或其衍生值來產生該防破解訊號。

【0013】 另請參閱圖 6 與圖 7（分別對應圖 4 與圖 5），雖然本發明已利用該防破解訊號來保護前述訊息與密鑰，然而本發明

之密鑰保護電路 110 亦可進一步包含一虛擬（Dummy）電路 600，以產生與該移位暫存處理電路 300 不同之能量分佈（例如產生相反之能量分佈，進而對該移位暫存處理電路 300 所產生的能量消耗進行補償），藉此使攻擊者更難以利用洩露之能量資訊來分析該密鑰之正確值。本實施例中，該虛擬電路 600 與移位暫存電路 300 之不同處在於該虛擬電路 600 包含複數個反相器 610，用來達到產生不同能量分佈之效果，然此僅係舉例，並非本發明之限制。

【0014】 請參閱圖 8，爲協調該密鑰保護電路 110 及該加密處理器 120 之運作，密碼裝置 100 可進一步包含：一狀態控制電路 130，例如一有限狀態機或其等效電路，用來依據一偵測訊號（簡稱 D）以及一預設條件控制該加密處理器 120 及/或該密鑰保護電路 110，其中該偵測訊號用來指示該訊息是否存在，該預設條件對應一預設時間或該防破解訊號之產生進度。舉例來說，當該狀態控制電路 130 依據該偵測訊號判斷有一訊息輸入，該狀態控制電路 130 即控制該密鑰保護電路 110 之雜湊演算電路 200 與移位暫存處理電路 300 來依據該訊息及密鑰產生該防破解訊號，接著該狀態控制電路 130 於一預設充足時間過後或者確認該防破解訊號已準備完成時（亦即前述預設條件滿足時），再控制該加密處理器 120 由該密鑰保護電路 110 取得該防破解訊號，或控制該密鑰保護電路 110 提供該防破解訊號予該加密處理器 120（未繪示），以執行後續的加密訊號之產生流程，接下來若仍有其它

訊息輸入，則依上述處理過程類推；而若該加密訊號已產生，且無其它訊息輸入或待處理之訊息，該狀態控制電路 130 可令該密鑰保護電路 110 及/或該加密處理器 120 回到一待命狀態（Idle State）。

【0015】 除上述之密碼裝置 100 外，本發明另揭露一種密鑰保護裝置，用來依據一訊息（簡稱 M）及一密鑰（簡稱 K）產生一防破解訊號，該防破解訊號用來保護該訊息及該密鑰。如圖 9 所示，該密鑰保護裝置 900 之一實施例包含：一防破解訊號產生電路 910，用來依據該訊息以及該密鑰產生該防破解訊號；以及一緩衝器 920，用來依據一控制訊號（簡稱 C）輸出該防破解訊號。

【0016】 承上所述，本實施例中，該防破解訊號產生電路 910 係等效於圖 1 之密鑰保護電路 110，因此，如圖 10 所示，該防破解訊號產生電路 910 同樣可包含：一雜湊演算電路 912，用來依據該訊息以及該密鑰產生至少一雜湊值，該至少一雜湊值係用來產生或作爲該防破解訊號；及/或一移位暫存處理電路 914，用來依據該訊息以及該密鑰產生該防破解訊號，或依據該至少一雜湊值產生該防破解訊號。由於該雜湊演算電路 912 及移位暫存處理電路 914 之實施細節與變化分別與圖 2 之雜湊演算電路 200 及圖 3 之移位暫存處理電路 300 相同，因此重複及不必要之說明在此予以節略。另外，密鑰保護裝置 900 可進一步包含：一狀態控制電路（例如圖 8 之狀態控制電路 130），用來依據一偵測訊號及一

預設條件產生該控制訊號，藉此控制該緩衝器 920 輸出該防破解訊號，其中該偵測訊號用來指示該訊息是否存在，該預設條件對應一預設時間或該防破解訊號之產生進度。由於本技術領域人士可參考圖 8 及其相關說明來瞭解本實施例之狀態控制電路之實施細節與變化，因此冗餘之說明在此予以節略。

【0017】 本發明另揭露一種密碼方法，用來保護一訊息以及一密鑰，可藉由圖 1 之密碼裝置 100 或其等效裝置來實現。如圖 11 所示，該密碼方法之一實施例包含：

步驟 S110：依據一訊息及一密鑰產生一防破解訊號。本步驟可藉由圖 1 之密鑰保護電路 110 或其等效電路來執行；以及

步驟 S120：依據該防破解訊號改變處理該密鑰之時間以產生一加密訊號，或依據該防破解訊號分別處理該訊息及該密鑰以分別產生一防破解訊息及一防破解密鑰，再依據該防破解訊息及該防破解密鑰產生該加密訊號。本步驟可藉由圖 1 之加密處理器 120 或其等效電路來執行。

【0018】 請參閱圖 12，爲了能產生適當之防破解訊號以供步驟 S120 使用，步驟 S110 可包含：

步驟 S112：依據該訊息以及該密鑰產生至少一雜湊值。本步驟可藉由圖 2 之雜湊演算電路 200 或其等效電路來執行；以及

步驟 S114：依據該至少一雜湊值產生該防破解訊號或將該至少一雜湊值作爲該防破解訊號。本步驟可藉由圖 3 之移位暫存處理電路 300 或其等效電路來執行，或直接由圖 2 之雜湊演算電路 200

