



(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 I597960 B

(45)公告日：中華民國 106 (2017) 年 09 月 01 日

(21)申請案號：104134051

(22)申請日：中華民國 104 (2015) 年 10 月 16 日

(51)Int. Cl. : *H04L9/06 (2006.01)* *H04L9/14 (2006.01)*

(30)優先權：2014/10/27 世界智慧財產權組織 PCT/US14/62407

(71)申請人：慧與發展有限責任合夥企業(美國) HEWLETT PACKARD ENTERPRISE
DEVELOPMENT LP (US)

美國

(72)發明人：哈伯 史塔特 HABER, STUART (US)；程 立群 CHEN, LIQUN (GB)

(74)代理人：惲軼群；劉法正

(56)參考文獻：

TW 201438449A

EP 1722502A1

US 2012/0179920A1

US 2012/0321076A1

US 2013/0136258A1

審查人員：陳怡婷

申請專利範圍項數：15 項 圖式數：8 共 37 頁

(54)名稱

金鑰分裂技術

KEY SPLITTING

(57)摘要

依據一實例，金鑰分裂可包括運用藉使用一遮罩所遮罩的一主金鑰之一經遮罩版本。

According to an example, key splitting may include utilizing a masked version of a master key that is masked by using a mask.

指定代表圖：

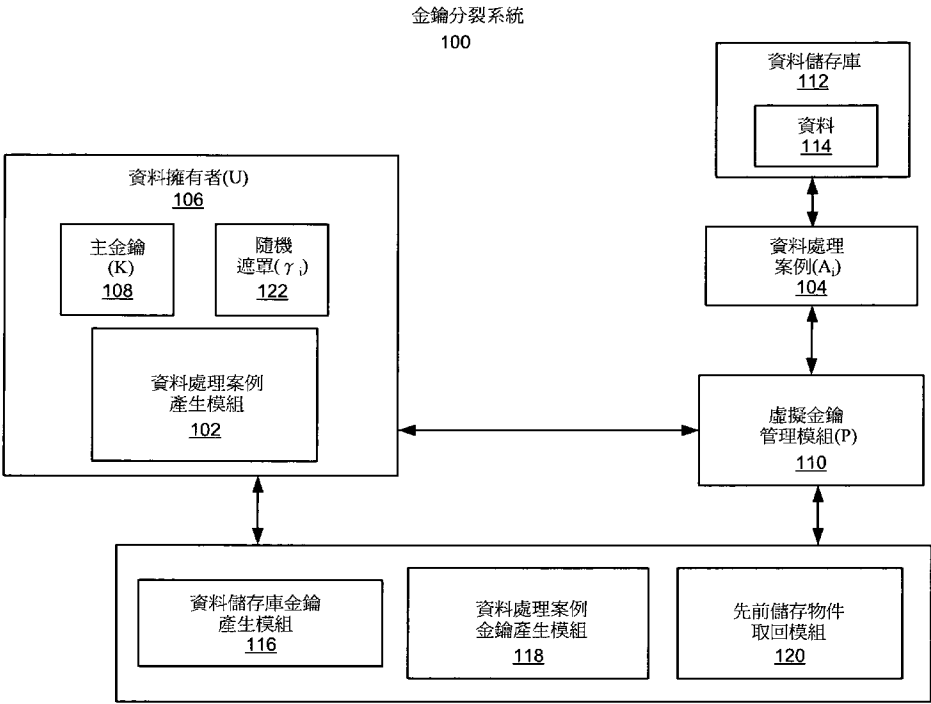


圖1

符號簡單說明：

- 100 . . . 系統
- 102 . . . 資料處理案例產生模組
- 104 . . . 資料處理案例
- 106 . . . 資料擁有者
- 108 . . . 主金鑰
- 110 . . . 虛擬金鑰管理模組
- 112 . . . 資料儲存庫
- 114 . . . 資料
- 116 . . . 資料儲存庫金鑰產生模組
- 118 . . . 資料處理案例金鑰產生模組
- 120 . . . 先前儲存物件取回模組
- 122 . . . 隨機遮罩

公告本

雙面影印

發明摘要

※ 申請案號：104134051

※ 申請日：104.10.16.

