I402675

(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 I402675B1**

(45)公告日： 中華民國 102 (2013) 年 07 月 21 日

(21)申請案號：098136953 (22)申請日： 中華民國 98 (2009) 年 10 月 30 日

(51)Int. Cl.： *G06F12/14 (2006.01)* *H04L9/00 (2006.01)*

(30)優先權：2008/10/30 美國 12/262,092

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

(72)發明人：哈奇思菲力普麥可 HAWKES, PHILIP MICHAEL (AU)；霄路 XIAO, LU (CA)；羅斯葛瑞格里高登 ROSE, GREGORY GORDON (AU)；米蘭朵夫史迪 MILLENDORF, STEVE (US)

(74)代理人：李世章

(56)參考文獻：

TW 514844 US 6061449

US 2006/0265563A1

審查人員：林彥廷

申請專利範圍項數：49 項 圖式數：13 共 0 頁

(54)名稱

低等待時間的區塊密碼術

LOW LATENCY BLOCK CIPHER

(57)摘要

提供了一種保護資料的區塊密碼術，其藉由基於資料要被儲存的記憶體位址加密該資料來保護該資料。當加密資料以供儲存在該記憶體位址中時，該記憶體位址在第一多個區塊密碼回合中被加密。使用來自第一多個區塊密碼回合的資訊來產生資料回合密鑰。把要被儲存的資料與經加密的記憶體位址相組合併且在第二多個區塊密碼回合中藉由使用這些資料回合密鑰來加密。經加密資料隨後儲存在該記憶體位置中。當解密資料時，記憶體位址如之前般被再次加密，而經加密的儲存資料在第二多個區塊密碼回合中藉由使用資料回合密鑰來解密以獲得經部分解密的資料。把經部分解密的資料與經加密的記憶體位址相組合以獲得完全解密的資料。

A block cipher is provided that secures data by encrypting it based on the memory address where it is to be stored. When encrypting data for storage in the memory address, the memory address is encrypted in a first plurality of block cipher rounds. Data round keys are generated using information from the first plurality of block cipher rounds. Data to be stored is combined with the encrypted memory address and encrypted in a second plurality of block cipher rounds using the data round keys. The encrypted data is then stored in the memory location. When decrypting data, the memory address is again encrypted as before while the encrypted stored data is decrypted in a second plurality of the block cipher rounds using the data round keys to obtain a partially decrypted data. The partially decrypted data is combined with the encrypted memory address to obtain fully decrypted data.

302~328・・・區塊密碼術方塊圖

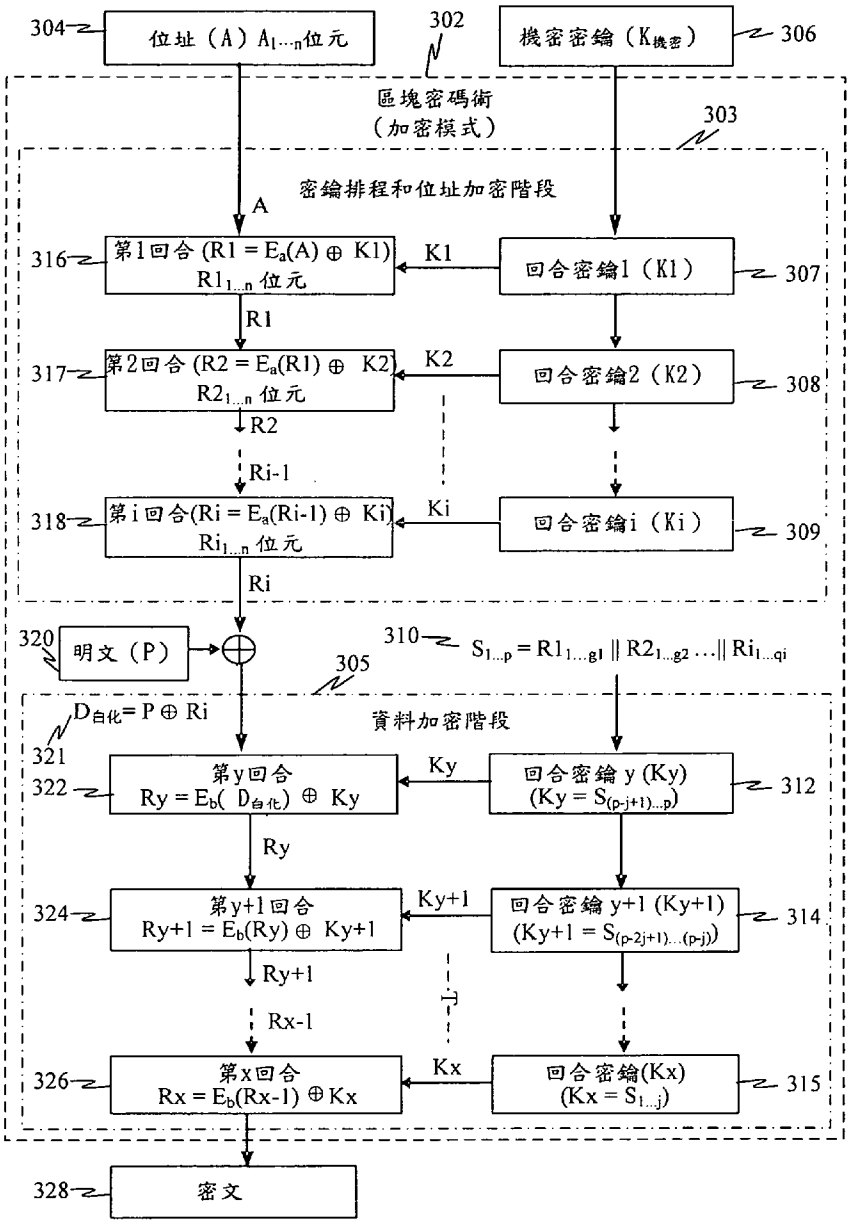

圖3

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫；惟已有申請案號者請填寫）

※ 申請案號：98136953

※ 申請日期：2009 年 10 月 30 日　　※IPC 分類：

G06F 12/14 (2006.01)

H04L 9/00 (2006.01)

一、發明名稱：（中文/英文）

低等待時間的區塊密碼術 / LOW LATENCY BLOCK CIPHER

二、中文發明摘要：

提供了一種保護資料的區塊密碼術，其藉由基於資料要被儲存的記憶體位址加密該資料來保護該資料。當加密資料以供儲存在該記憶體位址中時，該記憶體位址在第一多個區塊密碼回合中被加密。使用來自第一多個區塊密碼回合的資訊來產生資料回合密鑰。把要被儲存的資料與經加密的記憶體位址相組合併且在第二多個區塊密碼回合中藉由使用這些資料回合密鑰來加密。經加密資料隨後儲存在該記憶體位置中。當解密資料時，記憶體位址如之前般被再次加密，而經加密的儲存資料在第二多個區塊密碼回合中藉由使用資料回合密鑰來解密以獲得經部分解密的資料。把經部分解密的資料與經加密的記憶體位址相組合以獲得完全解密的資料。

三、英文發明摘要：

A block cipher is provided that secures data by encrypting it

based on the memory address where it is to be stored. When encrypting data for storage in the memory address, the memory address is encrypted in a first plurality of block cipher rounds. Data round keys are generated using information from the first plurality of block cipher rounds. Data to be stored is combined with the encrypted memory address and encrypted in a second plurality of block cipher rounds using the data round keys. The encrypted data is then stored in the memory location. When decrypting data, the memory address is again encrypted as before while the encrypted stored data is decrypted in a second plurality of the block cipher rounds using the data round keys to obtain a partially decrypted data. The partially decrypted data is combined with the encrypted memory address to obtain fully decrypted data.

四、指定代表圖：

(一)本案指定代表圖為：第（ 3 ）圖。

(二)本代表圖之元件符號簡單說明:

302~328　　區塊密碼術方塊圖

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

六、發明說明：

【發明所屬之技術領域】

一個特徵涉及記憶體內容的保護，尤其涉及使用區塊密碼術來保護儲存至記憶體設備的內容的方法。

【先前技術】

數位處理器存在於諸如蜂巢式電話、電腦、個人數位助理（PDA）、無線網路存取點等的許多設備中。使儲存在記憶體中的程式和資料得到保護以對抗具有相當尖端的工具的攻擊者的需要日漸增長。數位版權管理應用也强加此類限制以控制對數位資料或硬體的存取或使用。例如，中央處理單元（CPU）通常具有某種晶片上記憶體儲存器，可以藉由確保資料存取線被埋藏在 CPU 或板內，以使得存取該資料的企圖將毀壞該設備，並且可以想見在資料能被存取到之前就加擾或毀壞該資料來保全該晶片上記憶體儲存器。

出於規模和經濟的原因，希望能夠將記憶體封裝在單獨的晶片中。然而，將記憶體設備封裝在單獨的晶片中會使攻擊者要藉由使用諸如探針之類的簡單工具來存取記憶體設備相對容易，因爲資料在其於 CPU 與記憶體晶片之間往來時是曝露的。

一種解決在將資料儲存至分離的儲存晶片時缺乏安全性的方法是在 CPU 上進行加密程序，以使得被寫到記憶體晶片的資料對攻擊者而言是無用的。反之，當從記憶體取回資料

時，該資料由 CPU 解密。關於特定記憶體區塊的位址資訊以及僅爲 CPU 所知的密碼學密鑰是該加密演算法的其他輸入。

由於記憶體位置能被重複寫入，且常常是用模式化資料來寫入，因而流密碼術以及對應的用於區塊密碼術的操作模式諸如計數器模式（CTR）之類並不合適。將位址用作如密碼術區塊鏈結（CBC）的模式的初始化向量的區塊密碼術在此是合適的機制。（見 FIPS 特種出版物 800-38A——Modes of operation for Block Cipher（用於區塊密碼術的操作模式））。然而，與密碼術固有的區塊大小相比，在一次操作中要被加密的記憶體區塊通常很小（例如，往往只是單個區塊）。因此，當應用到單個區塊時，考慮將 CBC 模式作爲「鏈結」是反直觀的。

現代區塊密碼術具有常被稱爲疊代區塊密碼術的結構。每次疊代被稱爲一*回合*，並且重複的函數被稱爲*回合函數*（例如，4 到 32 回合之間的任何回合是典型的）。在每一回合中，當被應用到輸入區塊時，回合函數達成一定量的混亂性和擴散性。爲了加密輸入區塊，該密碼術產生該輸入區塊的置換。解密是藉由逆向地運行該程序來達成的。若視作黑單元，則該密碼術接收固定大小的單個資料區塊以及機密密鑰作爲輸入，重複地將回合函數應用到該輸入區塊，並且輸出單個密碼術輸出區塊。某些密碼術允許可變大小的密鑰，並且密鑰大小可以小於、等於或大於區塊大小。例如，高級加密標準（AES）演算法具有 128 位元的區塊大小，並且能接受 128、192 或 256 位元的密鑰。

在密碼術內有數個回合（例如，在具有 128 位元密鑰的 AES 情形中爲 10 回合）。每一回合具有回合密鑰作爲其輸入的一部分。這些回合密鑰是在被稱爲*密鑰排程*的程序中從機密密鑰推導出來的。每一回合旨在對區塊和回合密鑰的部分執行某種非線性替換，其後繼以某種（通常爲線性的）擴散操作以將每一替換的效果鋪開到整個區塊。這些動作旨在挫敗諸如線性和差分密碼學分析之類的公知形式的密碼學分析。

爲了加密向記憶體發送的資料，記憶體位址可被用作初始化向量。這將保證具有相同資料的不同記憶體位址將仍然被不同地加密。該加密可被記載爲：

$$C = E_K(P \oplus A)$$

其中 P 是輸入*明文*（原始資料區塊），A 是記憶體位址，C 是輸出*密文*（將在記憶體晶片中出現在位址 A 處的輸出資料區塊），⊕是逐位元互斥或（XOR）運算，而 E_K 表示使用區塊密碼術以機密密鑰 K 來加密該資料區塊。相應地，當要從記憶體中讀回資料時，將使用逆操作。

$$P = D_K(C) \oplus A$$

其中 D_K 表示在其解密模式中使用區塊密碼術。然而，與記憶體存取速度相比，典型的區塊密碼術應用具有相當高的等

待時間。對於批量加密而言，管線化解決了這個問題，但是當加密單個記憶體位置時，管線化並無幫助。

因此，需要一種對少數記憶體位置實現區塊密碼術加密同時減少等待時間的方法。

【發明內容】

提供了一種保護資料的區塊密碼術，其藉由基於資料要被儲存的記憶體位址加密該資料來保護該資料。當加密資料以供儲存在該記憶體位址中時，該記憶體位址在第一多個區塊密碼回合中被加密。使用來自第一多個區塊密碼回合的資訊來產生資料回合密鑰。把要被儲存的資料與經加密記憶體位址相組合併且在第二多個區塊密碼回合中藉由使用這些資料回合密鑰來加密。經加密資料隨後被儲存在該記憶體位置中。當解密資料時，記憶體位址如之前般被再次加密，而經加密的儲存資料在第二多個區塊密碼回合中藉由使用資料回合密鑰來解密以獲得經部分解密的資料。把經部分解密的資料與經加密記憶體位址相組合以獲得完全解密的資料。

在記憶體位址中資料加密的一個示例中，該記憶體位址是在第一多個區塊密碼回合中被加密的。加密記憶體位址可包括：(a)根據第一變換函數變換該記憶體位址，(b)將經變換的記憶體位址與回合密鑰混合，(c)將記憶體位址分段，及/或(d)對不同的記憶體位址片段執行位元替換。記憶體位址可能在資料被儲存之前就可用。因此，加密記憶體位址可在資

料可用之前開始。

資料回合密鑰可藉由使用來自第一多個區塊密碼回合中的一回合或更多回合的資訊來產生。產生資料回合密鑰可包括：(a)從關於第一多個區塊密碼回合中的至少一些回合的經加密記憶體位址提取多個位元，(b)從提取出的多個位元的片段選擇資料回合密鑰，及/或(c)將提取出的多個位元級聯到字串中，這些資料回合密鑰從該字串中選擇。

資料可與第一多個區塊密碼回合之後的經加密記憶體位址相組合。例如，可藉由可逆操作（例如，模加/模減、逐位元 XOR 運算等）使資料與經加密記憶體位址相組合。資料可隨後在第二多個區塊密碼回合中藉由使用這些資料回合密鑰來加密。第二多個區塊密碼回合多於第一多個區塊密碼回合。加密資料可包括：(a)根據第二變換函數變換資料，(b)將經變換的資料與這些資料回合密鑰中的一或多個混合，(c)將資料分段成多個資料片段，及/或(d)對不同的資料片段執行位元替換。

記憶體位址可在第一多個區塊密碼回合上被疊代地加密，並且資料可在第二多個區塊密碼回合上被疊代地加密。在一個示例中，用於第二多個區塊密碼回合中較早回合的資料回合密鑰可使用來自源於第一多個區塊密碼回合中較晚回合的經加密記憶體位址的位元來產生。經加密資料可隨後被儲存在該記憶體位址中。

在解密記憶體位址中的資料的另一個示例中，該記憶體位址在第一多個區塊密碼回合中被加密以獲得經加密記憶

體位址。加密記憶體位址可在資料可用之前開始。

加密記憶體位址可包括：(a)根據第一變換函數變換記憶體位址，(b)將經變換的記憶體位址與回合密鑰混合，(c)將記憶體位址分段，及/或(d)對不同的記憶體位址片段執行位元替換。

資料回合密鑰可藉由使用來自第一多個區塊密碼回合中的一回合或更多回合的資訊來產生。產生資料回合密鑰可包括：(a)從關於第一多個區塊密碼回合中的至少一些回合的經加密記憶體位址提取多個位元，(b)從提取出的多個位元的片段選擇這些資料回合密鑰，及/或將提取出的多個位元級聯到字串中，這些資料回合密鑰從該字串中選擇。