或其等效電路來執行。

【0019】 另外，爲了確保該防破解訊號之內容不重複以針對每一訊息增加保護程度，步驟 S110 可包含：

步驟 S116（未圖示）：依據該訊息及該密鑰執行一移位暫存處理以及一邏輯運算處理以產生該防破解訊號。本步驟可藉由圖 3 之移位暫存處理電路 300 或其等效電路來執行；或

步驟 S118（未圖示）：承步驟 S112 及步驟 S114，依據該至少一雜湊值執行該移位暫存處理以及該邏輯運算處理，藉此產生該防破解訊號。本步驟同樣可藉由圖 3 之移位暫存處理電路 300 或其等效電路來執行。

【0020】 本發明亦揭露一種密鑰保護方法，用來依據一訊息以及一密鑰產生一防破解訊號，該防破解訊號用來保護該訊息及該密鑰，該密鑰保護方法可藉由圖 9 之密鑰保護裝置 900 或其等效裝置來實現。如圖 13 所示，該密鑰保護方法之一實施例包含：

步驟 S210：依據該訊息與該密鑰產生該防破解訊號。本步驟可藉由圖 9 之防破解訊號產生電路 910 或其等效電路來執行；以及

步驟 S220：依據一偵測訊號以及一預設條件輸出該防破解訊號，其中該偵測訊號用來指示該訊息是否存在，該預設條件對應一預設時間或該防破解訊號之產生進度。本步驟可藉由圖 8 之狀態控制電路 130 或其等效電路來執行。

【0021】 類似地，如圖 14 所示，爲了能產生適當之防破解訊號以保護該訊息及密鑰，步驟 S210 可進一步包含：

步驟 S212：依據一訊息與一密鑰產生至少一雜湊值。本步驟可藉由圖 9 之雜湊演算電路 912 來執行；以及

步驟 S214：依據該至少一雜湊值產生該防破解訊號或將該至少一雜湊值作爲該防破解訊號。本步驟可藉由圖 9 之移位暫存處理電路 914 或其等效電路來執行，或直接由圖 9 之雜湊演算電路 912 或其等效電路來執行。

【0022】 同樣地，爲了確保該防破解訊號之內容不重複以針對每一訊息增加保護程度，步驟 S210 可包含：

步驟 S216（未圖示）：依據該訊息及該密鑰執行一移位暫存處理以及一邏輯運算處理以產生該防破解訊號。本步驟可藉由圖 9 之移位暫存處理電路 914 或其等效電路來執行；或

步驟 S218（未圖示）：承步驟 S212 與步驟 S214，依據該至少一雜湊值執行該移位暫存處理以及該邏輯運算處理以產生該防破解訊號。本步驟同樣可藉由圖 9 之移位暫存處理電路 914 或其等效電路來執行。

【0023】 請注意，由於本技術領域具有通常知識者可藉由前揭裝置實施例之內容來瞭解本發明之方法實施例的細節及可能的實施變化，因此在不影響揭露要求及可實施性的前提下，重複及不必要之說明將不予贅述。另請注意，本發明之實施例僅係範例，並非實施限制，在實施爲可能的前提下，本技術領域人士可僅實施任一實施例之部分技術特徵或結合不同實施例之技術特徵來實施本發明，例如圖 1 之加密處理器 120 可先依據該防破解

訊號來處理該訊息及密鑰以產生該防破解訊息及防破解密鑰，接著再基於該防破解訊號之特性於非特定時間點利用該防破解密鑰對該防破解訊息進行處理來得到該加密訊號，藉此進一步增加安全性。

【0024】 綜上所述，本發明所揭露之密碼裝置與方法以及密鑰保護裝置與方法在無獨立/外部亂數來源的情形下即可對欲保護之訊息及密鑰施以隱藏及/或遮罩保護，且在無等量電力消耗或雜亂電力消耗之設計下亦能提供足夠之保護，換句話說，本發明無需複雜或耗功的電路設計即可抵抗側通道攻擊，進而達到資訊保護及安全通訊之目的。

【0025】 綜上所述，雖然本案已以實施例揭露如上，然其並非用以限定本案。本案所屬技術領域中具有通常知識者，在不脫離本案之精神和範圍內，當可作各種之更動與潤飾。因此，本案之保護範圍當視後附之申請專利範圍所界定者爲準。

【符號說明】

【0026】

100 密碼裝置

110 密鑰保護電路

120 加密處理器

130 狀態控制電路

200 雜湊演算電路

210 雜湊演算單元

220　雜湊演算單元

300　移位暫存處理電路

310　暫存單元

320　邏輯運算單元

400　緩衝器

600　虛擬電路

610　反相器

900　密鑰保護裝置

910　防破解訊號產生電路

912　雜湊演算電路

914　移位暫存處理電路

920　緩衝器

M　訊息

K　密鑰

D　偵測訊號

C　控制訊號

S110　依據一訊息及一密鑰產生一防破解訊號

S120　依據該防破解訊號改變處理該密鑰之時間以產生一加密訊號，或依據該防破解訊號分別處理該訊息及該密鑰以產生該加密訊號

S112　依據該訊息以及該密鑰產生至少一雜湊值

Si14　依據該至少一雜湊值產生該防破解訊號或將該至少一雜湊值作爲該防破解訊號

S210　依據一訊息與一密鑰產生一防破解訊號

S220　依據一偵測訊號以及一預設條件輸出該防破解訊號

S212　依據該訊息與該密鑰產生至少一雜湊值

S214　依據該至少一雜湊值產生該防破解訊號或將該至少一雜湊值作爲該防破解訊號

發明摘要

公告本

※ 申請案號：102118148

※ 申請日：102.5.23

※IPC 分類：H04L 9/08 (2006.01)
H04L 9/06 (2006.01)

