201701186

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201701186 A

(43)公開日： 中華民國 106 (2017) 年 01 月 01 日

(21)申請案號：105114018 (22)申請日： 中華民國 105 (2016) 年 05 月 05 日

(51)Int. Cl.： *G06F21/78 (2013.01)* *G06F12/14 (2006.01)*

(30)優先權：2015/06/12 美國 14/738,240

(71)申請人：高通公司 (美國) QUALCOMM INCORPORATED (US)
美國

(72)發明人：貝諾特 奧利佛 珍 BENOIT, OLIVIER JEAN (US)；卡馬羅塔 羅莎里歐 CAMMAROTA, ROSARIO (US)

(74)代理人：陳長文

申請實體審查：無 申請專利範圍項數：30 項 圖式數：10 共 32 頁

(54)名稱

實體不可複製功能輔助之記憶體加密裝置技術

PHYSICALLY UNCLONABLE FUNCTION ASSISTED MEMORY ENCRYPTION DEVICE TECHNIQUES

(57)摘要

本發明提供用於加密一計算裝置之記憶體中之資料的技術。根據本發明之用於保護一記憶體中之資料的一種實例方法包括使用處理器之一記憶體加密裝置加密與一儲存請求相關聯的資料以產生經加密資料。加密該資料包括：獲得一查問值，提供該查問值至一實體不可複製功能模組以獲得一回覆值，以及使用該回覆值作為一加密密鑰來加密與該儲存請求相關聯的該資料以產生該經加密資料。該方法亦包括在該記憶體中儲存該經加密資料及與該經加密資料相關聯的該查問值。

Techniques for encrypting the data in the memory of a computing device are provided. An example method for protecting data in a memory according to the disclosure includes encrypting data associated with a store request using a memory encryption device of the processor to produce encrypted data. Encrypting the data includes: obtaining a challenge value, providing the challenge value to a physically unclonable function module to obtain a response value, and encrypting the data associated with the store request using the response value as an encryption key to generate the encrypted data. The method also includes storing the encrypted data and the challenge value associated with the encrypted data in the memory.

指定代表圖：

TW 201701186 A

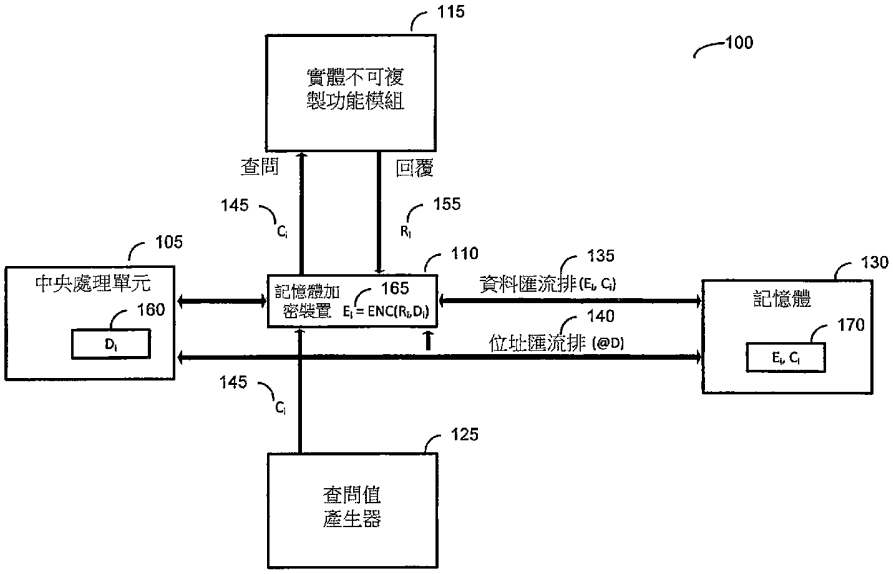

圖1

符號簡單說明：

100・・・計算裝置

105・・・中央處理單元

110・・・記憶體加密裝置

115・・・實體不可複製功能模組

125・・・查問值產生器

130・・・記憶體

135・・・資料匯流排

140・・・位址匯流排

145・・・查問值

155・・・回覆值

160・・・資料

165・・・經加密資料

170・・・記憶體位置

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】

實體不可複製功能輔助之記憶體加密裝置技術

PHYSICALLY UNCLONABLE FUNCTION ASSISTED MEMORY ENCRYPTION DEVICE TECHNIQUES

【技術領域】

本發明係關於用於保護待儲存於計算裝置之記憶體中之資料的技術，且更特定言之係關於用於加密待儲存於計算裝置之記憶體中之資料的技術。

【先前技術】

計算裝置之記憶體的內容容易受到來自惡意方之攻擊，該等惡意方可嘗試獲得對計算裝置之記憶體之內容的未經授權存取及/或藉由假定對正在由計算裝置之處理器執行之程式碼流程之控制而取得對計算裝置之控制。已做出依賴於儲存或建置於計算裝置之處理器中的一或多個加密密鑰的加密儲存於計算裝置之記憶體中之資料的一些嘗試，但此等方法易受攻擊者可獲得內建式密鑰並破解所提供之加密的攻擊及/或反向工程化。

【發明內容】

根據本發明之用於保護記憶體中之資料的實例方法包括使用處理器之記憶體加密裝置加密與儲存請求相關聯的資料以產生經加密資料。加密資料包括：獲得查問(challenge)值，提供查問值至實體不可複製功能模組以獲得回覆值，以及使用回覆值作為加密密鑰來加密與儲存請求相關聯的資料以產生經加密資料。該方法亦包括在記憶體中儲存經加密資料及與經加密資料相關聯的查問值。

此方法之實施可包括以下特徵中之一或多者。獲得查問值包括自與處理器相關聯的亂數產生器獲得查問值。使用查問值加密與儲存請求相關聯的資料包括將互斥或(XOR)運算應用於與儲存請求相關聯的資料及回覆值以產生經加密資料。使用查問值加密與儲存請求相關聯的資料包括將互斥或(XOR)運算應用於與儲存請求相關聯的資料、產生經加密資料之回覆值，以及與經加密資料待寫入於其中之記憶體位置相關聯的位址。回應於讀取請求自記憶體獲得經加密資料及與經加密資料相關聯的查問值；及解密經加密資料以產生經解密資料。解密資料包括：提供查問值至強大的實體不可複製功能模組以獲得經恢復回覆值，以及使用經恢復回覆值解密與儲存請求相關聯的資料。提供經解密資料至處理器。使用經恢復回覆值解密與儲存請求相關聯的資料包括將互斥或(XOR)運算應用於經加密資料及經恢復回覆值以產生經解密資料。使用經恢復回覆值解密與儲存請求相關聯的資料包括將互斥或(XOR)運算應用於經加密資料、經恢復回覆值，以及與經加密資料寫入至的記憶體位置相關聯之位址，以產生經加密資料。

根據本發明之設備包括用於使用處理器之記憶體加密裝置加密與儲存請求相關聯之資料以產生經加密資料的構件。用於回應於儲存請求而加密資料的構件包括：用於獲得查問值的構件，用於提供查問值至實體不可複製功能模組以獲得回覆值的構件，以及用於使用回覆值作為加密密鑰來加密與儲存請求相關聯之資料以產生經加密資料的構件。該設備亦包括用於在記憶體中儲存經加密資料及與經加密資料相關聯之查問值的構件。用於獲得查問值的構件包含用於自與處理器相關聯之亂數產生器獲得查問值的構件。

此設備之實施可包括以下特徵中之一或多者。用於使用查問值加密與儲存請求相關聯之資料的構件包括用於將互斥或(XOR)運算應用於與儲存請求相關聯之資料及回覆值以產生經加密資料的構件。用