經加密資料可從該記憶體位址取回。經加密資料可在第二多個區塊密碼回合中藉由使用這些資料回合密鑰來解密以獲得經部分解密的資料。解密經加密資料可包括：(a)根據第二逆變換函數變換經加密資料，(b)將變換後的經加密資料與這些資料回合密鑰中的一或多個混合，(c)將經加密資料分段成多個經加密資料片段，及/或(d)對不同的經加密資料片段執行位元替換。

可將經部分解密的資料與經加密記憶體位址相組合以獲得完全解密的資料。在一個示例中，可藉由可逆操作（例如，模加/模減、逐位元 XOR 運算等）使經部分解密的資料與經加密記憶體位址相組合。用於第二多個區塊密碼回合中較早回合的資料回合密鑰是藉由使用來自源於第一多個區塊密碼回合中較早回合的經加密記憶體位址的位元來產生的。第

二多個區塊密碼回合多於第一多個區塊密碼回合。第一多個區塊密碼回合可與第二多個區塊密碼回合並發地執行。

這些方法可在硬體、軟體、及/或其組合中實現。

【實施方式】

在以下說明中，提供了具體細節以提供對諸實施例的透徹理解。但是，本領域一般技藝人士將可理解，沒有這些具體細節也可實踐這些實施例。例如，電路可能以方塊圖形式示出，也可能根本不被示出，以免使這些實施例被不必要的細節混淆。在其他實例中，公知的電路、結構和技術可能不被具體示出以免混淆這些實施例。

綜述

若干新穎特徵解決了因使用區塊密碼術來向/從記憶體寫入和讀取受保護資料所引起的等待時間。一般而言，讀取操作要比寫入操作多許多。在現有技術中，加密和解密操作在資料於內部匯流排上可用（寫入）或者已從記憶體取回（讀取）之後才開始。但是在典型的硬體設計中，位址資訊遠在資料之前就可用，在讀取記憶體的情形中尤其如此。

圖 1 是圖示藉由在明文輸入區塊可用之前先部分處理區塊密碼術藉此減少區塊密碼術的等待時間來改善區塊密碼術加密處理的第一特徵的方塊圖。此加密程序可作爲記憶體寫入操作的一部分來執行並且包括在其中記憶體位址 A 106

被加密的位址階段 102 以及在其中資料被加密的資料階段 104。使用記憶體位址 A 106 和用於區塊密碼術 100 的機密密鑰 108 來預處理疊代區塊密碼術的數個密碼回合。明文資料 112 在若干回合區塊密碼術加密之後被插入 110（例如，與位址階段 102 的結果逐位元 XOR）。具體而言，區塊密碼術 100 的一些回合（即，位址階段回合 102）在明文資料 112 被引入之前執行，而一些回合（即，資料階段回合 104）在明文資料 112 被引入之後執行以產生密文 114。位址階段 102 可以不僅加密記憶體位址 A 106 還可使用那些回合的結果來產生用於後續資料階段回合 104 的加密密鑰（即，密鑰排程）。在明文資料 112 被引入之前和之後所進行的密碼回合的數目可以相同或不同。此加密程序利用了記憶體位址 A 106 在明文資料 112 之前就可用這一事實來減少在加密要被儲存至記憶體中的資料時的等待時間。

補充地，可爲區塊密碼術執行更高效率的密鑰排程。用於區塊密碼術的每一回合的回合密鑰可在實際明文資料可用之前基於位址資料和機密密鑰來產生。因爲這些回合密鑰是基於記憶體位址產生的，所以這意味著區塊密碼術變換對於每個記憶體位址而言均將是不同的，藉此嚴格地約束對密碼術分析可用的資源並且增加了該區塊密碼術的安全性。

圖 2 是圖示藉由將區塊密碼術的第一部分與區塊密碼術的第二部分並行處理藉此減少區塊密碼術的等待時間來改善區塊密碼術解密的第二特徵的方塊圖。此解密程序可作爲記憶體讀取操作的一部分來執行並且包括在其中記憶體位

址 A 206 被加密的位址階段 202 以及在其中資料被解密的資料階段 204。不是如在一般解密方法中般逆向地運行整個區塊密碼術，而是從密文 214 開始逆向地處理區塊密碼密碼術 200 的資料階段 204。與此同時，藉由將記憶體位址 A 206 和密鑰 208 用作輸入來前向地運行區塊密碼術 200 的位址階段 202。當這些程序在中間 210 相遇時，藉由對經部分解密的密文與經部分加密的記憶體位址進行 XOR 來推導明文資料 212。

使用區塊密碼術的高效率加密

圖 3 是圖示配置成加密要被儲存在記憶體中的資料的區塊密碼術的示例的方塊圖。在此程序中，記憶體位址 A 304 可能在要被儲存的資料區塊（即，明文 320）可用之前就可用。當資料（明文 320）被存入記憶體時，可採用疊代區塊密碼術 302 來加密該資料例如，CPU 可在將資料發送給記憶體設備以供儲存之前先加密該資料。在此示例中，區塊密碼術 302 可包括密鑰排程和位址加密階段 303 以及資料加密階段 305。

在密鑰排程和位址加密階段 303 中，使用記憶體位址 A 304 和用於區塊密碼術的機密密鑰 $K_{機密}$ 306 來預處理該疊代區塊密碼術的數個回合。例如，在實際明文資料區塊 P 320 可用之前，先基於機密密鑰 $K_{機密}$ 306 來產生用於區塊密碼術 302 的相應位址加密回合 316、317 和 318 的多個回合密鑰 K1 307、K2 308 和 Ki 309。每個回合密鑰 K1 307、K2 308

和 Ki 309 可基於在前的回合密鑰（例如，K1 基於 $K_{機密}$，K2 基於 K1，依此類推）來推導。根據一個示例，機密密鑰 306 可以是 w 位元長並且每個回合密鑰 K1、K2 和 Ki 是 n 位元長，其中 n<w。每個回合密鑰 K1、K2 和 Ki 是藉由從機密密鑰取毗連的 n 個位元來產生的，其中機密密鑰 306 被認爲在末端捲繞。每個回合密鑰 K1、K2 和 Ki 可使用機密密鑰 306 不同群組的毗連位元序列。

區塊密碼術 302 的多個位址加密回合 316、317 和 318 可基於記憶體位址 304 和相應的回合密鑰 K1 307、K2 308 和 Ki 309 來產生。例如，第 1 回合 316 使用第一線性及/或非線性函數 E_a 來變換記憶體位址 A 304 的全部或部分，並且基於與密鑰 K1 的可逆操作（例如，模加/模減、逐位元 XOR 運算等）來對其進行進一步變換（例如，$R1 = E_a(A) \oplus K1$）。類似地，第 2 回合 317 使用第一線性及/或非線性函數 E_a 來變換第 1 回合 316 的結果 R1 並且基於與相應密鑰 K2 的可逆操作（例如，逐位元 XOR 運算）來進一步變換該結果（例如，$R2 = E_a(R1) \oplus K2$）。此程序可被重複多次以將每個變換操作的效果擴散到整個區塊。例如，第 i 回合 318 使用第一線性及/或非線性函數 E_a 來變換在前回合的結果 Ri -1 並且基於與相應密鑰 Ki 的可逆操作（例如，逐位元 XOR 運算等）來進一步變換該結果（例如，$Ri = E_a(Ri -1) \oplus Ki$）。注意，這些第一區塊密碼回合 303（記憶體位址加密階段）甚至可以在資料可供在資料加密階段 305 中加密用之前就被（至少部分地）執行。藉由在明文資料區塊 P 320 可用之前部分處理

（或預處理）區塊密碼術，區塊密碼術中的等待時間（即，延遲）可得以減少。

補充地，在密鑰排程階段 303 期間，可產生用於資料加密階段 305 的密鑰 312、314 和 315 以節約時間。資料加密階段 305 密鑰 Ky、Ky+1 和 Kx 可基於位址加密階段 303 的每個密碼回合結果 R1、R2、Ri 的結果來產生。在一個示例中，回合結果 R1、R2 和 Ri 可以是 n 位元長（其中 n 是正整數）並且來自這些回合中的至少多回合的數個位元 g 被用來產生資料加密階段密鑰 Ky、Ky+1 和 Kx，其中 g 是小於 n 的整數。例如，位元集 S 310 可藉由級聯（符號 ||）從各回合結果 R1、R2、Ri 提取出的位元以使得 $S_{1...p} = R1_{1...g1} || R2_{1...g2} ... || Ri_{1...gi}$ 來獲得，其中 p 是圖示該位元集 S 310 中總位元數的整數值。注意，在一些實現中，用於每一回合的位元數 g1、g2、...、gi 可以是相同的，而在其他實現中，位元數 g1、g2、...、gi 可以是不同的。在密鑰排程階段 303 期間，資料加密階段密鑰 Ky、Ky+1 和 Kx 可藉由爲每個密鑰從位元集 S 310 提取位元片段來產生。在一個示例中，對應於密鑰排程和位址加密階段 303 中那些較晚密碼回合的位元可被用於資料加密階段 305 中那些較早的密鑰。例如，密鑰 Ky 312 可從位元集 S 310 的位元 $S_{(p-j+1)...p}$ 取得，這些位元 $S_{(p-j+1)...p}$ 在此示例中對應於來自 $Ri_{1...g}$ 的位元的子集，其中 $j<g$（對於 g = g1, g2, ... , gi）。類似地，密鑰 Ky+1 314 可以等於位元集 S 310 的位元 $S_{(p-2j+1)...(p-j)}$ 且密鑰 Kx 可以等於位元集 S 310 的位元 $S_{1...j}$。在一些實現中，在 $j<g$ 的場合，

密鑰排程階段 303 中回合的數目可以小於資料階段 305 中回合的數目。例如，在回合結果 R1、R2 和 Ri 是 63 位元長（即，n=63）的場合，可以從每一回合提取 45 個位元（即，g=45）以用於位元集 S 310 並且每個資料階段密鑰 Ky 312、Ky+1 314 和 Kx 315 可以是 32 位元長（即，j=32）。

一般意義下，可以使用一或多個回合密鑰函數 KSx 來產生回合密鑰 K1、K2、Ki、Ky、Ky+1 ... Kx 中的每一個。在一個示例中，第一密鑰排程函數 KS1 可被用來產生（用於位址加密階段的）密鑰 K1、K2、Ki 並且第二密鑰排程函數 KS2 可被用來產生（用於資料加密階段的）密鑰 Ky、Ky+1、Kx。例如，第一密鑰排程函數 KS1 可被用來產生密鑰 Ki，以使得 $Ki=KS1(K_{\text{機密}}, i)$，其中「i」是位址加密階段 303 的回合號，而第二密鑰排程函數 KS2 可被用來產生密鑰 Ky+i，以使得 $Ky+i=KS2(S_{1...p}, i)$，其中「y+i」是資料加密階段 305 的回合號。

當明文資料區塊 P 320 變成可用時，其可在區塊密碼術 302 中的一回合或更多回合 316、317 和 318 已被執行之後（例如，在密鑰排程階段 303 之後）被插入區塊密碼術 302。明文資料區塊 P 320 可在通常被稱爲*白化*的程序中藉由使其（在逐位元的基礎上）與最新近被預處理的回合（即，第 i 回合 318）的結果 Ri 進行 XOR 來插入區塊密碼術 302 中。在明文資料區塊 P 320 已被引入之後，使用相應的回合密鑰 Ky 312、Ky+1 314 以及 Kx 315 來執行資料加密階段 305 中的一回合或更多回合 332、324 和 326。

在資料加密階段 305 期間第 y 回合 322 處，由第二線性及/或非線性函數 E_b 來變換經白化的資料區塊 $D_{白化}$ 321 並且基於與相應回合密鑰 Ky 的可逆操作（例如，逐位元 XOR 運算）對其進行進一步變換（例如，$Ry = E_b(D_{白化}) \oplus Ky$）。類似地，在第 y+1 回合 324 處，使用第二線性及/或非線性函數 E_b 來變換第 y 回合 322 的結果 Ry 並且基於與相應密鑰 Ky+1 的可逆操作（例如，模加/模減、逐位元 XOR 運算等）來進一步變換該結果（例如，$Ry+1 = E_b(Ry) \oplus Ky+1$）。此程序可被重複多次以將每個變換操作的效果擴散到整個區塊。例如，第 x 回合 326 使用第二線性及/或非線性函數 E_b 來變換在前回合的結果 Rx-1 並且基於與相應密鑰 Kx 的可逆操作（例如，逐位元 XOR 運算等）來進一步變換該結果（例如，$Rx = E_b(Rx-1) \oplus Kx$）以獲得密文 328。

在各種實現中，密鑰排程和位址加密階段 303 以及資料加密階段 305 的回合的數目可以相同或不同。在資料解密階段 305 期間回合的數目可被選擇成減少區塊密碼術 302 的等待時間同時引入向明文資料區塊 P 320 提供充足的擴散以減少區塊密碼術 302 的等待時間。

圖 4 是圖示配置成加密明文資料的區塊密碼術設備的功能性元件的方塊圖。區塊密碼術設備 402 可基於明文資料 404 要被儲存至的記憶體位址 406 以及機密密鑰 408 來加密該明文資料 404。區塊密碼術設備 402 可包括位址加密模組 412，其根據變換或加密函數以及由回合密鑰產生器 416 提供的密鑰來變換及/或加密此記憶體位址 406。回合密鑰產生器 416

可被配置成基於機密密鑰 408 來產生一或多個回合密鑰。密鑰排程模組 414 也可基於位址加密模組 412 的結果產生一或多個資料密鑰。該一或多個資料密鑰可被儲存在資料密鑰儲存 422 模組中。可在多回合中藉由在每一回合中使用來自回合密鑰產生器 416 的不同回合密鑰來疊代地執行位址加密和資料排程功能。在多回合之後，組合器 418 可使用可逆操作（例如，模加/模減、逐位元 XOR 等）將明文資料 404 與位址加密模組 412 的最後結果相組合。結果得到的經白化的明文資料可隨後由資料加密模組 420 在一回合或更多回合中藉由使用來自資料密鑰儲存 422 的儲存著的資料密鑰以及變換或加密函數來疊代地變換或加密以產生密文 424。密文 424 可隨後被儲存在記憶體設備 426 中該記憶體位址 406 處。

根據一個示例，該區塊密碼術設備可被實現在具有位元組可定址記憶體的系統中。例如，實現該區塊密碼術的 CPU 的字長可以是 32 位元，並且記憶體位址也可以是 32 位元。如先前所提及的，該區塊密碼術設備可被配置成執行位址加密階段和資料加密階段。

圖 5 是圖示記憶體位址加密或變換模組的一個示例的方塊圖。在位址加密階段 502 期間，可藉由運行多個替換--置換密碼回合來變換輸入記憶體位址（被填充到 64 位元）。可隨意任選地，輸入記憶體位址 504 可首先藉由與回合密鑰進行 XOR 來白化。位址分段模組 506 可將 64 位元記憶體位址 504 劃分成 8 個 8 位元片段。每個 8 位元片段隨後藉由 8×8 替換單元 508（例如，高級加密標準（AES）8×8 替換單元）。