【發明名稱】(中文/英文)

密碼裝置以及密鑰保護方法

CRYPTOGRAPHIC DEVICE AND SECRET KEY PROTECTION METHOD

【中文】

本發明揭露一種密碼裝置與一種密鑰保護方法。該密碼裝置於處理一訊息時保護該密碼裝置之一密鑰，包含：一密鑰保護電路，利用一雜湊演算電路依據該訊息及該密鑰產生一防破解訊號；以及一加密處理器，用來依據該防破解訊號處理該訊息及該密鑰，以產生一加密訊息。另外，該密鑰保護方法應用於一密碼裝置，用來於該密碼裝置處理一訊息時保護該密碼裝置之一密鑰，包含：依據該訊息與該密鑰產生一雜湊值；依據該雜湊值產生一防破解訊號；以及依據該防破解訊號處理該訊息及該密鑰，以產生一加密訊息。

【英文】

The present invention discloses a cryptographic device and a secret key protection method. The cryptographic device protects a

secret key of the cryptographic device when processing a message, and comprises: a secret key protection circuit for generating an indecipherable signal according to the message and the secret key with a hash calculation circuit; and a cryptographic processor for processing the message and the secret key with the indecipherable signal to thereby generate an encrypted message. Besides, the secret key protection method is applicable to a cryptographic device for protecting a secret key of the cryptographic device when the cryptographic device processes a message, and comprises: generating a hash value according to the message and the secret key; generating an indecipherable signal according to the hash value; and generating an encrypted message according to the message and the secret key with the indecipherable signal.

申請專利範圍

1.一種密碼（Cryptographic）裝置，於處理一訊息時保護該密碼裝置之一密鑰，包含：

一密鑰保護電路，利用一雜湊（Hash）演算電路依據該訊息及該密鑰產生一防破解（Indecipherable）訊號；以及

一加密處理器，用來依據該防破解訊號處理該訊息及該密鑰，以產生一加密訊號。

2.如請求項第 1 項所述之密碼裝置，其中該加密處理器依據該防破解訊號改變處理該密鑰之時間並利用該密鑰處理該訊息以產生該加密訊號，或依據該防破解訊號分別處理該訊息及該密鑰以產生一防破解訊息與一防破解密鑰，再依據該防破解訊息及該防破解密鑰產生該加密訊號。