於使用查問值加密與儲存請求相關聯之資料的構件包括：用於將互斥或(XOR)運算應用於與儲存請求相關聯的資料、產生經加密資料之回覆值，以及與經加密資料待寫入於其中之記憶體位置相關聯的位址的構件。用於回應於讀取請求自記憶體獲得經加密資料及與經加密資料相關聯之查問值的構件，以及用於解密經加密資料以產生經解密資料的構件。用於解密資料的構件包括：用於提供查問值至強大的實體不可複製功能模組以獲得經恢復回覆值的構件，以及用於使用經恢復回覆值解密與儲存請求相關聯之資料的構件。用於提供經解密資料至處理器的構件。用於使用經恢復回覆值解密與儲存請求相關聯之資料的構件包括用於將互斥或(XOR)運算應用於經加密資料及經恢復回覆值以產生經解密資料的構件。用於使用經恢復回覆值解密與儲存請求相關聯之資料的構件包括用於將互斥或(XOR)運算應用於經加密資料、經恢復回覆值，以及與經加密資料寫入至的記憶體位置相關聯之位址以產生經加密資料的構件。

根據本發明之計算裝置包括處理器、記憶體及記憶體加密裝置。記憶體加密裝置經組態以加密與自處理器接收之儲存請求相關聯之資料以產生經加密資料。當加密資料時，記憶體加密裝置經組態以獲得查問值，提供查問值至實體不可複製功能模組以獲得回覆值，以及使用回覆值作為加密密鑰來加密與儲存請求相關聯的資料以產生經加密資料。記憶體加密裝置亦經組態以在記憶體中儲存經加密資料及與經加密資料相關聯之查問值。

記憶體加密裝置經組態以自與處理器相關聯之亂數產生器獲得查問值。記憶體加密裝置經組態以藉由將互斥或(XOR)運算應用於與儲存請求相關聯之資料及回覆值，使用查問值加密與儲存請求相關聯之資料，以產生經加密資料。記憶體加密裝置經組態以藉由將互斥或(XOR)運算應用於與儲存請求相關聯的資料、產生經加密資料之回覆

值，以及與經加密資料待寫入於其中之記憶體位置相關聯的位址，使用查問值加密與儲存請求相關聯之資料。記憶體加密裝置經進一步組態以：回應於讀取請求自記憶體獲得經加密資料及與經加密資料相關聯之查問值；及解密經加密資料以產生經解密資料。當解密資料時，記憶體加密裝置經組態以：提供查問值至強大的實體不可複製功能模組以獲得經恢復回覆值，以及使用經恢復回覆值解密與儲存請求相關聯之資料。記憶體加密裝置經組態以提供經解密資料至處理器。記憶體加密裝置經組態以藉由將互斥或(XOR)運算應用於經加密資料及經恢復回覆值，使用經恢復回覆值解密與儲存請求相關聯之資料，以產生經解密資料。記憶體加密裝置經組態以藉由將互斥或(XOR)運算應用於經加密資料、經恢復回覆值，以及與經加密資料寫入至之記憶體位置相關聯的位址，使用經恢復回覆值來解密與儲存請求相關聯之資料，以產生經加密資料。

根據本發明之實例非暫時性電腦可讀媒體其上儲存有用於保護記憶體中之資料的電腦可讀指令。該等指令經組態以致使電腦獲得查問值，提供查問值至實體不可複製功能模組以獲得回覆值，使用回覆值作為加密密鑰來加密與儲存請求相關聯之資料以產生經加密資料，以及儲存經加密資料及與經加密資料相關聯的查問值。

此非暫時性電腦可讀媒體之實施可包括以下特徵中的一或多者。經組態以致使電腦獲得查問值之指令包括經組態以致使電腦自亂數產生器獲得查問值的指令。經組態以致使電腦獲得查問值之指令包括經組態以致使電腦自單調計數器獲得查問值的指令。經組態以致使電腦使用查問值加密與儲存請求相關聯之資料的指令包括經組態以致使電腦將互斥或(XOR)運算應用於與儲存請求相關聯之資料及回覆值以產生經加密資料的指令。經組態以致使電腦使用查問值加密與儲存請求相關聯之資料的指令包括經組態以致使電腦將互斥或(XOR)運算

應用於與儲存請求相關聯之資料、產生經加密資料之回覆值，以及與經加密資料待寫入於其中的記憶體位置相關聯之位址的指令。經組態以致使電腦執行以下操作之指令：回應於讀取請求自經加密資料儲存於其中的記憶體獲得經加密資料及與經加密資料相關聯的查問值，提供查問值至實體不可複製功能模組以獲得經恢復回覆值，使用經恢復回覆值解密與儲存請求相關聯之資料，以及提供經解密資料至處理器。

【圖式簡單說明】

圖1為可用以實施本文所揭示之技術的計算裝置100之方塊圖。

圖2為用於根據本文所論述之技術保護記憶體中之資料的實例處理程序之流程圖。

圖3為用於根據本文所揭示之技術加密資料之實例處理程序之流程圖。

圖4為用於根據本文所論述之技術獲得查問值之實例處理程序的流程圖。

圖5為用於根據本文所揭示之技術加密資料之實例處理程序的流程圖。

圖6為用於根據本文所論述之技術加密資料之實例處理程序的流程圖。

圖7為用於根據本文所揭示之技術解密資料之實例處理程序之流程圖。

圖8為用於根據本文所揭示之技術解密資料之實例處理程序之流程圖。

圖9為用於根據本文所揭示之技術解密資料之實例處理程序之流程圖。

圖10為用於根據本文所揭示之技術解密資料之實例處理程序之

流程圖。

【實施方式】

揭示用於使用為儲存於計算裝置之記憶體中的資料提供強大保護的記憶體加密裝置保護計算裝置之記憶體中之資料的技術。本文所論述之技術在資料儲存於計算裝置的記憶體中之前使用記憶體加密裝置(MED)加密資料。本文所論述之技術的MED可使用實體不可複製功能(PUF)模組產生待由MED使用以加密跨匯流排傳輸及/或儲存於計算裝置之記憶體中的資料的密鑰。加密密鑰從不跨資料匯流排傳輸或與經加密資料一起儲存或處於晶片中。替代地，使用查問值自PUF模組獲得可用作加密密鑰以加密特定資料集合的回覆值。查問值與經加密資料一起被儲存，且MED可使用查問值恢復用以加密經加密資料之加密密鑰。即使攻擊者能夠獲得與經加密資料之特定部分相關聯的查問值，攻擊者仍僅將能夠自PUF獲得與彼特定查問-回覆對相關聯的密鑰。MED可經組態以將不同查問用於待加密的資料之每一部分。舉例而言，MED可被組態以使得可用由PUF模組供應的不同密鑰加密資料之每一區塊，且可將恢復此密鑰之查問與資料之經加密區塊一起儲存於記憶體中。當處理器需要資料之經加密區塊時，MED可自記憶體擷取資料之經加密區塊及查問值，藉由提供查問值至PUF自PUF獲得加密密鑰，並解密經加密資料之區塊。

用於本文所揭示之技術的MED為針對習知MED的改良，習知MED依賴於模糊即安全(security by obscurity)來確保在內部及/或外部記憶體中及匯流排上之資料機密性。習知MED使用嵌入於晶片之矽中的私密密鑰加密資料。此習知方法易受密碼分析攻擊。密碼分析可用以揭示嵌入於晶片之矽中的一或多個密鑰。一旦攻擊者擁有此等密鑰，攻擊者便可解密藉由MED加密的資料。在本文所揭示之技術中使用PUF不會面臨此等缺點，此係因為MED所使用的密鑰並不儲存於