※IPC 分類：H04L 9/06 (2006.01)

H04L 9/14 (2006.01)

【發明名稱】(中文/英文)

金鑰分裂技術

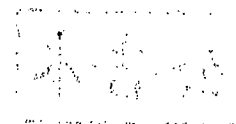
Key Splitting

【中文】

依據一實例，金鑰分裂可包括運用藉使用一遮罩所遮罩的一主金鑰之一經遮罩版本。

【英文】

According to an example, key splitting may include utilizing a masked version of a master key that is masked by using a mask.

**【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...系統	112...資料儲存庫
102...資料處理案例產生模組	114...資料
104...資料處理案例	116...資料儲存庫金鑰產生模組
106...資料擁有者	118...資料處理案例金鑰產生模組
108...主金鑰	120...先前儲存物件取回模組
110...虛擬金鑰管理模組	122...隨機遮罩

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

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)

金鑰分裂技術

Key Splitting

【技術領域】

[0001] 本發明係有關於金鑰分裂技術。

【先前技術】

[0002] 加密乃編碼資訊之方法使得加密資訊由經授權的實體讀取。至於加密，典型地稱作為明文的資訊係使用加密方法加密。加密資訊稱作為密文。為了讀取密文，典型地使用一金鑰以解密該密文。

【發明內容】

[0003] 依據本發明之一實施例，係特地提出一種非暫態電腦可讀取媒體已經於其上儲存機器可讀取指令用以提供金鑰分裂，該等機器可讀取指令當執行時使得至少一個處理器用以：產生一主金鑰；產生一隨機遮罩；藉使用該隨機遮罩而產生該主金鑰的一經遮罩版本；轉送該主金鑰的該經遮罩版本給一金鑰管理器；回應於轉送該主金鑰的該經遮罩版本，自該金鑰管理器接收一新遮罩；及基於該新遮罩及該隨機遮罩而決定一資料金鑰。

【圖式簡單說明】

[0004] 本文揭示之特徵係於下列圖式例示而非限制性，其中類似的元件符號指示類似的元件，附圖中：

[0005]圖1例示依據本文揭示之一實施例一種金鑰分裂系統之架構；

[0006]圖2例示依據本文揭示之一實施例用於圖1之金鑰分裂系統的一資料處理案例產生協定之流程圖；

5 [0007]圖3例示依據本文揭示之一實施例用於圖1之金鑰分裂系統的一資料儲存庫金鑰產生協定之流程圖；

[0008]圖4例示依據本文揭示之一實施例用於圖1之金鑰分裂系統的一資料處理案例金鑰產生協定之流程圖；

10 [0009]圖5例示依據本文揭示之一實施例用於圖1之金鑰分裂系統的一先前儲存物件取回協定之流程圖；

[0010]圖6例示依據本文揭示之一實施例一種金鑰分裂方法；

[0011]圖7例示依據本文揭示之一實施例該金鑰分裂方法之進一步細節；及

15 [0012]圖8例示依據本文揭示之一實施例一種電腦系統。

【實施方式】

較佳實施例之詳細說明

20 [0013]為求簡明與例示目的，本文揭示係主要參考實例描述。於後文詳細說明部分中，陳述無數特定細節以供徹底瞭解本文揭示。但顯然易知不限於此等特定細節可實施本文揭示。於其它情況下，若干方法及結構並未以細節描述以免不必要地遮掩本文揭示。

[0014]於本文揭示之全文中，「一(a)」及「一(an)」等

詞意圖表示特定元件中之至少一者。如此處使用，「包括」一詞表示包括但非限制性，「包括有」一詞表示包括有但非限制性。「基於」一詞表示至少部分基於。

[0015]資料之加密及解密用的對稱性金鑰典型地包括使用相同密碼金鑰用於明文的加密及密文的解密兩者。至於該等對稱性金鑰，金鑰典型地為相同，或在二金鑰間可能進行變換。用於資料的加密及解密之非對稱性金鑰典型地包括兩個分開的金鑰，其中一者為秘密(或專用)及其中一者為公開。至於資料的加密及解密，金鑰分裂典型地包括一金鑰分割或解密過程分割成二或多個部分，因此若未藉將全部的部分統一而重建該金鑰，則任何部分本身皆無法使用。