3.如請求項第 2 項所述之密碼裝置，其中該加密處理器依據該防破解訊號分別對該訊息及該密鑰執行一遮罩（Masking）運算以產生該防破解訊息及該防破解密鑰。

4.如請求項第 1 項所述之密碼裝置，其中該雜湊演算電路依據該訊息與該密鑰產生一雜湊值，該密鑰保護電路進一步包含：

一移位暫存處理電路，用來依據該雜湊值產生該防破解訊號；以及

一緩衝器，用來接收並儲存該防破解訊號。

5.如請求項第 4 項所述之密碼裝置，其中該移位暫存處理電路包含：

複數個暫存單元，包含：

一輸入暫存單元，用來接收該雜湊值；以及

一輸出暫存單元，用來輸出該防破解訊號；以及

一邏輯運算單元，用來依據該雜湊值產生一邏輯運算值，並利用該邏輯運算值產生該防破解訊號。

6.如請求項第 4 項所述之密碼裝置，其中該密鑰保護電路進一步包含：

一虛擬（Dummy）電路，用來補償該移位暫存處理電路造成之能量消耗。

7.如請求項第 1 項所述之密碼裝置，其中該雜湊演算電路包含：

一第一雜湊演算單元，用來依據該訊息產生一雜湊值之一部分；以及

一第二雜湊演算單元，用來依據該密鑰產生該雜湊值之另一部分。

圖式

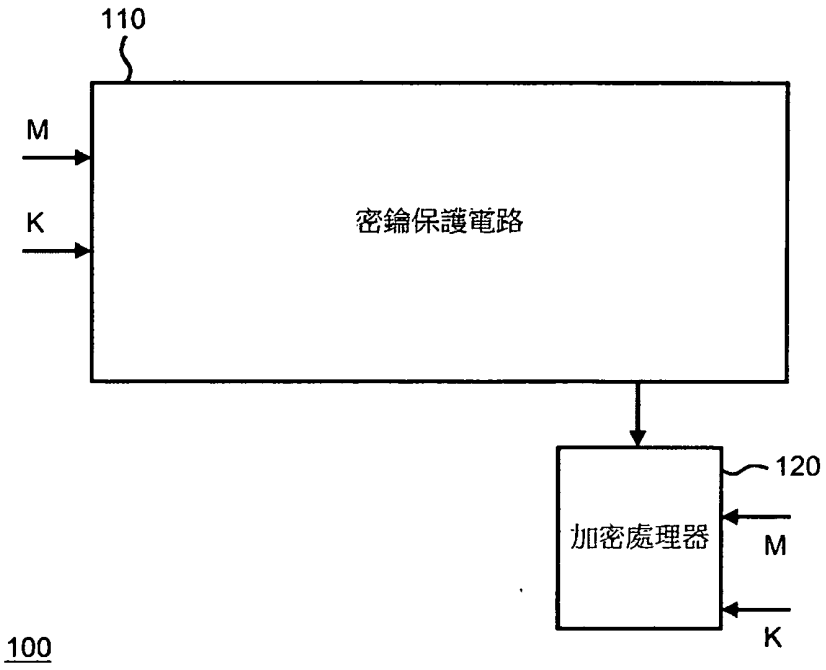

圖 1

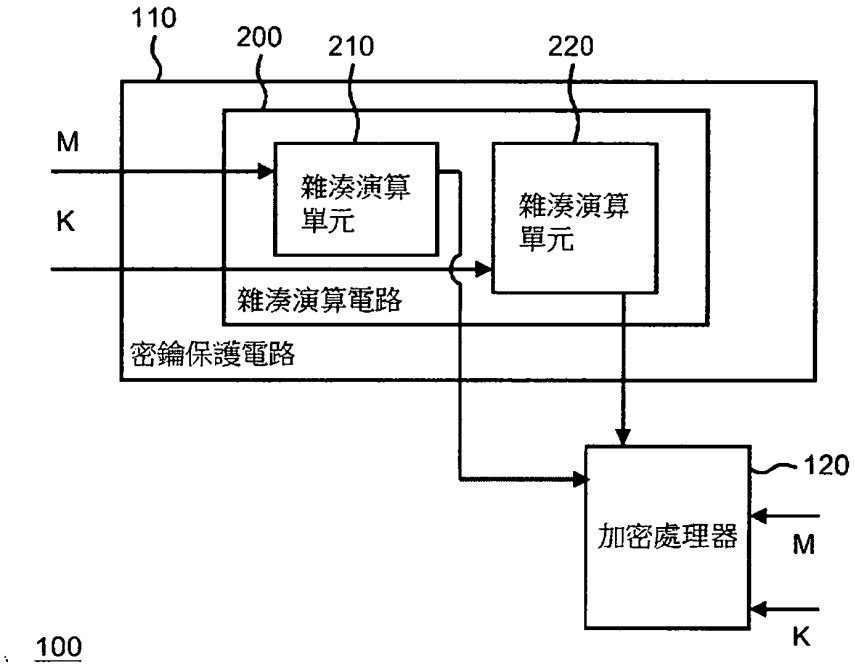
110
200
210
220
M
K
雜湊演算單元
雜湊演算單元
雜湊演算電路
密鑰保護電路
120
加密處理器
M
K
100

圖 2a

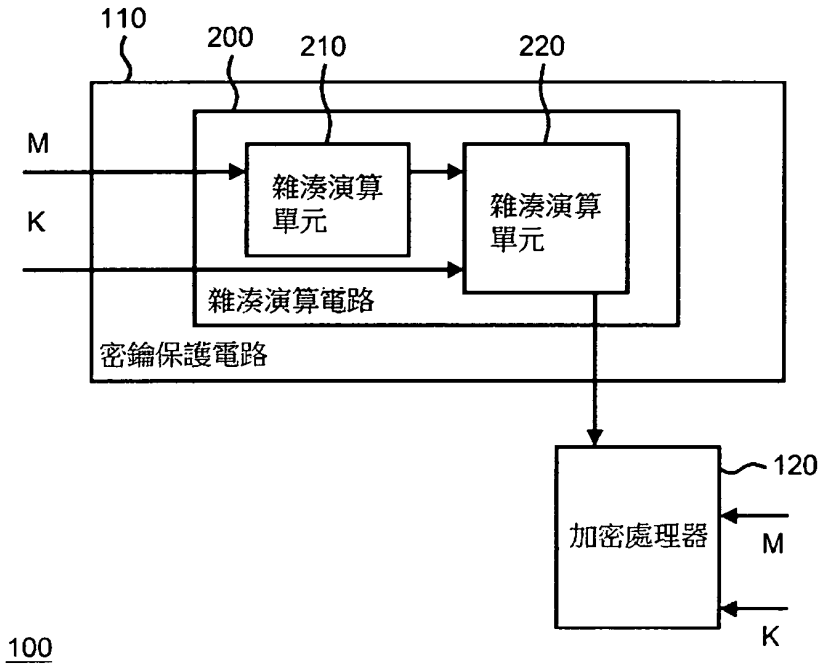
110
200
210
220
M
K
雜湊演算單元
雜湊演算單元
雜湊演算電路
密鑰保護電路
120
加密處理器
M
K
100