矽中並根據需要由PUF產生。

實例硬體

圖1為可用以實施本文所揭示之技術的計算裝置100之方塊圖。計算裝置可用以至少部分實施圖2至圖10中所說明之處理程序。計算裝置100包含CPU 105、記憶體加密裝置(MED)110、實體不可複製功能模組115、查問值產生器125及記憶體130。圖1中所說明之實例計算裝置100僅為用以說明本文所論述之概念的實例。本文所論述之技術可實施於可具有本文中未說明之及/或替代包括於圖1中所說明之實例中之組件的額外組件的計算裝置上。

中央處理單元(CPU)105(在本文中亦被稱作處理器)包含用於實施電腦程式指令之電子電路。CPU 105可包含用以基於電腦程式指令執行各種動作(包括基本算術、邏輯運算、控制操作及輸入/輸出(I/O)操作)的組件。CPU 105可經組態以接收致使CPU 105在記憶體130中儲存資料的儲存指令及致使CPU 105擷取儲存於記憶體130中之資料的讀取指令。

MED 110可經組態以加密待儲存於記憶體130中及/或跨資料匯流排135發送之資料，並儲存經加密資料及與經加密資料相關聯的查問值。MED 110可實施圖2至圖10中所說明之加密及解密處理程序。MED 110可經組態以回應於來自CPU 105之儲存資料請求(例如，其中CPU 105提供資料160至MED 110)而執行加密步驟。MED 110可加密資料160並輸出經加密資料165，可藉由跨資料匯流排135發送經加密資料165及與經加密資料165相關聯之查問值145至記憶體130而將其儲存於記憶體130中。經加密資料及與經加密資料165相關聯的查問值145可儲存在記憶體130中之記憶體位置170處。在圖1中所說明之實例中，僅存在經加密資料165之單個例項及與經加密資料之該單個例項相關聯的查問值145以簡化本文所揭示之概念的說明。然而，MED

110可儲存經加密資料165之多個例項及與經加密資料165的此等例項中之每一者相關聯的查問值。

MED 110可經組態以對區塊中之資料操作，以使得使用與資料之每一區塊相關聯的密鑰加密資料之彼特定區塊。可藉由呈遞查問值145至PUF模組115以獲得回覆值155而獲得加密密鑰。MED 110可使用此回覆值之全部或一部分作為將用以加密資料160的加密密鑰。MED 110可經組態以使用各種加密技術。舉例而言，MED 110可經組態以藉由將互斥或(XOR)運算應用於資料160及自PUF模組115接收之回覆值或其部分而加密資料160。在此內容脈絡中使用XOR演算法加密資料160可為經加密資料160提供強大的加密保護，此係因為可使用由查問值產生器125(下文論述)提供之查問值145自PUF模組115獲得加密密鑰，以隨機密鑰選擇性地加密記憶體之每一區塊或待加密的記憶體之其他區段。MED 110亦可經組態以使用其他加密演算法(諸如，進階加密標準(AES)演算法或其他加密演算法，且不受限於僅XOR或AES演算法)來加密資料160。

PUF模組115可使用各種技術來實施。在一個實例實施中，PUF模組115可包含複數個環形振盪器。該複數個環形振盪器(RO)可經同時啟用且其輸出可發送至兩個或兩個以上交換器(多工器)。查問值充當至交換器之輸入，其致使每一切換器接著自該複數個RO中選擇單個RO。發送至交換器之查問值可經設計以使得每一切換器選擇不同RO。即使可能在製造中已經嘗試使所選擇的RO中之每一者相同，該等所選擇的RO仍可歸因於半導體層級處之微小製造變化而各具有與其相關聯之稍微不同諧振頻率。可藉由如由一對計數器量測/儲存之此等所選擇環形振盪器之頻率的兩兩比較而產生回覆值155。舉例而言，若第一計數器偵測到比第二計數器更高的頻率，則可產生邏輯「1」，否則可產生邏輯「0」。以此方式，所進行的比較表示查問/回

覆機制，其中所選擇的RO對係查問值，且RO頻率比較結果係回覆值。該複數個環形振盪器實施僅為可用以實施PUF模組115之實施類型的一個實例。提供基於CPU 105之組件、記憶體130及/或計算裝置100之難以預測、易於評估以及可靠地提供一致結果的其他組件的實體特性之PUF的其他技術可用以實施PUF模組115。

MED 110亦可經組態以存取儲存於記憶體130中之經加密資料165及與經加密資料165相關聯的查問值145，並解密經加密資料165以恢復原始未加密資料160。MED 110可實施圖7至圖10中所說明之解密處理程序。MED 110可經組態以回應於來自CPU 105之讀取資料請求(例如，其中CPU 105提供待讀取的資料之位址至MED 110)而執行解密步驟。MED 110可經組態以存取在記憶體130中之記憶體位置170處的經加密資料165及與經加密資料165相關聯之查問值145。其中記憶體位置170對應於在讀取資料請求中請求的資料之記憶體位置。由於經加密資料165之每一例項寫入至記憶體130中之獨立記憶體位置，因此與儲存於記憶體130中的經加密資料165之例項相關聯的記憶體位置170將針對儲存於記憶體130中的經加密資料165之每一例項而改變。MED 110可使用與自記憶體位置170擷取的經加密資料相關聯之查問值145擷取用以加密經加密資料115之加密密鑰。MED 110可提供查問值145至PUF模組115以自PUF模組115獲得回覆值。假定查問值當在記憶體130中時未被更改或損壞，PUF模組115應提供與用以加密經加密資料之回覆值155相同的經恢復回覆值。MED 110可選擇經恢復回覆值的全部或一部分用作解密經加密資料165之密鑰。MED 110可經組態以選擇經恢復回覆值之與自回覆值155選擇之部分相同的部分及/或執行與對回覆值155所執行之操作相同的操作以重新產生用以加密經加密資料165之密鑰。

計算裝置亦可包括查問值產生器125。查問值產生器125可包括

可經組態以提供亂數至MED 110的亂數產生器(RNG)，MED 110可將該亂數用作呈遞至PUF模組115之查問值145以獲得可繼而用以加密來自CPU 105之資料160的回覆值155。查問值產生器125包括每當讀取唯一值時可提供該值的單調計數器，且MED 110可經組態以自單調計數器讀取計數器值，MED 110可將該計數器值用作用於加密資料之加密密鑰。MED 110亦可使用其他類型之查問值產生器產生待呈遞至PUF模組115之查問值。查問值之大小可改變並可取決於待加密資料所針對的記憶體130之大小。查問值可包括足夠數目個位元以確保可用唯一查問值保護記憶體130之每一區塊。

為清楚起見，MED 110、PUF模組115及查問值產生器125已各自經說明為與CPU 105分離之組件。然而，MED 110、PUF模組115及查問值產生器125中之一或多者可經實施為CPU 105之組件。

實例實施

圖2為用於根據本文所論述之技術保護記憶體中之資料的實例處理程序之流程圖。圖2中所說明之處理程序可藉由圖1中所說明之計算裝置100實施。除非另外說明，否則計算裝置100之記憶體加密裝置110可提供用於執行圖2中所說明之處理程序的各個階段的構件。

可使用處理器之記憶體加密裝置來加密與儲存請求相關聯之資料以產生經加密資料(階段205)。MED 110可自CPU 105接收儲存未加密資料160的儲存請求。未加密資料160可包含資料區塊或可包含待儲存於計算裝置100之記憶體130中的資料之不同大小部分。MED 110可經組態以呈遞查問值145至PUF模組115以自PUF模組115獲得回覆值155。MED 110可使用回覆值155之全部或一部分作為加密資料160之加密密鑰。圖3說明MED 110可用以加密資料160的實例處理程序。MED 110可經組態以使用各種加密演算法(諸如XOR加密演算法、AES演算法及/或其他加密演算法)來加密資料160。