[0016]認證過程可包括決定所接收的資料是否為所發送的資料之過程。認證過程也可包括藉由使用例如基於雜湊之訊息認證(HMAC)認證資料之真實性，及其它驗證技術。

[0017]金鑰管理可包括用於資料的加密、解密、或認證，及/或用於產生額外金鑰的金鑰管理。舉例言之，用於金鑰管理，各個主金鑰及其相應的加密資料項之集合可置於單一資料擁有者的控制之下。此類型金鑰管理可用作為計算系統之部分，該計算系統使用對稱性金鑰密碼機制(其包括對稱性加密及對稱性認證處理)提供密碼服務。用於此種基於對稱性金鑰之密碼服務，一訊息的發送者與接收者，或一儲存檔案之作者與讀者通常分享相同特定加密/解

密金鑰或相同特定認證金鑰、或其中各自一者。存取此種金鑰可以由可能包含金鑰分裂能力的一金鑰管理器管理。

[0018]如此處描述，金鑰分裂典型地包括一金鑰的分裂或解密處理的分裂成二或多個部分，因而其本身並無任何部分可用以重建該金鑰。反而，各個部分可能需要統合來重建該金鑰。如此，金鑰分裂給一資料擁有者(後文標示為U，或用戶U)藉由防止其它實體確定該金鑰或解密程序而控制諸如資料的加密、解密、或認證等面向。

[0019]至於金鑰分裂，資料擁有者U可利用一金鑰管理器(後文標示為P)用於管理供資料保護用的金鑰。資料擁有者U可形成提供資料保護的短暫資料處理案例(特定第i個資料處理案例標示為 A_i)。舉例言之，一短暫資料處理案例可代表資料擁有者U在一集合資料上執行資料的加密或解密，及其後可拋棄該短暫資料處理案例。金鑰管理器可能無法信賴知曉金鑰值。

[0020]於若干實施例中，與金鑰管理器P之通訊可使用部分同型加密技術，諸如ElGamal加密。ElGamal加密技術為基於迪赫(Diffie-Hellman)金鑰交換的用於公鑰密碼術之非對稱性金鑰加密法。至於與金鑰管理器P通訊，也可使用其它類型的加密技術。

[0021]至於金鑰分裂，資料擁有者U可形成一主金鑰(後文標示為K)。代表資料擁有者用於管理資料物件(亦即由該使用者所擁有的資料之部分)的特定金鑰可從主金鑰K推導而得。為了處理針對個別資料物件的特定金鑰，資料擁有

者U可啟動一短暫資料處理案例 A_i 的形成，且可發送在該金鑰管理器的公鑰之下加密的主金鑰K給資料處理案例 A_i 。資料處理案例 A_i 可產生一隨機遮罩 γ_i 。

[0022]資料處理案例 A_i 可使用一非對稱性金鑰加密法的同型性質組合隨機遮罩 γ_i 之加密與主金鑰K之加密。同型性質可指一種加密形式，其允許在密文上進行特定類型的運算，且產生一加密結果，其當解密時匹配在用以產生該密文的原先文本上進行操作的結果。於此一實施例中，經由隨機遮罩 γ_i 之加密與主金鑰K之加密的組合所產生的密文為 $K*\gamma_i$ (亦即K與 γ_i 的乘積)之加密。K與 γ_i 的密文可於包括同型性質的非對稱性金鑰加密法潛在的群組結構(例如，用於ElGamal加密的群組G)決定。資料處理案例 A_i 可發送此種密文給金鑰管理器P。又，資料處理案例 A_i 可紀錄隨機遮罩 γ_i 之值。

[0023]隨機遮罩 γ_i 可用作為由金鑰管理器P與該資料處理案例之短暫例示分享的一遮罩。隨機遮罩 γ_i 可為暗中分享，在於金鑰管理器P並不知曉隨機遮罩 γ_i 之值。如此，金鑰管理器P經由其暗中知識而非明確知識而調用隨機遮罩 γ_i 的使用。金鑰管理器P可使用一密鑰以解密該經遮罩的主金鑰(亦即K及 γ_i 之密文)用以獲得該值 $K*\gamma_i$ (亦即K與 γ_i 的乘積)，且儲存該值用來與資料處理案例 A_i 通訊。