圖 2b

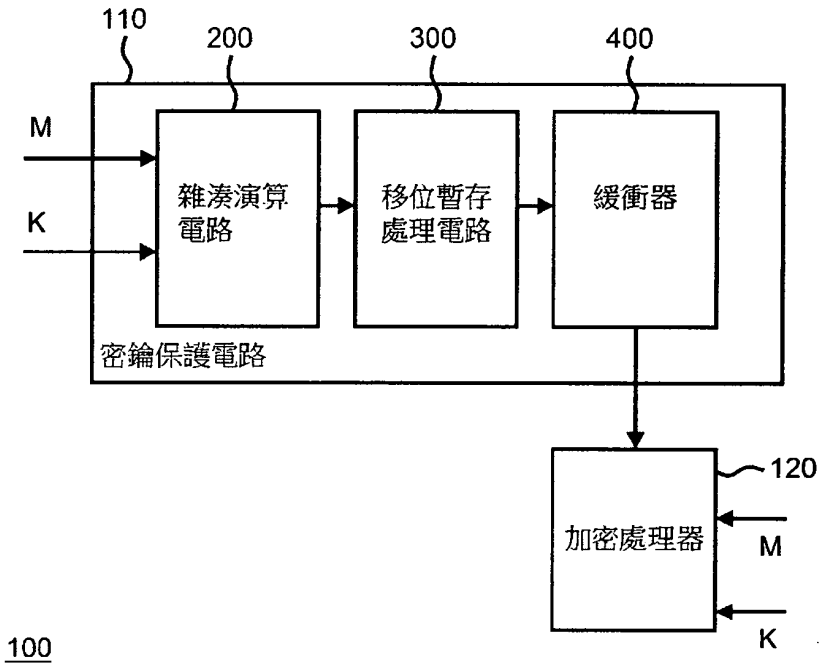
110
200
300
400
M
K
雜湊演算電路
移位暫存處理電路
緩衝器
密鑰保護電路
120
加密處理器
M
K
100

圖 3

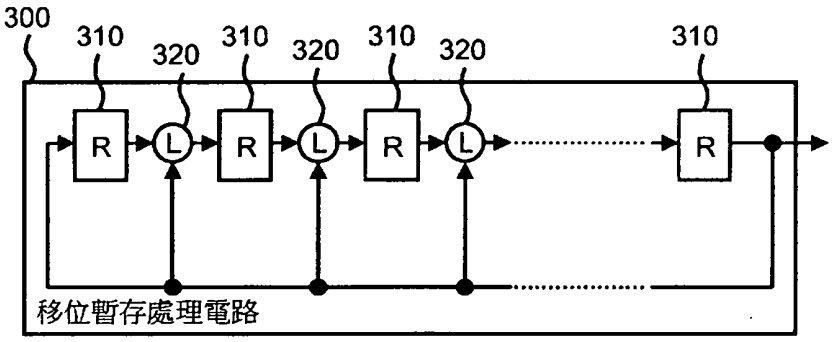

圖 4

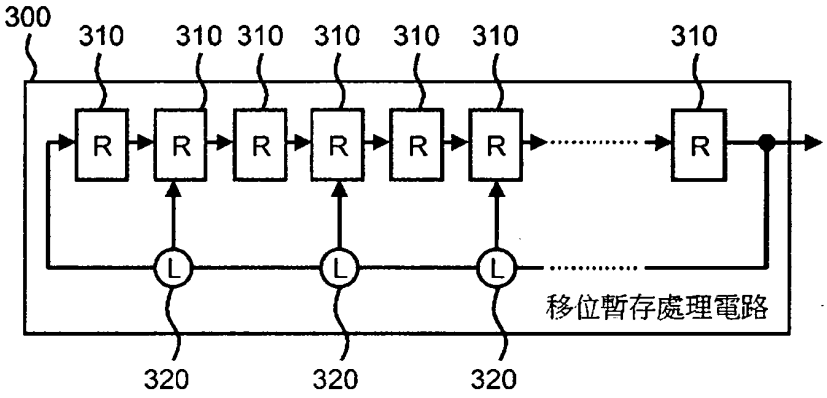
300
310
310
310
310
310
310
310
R
R
R
R
R
R
R
L
L
L
移位暫存處理電路
320
320
320

圖 5

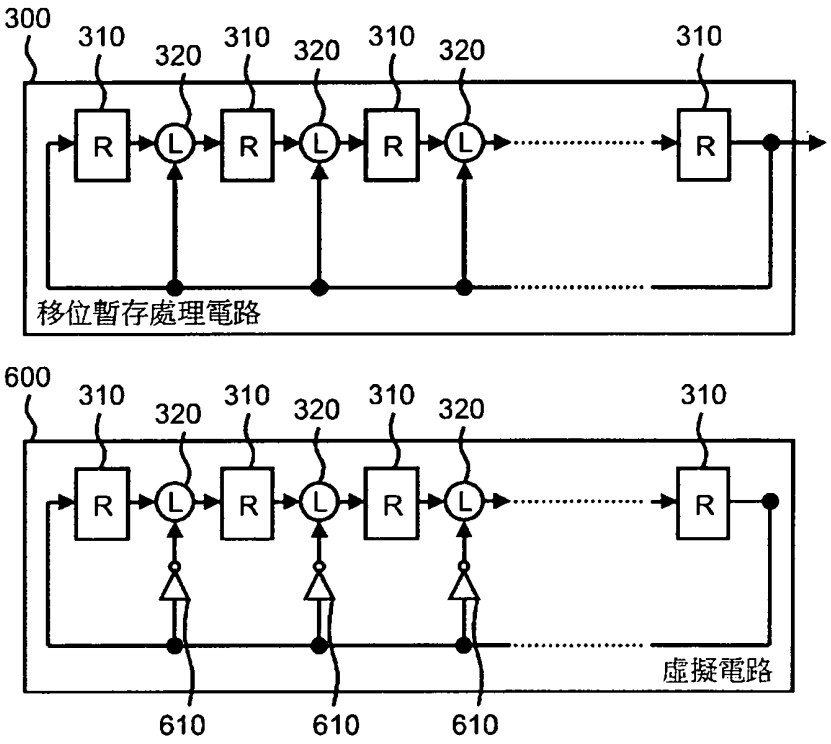
300
310
320
310
320
310
320
310
R
L
R
L
R
L
R
移位暫存處理電路
600
310
320
310
320
310
320
310
R
L
R
L
R
L
R
虛擬電路
610
610
610