來自每個替換單元 508 的結果可隨後被傳遞給變換模組 510，後者對分段的全集執行線性變換。該線性變換可例如用矩陣乘法 $Y=CX$ 來實現，其中 X 是記憶體位址向量，C 是變換矩陣，而 Y 是輸出向量。在一個示例中，變換矩陣 C 可以是 $GF(2^8)$（GF：伽羅瓦域）上如具有分支號 9 的最大距離可分（MDS）映射的 8×8 矩陣。矩陣 C 在當且僅當其所有子矩陣都非奇異時可以是 MDS 的。區塊密碼術中的許多擴散層（例如，SHARK 和 Khazad）可以達到此要求。密鑰混合模組 512 隨後將經變換的記憶體位址與 64 位元回合密鑰混合（例如，使用逐位元 XOR）。對於每一密碼回合，資料回合密鑰提取模組 514 可隨後從過渡期的經加密記憶體位址提取多個位元以獲得可在後續資料加密程序中使用的一或多個資料回合密鑰 518。這些密碼回合（例如，包括分段 506、S-單元層 508、變換 510 以及密鑰混合 512）中的多回合可用在每一密碼回合結束時執行資料回合密鑰提取 514 的方式來執行。

圖 6 是圖示明文資料加密或變換模組的一個示例的方塊圖。在資料加密階段 602 期間，明文資料 604 可首先由逐位元 XOR 模組 605 用來自位址加密階段的經加密記憶體位址 603 來白化。經加密記憶體位址 603 可對應於經加密明文資料要被儲存至的記憶體位址。例如，如果明文資料 604 是以 32 位元的區塊來處理的，那麼可將該明文資料 604 與來自記憶體位址階段的輸出中的 32 位元進行 XOR。用於資料加密階段的回合密鑰可以從記憶體位址加密階段推導。資料分段

模組 606 將明文資料 604 劃分或拆分成四個 8 位元片段。每個 8 位元片段藉由替換單元 608(例如，AES 8×8 替換單元)。來自替換單元 608 的結果隨後由線性變換模組 610 來變換（例如，AES MDS 映射）。密鑰混合模組 612 可隨後將結果得到的經變換明文資料與相應的回合密鑰進行逐位元 XOR。此程序可藉由對每一回合使用不同的回合密鑰來重複多次。資料加密階段 602 的最末密碼回合的結果是輸出密文 614，該輸出密文 614 能被儲存至在相應的位址加密階段期間使用的記憶體位址中。

圖 7 圖示使用要儲存資料的記憶體位址來加密該資料的區塊密碼術資料加密方法。在此方法中，執行密碼回合的第一集合以在資料實際上就緒或可供儲存之前就加密記憶體位址並產生資料回合密鑰。隨後，執行密碼回合的第二集合以加密該資料。

處理器可在資料實際上被接收到之前就獲得關於要被儲存的資料的記憶體位址 702。記憶體位址可在第一多個區塊密碼回合中被加密 704。這樣的記憶體位址加密可包括：(a)將記憶體位址分段成多個記憶體位址片段，(b)對不同的記憶體位址片段執行位元替換，(c)根據第一變換函數變換記憶體位址，及/或(d)將經變換的記憶體位址與回合密鑰混合。記憶體位址可在第一多個區塊密碼回合上被疊代地加密。

資料回合密鑰可藉由使用來自第一多個區塊密碼回合中的一回合或更多回合的資訊來產生 706。資料回合密鑰可如下來產生：(a)從關於第一多個區塊密碼回合中的至少一些回

合的經加密記憶體位址提取多個位元，(b)從提取出的多個位元的片段選擇資料回合密鑰，及/或(c)將提取出的多個位元級聯到字串中，這些資料回合密鑰從該字串中選擇。

要被儲存的資料可隨後在第一多個區塊密碼回合之後與經加密記憶體位址相組合 708。在一個示例中，可藉由可逆操作（例如，逐位元 XOR 運算）使資料與經加密記憶體位址相組合。資料可隨後在第二多個區塊密碼回合中藉由使用這些資料回合密鑰來加密 710。這樣的資料加密可包括：(a)將資料分段成多個資料分段，(b)對不同的資料分段執行位元替換，(c)根據第二變換函數來變換資料，及/或(d)將經變換的資料與這些資料回合密鑰中的一或多個混合。資料可在第二多個區塊密碼回合上被疊代地加密。在一個示例中，使用來自源於第一多個區塊密碼回合中較晚回合的經加密記憶體位址的位元來產生用於第二多個區塊密碼回合中較早回合的資料回合密鑰。第二多個區塊密碼回合可以多於第一多個區塊密碼回合。經加密資料可隨後被儲存在該記憶體位址中 712。

使用區塊密碼術的高效率解密

圖 8 是圖示區塊密碼術解密從記憶體位址讀取的資料的處理的方塊圖。資料可以在先前已使用例如圖 1 和 3-7 中所圖示的方法被加密。在解密模式中，不是如在一般解密方法中般逆向地運行整個區塊密碼術，而是從密文 828 開始逆向地處理區塊密碼術 802 的第二階段 805 同時並發地前向執行

第一階段 803。一般而言，將區塊密碼回合的第一集合 803 與區塊密碼回合的第二集合 805 並行地執行，藉此減少區塊密碼術 802 的等待時間。即，這些第一區塊密碼回合 803（記憶體位址加密階段）甚至可以在經加密資料可用或被取回以供由這些第二區塊密碼回合 805 處理之前就被（至少部分地）執行。在密鑰排程和位址加密階段 803 中，記憶體位址 804（密文資料 828 即從該記憶體位址 804 取回）在多個密碼回合中被加密。同時，在資料解密階段 805 中，在多個密碼回合中使用在密鑰排程階段 803 中產生的資料回合密鑰來解密密文資料 828。來自這兩個階段 803 和 805 的結果隨後被組合（例如，XOR）以產生原始的明文 820。

在密鑰排程和位址加密階段 803 中，從中取回密文資料 828 的記憶體位址 804 被加密。使用記憶體位址 A 804 和用於區塊密碼術 802 的機密密鑰 $K_{機密}$ 806 來處理疊代區塊密碼術 802 的數個回合。例如，基於機密密鑰 $K_{機密}$ 806 來產生用於區塊密碼術 802 的相應位址加密回合 816、817 和 818 的多個回合密鑰 K1 807、K2 808 和 Ki 809。每個回合密鑰 K1 807、K2 808 和 Ki 809 可基於先前回合密鑰（例如，K1 基於 $K_{機密}$，K2 基於 K1，依此類推）來推導。根據一個示例，機密密鑰 806 可以是 w 位元長並且每個回合密鑰 K1、K2 和 Ki 是 n 位元長，其中 n<w。每個回合密鑰 K1、K2 和 Ki 是藉由從機密密鑰 806 取毗連的 n 位元來產生的，其中機密密鑰 806 被認爲在末端捲繞。每個回合密鑰 K1、K2 和 Ki 可使用機密密鑰 806 的不同群組的毗連位元序列。

區塊密碼術 802 的多個位址加密回合 816、817 和 818 是基於記憶體位址 804 和相應回合密鑰 K1 807、K2 808 和 Ki 809 來產生的。例如，第 1 回合 816 使用第一線性及/或非線性函數 E_a 來變換記憶體位址 A 804 的全部或部分並且基於與密鑰 K1 的可逆操作（例如，模加/模減、逐位元 XOR 等）來對其進行進一步變換（例如，$R1 = E_a(A) \oplus K1$）。類似地，第 2 回合 817 使用第一線性及/或非線性函數 E_a 來變換第 1 回合 816 的結果 R1 並且基於與相應密鑰 K2 的逐位元 XOR 來進一步變換該結果（例如，$R2 = E_a(R1) \oplus K2$）。此程序可被重複多次以將每個變換操作的效果擴散到整個區塊。例如，第 i 回合 818 使用第一線性及/或非線性函數 E_a 來變換先前回合的結果 Ri-1 並且基於與相應密鑰 Ki 的逐位元 XOR 來進一步變換該結果（例如，$Ri = E_a(Ri-1) \oplus Ki$）。

補充地，在密鑰排程階段 803 期間，可產生用於資料解密階段 805 的密鑰 812、814 和 815 以節約時間。資料解密階段 805 密鑰 Ky、Ky+1 和 Kx 可基於密鑰排程階段密鑰 K1、K2 和 Ki 來產生。在一個示例中，密碼回合結果 R1、R2 和 Ri 可以是 n 位元長（其中 n 是正整數）並且來自這些密鑰中的每一個的數個位元 g 被用來產生資料階段密鑰 Ky、Ky+1 和 Kx，其中 g 是小於 n 的整數。例如，位元集 S 810 可藉由級聯（符號 ||）從各個回合結果 R1、R2、Ri 提取出的位元以使得 $S_{1...p} = R1_{1...g1} || R2_{1...g2} ... || Ri_{1...gi}$ 來產生，其中 p 是圖示位元集 S 810 中總位元數的整數值。注意，在一些實現中，用於每一回合的位元數 g1、g2、...、gi 可以是相同的，

而在其他實現中，位元數 g1、g2、...、gi 可以是不同的。在密鑰排程階段 803 期間，資料加密階段密鑰 Ky、Ky+1 和 Kx 可藉由爲每個密鑰從位元集 S 810 提取位元片段來產生。

在一個示例中，對應於密鑰排程階段 803 中那些較早回合的位元可被用於資料解密階段 805 中那些較早的密碼回合密鑰。這允許與位址加密階段 803 並發或並行地執行資料解密階段 805。例如，密鑰 Kx 815 可以等於位元集 S 810 的位元 $S_{1...j}$，這些位元 $S_{1...j}$ 對應於從第一密碼回合 $R1_{1...g1}$ 816 提取出的位元中的一些。因此，一旦 R1 結果被產生，就能獲得解密密鑰 Kx 815。類似地，密鑰 Ky+1 314 可以等於位元集 S 310 的位元 $S_{(p-2j+1)...(p-j)}$。同樣，密鑰 Ky 814 可從位元集 S 810 的位元 $S_{(p-j+1)...p}$ 取得，這些位元 $S_{(p-j+1)...p}$ 在此示例中對應於來自 $Ri_{1...g}$ 的位元的子集，其中 j<g。在一些實現中，在 j<g 的場合，密鑰排程階段 803 中密碼回合的數目可以小於資料解密階段 805 中回合的數目。例如，當回合結果 R1、R2 和 Ri 是 63 位元長（即，n=63）時，可以從每一回合提取 45 個位元（即，g=45）以用於位元集 S 310，並且每個資料解密階段密鑰 Kx 815、Ky+1 814 和 Ky 812 可以是 32 位元長（即，j=32）。

一般而言，可使用一或多個回合密鑰函數 KSx 來產生回合密鑰 K1、K2、Ki、Ky、Ky+1 ... Kx 中的每一個。在一個示例中，可使用第一密鑰排程函數 KS1 來產生（用於位址加密階段的）密鑰 K1、K2、Ki 並且可使用第二密鑰排程函數 KS2 來產生（用於資料解密階段的）密鑰 Ky、Ky+1、Kx。

例如，第一密鑰排程函數 KS1 可被用來產生密鑰 Ki，以使得 $Ki=KS1(K_{機密}, i)$，其中「i」是位址加密階段 803 的回合號，而第二密鑰排程函數 KS2 可被用來產生密鑰 Ky+i，以使得 $Ky+i=KS2(S_{1...p}, i)$，其中「y+i」是資料解密階段 805 的回合號。

在資料解密階段期間，使用密鑰 Kx、Ky+1 和 Ky 在多個回合上解密密文資料（ct）828。例如，第 x 回合 826 使用線性及/或非線性解密函數 D_b 來變換結果密文（ct）828 並且基於與相應密鑰 Kx 的操作（例如，可逆模加/模減、逐位元 XOR 等）來進一步變換該結果（例如，$Rx = D_b(ct) \oplus Kx$）以獲得結果 Rx。此解密程序可被重複多次以撤銷對儲存著的資料的加密。例如，在第 y+1 回合 824 處使用線性及/或非線性解密函數 D_b 來變換來自先前回合的結果 Ry+1 並且基於與相應密鑰 Ky+1 的逐位元 XOR 來進一步變換該結果（例如，$Ry = D_b(Ry+1) \oplus Ky+1$）以獲得輸出 Ry。在第 y 回合 822 處，結果 Ry 由線性及/或非線性解密函數 D_b 變換並且基於與相應回合密鑰 Ky 的逐位元 XOR 被進一步變換（例如，$D_{白化} = D_b(Ry) \oplus Ky$）以獲得經白化的資料區塊 $D_{白化}$ 821。隨後，使用可逆操作（例如，模加/模減，逐位元 XOR 等）將經白化的資料區塊 $D_{白化}$ 與來自位址加密階段 803 的結果 Ri（例如，經加密位址）相組合以獲得明文資料區塊 P 820。

在各種實現中，密鑰排程和位址加密階段 803 以及資料解密階段 805 的回合的數目可以相同或不同。在資料解密階段 805 中使用的解密函數 D_b 可被選擇成撤銷由在資料加密

階段 305（圖 3）中使用的加密函數 E_b 所作的加密。例如，解密函數 D_b 可以是加密函數 E_b 變換的逆變換。

圖 9 是圖示配置成解密密文資料的區塊密碼術設備的功能性元件的方塊圖。區塊密碼術設備 902 可包括位址加密模組 912，其根據變換或加密函數以及由回合密鑰產生器 916 提供的密鑰來變換及/或加密記憶體位址 906。注意，記憶體位址 906 可以是從記憶體設備 926 中取回密文資料 924 的位置。回合密鑰產生器 916 可被配置成基於機密密鑰 908 來產生一或多個回合密鑰。密鑰排程模組 914 也可基於位址變換模組 912 的結果產生一或多個資料密鑰。該一或多個資料密鑰可被儲存在資料密鑰儲存 922 模組中。可在多個回合中藉由在每一回合中使用來自回合密鑰產生器 916 的不同回合密鑰來疊代地執行位址加密和資料排程功能。並發地或並行地，密文資料 924 可由資料解密模組 920 在一回合或更多回合中藉由使用來自資料密鑰儲存 922 的儲存著的資料密鑰及/或變換或解密函數來疊代地變換或解密以產生經白化的明文資料。在多個解密回合之後，組合器 918 可使用可逆操作（例如，模加/模減，逐位元 XOR 等）將資料解密模組 920 的最後結果（經白化的明文資料）與位址加密模組 912 的最後結果相組合以獲得明文資料 904。

注意，在位址加密模組 912 中，記憶體位址可如由區塊密碼術設備在加密模式中所作般被加密。例如，位址加密模組 912 可包括如圖 5 中所圖示的多個替換--置換密碼回合。

圖 10 是圖示密文資料解密或逆變換模組的一個示例的方

塊圖。例如，此密文資料解密或逆變換模組 1002 可作爲資料解密模組 920(圖 9)的一部分被包括。密鑰混合模組 1012 可在輸入密文 1014 與相應的密碼回合密鑰之間執行逐位元 XOR 運算。用於資料解密階段的密碼回合密鑰可以從記憶體位址加密階段推導。來自密鑰混合模組 1012 的結果隨後由線性逆變換模組 1010(例如，AES MDS 映射)來變換。來自線性逆變換模組 1010 的結果隨後由資料分段模組 1009 分段成多個 8 位元資料片段。隨後使該多個 8 位元資料片段藉由替換單元 1008(例如，AES 8×8 替換單元)。替換單元 1008 可逆反資料加密替換單元 608(圖 6)的那些替換單元。

資料組合器模組 1006 可組合來自替換單元 1008 的結果得到的輸出以產生輸出白化明文資料。此程序可藉由對每一回合使用不同的回合密鑰來重複多次。資料加密階段 1002 的最末密碼回合的結果是經白化的明文資料。隨後，由逐位元 XOR 模組 1005 將經白化的明文資料與經加密記憶體位址 1003 相組合以產生輸出明文資料 1004。注意，經加密記憶體位址 1003 可對應於從中取回此輸入密文資料 1014 的記憶體位址。