可將經加密資料及與經加密資料相關聯之查問值儲存於計算裝置之記憶體中(階段210)。經加密資料165可經由資料匯流排135提供至記憶體130以用於儲存在記憶體位置170處。用以自PUF模組115獲得密鑰之查問值亦可與經加密資料165一起儲存在記憶體130之記憶體位置170處。與經加密資料相關聯之查問值145可用以自PUF模組115擷取解密資料所需要的加密密鑰。查問值145僅與經加密資料165一起儲存。因此，即使攻擊者能夠存取記憶體位置170以獲得經加密資料165及查問值145，單獨的查問值145仍不足以解密經加密資料165，且由於加密密鑰係由PUF模組115產生，因此攻擊者不大可能能夠僅單獨自查問值145預測自回覆值155導出的加密密鑰。

圖3為用於根據本文所揭示之技術加密資料之實例處理程序之流程圖。圖3中所說明之處理程序可用以實施圖2中所說明之處理程序的階段205。圖3中所說明之處理程序可藉由圖1中所說明之計算裝置100實施。除非另外說明，否則計算裝置100之記憶體加密裝置110可提供用於執行圖3中所說明之處理程序的各個階段的構件。

可獲得查問值(階段305)。查問值145為待提供至PUF模組115之值，PUF模組115回應於查問值145而產生回覆值155。MED 110可經組態以每當MED 110接收來自CPU 105之儲存請求時獲得新的查問值。查問值可為亂數，且可自查問值產生器125獲得。MED 110亦可經組態以使用用於產生查問值之其他技術。

可提供查問值至實體不可複製功能(PUF)模組以獲得回覆值(階段310)。MED 110可提供查問值145至PUF模組115以獲得回覆值155。PUF模組115之性質使得非常難以基於查問值145預測自PUF模組115獲得的回覆值155。

可使用回覆值作為加密密鑰來加密與儲存請求相關聯之資料以產生經加密資料(階段315)。MED 110可經組態以使用回覆值155之至

少一部分作為加密密鑰將加密演算法應用於資料160以產生經加密資料165。MED 110可經組態以應用用於加密資料之不同加密技術。圖4及圖5提供其中MED 110應用XOR加密演算法以加密資料160的處理程序之實例。MED 110可經組態以使用回覆值155之至少一部分作為加密密鑰將其他類型之加密演算法(諸如，AES演算法)應用於資料160。

圖4為用於根據本文所論述之技術獲得查問值之實例處理程序的流程圖。圖4中所說明之處理程序可用以實施圖3中所說明之處理程序的階段305。圖4中所說明之處理程序可藉由圖1中所說明之計算裝置100實施。除非另外說明，否則計算裝置100之記憶體加密裝置110可提供用於執行圖4中所說明之處理程序的各個階段的構件。

可向亂數產生器請求查問值(階段405)。如上文所論述，查問值產生器125可包括亂數產生器，且MED 110可經組態以向RNG請求亂數值，MED 110可將該亂數值用作待呈遞至PUF模組115的查問值145以便獲得可用作用於加密資料160之加密密鑰的回覆值155。查問值產生器125亦可包括每當讀取唯一值時可提供該值的單調計數器，且MED 110可經組態以自單調計數器讀取計數器值，MED 110可將該計數器值用作用於加密資料之加密密鑰。MED 110亦可使用其他類型之查問值產生器產生待呈遞至PUF模組115之查問值。

可自查問值產生器接收查問值(階段410)。查問值產生器125可經組態以提供查問值至MED 110。MED 110可經組態以提供如自查問值產生器125接收之查問值至PUF模組115。MED 110亦可經組態以對查問值執行一或多個操作以便獲得待提供至PUF模組115之查問值145。舉例而言，MED 110可經組態以自自查問值產生器125接收之查問值中選擇預定數目個位元。舉例而言，MED 110可經組態以選擇自查問值產生器125接收之查問值的前4個位元及最後4個位元。MED 110亦可經組態以調整亂數值以落在由PUF模組115預期的查問值之預定範

圍內。所提供之實例意謂提供說明MED 110可對自查問值產生器125獲得之值執行的處理中之一些處理的實例且不意謂為排他性的。

圖5為用於根據本文所揭示之技術加密資料之實例處理程序的流程圖。圖5中所說明之處理程序可用以實施圖3中所說明之處理程序的階段315。圖5中所說明之處理程序可藉由圖1中所說明之計算裝置100實施。除非另外說明，否則計算裝置100之記憶體加密裝置110可提供用於執行圖5中所說明之處理程序的各個階段的構件。

可將互斥或(XOR)運算應用於來自PUF模組之回覆值及與讀取請求相關聯的資料(階段505)。MED 110可經組態以將XOR運算應用於資料160及自PUF模組115接收之回覆值155的至少一部分。舉例而言，MED 110可經組態以自待用作加密密鑰之回覆值155選擇預定數目個位元。舉例而言，MED 110可經組態以選擇自查問值產生器125接收的查問值之前X數目個位元及最後Y數目個位元，其中X及Y為整數值，且X及Y合計為待加密的資料160之位元的數目。MED 110亦可經組態以對回覆值執行其他操作以便獲得密鑰。舉例而言，MED 110可經組態以將取模運算應用於回覆值以將加密密鑰保持在預定位元範圍或預定數目個位元內。

可輸出經加密資料(階段510)。MED 110可經組態以輸出經加密資料160。MED 110可經組態以在記憶體130之記憶體位置170處儲存經加密資料165。MED 110亦可經組態以提供經加密資料165至CPU 105，CPU 105可經組態以處理經加密資料。

圖6為用於根據本文所論述之技術加密資料之實例處理程序的流程圖。圖6中所說明之處理程序可用以實施圖3中所說明之處理程序的階段315。圖6中所說明之處理程序可由圖1中所說明之計算裝置100實施。除非另外說明，否則計算裝置100之記憶體加密裝置110可提供用於執行圖6中所說明之處理程序的各個階段的構件。圖6中所說明之處

理程序類似於圖5中所說明之處理程序，但圖6中所說明之處理程序亦使用經加密資料165待儲存於其中的記憶體130之位址位置170之位址以進一步加密資料。MED 110可經組態以對來自PUF模組115之回覆值(充當加密密鑰)、待加密之資料160及與經加密資料待以任何次序儲存於其中的記憶體位置相關聯之位址170執行XOR運算，此係因為XOR運算為可轉移的。因此，在圖6中所說明之處理程序中執行此等操作的次序僅為用於使用此三個值加密資料160的處理程序之一個實例，且可以不同次序執行其他實施。

可將互斥或(XOR)運算應用於來自PUF模組之回覆值及與讀取請求相關聯的資料以產生中間值(階段605)。中間值類似於在圖5中所說明之處理程序的階段505中產生的彼值。

可將互斥或(XOR)運算應用於中間值及與其中儲存經加密資料的記憶體位置相關聯之位址值(階段610)。MED 110可將XOR運算應用於與記憶體130中之記憶體位置170相關聯之位址值及在階段605中判定的中間值以產生經加密資料165。

可輸出經加密資料(階段615)。MED 110可經組態以輸出經加密資料160。MED 110可經組態以在記憶體130之記憶體位置170處儲存經加密資料165。MED 110亦可經組態以提供經加密資料165至CPU 105，CPU 105可經組態以處理經加密資料。

圖7為用於根據本文所揭示之技術解密資料之實例處理程序之流程圖。圖7中所說明之處理程序可在圖2中所說明之處理程序之後並可用以解密根據圖2中所說明之處理程序加密的資料。圖7中所說明之處理程序可藉由圖1中所說明之計算裝置100實施。除非另外說明，否則計算裝置100之記憶體加密裝置110可提供用於執行圖7中所說明之處理程序的各個階段的構件。