圖 6

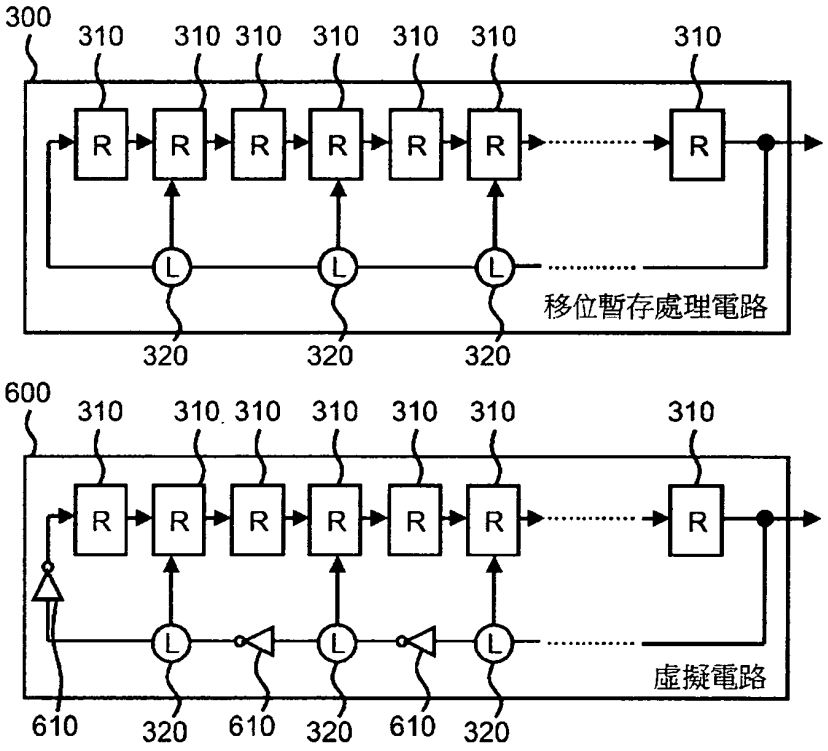

圖 7

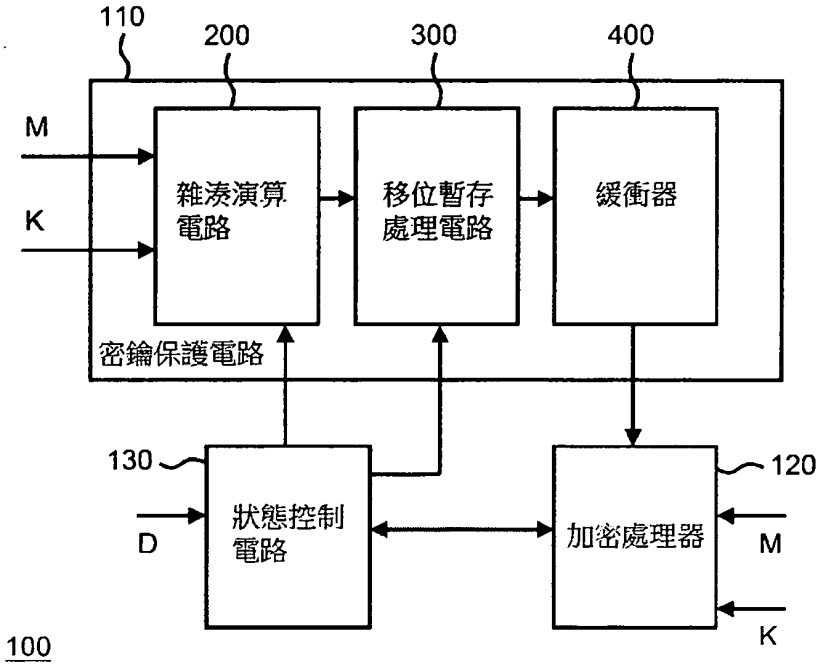
110
200
300
400
M
K
雜湊演算電路
移位暫存處理電路
緩衝器
密鑰保護電路
130
D
狀態控制電路
加密處理器
120
M
K
100