[0024]用於個別資料物件的加密、解密、及/或其它認證的金鑰可形成為 α_j/K 形式，於該處 α_j 為一隨機值，使得資料處理案例 A_i 知曉該金鑰，同時金鑰管理器P知曉 α_j 且儲存

α_j 作為此一金鑰的遮罩。舉例言之，金鑰管理器可選取一隨機值 α_j ，及發送 $\alpha_j/(K*\gamma_i)$ 給知曉 γ_i 的資料處理案例 A_i ，使得資料處理案例可決定 $[\alpha_j/(K*\gamma_i)]*\gamma_i$ 用以回復 α_j/K 。此等值有關 α_j 、 K 、及 γ_i ，及全部相關運算可在包括同型性質的潛在群組(例如，用於EIGamal加密的群組 G)進行。前文就針對個別資料物件之一特定金鑰產生描述之方法，在本資料處理案例 A_i 不再存在之後，稍後可用以使用針對本金鑰 α_j/K 的原先遮罩，及 γ_i 之新值其係用作為與本資料處理案例分享的遮罩，允許金鑰管理器 P 提供新形成的資料處理案例以回復該金鑰。

[0025]依據實施例，此處揭示一種金鑰分裂系統及用於金鑰分裂之方法。至於金鑰分裂，系統及方法大致可運用任何安全通訊系統，無需同型加密技術。安全通訊系統之非限制性實例可包括系統其使用安全非對稱性加密技術，諸如RSA、橢圓曲線密碼術等。同型加密大致上描述為加密形式，其允許在密文上進行特定類型的運算，及產生一加密結果，其當解密時匹配在明文上執行操作的結果。需要避免使用同型加密技術可減低運算成本(例如，處理時間、儲存、能量利用等)。舉例言之，至於使用包括同型性質的非對稱性金鑰加密方法，此等技術基於相對較長群組元件(例如，2048位元長度)的使用可以是運算成本密集，比較相對較短的位元字符號(例如，128或256位元長度)，其可用於此處揭示的系統及方法實例。

[0026]針對此處揭示的系統及方法實例，隨機遮罩 γ_i 可

由資料擁有者選擇(亦即資料擁有者U可選擇針對遮罩 γ_i 的一隨機值),使得非對稱性加密技術可用於金鑰分裂。至於如此處使用的資料擁有者U一詞,如由資料擁有者U執行的所描述功能及資料擁有者U相關的資訊可由資料擁有者計算裝置所執行及相關。概略言之,用於此處揭示的系統及方法,資料擁有者U可選擇一隨機遮罩 γ_i ,在金鑰管理器的公鑰之下加密 $\gamma_i * K$,且發送明文連同隨機遮罩 γ_i 給資料處理案例 A_i 。「*」符號可表示任何運算,諸如XOR、乘法、加法等。資料處理案例 A_i 可紀錄隨機遮罩 γ_i ,及轉送密文給金鑰管理器P,其可解密及紀錄 $\gamma_i * K$ 。至於如此處使用的金鑰管理器P一詞,如由金鑰管理器P執行的所描述功能及金鑰管理器P相關的資訊可由資料擁有者計算裝置所執行及相關。

[0027]針對此處揭示的系統及方法實例,值 K 、 γ_i 、及 α_j 可以是適當長度的位元字符串,有關一群組的元件其為固定長度的位元字符串,逐位元XOR作為群組運算。前述金鑰分裂服務的運算 $K * \gamma_i$ 、 α_j / K 等可以是此一方便群組中的運算。金鑰之長度可根據管理金鑰的密碼服務(例如加密、解密、或認證方法之細節)而予選擇。

[0028]針對此處揭示的系統及方法實例,比較同型加密技術的使用,假設安全對稱性金鑰系統之金鑰長度為256位元,在256位元上的XOR運算通常比同型加密運算更為有效。就密碼分析技術而言,此等256位元值可考慮為安全。隨著運算威力的提高(例如遵照摩爾定律等)且隨著密碼分