圖 11 圖示用於藉由使用在解密經加密資料的同時並發地加密記憶體位址以減少區塊密碼術的等待時間的區塊密碼術來解密經加密資料的方法。獲得關於要被取回的經加密資料的記憶體位址 1102。該記憶體位址在第一多個區塊密碼回合中被加密以獲得經加密記憶體位址 1104。這樣的位址加密可利用基於機密密鑰產生的多個回合密鑰。補充地，加密記

憶體位址可包括(a)將經變換的記憶體位址與回合密鑰混合，(b)根據第一變換函數變換記憶體位址，(c)將記憶體位址分段，及/或(d)對不同的記憶體位址片段執行位元替換。

資料回合密鑰也可藉由使用來自第一多個區塊密碼回合中的一回合或更多回合的資訊來產生1106。即，來自第一多個區塊密碼回合中的至少一些回合的經部分加密的記憶體位址可被用來產生這些資料回合密鑰。例如，產生資料回合密鑰可包括(a)從關於第一多個區塊密碼回合中的至少一些回合的經加密記憶體位址提取多個位元，(b)從提取出的多個位元的片段選擇這些資料回合密鑰，及/或(c)將提取出的多個位元級聯到字串中，這些資料回合密鑰從該字串中選擇。

經加密資料可從記憶體位址取回1108並且在第二多個區塊密碼回合中藉由使用這些資料回合密鑰來解密以獲得經部分解密的資料1110。用於第二多個區塊密碼回合中較早回合的資料回合密鑰可使用來自源於第一多個區塊密碼回合中那些較早回合得到的經加密記憶體位址的位元來產生。在一個示例中，解密經加密資料可包括(a)將變換後的經加密資料與這些資料回合密鑰中的一或多個混合，(b)根據第二逆變換函數來變換經加密資料，(c)將經加密資料分段成多個經加密資料片段，及/或(d)對不同的經加密資料片段執行位元替換。可將經部分解密的資料與經加密記憶體位址相組合以獲得完全解密的資料1112。在一個示例中，藉由可逆操作（例如，逐位元XOR運算）使經部分解密的資料與經加密記憶體位址相組合。

第一多個區塊密碼回合可與第二多個區塊密碼回合並發地執行，藉此加速解密程序。另外，第二多個區塊密碼回合可以多於第一多個區塊密碼回合。

用於區塊密碼術的高效率密鑰排程

根據一個特徵，可執行密鑰排程從而高效率地加密和解密資料。在位址加密階段期間，多個密碼回合可被疊代地執行以加密記憶體位址，其中記憶體位址是資料要被儲存或者要從中取回資料的位置。每個密碼回合產生經加密記憶體位址。由這些密碼回合中的一回合或更多回合產生的經加密記憶體位址可被（完全或部分地）用來產生資料加密/解密階段回合密鑰。

圖 12 是圖示如何可基於來自區塊密碼術的位址加密回合的結果來產生用於資料加密和解密回合的回合密鑰的示例的方塊圖。當區塊密碼術在加密資料時，基於位址加密階段 1202 的結果來產生資料回合密鑰。位址加密階段 1202 的較早回合（例如，R1 1206、R2 1208...）的結果被用來產生要在資料加密階段 1204 中使用的較晚資料加密回合密鑰（密鑰-E6 1212、密鑰-E5 1214...）。類似地，位址加密階段 1202 的較晚回合（例如，R3 1210...）的結果被用來產生較早資料加密回合密鑰（密鑰-E1 1222、密鑰-E2 1220...）。

類似地，當區塊密碼術在解密資料時，基於位址加密階段 1202 的結果來產生資料回合密鑰。位址加密階段 1202 的較早回合（例如，R1 1206、R2 1208...）的結果被用來產生

要在資料解密階段 1224 中使用的較早資料加密回合密鑰(密鑰-D1 1226、密鑰-D2 1228...)。類似地，位址加密階段 1202 的較晚回合（例如，R3 1210...）的結果被用來產生較晚資料解密回合密鑰（密鑰-D6 1236、密鑰-D5 1234...）。因此，這允許資料解密階段 1224 與位址加密階段 1202 並發地（例如，在時間段上交疊或者並行地）執行，從而更高效率地解密資料。

注意到在各種實現中，位址加密階段、資料加密階段 1204 及/或資料解密階段 1224 的密碼回合的數目可以多於或少於此示例中所示的那些數目。補充地，根據一個可隨意任選的特徵，可爲明文資料的白化操作保留位址加密階段 1202 的最末回合（例如，R4 1211）的結果的至少某個部分。因此，位址加密階段 1202 的該最末回合（例如，R4 1211）的這個結果不可被用於資料回合密鑰產生。

在一些實現中，資料加密回合密鑰（或資料解密回合密鑰）可基於來自位址加密階段 1202 的一或多個結果（例如，R1 1206、R2 1208...）的位元的子集。例如，密鑰-E1 1222 可基於來自 R3 1210 的位元的子集，而密鑰-E2 可基於來自 R2 1208 和 R3 1210 兩者的位元的子集。

注意，由於記憶體位址由區塊密碼術用來產生用於資料加密/解密階段 1204/1224 的加密/解密密鑰，因而這意味著對於每個記憶體位址而言，明文/密文的區塊密碼術變換將是不同的，從而嚴格地約束對密碼術分析可用的資源並且增加了區塊密碼術的安全性。應注意，較早的回合未必要與較晚的

回合具有相同的區塊大小。例如，記憶體要以 32 位元的區塊來加密而位址可能大於 32 位元是相當可能的。經由這些第一回合中的並行化可獲得效率增益。

根據區塊密碼術的一個示例，資料加密/解密可以是位元組可定址記憶體。具體而言，執行區塊密碼術的處理器的字（資料區塊）是 32 位元，並且位址也是 32 位元。來自位址加密階段的結果的最後 32 位元可被用作白化密鑰。來自位址加密結果（例如，經加密記憶體位址）的其餘位元可被級聯到用於資料加密回合密鑰的集合 S 中。可爲每一資料加密回合 n（例如，對於 n=0...5）選擇 32 位元長的資料加密回合密鑰，以使得加密回合密鑰（密鑰-En）=集合 S 的位元 32*(5-n)到 32*(5-n)+31。反之，可爲每一資料解密回合 n（例如，對於 n=0...5）選擇 32 位元長的資料解密回合密鑰，以使得解密回合密鑰（密鑰--Dn）=集合 S 的位元 32*n 到 32*n+31。

圖 13 是圖示可被配置成執行高效率的區塊密碼術加密和解密的設備的方塊圖。處理電路 1302 可耦合至記憶體設備 1306。處理電路 1302 可向/從記憶體設備 1306 寫入和讀取資料。處理電路 1302 可被配置成執行區塊密碼術 1304，該區塊密碼術 1304 加密要被儲存至記憶體設備 1306 的資料/解密要從記憶體設備 1306 取回的資料。這樣的加密和解密可基於資料被寫入或者從中讀取資料的實際記憶體位址。例如，區塊密碼術 1304 可執行圖 1 -12 中描述的操作中的一或多個。

應認識到，一般而言，本案中所描述的絕大多數處理可

以用類似的方式來實現。（諸）電路或電路工段中的任何哪個可單獨或組合實現爲具有一或多個處理器的積體電路的一部分。這些電路中的一或多個可以在積體電路、高階 RISC 機（ARM）處理器、數位信號處理器（DSP）、通用處理器等上實現。

還應注意，這些實施例可能是作爲被圖示爲流程圖、流程圖、結構圖、或方塊圖的程序來描述的。儘管流程圖可能會把諸操作描述爲順序程序，但是這些操作中有許多能夠並行或並發執行。另外，這些操作的次序可以被重新安排。程序在其操作完成時終止。程序可以對應於方法、函數、規程、子常式、副程式等。當程序對應於函數時，其終止對應於該函數返回到調用方函數或主函數。

如在本案中所使用的，術語「元件」、「模組」、「系統」等旨在指示電腦相關實體，任其是硬體、韌體、軟硬體組合、軟體，還是執行中的軟體。例如，元件可以是但不被限定於在處理器上運行的程序、處理器、物件、可執行件、執行的線程、程式、及/或電腦。作爲圖示，在計算設備上運行的應用和該計算設備兩者皆可以是元件。一或多個元件可常駐在程序及/或執行的線程中，且元件可以局部化在一台電腦上及/或分布在兩台或更多台電腦之間。此外，這些元件能從其上儲存著各種資料結構的各種電腦可讀取媒體來執行。各元件可借助於本地及/或遠端來通訊，諸如根據具有一或多個資料封包的信號（例如，來自借助於該信號與本地系統、分散式系統中的另一元件互動、及/或跨諸如網際網路等

網路上與其他系統互動的一個元件的資料）。

不僅如此，儲存媒體可以代表用於儲存資料的一或多個設備，包括唯讀記憶體（ROM）、隨機存取記憶體（RAM）、磁片儲存媒體、光學儲存媒體、快閃記憶體設備、及/或其他用於儲存資訊的機器可讀取媒體。術語「機器可讀取媒體」包括，但不被限定於，可攜式或固定的儲存設備、光學儲存設備、無線通道以及能夠儲存、包含或承載指令及/或資料的各種其他媒體。

此外，諸實施例可以由硬體、軟體、韌體、中介軟體、微代碼、或其任何組合來實現。當在軟體、韌體、中介軟體或微碼中實現時，執行必要任務的程式碼或代碼區段可被儲存在諸如儲存媒體或其他儲存之類的機器可讀取媒體中。處理器可以執行這些必要的任務。代碼區段可表示規程、函數、副程式、程式、常式、子常式、模組、套裝軟體、類，或是指令、資料結構、或程式語句的任何組合。藉由傳遞及/或接收資訊、資料、引數、參數、或記憶體內容，一代碼區段可被耦合到另一代碼區段或硬體電路。資訊、引數、參數、資料等可以經由包括記憶體共享、訊息傳遞、權杖傳遞、網路傳輸等任何合適的手段被傳遞、轉發、或傳輸。

圖 1、2、3、4、5、6、7、8、9、10、11、12、及/或 13 中圖示的元件、步驟、及/或功能之中的一或多個可以被重新安排及/或組合成單個元件、步驟、或功能，或可以實施在數個元件、步驟、或功能中。也可以添加更多的元件、組件、步驟、及/或功能。圖 3、4、8、9 及/或 13 中圖示的裝置、

設備、及/或元件可被配置成執行圖 1、2、5、6、7、10、11 及/或 12 中描述的方法、特徵、或步驟中的一或多個。本文中描述的新穎演算法可以在軟體及/或嵌入式硬體中高效率地實現。

本領域技藝人士將可進一步領會，結合本文中公開的實施例描述的各種圖示性邏輯區塊、模組、電路、和演算法步驟可被實現爲電子硬體、電腦軟體、或兩者的組合。爲清楚地圖示硬體和軟體的這種可互換性，各種圖示性元件、方塊、模組、電路、和步驟在上文中以其功能性的形式進行了一般化描述。這樣的功能性是實現成硬體還是軟體取決於具體應用和加諸整體系統上的設計約束。

這些實施例的描述旨在圖示，而並非旨在限定請求項的範圍。由此，本發明的教導能現成地應用於其他類型的裝置，並且許多替換、改動、和變形對於本領域技藝人士將是明顯的。

【圖式簡單說明】

在結合附圖理解下面闡述的詳細描述時，本發明各態樣的特徵、本質和優點將變得更加明瞭，在附圖中，相近參考標記貫穿始終作相應標識。

圖 1 是圖示藉由在明文輸入區塊可用之前先部分處理區塊密碼術藉此減少區塊密碼術的等待時間來改善區塊密碼術加密處理的第一特徵的方塊圖。

圖 2 是圖示藉由將區塊密碼術的第一部分與區塊密碼術的第二部分並行處理藉此減少區塊密碼術的等待時間來改善區塊密碼術解密的第二特徵的方塊圖。

圖 3 是圖示配置成加密要被儲存在記憶體中的資料的區塊密碼術的示例的方塊圖。

圖 4 是圖示配置成加密明文資料的區塊密碼術設備的功能性元件的方塊圖。

圖 5 是圖示記憶體位址加密或變換模組的一個示例的方塊圖。

圖 6 是圖示明文資料加密或變換模組的一個示例的方塊圖。

圖 7 圖示使用要儲存資料的記憶體位址來加密該資料的區塊密碼術資料加密方法。

圖 8 是圖示區塊密碼術解密從記憶體位址讀取的資料的處理的方塊圖。

圖 9 是圖示配置成解密密文資料的區塊密碼術設備的功能性元件的方塊圖。

圖 10 是圖示密文資料解密或逆變換模組的一個示例的方塊圖。

圖 11 圖示用於藉由使用在解密經加密資料的同時並發地加密記憶體位址以減少區塊密碼術的等待時間的區塊密碼術來解密經加密資料的方法。

圖 12 是圖示如何可基於來自區塊密碼術的位址加密回合的結果來產生用於資料加密和解密回合的回合密鑰的示例

的方塊圖。

圖13是圖示可配置成執行高效率的區塊密碼術加密和解密的設備的方塊圖。

【主要元件符號說明】

100~114	加密方塊圖
200~214	解密方塊圖
302~328	區塊密碼術方塊圖
404~426	區塊密碼術設備方塊圖
502~516	記憶體位址加密或變換模組方塊圖
602~614	加密或變換模組方塊圖
702~712	步驟流程
802~828	資料處理方塊圖
902~926	區塊密碼術設備方塊圖
1002~1014	密文資料解密或逆變換模組方塊圖
1102~1112	步驟流程
1202~1236	回合密鑰方塊圖
1302~1308	加密和解密設備方塊圖

七、申請專利範圍：

1. 一種加密資料以供儲存在一儲存裝置之一記憶體位址中的方法，該方法包括以下步驟：

在一第一複數個連續迭代區塊密碼回合中加密該記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

使用來自該第一複數個迭代區塊密碼回合中的一或更多個中介回合的資訊來產生資料回合密鑰；

在該第一複數個迭代區塊密碼回合之後將該資料與經加密的該記憶體位址相組合以獲得一組合資料；

在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來加密該組合資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入；以及

儲存經加密之該組合資料在該儲存裝置之該記憶體位址中。

2. 如請求項 1 之方法，其中加密該記憶體位址之步驟開始於該資料可用之前。

3. 如請求項 1 之方法，其中加密該記憶體位址之步驟包括以下步驟：

根據一第一變換函數變換該記憶體位址；以及

將經變換的該記憶體位址與一回合密鑰混合。

4. 如請求項 1 之方法，其中產生該等資料回合密鑰之步驟包括以下步驟：

從該第一複數個連續迭代區塊密碼回合中的至少一些回合的經加密之該記憶體位址之複數個中介回合提取複數個位元；以及

從所提取出之該複數個位元的片段選擇該等資料回合密鑰。

5. 如請求項 4 之方法，其中產生該等資料回合密鑰之步驟包括以下步驟：

將所提取出之該複數個位元序連到一字串中，該等資料回合密鑰從該字串中選擇。

6. 如請求項 4 之方法，其中用於該第二複數個區塊密碼回合中較早回合的該等資料回合密鑰是使用來自該第一複數個連續迭代區塊密碼回合中較晚回合的經加密之該記憶體位址的位元而產生。