可回應於來自CPU 105之讀取請求而自記憶體130獲得經加密資

料165及與經加密資料相關聯之查問值145 (階段705)。讀取請求可指定儲存經加密資料165及與經加密資料相關聯之查問值145所在的記憶體位置170之位址。如上文所論述，MED 110可儲存經加密資料165之多個例項及與經加密資料165之例項中之每一者相關聯的各別查問值145。因此，經加密資料165之每一例項將與可發現經加密資料165之彼例項所在的記憶體130中之各別記憶體位置170相關聯。

可解密經加密資料165以產生經解密資料160(階段710)。MED 110可使用與經加密資料165相關聯之查問值145解密經加密資料110。MED 110可經組態以基於MED 110用以加密資料的加密技術使用適當解密技術解密經加密資料110。舉例而言，MED 110可經組態以使用如上文所論述之XOR技術加密資料。MED 110亦可經組態以亦使用其他技術(諸如，AES加密演算法)加密資料。圖8、圖9及圖10提供用於解密經加密資料165之實例處理程序，其中經加密資料165係使用XOR加密演算法來加密的。

可提供經解密資料160至CPU 105或計算裝置100之其他組件(階段715)。MED 110可提供經解密資料160至CPU 105或計算裝置100之其他組件。CPU 105可對經解密資料160執行一或多個操作，或經解密資料160可經提供至周邊裝置以由周邊裝置進行處理。舉例而言，經解密資料160可經提供至圖形處理器以用於判定在與計算裝置100相關聯之顯示器上顯示的資訊。其他類型之周邊裝置可接收經解密資料160以進行處理。

圖8為用於根據本文所揭示之技術解密資料之實例處理程序之流程圖。圖8中所說明之處理程序可用以實施圖7中所說明之處理程序的階段710。圖8中所說明之處理程序可藉由圖1中所說明之計算裝置100實施。除非另外說明，否則計算裝置100之記憶體加密裝置110可提供用於執行圖8中所說明之處理程序的各個階段的構件。

可將查問值145提供至PUF模組115以獲得經恢復回覆值(階段805)。儲存於記憶體130之記憶體位置170中的查問值145可經提供至PUF模組115以接收經恢復回覆值。MED 110可將經恢復回覆值用作用於解密經加密資料110之解密密鑰。在一些實施中，查問值145可儲存在記憶體130之不同於經加密資料165之記憶體位置的記憶體位置處。MED 110可經組態以維持經加密資料165之記憶體位置與相關聯於經加密資料165之每一例項的查問值145之記憶體位置之間的映射。

可使用經恢復回覆值解密經加密資料165(階段810)。MED 110可使用自PUF模組115獲得的回覆值之至少一部分作為解密密鑰來解密經加密資料110。MED 110可經組態以基於MED 110用以加密資料的加密技術使用適當解密技術解密經加密資料110。舉例而言，MED 110可經組態以使用如上文所論述之XOR技術加密資料。MED 110亦可經組態以亦使用其他技術(諸如，AES加密演算法)加密資料。圖9及圖10提供用於解密經加密資料165之實例處理程序，其中經加密資料165係使用XOR加密演算法來加密的。

圖9為用於根據本文所揭示之技術解密資料之實例處理程序之流程圖。圖9中所說明之處理程序可用以實施圖8中所說明之處理程序的階段810。圖9中所說明之處理程序可藉由圖1中所說明之計算裝置100實施。除非另外說明，否則計算裝置100之記憶體加密裝置110可提供用於執行圖9中所說明之處理程序的各個階段的構件。

可將互斥或(XOR)運算應用於經加密資料165及經恢復回覆值(階段905)。MED 110可經組態以回應於提供自記憶體130獲得之查問值145至PUF模組115而將XOR運算應用於經加密資料165及自PUF模組115接收之經恢復回覆值之至少一部分。舉例而言，MED 110可經組態以自待用作解密密鑰之經恢復回覆值中選擇預定數目個位元。所選擇的位元取決於最初自當加密經加密資料165時自PUF模組115獲得的

回覆值155選擇的那些位元。MED 110亦可經組態以對回覆值執行其他操作以便獲得密鑰，此取決於MED 110對回覆值155進行以產生加密經加密資料165所使用的密鑰的處理。

MED 110接著可輸出經解密資料(階段910)。MED 110可提供經解密資料160至CPU 105或計算裝置100之其他組件。

圖10為用於根據本文所揭示之技術解密資料之實例處理程序之流程圖。圖10中所說明之處理程序可用以實施圖8中所說明之處理程序的階段810。圖10中所說明之處理程序可藉由圖1中所說明之計算裝置100實施。除非另外說明，否則計算裝置100之記憶體加密裝置110可提供用於執行圖10中所說明之處理程序的各個階段的構件。圖10中所說明之處理程序類似於圖9中所說明之處理程序，但圖10中所說明之處理程序亦使用經加密資料165待儲存於其中的記憶體130之位址位置170之位址來解密資料。MED 110可經組態以對來自PUF模組115的經恢復回覆值(充當解密密鑰)、待解密之經加密資料165及與經加密資料165以任何次序儲存於其中的記憶體位置相關聯的位址170執行XOR運算，此係因為XOR運算為可轉移的。因此，在圖10中所說明之處理程序中執行此等操作的次序僅為用於使用此三個值解密經加密資料160的處理程序之一個實例，且可以不同次序執行其他實施。

可將互斥或(XOR)運算應用於經加密資料165及經恢復回覆值以產生中間值(階段1005)。第一XOR運算顛倒在圖6中所說明之處理程序之階段605中執行的XOR運算，其中來自PUF模組115之回覆值155的至少一部分用以對資料160執行第一加密操作以產生經加密資料165。

可將互斥或(XOR)運算應用於中間值及與經加密資料儲存於其中之記憶體位置相關聯的位址值以產生經解密資料(階段1010)。第二XOR運算顛倒在圖6中所說明之處理程序之階段610中執行的XOR運

算，其中與相關聯於正被解密的經加密資料165之記憶體位置170相關聯的位址值用以產生經加密資料165。經加密資料165現在應已返回至原始未加密狀態並應匹配最初由CPU 105提供至MED 110以用於加密的未加密資料160。

MED 110接著可輸出經解密資料(階段1015)。MED 110可提供經解密資料160至CPU 105或計算裝置100之其他組件。

取決於應用，可藉由各種構件實施本文中所描述之方法。舉例而言，此等方法可以硬體、韌體、軟體或其任何組合來實施。對於硬體實施，處理單元可在一或多個特殊應用積體電路(ASIC)、數位信號處理器(DSP)、數位信號處理裝置(DSPD)、可程式化邏輯裝置(PLD)、場可程式化閘陣列(FPGA)、處理器、控制器、微控制器、微處理器、電子裝置、經設計以執行本文中所描述的功能的其他電子單元或其組合內實施。

對於韌體及/或軟體實施，方法可用執行本文中所描述功能的模組(例如，程序、函數等等)來實施。在實施本文中所描述之方法時，可使用任何有形地體現指令的機器可讀媒體。舉例而言，軟體程式碼可儲存於記憶體中，並由處理器單元來執行。記憶體可在處理器單元內或處理器單元外部實施。如本文中所使用，術語「記憶體」係指任何類型之長期、短期、揮發性、非揮發性或其他記憶體，且並不限於任何特定類型之記憶體或特定數目的記憶體或特定類型的媒體。有形媒體包括機器可讀媒體之一或多個實體物品，諸如隨機存取記憶體、磁性儲存器、光學儲存媒體等等。

若以韌體及/或軟體實施，則可將功能作為一或多個指令或程式碼儲存於電腦可讀媒體上。實例包括以資料結構編碼的電腦可讀媒體及以電腦程式編碼的電腦可讀媒體。電腦可讀媒體包括實體電腦儲存媒體。儲存媒體可為可由電腦存取之任何可用媒體。藉由實例而非限