圖 8

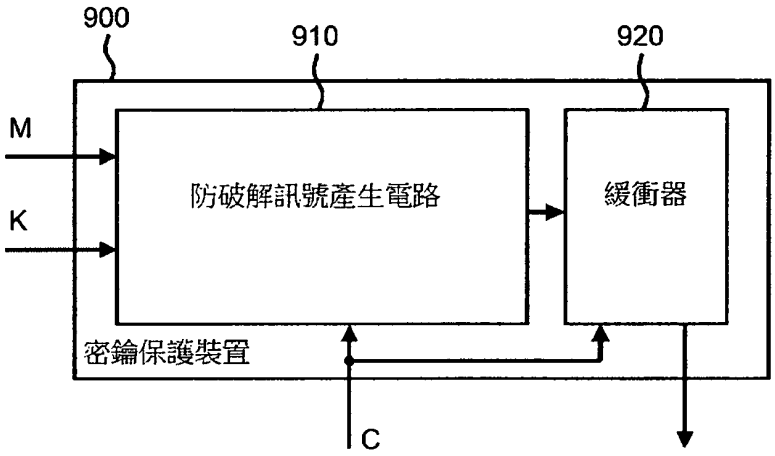

圖 9

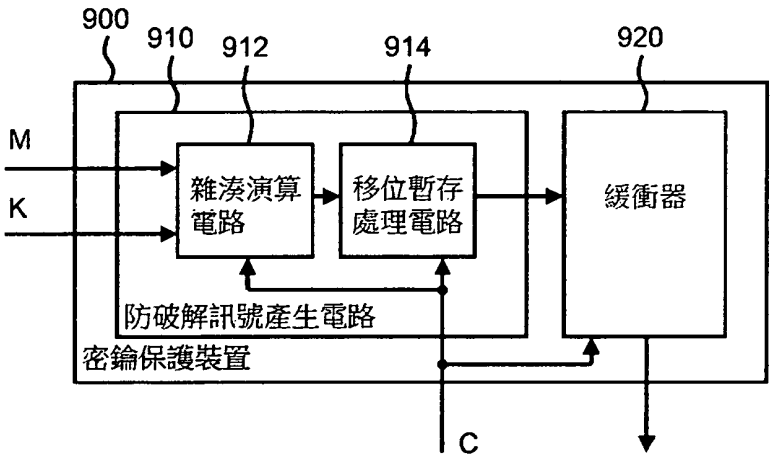
900
910
912
914
920
M
K
雜湊演算電路
移位暫存處理電路
緩衝器
防破解訊號產生電路
密鑰保護裝置
C

圖 10

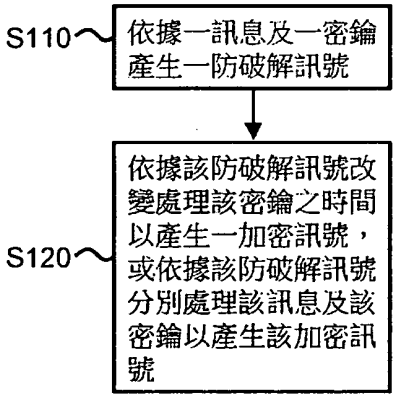
S110
依據一訊息及一密鑰產生一防破解訊號
S120
依據該防破解訊號改變處理該密鑰之時間以產生一加密訊號，或依據該防破解訊號分別處理該訊息及該密鑰以產生該加密訊號

圖 11

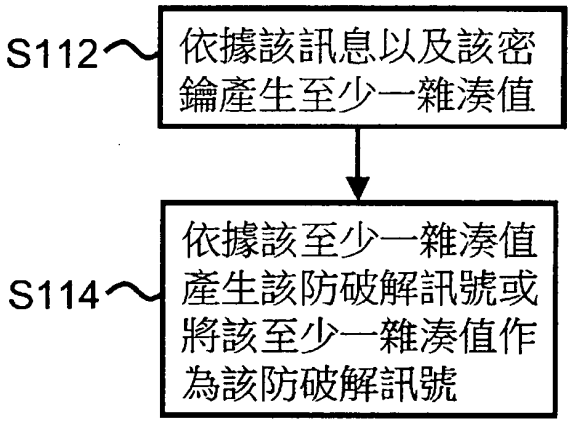
S112
依據該訊息以及該密鑰產生至少一雜湊值
S114
依據該至少一雜湊值產生該防破解訊號或將該至少一雜湊值作為該防破解訊號

圖 12

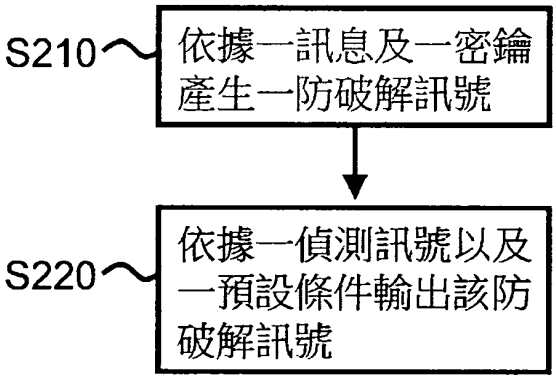
S210
依據一訊息及一密鑰產生一防破解訊號
S220
依據一偵測訊號以及一預設條件輸出該防破解訊號