7. 如請求項 1 之方法，其中該資料是藉由一可逆操作來與經加密之該記憶體位址相組合。

8. 如請求項 1 之方法，其中加密該組合資料之步驟包括以下步驟：

根據一第二變換函數變換該組合資料；以及

將經變換的該組合資料與該等資料回合密鑰中的一或更多個混合。

9. 如請求項 1 之方法，其中加密該組合資料之步驟還包括以下步驟：

將該組合資料分段成複數個資料片段；以及

對不同的該等資料分段執行位元替換。

10. 如請求項 1 之方法，其中該第二複數個區塊密碼回合中之區塊密碼回合數量多於該第一複數個連續迭代區塊密碼回合中之區塊密碼回合數量。

11. 如請求項 1 之方法，其中該組合資料在該第二複數個連續迭代區塊密碼回合上被連續地加密。

12. 如請求項 1 之方法，其中該等資料回合密鑰之產生係起始於該第一複數個連續迭代區塊密碼回合完成之前。

13. 如請求項 1 之方法，其中早先之資料回合密鑰是使用來自該第一複數個連續迭代區塊密碼回合中之較晚中介回合之資訊而計算。

14. 如請求項 1 之方法，其中該等資料回合密鑰之產生

與該記憶體位址之加密重疊。

15. 如請求項1之方法，其中來自該第一複數個連續迭代區塊密碼回合中之一或更多個中介回合之資訊係為二或更多個區塊密碼回合間之中介結果。

16. 如請求項1之方法，其中該等資料回合密鑰係複數個中介回合結果產生，該複數個中介回合結果來自用於經加密之該記憶體位址之該第一複數個連續迭代區塊密碼回合，且來自該第一複數個連續迭代區塊密碼回合之該複數個中介回合結果係以一反向產生以產生該等資料回合密鑰。

17. 如請求項1之方法，其中該等資料回合密鑰係複數個中介回合結果產生，該複數個中介回合結果來自用於經加密之該記憶體位址之該第一複數個連續迭代區塊密碼回合，且來自該第一複數個連續迭代區塊密碼回合之該複數個中介回合結果係以一同向產生以產生該等資料回合密鑰。

18. 一種區塊密碼術設備，包括：

一位址加密模組，用於在一第一複數個連續迭代區塊密碼回合中加密一記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

一密鑰排程模組，用於使用來自該第一複數個連續迭代區塊密碼回合中的一或更多個中介回合的資訊來產生資料

回合密鑰；

一組合器，用於在該第一複數個連續迭代區塊密碼回合之後將資料與經加密的該記憶體位址相組合以獲得一組合資料；以及

一資料加密模組，用於在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來加密該組合資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入。

19. 如請求項 18 之設備，其中加密該記憶體位址之步驟係開始於該資料可用之前。

20. 如請求項 18 之設備，其中該位址加密模組還被配置成：

根據一第一變換函數變換該記憶體位址；以及

將經變換的該記憶體位址與一回合密鑰混合。

21. 如請求項 18 之設備，其中該密鑰排程模組還被配置成：

從該第一複數個連續迭代區塊密碼回合中的至少一些回合的經加密之該記憶體位址提取複數個位元；以及

從所提取出之該複數個位元的片段選擇該等資料回合密鑰。

22. 如請求項 21 之設備，其中該密鑰排程模組還被配置成：

將所提取出之該複數個位元序連到一字串中，該等資料回合密鑰從該字串中選擇。

23. 如請求項 21 之設備，其中用於該第二複數個區塊密碼回合中較早回合的該等資料回合密鑰是使用來自該第一複數個連續迭代區塊密碼回合中較晚回合的經加密之該記憶體位址的位元而產生。

24. 如請求項 18 之設備，其中該資料加密模組還被配置成：

根據一第二變換函數變換該組合資料；以及

將經變換的該組合資料與該等資料回合密鑰中的一或更多個混合。

25. 如請求項 18 之設備，其中該資料加密模組還被配置成：

將該組合資料分段成複數個資料片段；以及

對不同的該等資料片段執行位元替換。

26. 如請求項 18 之設備，其中該第二複數個區塊密碼回合中之區塊密碼回合數量多於該第一複數個連續迭代區塊密碼回合中之區塊密碼回合數量。

27. 如請求項 18 之設備，其中該組合資料在該第二複數個連續迭代區塊密碼回合上被連續地加密。

28. 一種區塊密碼術設備，包括：

加密位址構件，用於在一第一複數個連續迭代區塊密碼回合中加密一記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

產生構件，用於使用來自該第一複數個連續迭代區塊密碼回合中的一或更多個中介回合的資訊來產生資料回合密鑰；

組合構件，用於在該第一複數個連續迭代區塊密碼回合之後將資料與經加密的該記憶體位址相組合以獲得一組合資料；以及

加密資料構件，用於在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來加密該組合資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入。

29. 一種包括一處理電路的處理器，該處理電路適於：

在一第一複數個連續迭代區塊密碼回合中加密一記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

使用來自該第一複數個連續迭代區塊密碼回合中的一或

更多個中介回合的資訊來產生資料回合密鑰；

在該第一複數個連續迭代區塊密碼回合之後將資料與經加密的該記憶體位址相組合以獲得一組合資料；以及

在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來加密該組合資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入。

30. 一種包括用於區塊密碼術加密的指令的非暫態機器可讀取媒體，該等指令在由一或更多個處理器執行時使該處理器：

在一第一複數個連續迭代區塊密碼回合中加密一記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

使用來自該第一複數個連續迭代區塊密碼回合中的一或更多個回合的資訊來產生資料回合密鑰；

在該第一複數個連續迭代區塊密碼回合之後將資料與經加密的該記憶體位址相組合以獲得一組合資料；以及

在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來加密該組合資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入。

31. 一種解密從一儲存裝置之一記憶體位址取回的資料的方法，該方法包括以下步驟：

在一第一複數個連續迭代區塊密碼回合中加密該記憶體

位址以獲得一經加密記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

使用來自該第一複數個連續迭代區塊密碼回合中的一或更多個中介回合的資訊來產生資料回合密鑰；

從該儲存裝置之該記憶體位址取回該經加密資料；

在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來解密該經加密資料以獲得一經部分解密的資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入；以及

將該經部分解密的資料與該經加密記憶體位址相組合以獲得完全解密的資料。

32. 如請求項 31 之方法，其中加密該記憶體位址之步驟係開始於該資料可用之前。

33. 如請求項 31 之方法，其中加密該記憶體位址之步驟包括以下步驟：

根據一第一變換函數變換該記憶體位址；以及

將經變換的該記憶體位址與一回合密鑰混合。

34. 如請求項 31 之方法，其中產生該等資料回合密鑰之步驟包括以下步驟：

從該第一複數個連續迭代區塊密碼回合中的至少一些回合的經加密之該記憶體位址之複數個中介回合提取複數個

位元；以及

從所提取出之該複數個位元的片段選擇該等資料回合密鑰。

35. 如請求項 34 之方法，其中產生該等資料回合密鑰之步驟包括以下步驟：

將所提取出之該複數個位元序連到一字串中，該等資料回合密鑰從該字串中選擇。

36. 如請求項 34 之方法，其中用於該第二複數個區塊密碼回合中較早回合的該等資料回合密鑰是使用來自該第一複數個連續迭代區塊密碼回合中較早回合的該經加密記憶體位址的位元而產生。

37. 如請求項 31 之方法，其中該經部分解密的資料是藉由一可逆操作來與該經加密記憶體位址相組合。

38. 如請求項 31 之方法，其中解密該經加密資料之步驟包括以下步驟：

根據一第二逆變換函數變換該經加密資料；以及

將變換後的該經加密資料與該等資料回合密鑰中的一或更多個混合。

39. 如請求項 31 之方法，其中該第二複數個區塊密碼

回合中之區塊密碼回合數量多於該第一複數個連續迭代區塊密碼回合中之區塊密碼回合數量。

40. 如請求項 31 之方法，其中該第一複數個連續迭代區塊密碼回合與該第二複數個區塊密碼回合並發地執行。

41. 一種區塊密碼術設備，包括：

一位址加密模組，用於在一第一複數個連續迭代區塊密碼回合中加密一記憶體位址以獲得一經加密記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

一密鑰排程模組，用於使用來自該第一複數個連續迭代區塊密碼回合中的一或更多個中介回合的資訊來產生資料回合密鑰；

一資料解密模組，用於在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來解密經加密資料以獲得一經部分解密的資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入；以及

一組合器，用於將該經部分解密的資料與該經加密記憶體位址相組合以獲得完全解密的資料。

42. 如請求項 41 之設備，其中加密該記憶體位址之步驟開始於該資料可用之前。

43. 如請求項 41 之設備，其中該密鑰排程模組還被配置成：

從該第一複數個連續迭代區塊密碼回合中的至少一些回合的該經加密記憶體位址提取複數個位元；以及

從所提取出之該複數個位元的片段選擇該等資料回合密鑰。

44. 如請求項 41 之設備，其中用於該第二複數個區塊密碼回合中較早回合的該等資料回合密鑰是使用來自該第一複數個連續迭代區塊密碼回合中較早回合的該經加密記憶體位址的位元而產生。

45. 如請求項 41 之設備，其中該第二複數個區塊密碼回合中之區塊密碼回合數量多於該第一複數個連續迭代區塊密碼回合中之區塊密碼回合數量。

46. 一種區塊密碼術設備，包括：

加密構件，用於在一第一複數個連續迭代區塊密碼回合中加密一記憶體位址以獲得一經加密記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

產生構件，用於使用來自該第一複數個連續迭代區塊密碼回合中的一或更多個中介回合的資訊來產生資料回合密鑰；

解密構件，用於在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來解密該經加密資料以獲得一經部分解密的資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入；以及

組合構件，用於將該經部分解密的資料與該經加密記憶體位址相組合以獲得一完全解密的資料。

47. 如請求項46之設備，還包括：

取回構件，用於從該記憶體位址取回該經加密資料。

48. 一種包括一處理電路的處理器，該處理電路適於：

在一第一複數個連續迭代區塊密碼回合中加密一記憶體位址以獲得一經加密記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

使用來自該第一複數個連續迭代區塊密碼回合中的一或更多個中介回合的資訊來產生資料回合密鑰；

在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來解密該經加密資料以獲得一經部分解密的資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入；以及

將該經部分解密的資料與該經加密記憶體位址相組合以獲得完全解密的資料。

49. 一種包括用於區塊密碼術解密的指令的非暫態機

器可讀取媒體，該等指令在由一或更多個處理器執行時使該處理器：

在一第一複數個連續迭代區塊密碼回合中加密該記憶體位址以獲得一經加密記憶體位址，其中一記憶體加密回合之一輸出係作為一下一個記憶體加密回合之一輸入；

使用來自該第一複數個連續迭代區塊密碼回合中的一或更多個中介回合的資訊來產生資料回合密鑰；

在一第二複數個連續迭代區塊密碼回合中使用該等資料回合密鑰來解密該經加密資料以獲得一經部分解密的資料，其中一資料加密回合之一輸出係作為一下一個資料加密回合之一輸入；以及

將該經部分解密的資料與該經加密記憶體位址相組合以獲得完全解密的資料。

八、圖式：

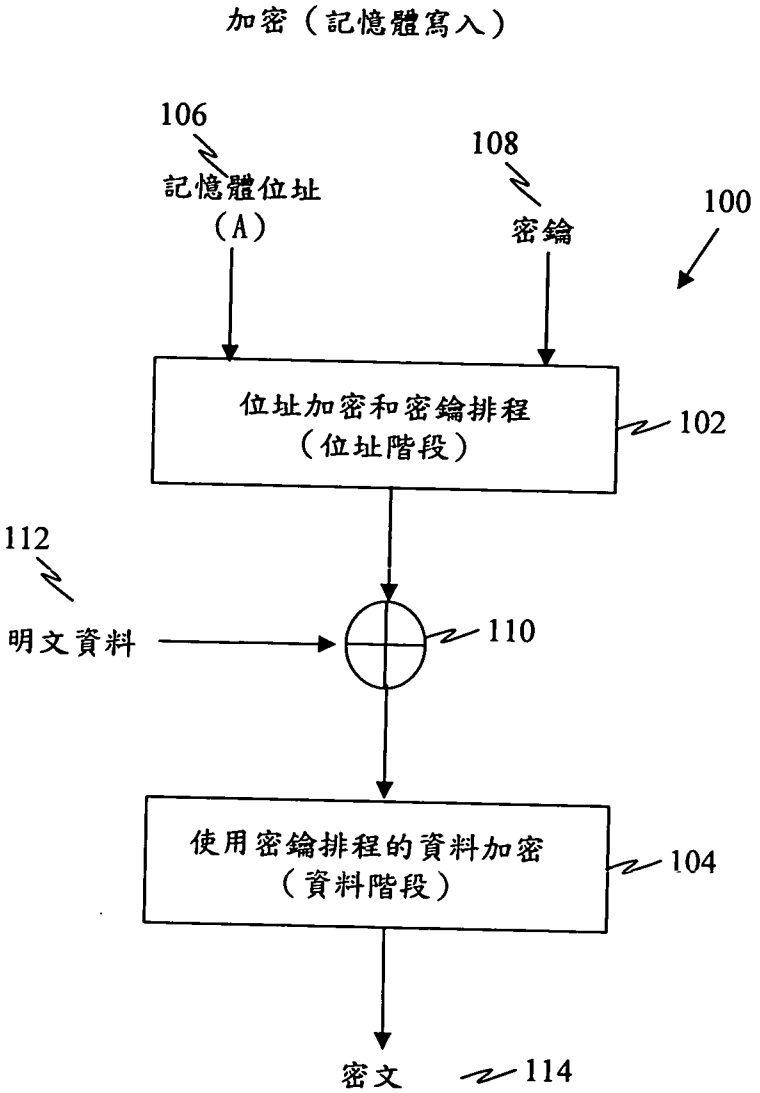
加密（記憶體寫入）
106
記憶體位址
（A）
108
密鑰
100
位址加密和密鑰排程
（位址階段）
102
112
明文資料
110
使用密鑰排程的資料加密
（資料階段）
104
密文
114

圖 1

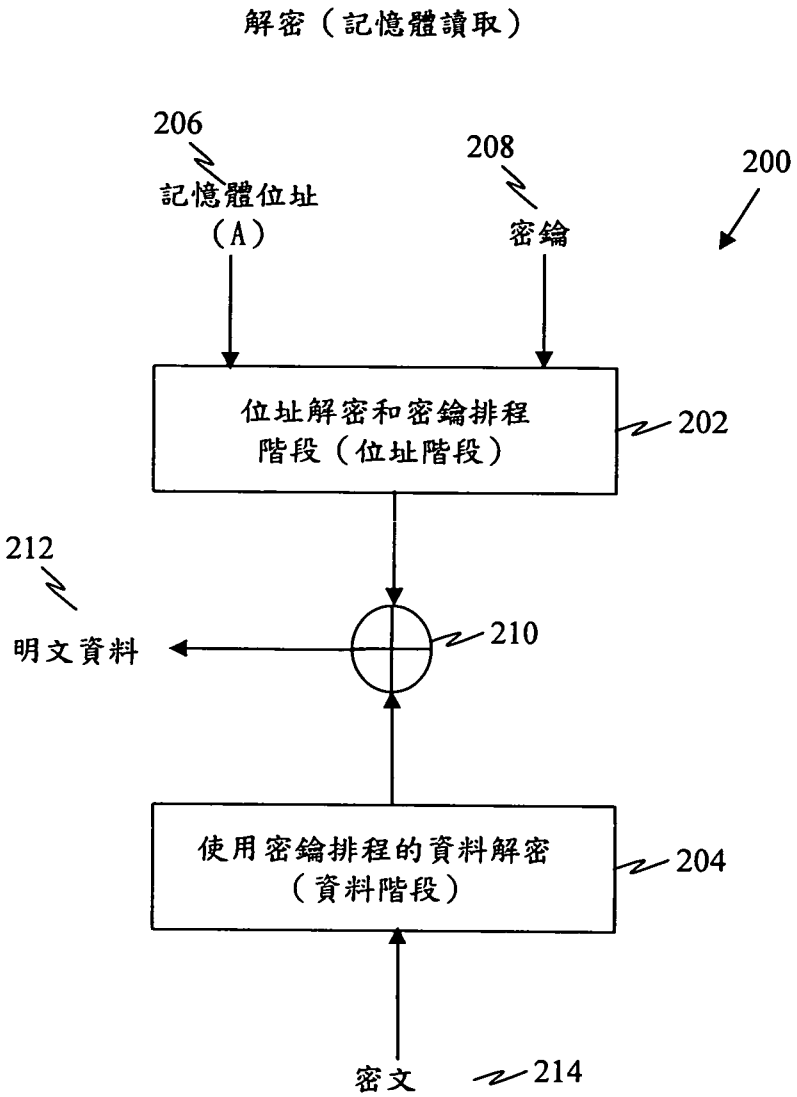
解密（記憶體讀取）
206
記憶體位址
（A）
208
密鑰
200
位址解密和密鑰排程
階段（位址階段）
202
212
明文資料
210
使用密鑰排程的資料解密
（資料階段）
204
密文
214