制方式，此類電腦可讀媒體可包含RAM、ROM、EEPROM、CD-ROM或其他光碟儲存器，磁碟儲存器或其他磁性儲存裝置，或可用於儲存呈指令或資料結構形式的所要程式碼且可由電腦存取的任何其他媒體；如本文中所使用，磁碟和光碟包括光碟(CD)、雷射光碟、光學光碟、數位多功能光碟(DVD)，以及藍光光碟，其中磁碟通常以磁性方式再現數據，而光碟用雷射以光學方式再現資料。以上之組合亦應包括於電腦可讀媒體之範疇內。此等媒體亦提供可為機器可讀之非暫時性媒體的實例，且其中電腦為可自此等非暫時性媒體讀取的機器之實例。

在不脫離本發明或申請專利範圍之精神或範疇的情況下，本文中所論述之一般原理可應用於其他實施。

【符號說明】

100	計算裝置
105	中央處理單元
110	記憶體加密裝置
115	實體不可複製功能模組
125	查問值產生器
130	記憶體
135	資料匯流排
140	位址匯流排
145	查問值
155	回覆值
160	資料
165	經加密資料
170	記憶體位置

201701186

發明摘要

※ 申請案號：105114018

※ 申請日：105.5.5　　※IPC 分類：G06F 21/78 (2013.01)　G06F 12/14 (2006.01)

【發明名稱】

實體不可複製功能輔助之記憶體加密裝置技術

PHYSICALLY UNCLONABLE FUNCTION ASSISTED MEMORY ENCRYPTION DEVICE TECHNIQUES

【中文】

本發明提供用於加密一計算裝置之記憶體中之資料的技術。根據本發明之用於保護一記憶體中之資料的一種實例方法包括使用處理器之一記憶體加密裝置加密與一儲存請求相關聯的資料以產生經加密資料。加密該資料包括：獲得一查問值，提供該查問值至一實體不可複製功能模組以獲得一回覆值，以及使用該回覆值作為一加密密鑰來加密與該儲存請求相關聯的該資料以產生該經加密資料。該方法亦包括在該記憶體中儲存該經加密資料及與該經加密資料相關聯的該查問值。

【英文】

Techniques for encrypting the data in the memory of a computing device are provided. An example method for protecting data in a memory according to the disclosure includes encrypting data associated with a store request using a memory encryption device of the processor to produce encrypted data. Encrypting the data includes: obtaining a challenge value, providing the challenge value to a physically unclonable function module to obtain a response value, and encrypting the data associated with the store request using the response value as an encryption key to generate the encrypted data. The method also includes storing the encrypted data and the challenge value associated with the encrypted data in the memory.

【代表圖】

【本案指定代表圖】：第（1）圖。

【本代表圖之符號簡單說明】：

100	計算裝置
105	中央處理單元
110	記憶體加密裝置
115	實體不可複製功能模組
125	查問值產生器
130	記憶體
135	資料匯流排
140	位址匯流排
145	查問值
155	回覆值
160	資料
165	經加密資料
170	記憶體位置

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

(無)

申請專利範圍

1. 一種用於保護一記憶體中之資料的方法，該方法包含：

使用與一處理器相關聯的一記憶體加密裝置加密與一儲存請求相關聯之資料以產生經加密資料，其中加密該資料包含：

獲得一查問值，

提供該查問值至一實體不可複製功能模組以獲得一回覆值，及

使用該回覆值作為一加密密鑰加密與該儲存請求相關聯之該資料以產生該經加密資料；及

在該記憶體中儲存該經加密資料及與該經加密資料相關聯之該查問值。

2. 如請求項1之方法，其中獲得該查問值包含自與該處理器相關聯的一亂數產生器獲得該查問值。

3. 如請求項1之方法，其中獲得該查問值包含自與該處理器相關聯之一單調計數器獲得該查問值。

4. 如請求項1之方法，其中使用該查問值加密與該儲存請求相關聯之該資料包含將一互斥或(XOR)運算應用於與該儲存請求相關聯之該資料及該回覆值以產生該經加密資料。

5. 如請求項1之方法，其中使用該查問值加密與該儲存請求相關聯之該資料包含將一互斥或(XOR)運算應用於與該儲存請求相關聯的該資料、產生該經加密資料之該回覆值，以及與該經加密資料待寫入於其中之一記憶體位置相關聯的一位址。

6. 如請求項1之方法，其進一步包含：

回應於一讀取請求而自該記憶體獲得該經加密資料及與該經加密資料相關聯之該查問值；及

解密該經加密資料以產生經解密資料，其中解密該資料包含：

提供該查問值至該實體不可複製功能模組以獲得一經恢復回覆值，及

使用該經恢復回覆值解密與該儲存請求相關聯之該資料，及

提供該經解密資料至該處理器。

7. 如請求項6之方法，其中使用該經恢復回覆值解密與該儲存請求相關聯之該資料包含將一互斥或(XOR)運算應用於該經加密資料及該經恢復回覆值以產生該經解密資料。

8. 如請求項6之方法，其中使用該經恢復回覆值解密與該儲存請求相關聯之該資料包含將一互斥或(XOR)運算應用於該經加密資料、該經恢復回覆值，以及與該經加密資料寫入至之一記憶體位置相關聯的一位址，以產生該經加密資料。

9. 一種設備，其包含：

用於獲得一查問值之構件；

用於提供該查問值至一實體不可複製功能模組以獲得一回覆值的構件；

用於使用該回覆值作為一加密密鑰加密與一儲存請求相關聯之資料以產生經加密資料的構件；及

用於儲存該經加密資料及與該經加密資料相關聯之該查問值的構件。

10. 如請求項9之設備，其中用於獲得該查問值的該構件包含用於自一亂數產生器獲得該查問值的構件。

11. 如請求項9之設備，其中用於獲得該查問值的該構件包含用於自一單調計數器獲得該查問值的構件。

12. 如請求項9之設備，其中用於使用該查問值加密與該儲存請求相關聯之該資料的該構件包含用於將一互斥或(XOR)運算應用於與該儲存請求相關聯之該資料及該回覆值以產生該經加密資料的構件。

13. 如請求項9之設備，其中用於使用該查問值加密與該儲存請求相關聯之該資料的該構件包含用於將一互斥或(XOR)運算應用於與該儲存請求相關聯的該資料、產生該經加密資料之該回覆值，以及與該經加密資料待寫入於其中之一記憶體位置相關聯的一位址的構件。

14. 如請求項9之設備，其進一步包含：

用於回應於一讀取請求自該經加密資料儲存於其中的一記憶體獲得該經加密資料及與該經加密資料相關聯之該查問值的構件；

用於提供該查問值至一實體不可複製功能模組以獲得一經恢復回覆值的構件；

用於使用該經恢復回覆值解密與該儲存請求相關聯之該資料的構件，及

用於提供該經解密資料至一處理器的構件。

15. 如請求項14之設備，其中用於使用該經恢復回覆值解密與該儲存請求相關聯之該資料的該構件包含用於將一互斥或(XOR)運算應用於該經加密資料及該經恢復回覆值以產生該經解密資料的構件。

16. 如請求項14之設備，其中用於使用該經恢復回覆值解密與該儲存請求相關聯之該資料的該構件包含用於將一互斥或(XOR)運算應用於該經加密資料、該經恢復回覆值，以及與該經加密資料寫入至之一記憶體位置相關聯的一位址以產生該經加密資料的