圖 13

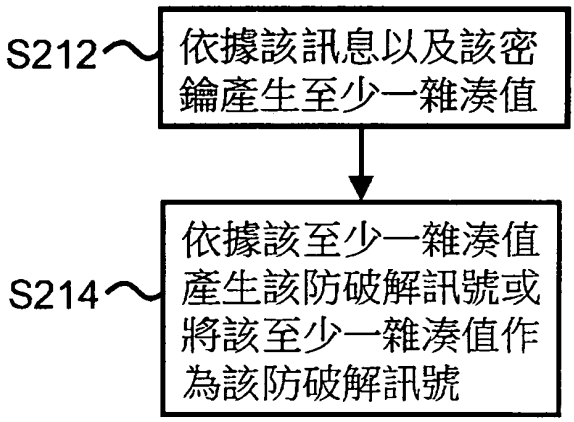
S212
依據該訊息以及該密鑰產生至少一雜湊值
S214
依據該至少一雜湊值產生該防破解訊號或將該至少一雜湊值作為該防破解訊號

圖 14

【代表圖】

【本案指定代表圖】：圖 8

【本代表圖之符號簡單說明】：

100　密碼裝置

110　密鑰保護電路

120　加密處理器

130　狀態控制電路

200　雜湊演算電路

300　移位暫存處理電路

400　緩衝器

M　訊息

K　密鑰

D　偵測訊號

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

無

8.如請求項第 1 項所述之密碼裝置，其中該雜湊演算電路包含：

一第一雜湊演算單元，用來依據該訊息與該密鑰其中之一產生一初始雜湊值；以及

一第二雜湊演算單元，用來依據該訊息與該密鑰其中另一及該初始雜湊值產生一雜湊值。

9.如請求項第 1 項所述之密碼裝置，其進一步包含：

一控制電路，用來依據一偵測訊號以及一預設條件控制該加密處理器或該密鑰保護電路，其中該偵測訊號用來指示該訊息是否存在，該預設條件對應至一預設時間與該防破解訊號之產生速度的其中之一。

10.如請求項第 9 項所述之密碼裝置，其中該控制電路依據該偵測訊號與該預設條件控制該加密處理器由該密鑰保護電路取得該防破解訊號或控制該密鑰保護電路提供該防破解訊號予該加密處理器。

11.一種密鑰保護方法，應用於一密碼（Cryptographic）裝置，用來於該密碼裝置處理一訊息時保護該密碼裝置之一密鑰，包含：

依據該訊息與該密鑰產生一雜湊值；

依據該雜湊值產生一防破解（Indecipherable）訊號；以及

依據該防破解訊號處理該訊息及該密鑰，以產生一加密訊號。

12.如請求項第 11 項所述之密鑰保護方法，其中依據該防破解訊號處理該訊息及該密鑰，以產生該加密訊號之步驟包含：

依據該防破解訊號改變處理該密鑰之時間；以及

利用該密鑰處理該訊息以產生該加密訊號。

13.如請求項第 11 項所述之密鑰保護方法，其中依據該防破解訊號處理該訊息及該密鑰，以產生該加密訊號之步驟包含：

依據該防破解訊號分別處理該訊息及該密鑰以分別產生一防破解訊息及一防破解密鑰；以及

依據該防破解訊息及該防破解密鑰產生該加密訊號。

14.如請求項第 13 項所述之密鑰保護方法，其中依據該防破解訊號分別處理該訊息及該密鑰以分別產生一防破解訊息及一防破解密鑰之步驟包含：

依據該防破解訊號分別對該訊息及該密鑰執行一遮罩（Masking）運算以產生該防破解訊息及該防破解密鑰。

15.如請求項第 11 項所述之密鑰保護方法，其中依據該雜湊

值產生該防破解訊號之步驟包含：

依據該雜湊值執行一移位暫存處理以產生該防破解訊號。

16.如請求項第 15 項所述之密鑰保護方法，其中依據該雜湊值執行該移位暫存處理以產生該防破解訊號之步驟包含：

接收該雜湊值；

依據該雜湊值執行一邏輯運算處理以產生一邏輯運算值；以及

依據該邏輯運算值產生該防破解訊號。

17.如請求項第 15 項所述之密鑰保護方法，其中依據該雜湊值執行該移位暫存處理以產生該防破解訊號之步驟更包含：

利用一虛擬（Dummy）電路補償該移位暫存處理造成之能量消耗。

18.如請求項第 11 項所述之密鑰保護方法，其中依據該訊息以及該密鑰產生該雜湊值之步驟包含：

依據該訊息產生該雜湊值之一部分；以及

依據該密鑰產生該雜湊值之另一部分。

19.如請求項第 11 項所述之密鑰保護方法，其中依據該訊息以及該密鑰產生該雜湊值之步驟包含：

依據該訊息與該密鑰其中之一產生一初始雜湊值；以及

依據該訊息與該密鑰其中另一及該初始雜湊值產生該雜湊值。

20.如請求項第 11 項所述之密鑰保護方法，其更包含步驟：

依據一偵測訊號以及一預設條件控制產生該防破解訊號之步驟以及產生該加密訊號之步驟的起始時間，其中該偵測訊號用來指示該訊息是否存在，該預設條件對應至一預設時間與該防破解訊號之產生速度的其中之一。