圖2

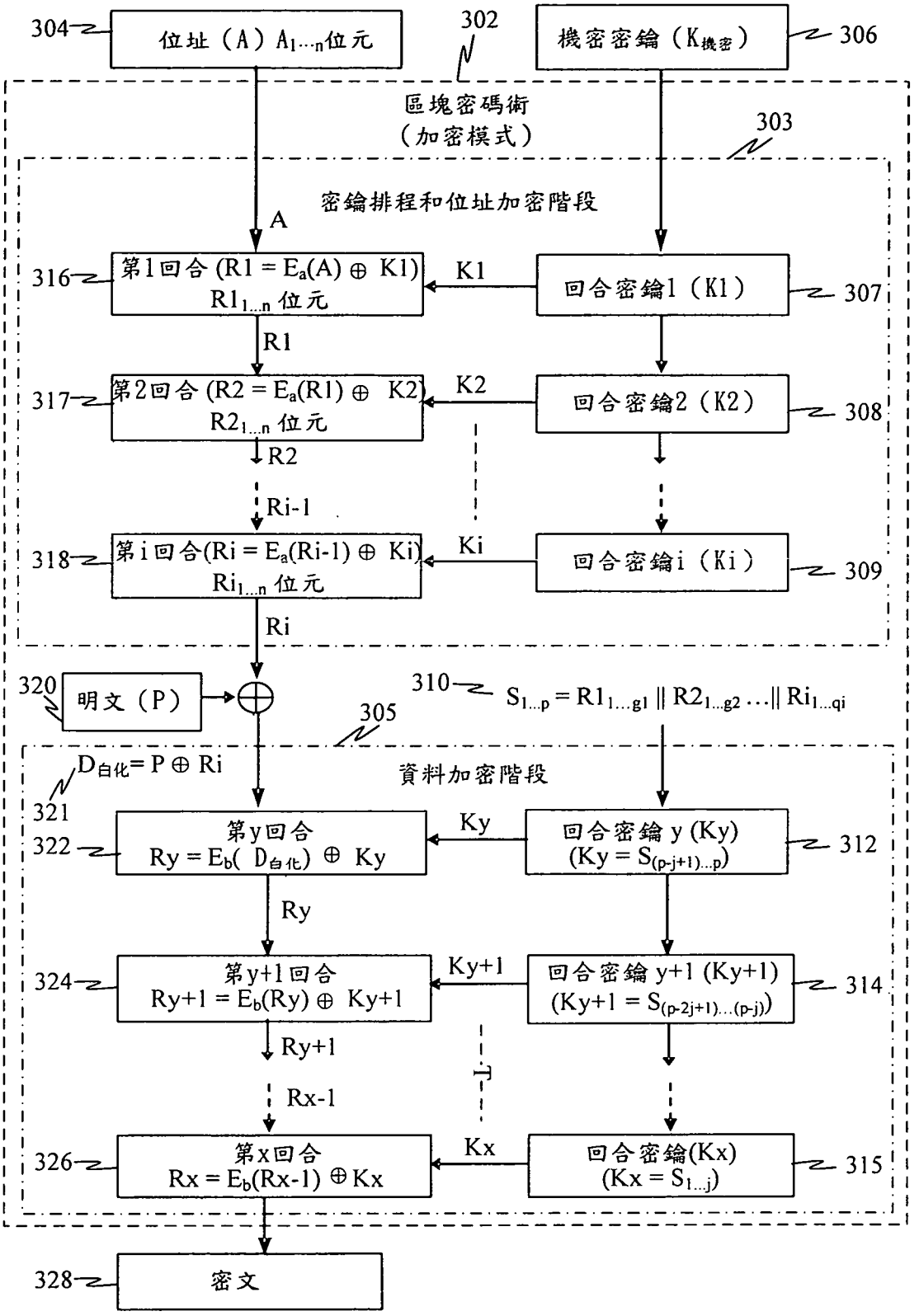
304
位址（A）$A_{1\cdots n}$位元
302
機密密鑰（$K_{機密}$）
306
區塊密碼術
（加密模式）
303
密鑰排程和位址加密階段
A
316
第1回合 ($R1 = E_a(A) \oplus K1$)
$R1_{1\cdots n}$ 位元
K1
回合密鑰1（K1）
307
R1
317
第2回合 ($R2 = E_a(R1) \oplus K2$)
$R2_{1\cdots n}$ 位元
K2
回合密鑰2（K2）
308
R2
Ri-1
318
第i回合($Ri = E_a(Ri-1) \oplus Ki$)
$Ri_{1\cdots n}$ 位元
Ki
回合密鑰i（Ki）
309
Ri
320
明文（P）
310
$S_{1\cdots p} = R1_{1\cdots g1} \| R2_{1\cdots g2} \cdots \| Ri_{1\cdots qi}$
305
$D_{白化} = P \oplus Ri$
資料加密階段
321
322
第y回合
$Ry = E_b(D_{白化}) \oplus Ky$
Ky
回合密鑰 y (Ky)
$(Ky = S_{(p-j+1)\cdots p})$
312
Ry
324
第y+1回合
$Ry+1 = E_b(Ry) \oplus Ky+1$
Ky+1
回合密鑰 y+1 (Ky+1)
$(Ky+1 = S_{(p-2j+1)\cdots(p-j)})$
314
Ry+1
Rx-1
J
326
第x回合
$Rx = E_b(Rx-1) \oplus Kx$
Kx
回合密鑰(Kx)
$(Kx = S_{1\cdots j})$
315
328
密文

圖3

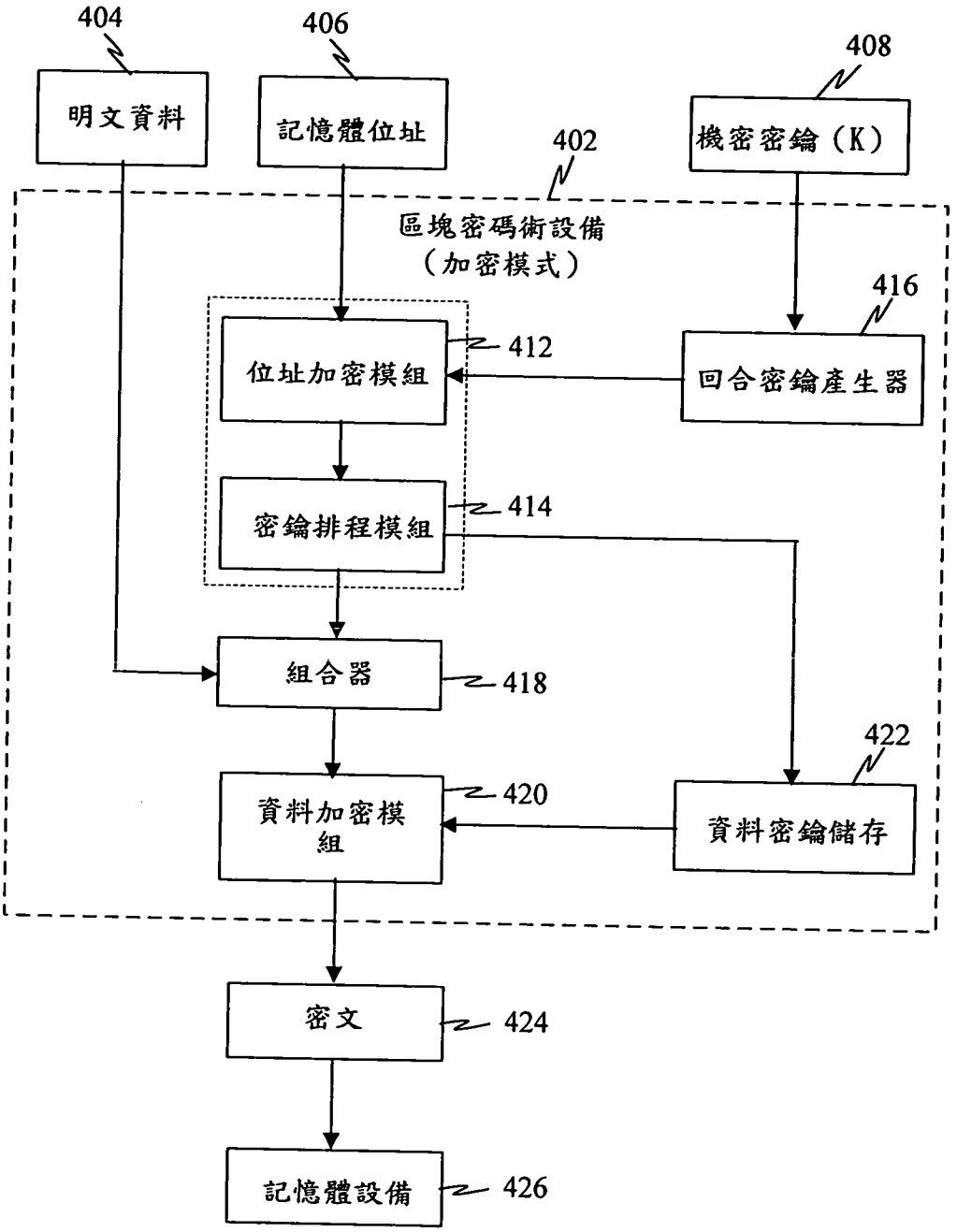
404
406
408
明文資料
記憶體位址
機密密鑰（K）
402
區塊密碼術設備
（加密模式）
416
位址加密模組
412
回合密鑰產生器
密鑰排程模組
414
組合器
418
422
資料加密模組
420
資料密鑰儲存
密文
424
記憶體設備
426

圖4

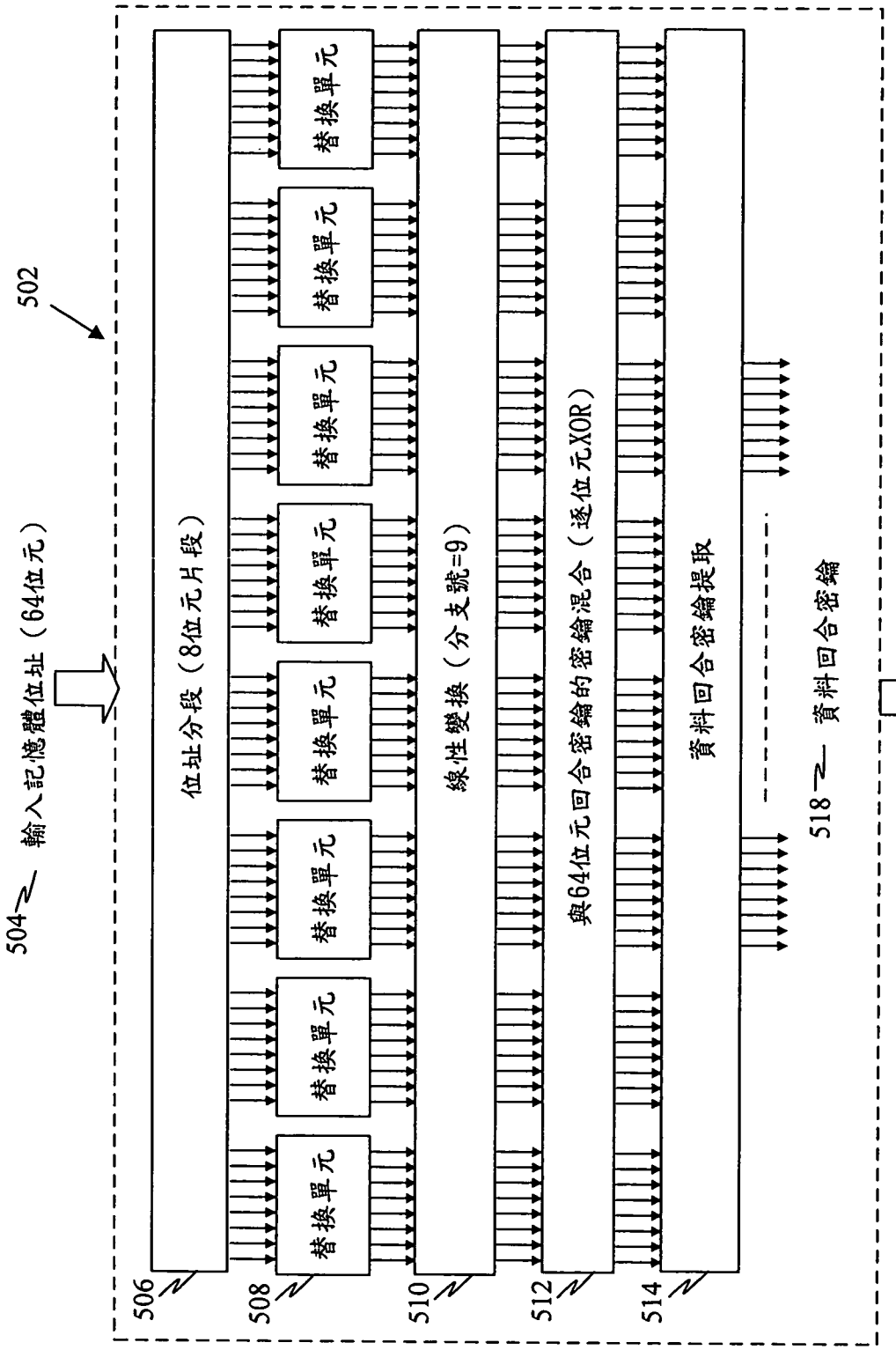
502
504
輸入記憶體位址（64位元）
位址分段（8位元片段）
替換單元
替換單元
替換單元
替換單元
替換單元
替換單元
替換單元
替換單元
線性變換（分支號=9）
與64位元回合密鑰的密鑰混合（逐位元XOR）
資料回合密鑰提取
518
資料回合密鑰
506
508
510
512
514
516
輸出經加密記憶體位址（64位元）