構件。

17. 一種計算裝置，其包含：

一處理器；及

一記憶體，其耦接至該處理器，且

該處理器包含一記憶體加密裝置，該記憶體加密裝置經組態以：

獲得一查問值；

提供該查問值至一實體不可複製功能模組以獲得一回覆值；

使用該回覆值作為一加密密鑰加密與自該處理器接收之一儲存請求相關聯的資料以產生經加密資料；及

在該記憶體中儲存該經加密資料及與該經加密資料相關聯之該查問值。

18. 如請求項17之計算裝置，其中該記憶體加密裝置經組態以自與該處理器相關聯的一亂數產生器獲得該查問值。

19. 如請求項17之計算裝置，其中該記憶體加密裝置經組態以自與該處理器相關聯之一單調計數器獲得該查問值。

20. 如請求項17之計算裝置，其中該記憶體加密裝置經組態以藉由將一互斥或(XOR)運算應用於與該儲存請求相關聯之該資料及該回覆值，使用該查問值加密與該儲存請求相關聯之該資料，以產生該經加密資料。

21. 如請求項17之計算裝置，其中該記憶體加密裝置經組態以藉由將一互斥或(XOR)運算應用於與該儲存請求相關聯的該資料、產生該經加密資料之該回覆值，以及與該經加密資料待寫入於其中之一記憶體位置相關聯的一位址，使用該查問值加密與該儲存請求相關聯之該資料。

22. 如請求項17之計算裝置，其中該記憶體加密裝置經進一步組態以：

回應於一讀取請求而自該記憶體獲得該經加密資料及與該經加密資料相關聯之該查問值；及

解密該經加密資料以產生經解密資料，其中該記憶體加密裝置經組態以：

提供該查問值至該實體不可複製功能模組以獲得一經恢復回覆值，及

使用該經恢復回覆值解密與該儲存請求相關聯之該資料，及

提供該經解密資料至該處理器。

23. 如請求項22之計算裝置，其中該記憶體加密裝置經組態以藉由將一互斥或(XOR)運算應用於該經加密資料及該經恢復回覆值，使用該經恢復回覆值解密與該儲存請求相關聯之該資料，以產生該經解密資料。

24. 如請求項22之計算裝置，其中該記憶體加密裝置經組態以藉由將一互斥或(XOR)運算應用於該經加密資料、該經恢復回覆值，以及與該經加密資料待寫入於其中之一記憶體位置相關聯的一位址，使用該經恢復回覆值解密與該儲存請求相關聯之該資料，以產生該經加密資料。

25. 一種非暫時性電腦可讀媒體，在其上儲存有用於保護一記憶體中之資料的電腦可讀指令，該等指令包含經組態以致使一電腦執行以下操作之指令：

獲得一查問值；

提供該查問值至一實體不可複製功能模組以獲得一回覆值；

使用該回覆值作為一加密密鑰加密與一儲存請求相關聯之資

料以產生經加密資料；及

儲存該經加密資料及與該經加密資料相關聯之該查問值。

26. 如請求項25之非暫時性電腦可讀媒體，其中經組態以致使該電腦獲得該查問值的該等指令包含經組態以致使該電腦自一亂數產生器獲得該查問值的指令。

27. 如請求項25之非暫時性電腦可讀媒體，其中經組態以致使該電腦獲得該查問值之該等指令包含經組態以致使該電腦自一單調計數器獲得該查問值的指令。

28. 如請求項25之非暫時性電腦可讀媒體，其中經組態以致使該電腦使用該查問值加密與該儲存請求相關聯之該資料的該等指令包含經組態以致使該電腦將一互斥或(XOR)運算應用於與該儲存請求相關聯之該資料及該回覆值以產生該經加密資料的指令。

29. 如請求項25之非暫時性電腦可讀媒體，其中經組態以致使該電腦使用該查問值加密與該儲存請求相關聯之該資料的該等指令包含經組態以致使該電腦將一互斥或(XOR)運算應用於與該儲存請求相關聯之該資料、產生該經加密資料之該回覆值，以及與該經加密資料待寫入於其中之一記憶體位置相關聯的一位址的指令。

30. 如請求項25之非暫時性電腦可讀媒體，其進一步包含經組態以致使該電腦執行以下操作之指令：

回應於一讀取請求自該經加密資料儲存於其中的一記憶體獲得該經加密資料及與該經加密資料相關聯之該查問值；

提供該查問值至該實體不可複製功能模組以獲得一經恢復回覆值；

使用該經恢復回覆值解密與該儲存請求相關聯之該資料；及

提供該經解密資料至一處理器。

圖式

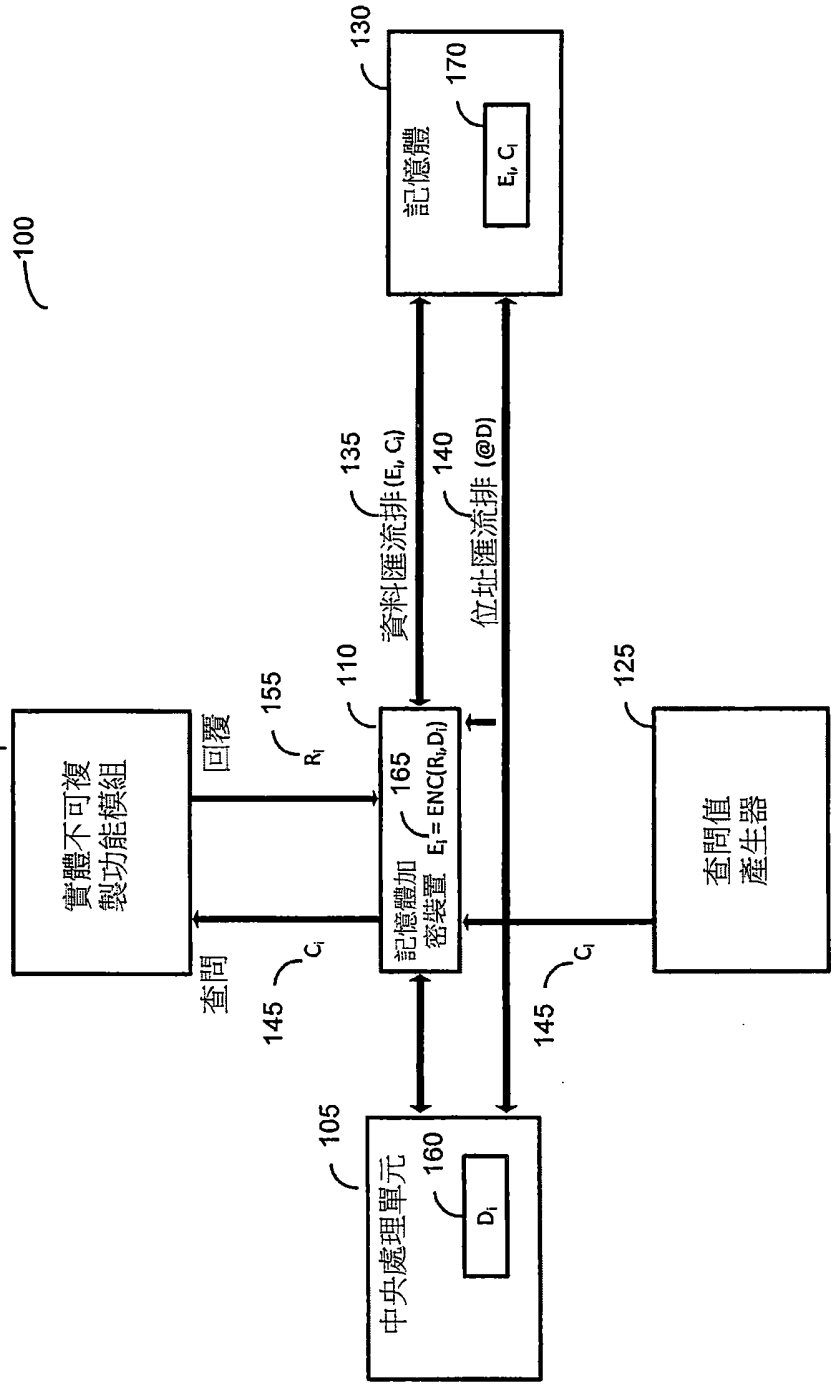
100
130
記憶體
170
E_i, C_i
135
資料匯流排 (E_i, C_i)
140
位址匯流排 (@D)
115
實體不可複製功能模組
回覆
155
R_i
110
記憶體加密裝置
165
$E_i = ENC(R_i, D_i)$
125
查問值產生器
查問
145
C_i
105
中央處理單元
160
D_i