圖5

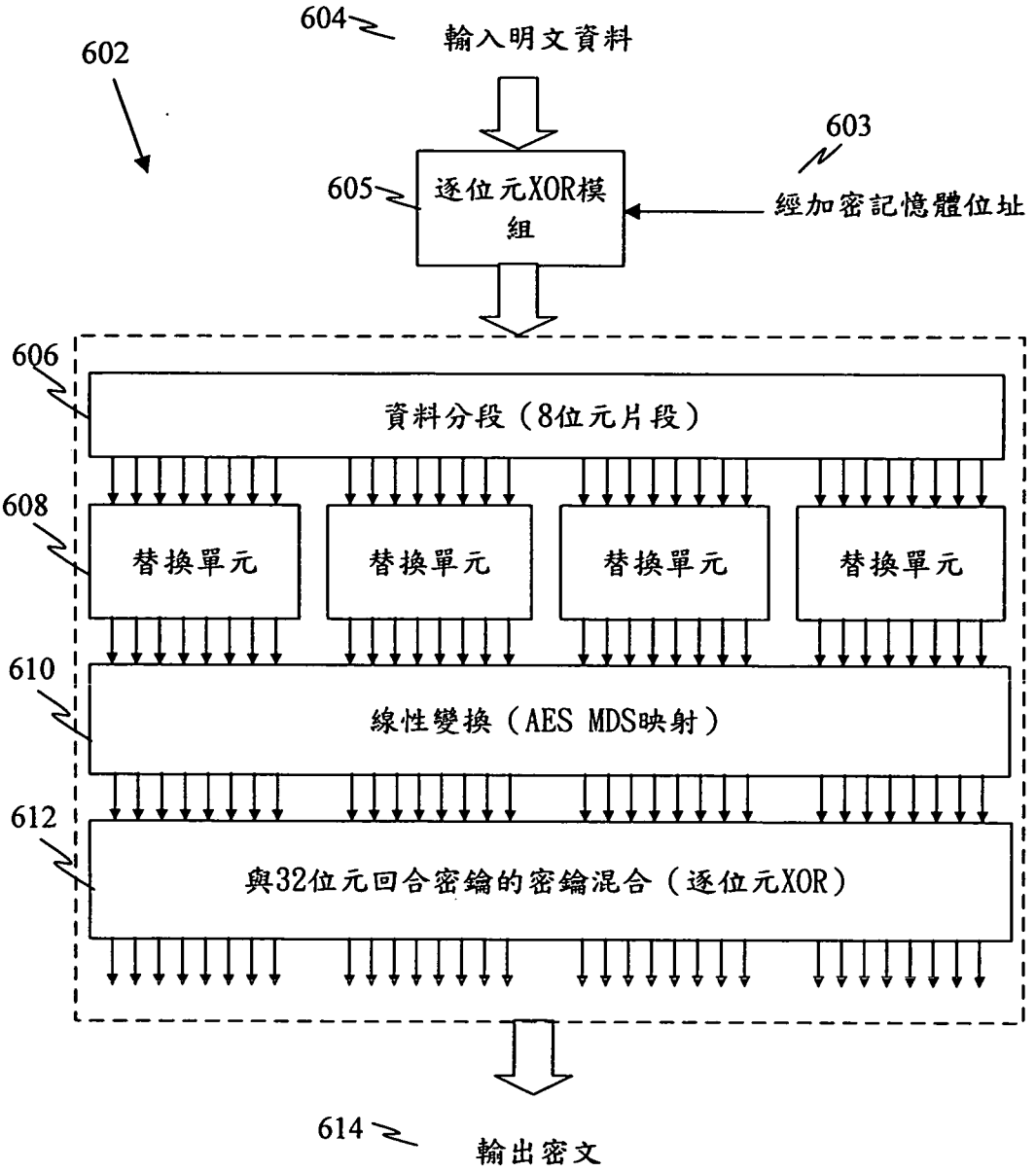
602
604
輸入明文資料
603
605
逐位元XOR模組
經加密記憶體位址
606
資料分段（8位元片段）
608
替換單元
替換單元
替換單元
替換單元
610
線性變換（AES MDS映射）
612
與32位元回合密鑰的密鑰混合（逐位元XOR）
614
輸出密文

圖6

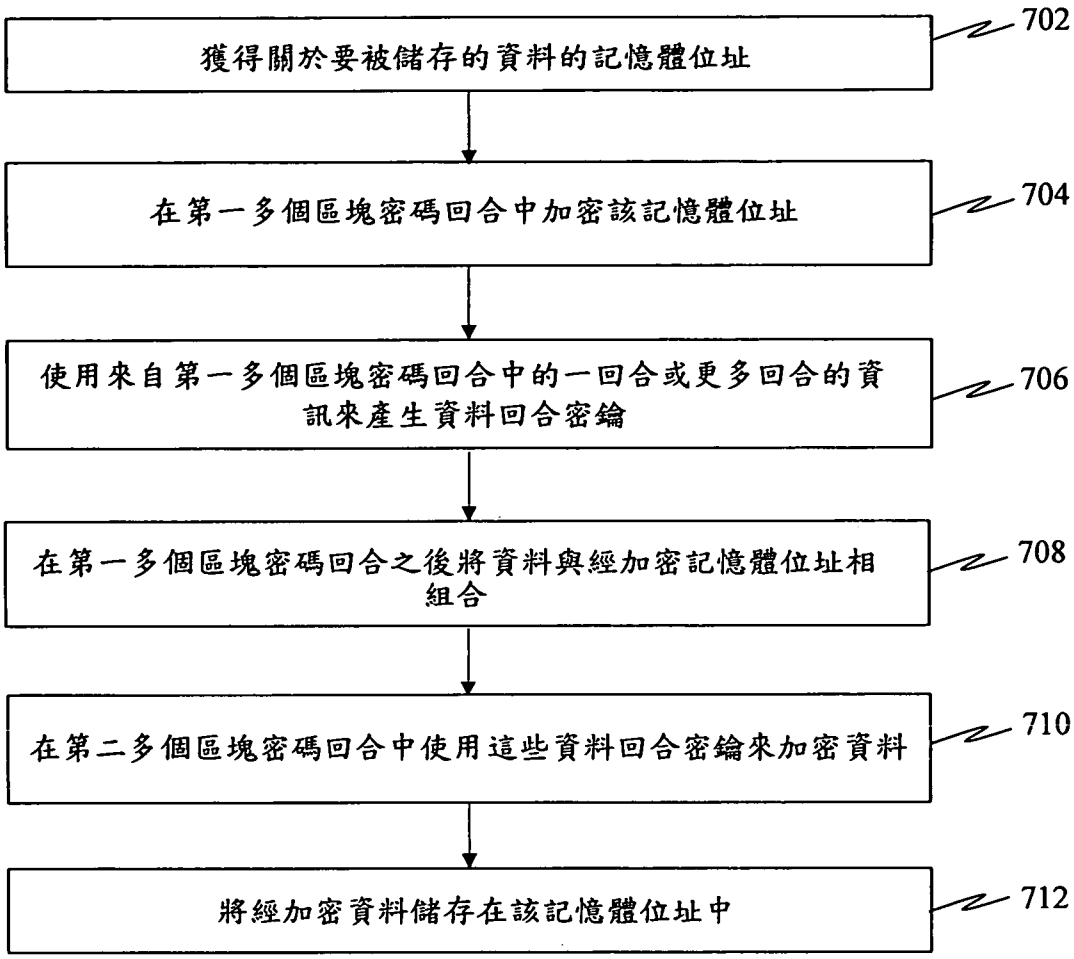
獲得關於要被儲存的資料的記憶體位址
702
在第一多個區塊密碼回合中加密該記憶體位址
704
使用來自第一多個區塊密碼回合中的一回合或更多回合的資訊來產生資料回合密鑰
706
在第一多個區塊密碼回合之後將資料與經加密記憶體位址相組合
708
在第二多個區塊密碼回合中使用這些資料回合密鑰來加密資料
710
將經加密資料儲存在該記憶體位址中
712

圖7

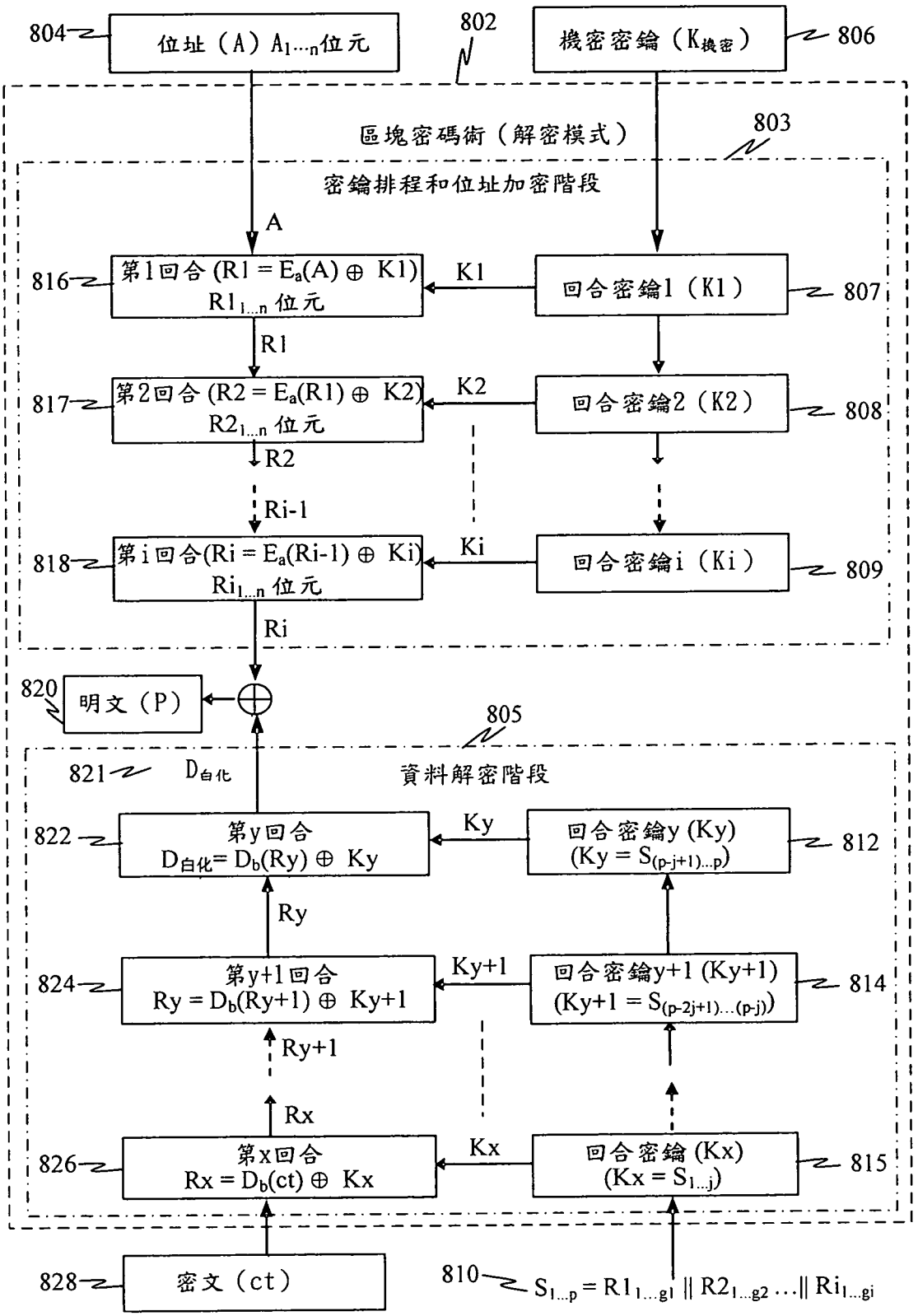
804
位址（A）$A_{1...n}$位元
802
機密密鑰（$K_{機密}$）
806
區塊密碼術（解密模式）
803
密鑰排程和位址加密階段
A
816
第1回合 ($R1 = E_a(A) \oplus K1$)
$R1_{1...n}$ 位元
K1
回合密鑰1（K1）
807
R1
817
第2回合 ($R2 = E_a(R1) \oplus K2$)
$R2_{1...n}$ 位元
K2
回合密鑰2（K2）
808
R2
Ri-1
818
第i回合($Ri = E_a(Ri-1) \oplus Ki$)
$Ri_{1...n}$ 位元
Ki
回合密鑰i（Ki）
809
Ri
820
明文（P）
805
821
$D_{白化}$
資料解密階段
822
第y回合
$D_{白化} = D_b(Ry) \oplus Ky$
Ky
回合密鑰y (Ky)
($Ky = S_{(p-j+1)...p}$)
812
Ry
824
第y+1回合
$Ry = D_b(Ry+1) \oplus Ky+1$
Ky+1
回合密鑰y+1 (Ky+1)
($Ky+1 = S_{(p-2j+1)...(p-j)}$)
814
Ry+1
Rx
826
第x回合
$Rx = D_b(ct) \oplus Kx$
Kx
回合密鑰 (Kx)
($Kx = S_{1...j}$)
815
828
密文（ct）
810
$S_{1...p} = R1_{1...g1} \| R2_{1...g2} \ldots \| Ri_{1...gi}$

圖8

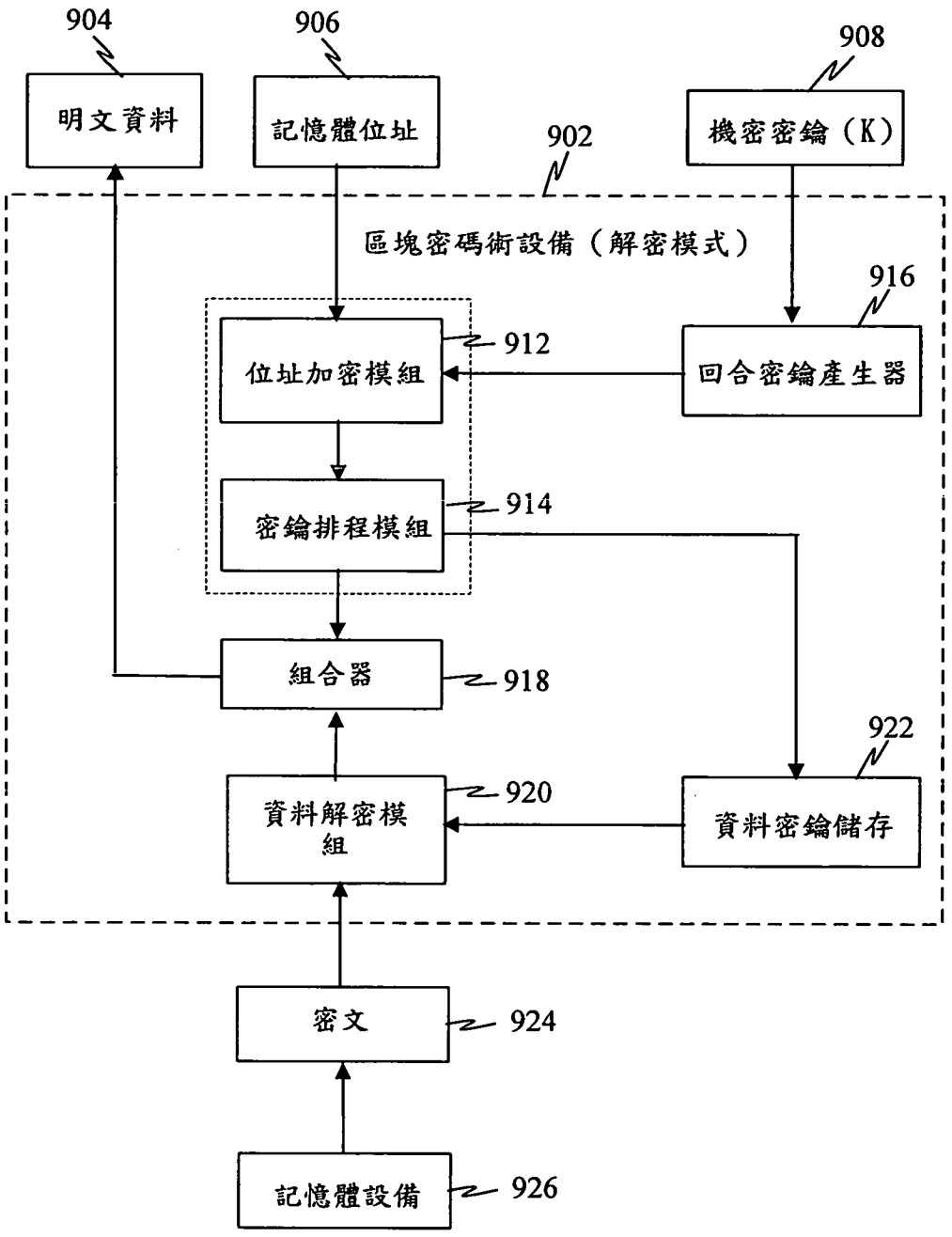
904
906
908
明文資料
記憶體位址
機密密鑰（K）
902
區塊密碼術設備（解密模式）
916
912
位址加密模組
回合密鑰產生器
914
密鑰排程模組
組合器
918
922
920
資料解密模組
資料密鑰儲存
密文
924
記憶體設備
926