圖1

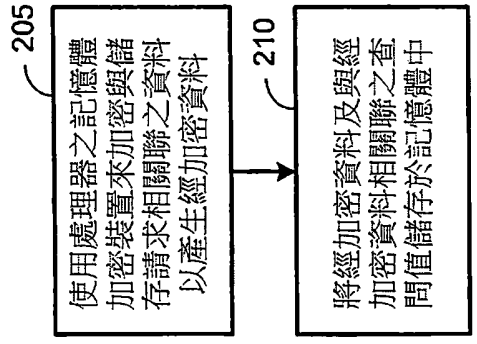
205
使用處理器之記憶體加密裝置來加密與儲存請求相關聯之資料以產生經加密資料
210
將經加密資料及與經加密資料相關聯之查問值儲存於記憶體中

圖2

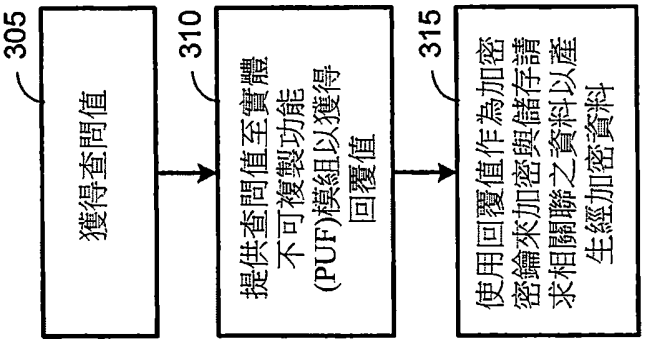
305
獲得查問值
310
提供查問值至實體不可複製功能(PUF)模組以獲得回覆值
315
使用回覆值作為加密密鑰來加密與儲存請求相關聯之資料以產生經加密資料

圖3

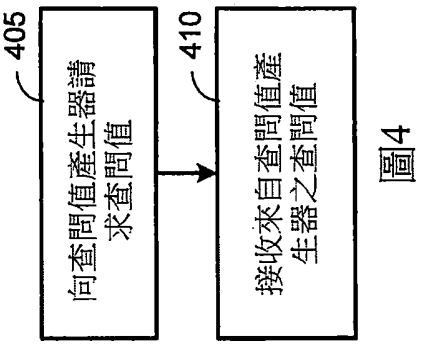
405
向查問值產生器請求查問值
410
接收來自查問值產生器之查問值

圖4

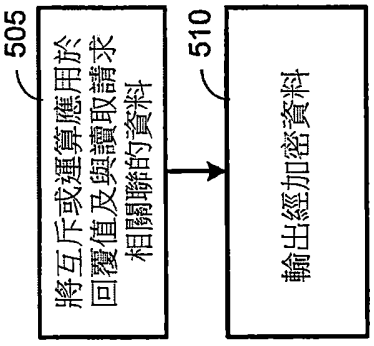
505
將互斥或運算應用於回覆值及與讀取請求相關聯的資料
510
輸出經加密資料

圖5

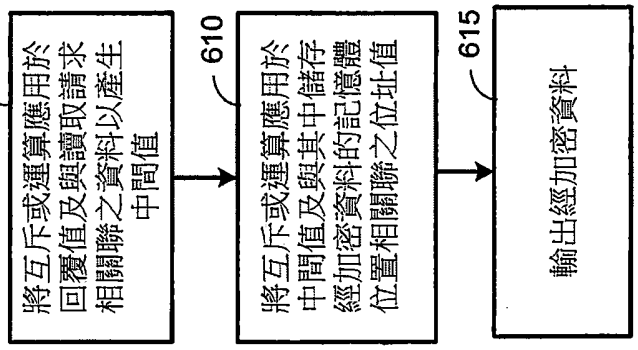
605
將互斥或運算應用於回覆值及與讀取請求相關聯之資料以產生中間值
610
將互斥或運算應用於中間值及與其中儲存經加密資料的記憶體位置相關聯之位址值
615
輸出經加密資料

圖6

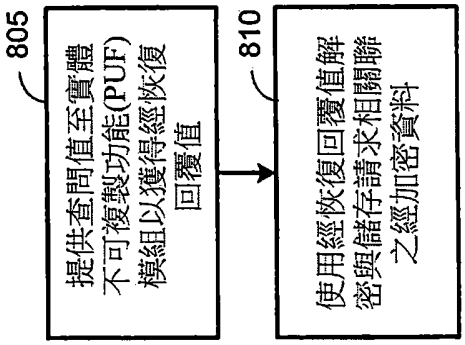
805
提供查問值至實體不可複製功能(PUF)模組以獲得經恢復回覆值
810
使用經恢復回覆值解密與儲存請求相關聯之經加密資料

圖8

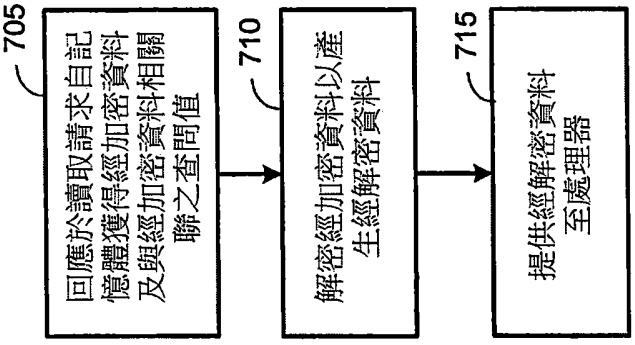
705
回應於讀取請求自記憶體獲得經加密資料及與經加密資料相關聯之查問值
710
解密經加密資料以產生經解密資料
715
提供經解密資料至處理器

圖7

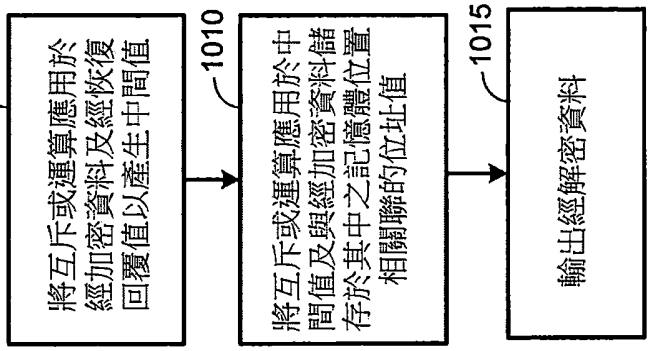
1005
將互斥或運算應用於經加密資料及經恢復回覆值以產生中間值
1010
將互斥或運算應用於中間值及與經加密資料儲存於其中之記憶體位置相關聯的位址值
1015
輸出經解密資料

圖10

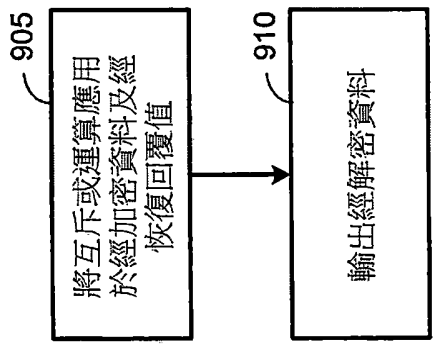
905
將互斥或運算應用於經加密資料及經恢復回覆值
910
輸出經解密資料

圖9