圖9

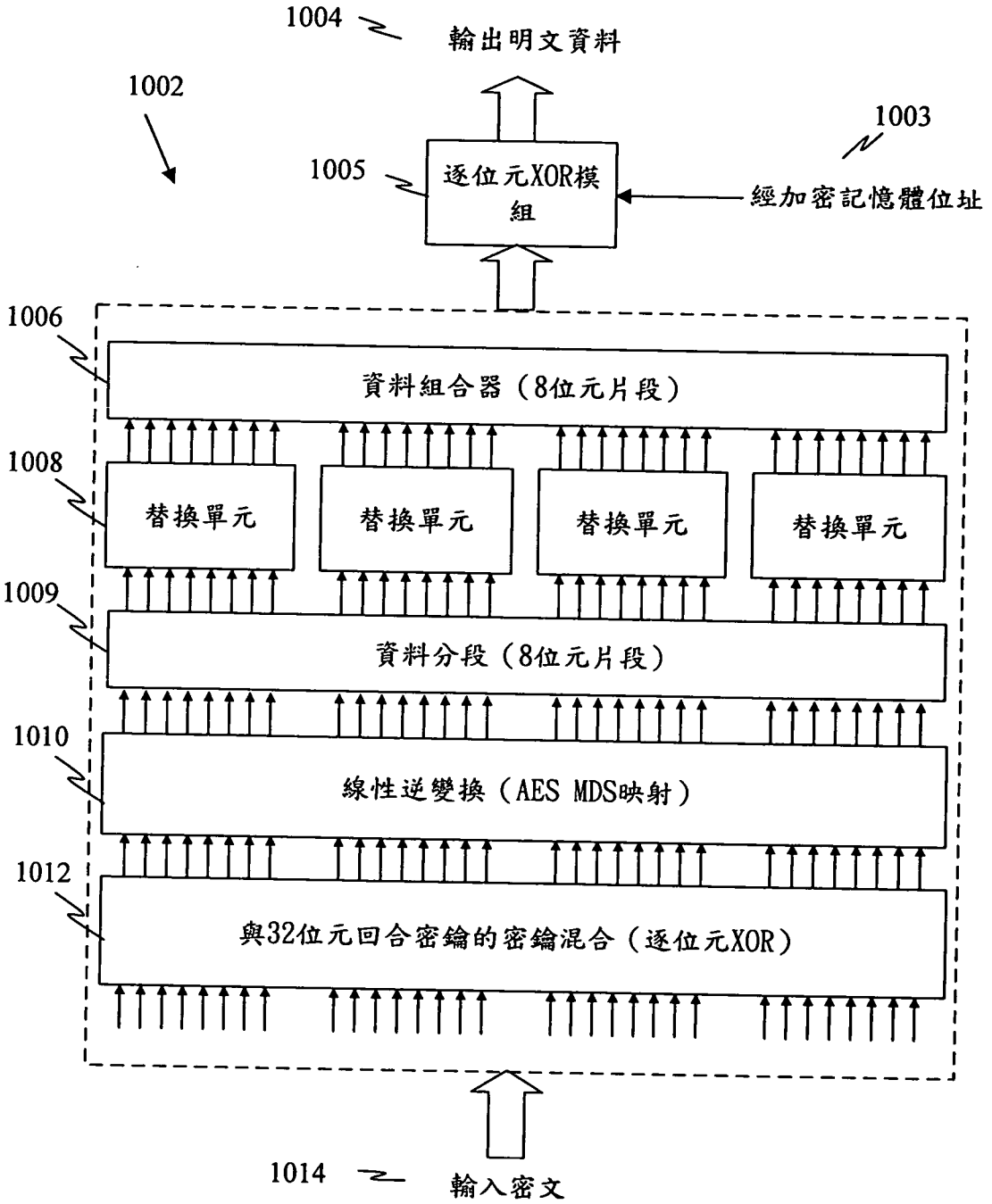
1004
輸出明文資料
1002
1003
1005
逐位元XOR模組
經加密記憶體位址
1006
資料組合器（8位元片段）
1008
替換單元
替換單元
替換單元
替換單元
1009
資料分段（8位元片段）
1010
線性逆變換（AES MDS映射）
1012
與32位元回合密鑰的密鑰混合（逐位元XOR）
1014
輸入密文

圖10

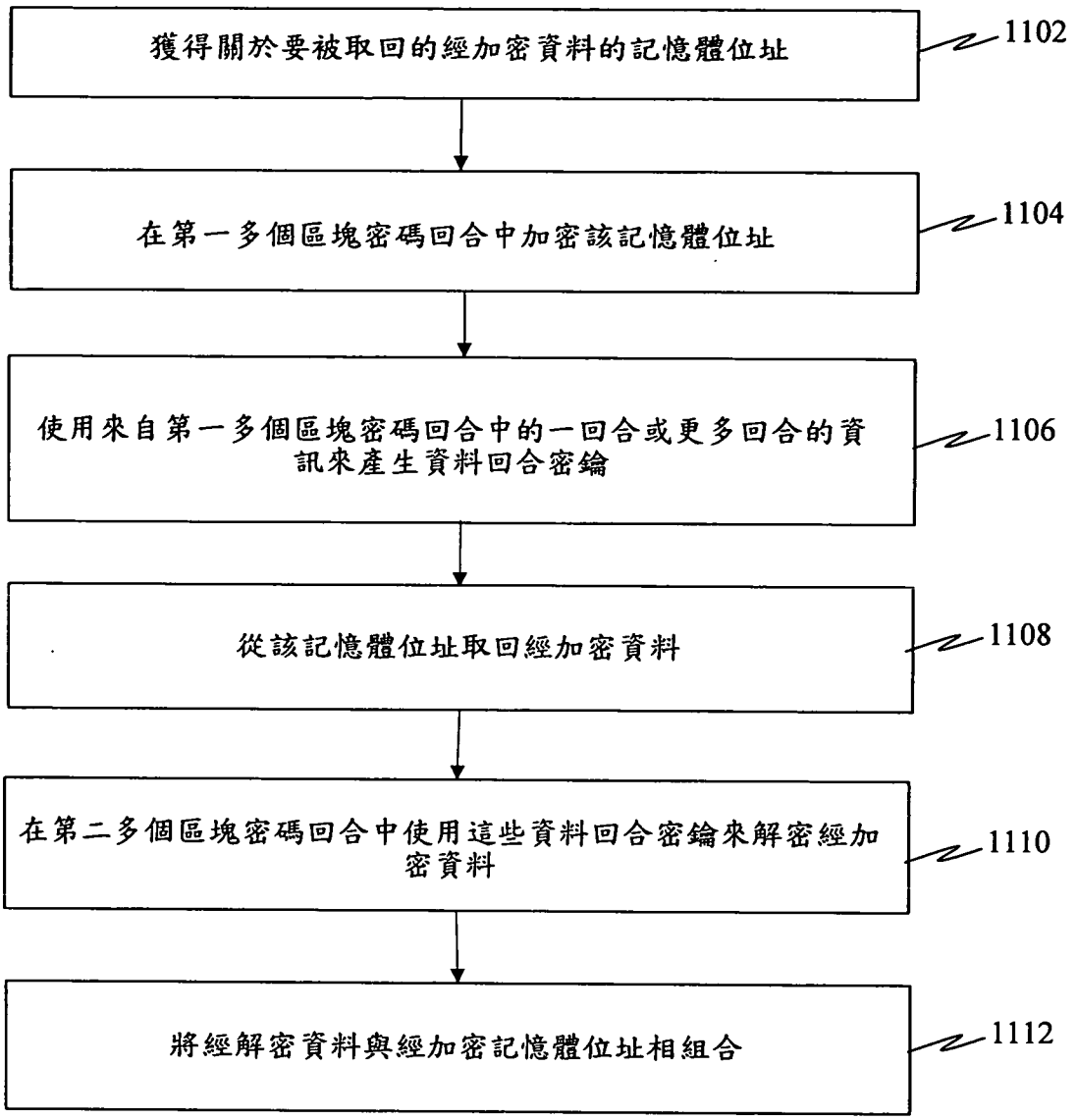
獲得關於要被取回的經加密資料的記憶體位址
1102
在第一多個區塊密碼回合中加密該記憶體位址
1104
使用來自第一多個區塊密碼回合中的一回合或更多回合的資訊來產生資料回合密鑰
1106
從該記憶體位址取回經加密資料
1108
在第二多個區塊密碼回合中使用這些資料回合密鑰來解密經加密資料
1110
將經解密資料與經加密記憶體位址相組合
1112

圖11

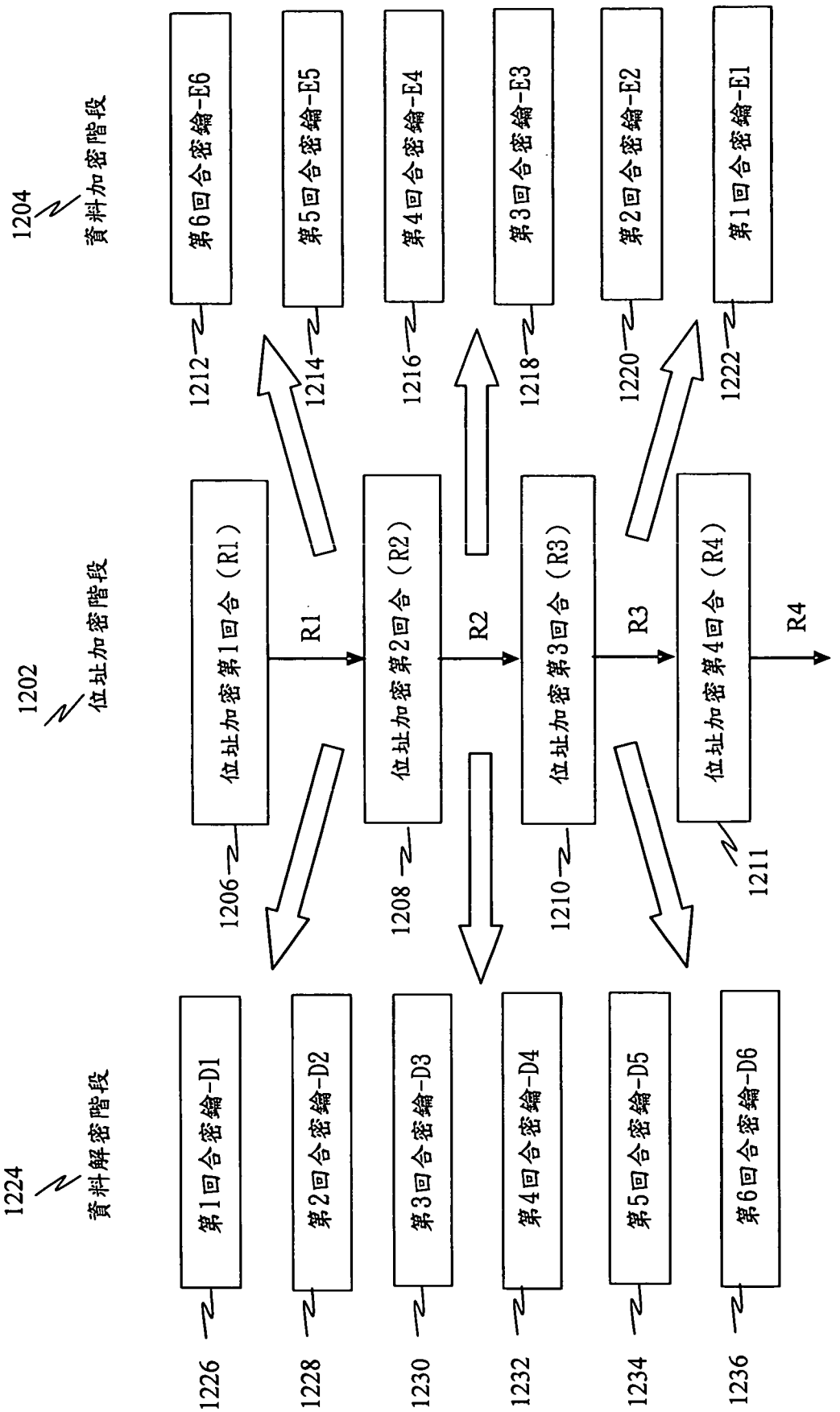
1202
位址加密階段
1204
資料加密階段
1224
資料解密階段
位址加密第1回合（R1）
位址加密第2回合（R2）
位址加密第3回合（R3）
位址加密第4回合（R4）
R1
R2
R3
R4
第1回合密鑰-D1
第2回合密鑰-D2
第3回合密鑰-D3
第4回合密鑰-D4
第5回合密鑰-D5
第6回合密鑰-D6
第6回合密鑰-E6
第5回合密鑰-E5
第4回合密鑰-E4
第3回合密鑰-E3
第2回合密鑰-E2
第1回合密鑰-E1
1206
1208
1210
1211
1212
1214
1216
1218
1220
1222
1226
1228
1230
1232
1234
1236

圖12

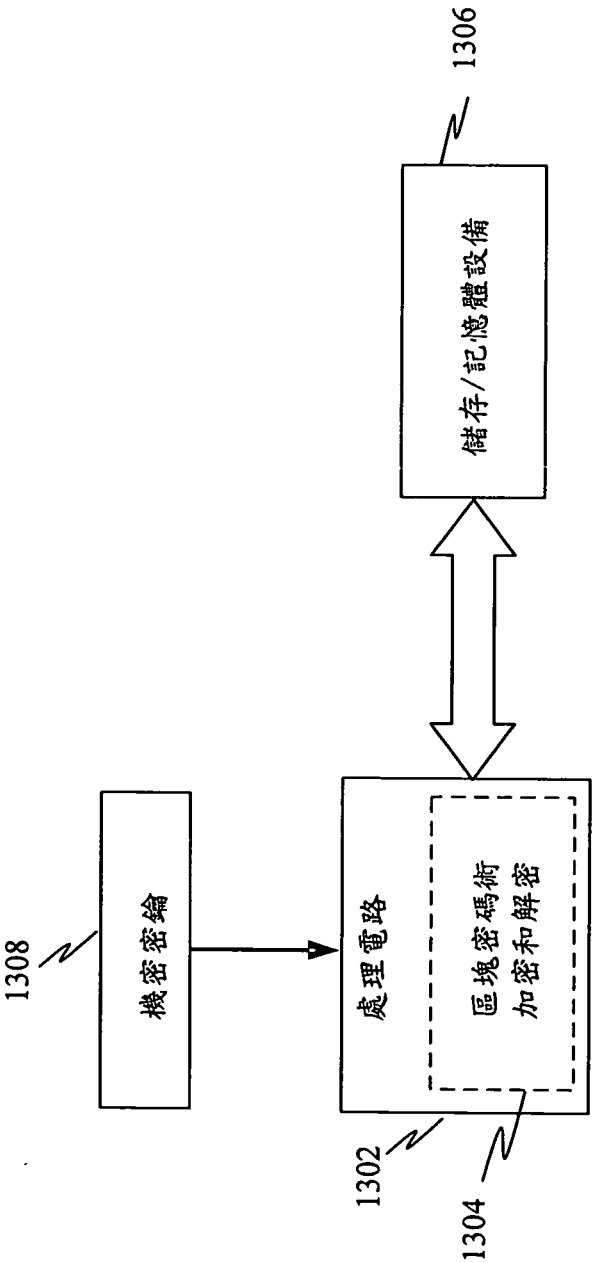

圖13