析的改良，此等位元長度可徐緩增長。可預期對稱性金鑰長度繼續維持比非對稱性金鑰長度相對地更短。又，針對此處揭示的系統及方法實例，也消弭了將群組元件 α_j/K 轉換成有用的對稱性金鑰的需要，原因在於此等值可直接用作為位元字符串。舉例言之，有關具有固定長度位元字符串的一群組的元件，以逐位元XOR作為群組運算，值K及 α_j 可以是具有適當長度的位元字符串。

[0029]依據一實施例，金鑰分裂系統可包括至少一個處理器及一記憶體儲存機器可讀取指令，其當由該至少一個處理器執行時使得該至少一個處理器自一實體(例如資料擁有者U)接收與欲被加密、解密、或認證的資料相關的一主金鑰K。用以加密、解密、或認證該資料的一資料金鑰 S_j 可自該主金鑰K及接收自該實體與該資料相關的一遮罩 γ_i 導算出。機器可讀取指令可進一步轉送主金鑰藉使用遮罩而予遮罩的一版本(例如 $K*\gamma_i$)給金鑰管理器P用以管理該資料金鑰 S_j 及產生一資料處理案例 A_i 用以運用該資料金鑰以加密、解密、或認證該資料。該等機器可讀取指令可進一步決定資料金鑰 S_j 用以基於藉資料處理案例 A_i 選取的一先前資料金鑰(例如，已知 S_j)而加密、解密、或認證該資料。

[0030]圖1例示依據本文揭示之一實施例一金鑰分裂系統100(後文又稱「系統100」)之架構。參考圖1及圖2，系統100描繪為包括一資料處理案例產生模組102用以產生一資料處理案例104的一例示i，資料處理案例104之第i個例示標示為 A_i 。資料處理案例產生模組102可實現一資料處理案例

產生協定200，如此處參考圖2描述。資料處理案例 A_i 可借助於一資料擁有者106(標示為U)實例化，該資料擁有者106保有一主金鑰108(標示為K)及一虛擬金鑰管理模組110(標示為P)。資料擁有者U也可選擇一隨機遮罩122(標示為 γ_i)以產生主金鑰K之遮罩版本，如此處參考資料處理案例產生協定200之描述。虛擬金鑰管理模組P，其可在與含資料擁有者U的系統分開的一系統，或其可在與資料擁有者U的相同系統，可輔助各種加密金鑰跨資料處理案例104的不同例示 A_i 之維持。用於資料處理案例產生協定200，在資料擁有者U與虛擬金鑰管理模組P之間可能無需通訊。

[0031]為了自包括資料114的一資料儲存庫112取回已解密資料，資料擁有者U可啟動一資料處理案例 A_i 。資料處理案例 A_i 可以是短暫的。資料處理案例 A_i 可用來與虛擬金鑰管理模組P互動以便重建特定金鑰。資料處理案例 A_i 之不同例示間之狀態可由資料擁有者U在全部例示 A_i 使用相同主金鑰K而予維持，且由虛擬金鑰管理模組P儲存該特定金鑰 $S_j * K$ (於該處 S_j 表示一字符串，表示用於加密、解密、或認證、或驗證一資料物件的真實性之第j個特定金鑰)之一經遮罩版本而予維持。

[0032]系統100之一資料儲存庫金鑰產生模組116可產生一新特定金鑰 S_j ，用以加密、解密、或認證、或驗證在資料儲存庫112上的資料114的真實性。資料儲存庫金鑰產生模組116可由資料擁有者U及/或由虛擬金鑰管理模組P具體實施，但顯示為於圖1之系統100之實例中獨立實施。如

此處參考圖3之描述，資料儲存庫金鑰產生模組116可具體實施一資料儲存庫金鑰產生協定300。資料儲存庫金鑰產生模組116可提供用於此種特定金鑰 S_j 之盲目(亦即經遮罩)版本由虛擬金鑰管理模組P的儲存及使用。

5 [0033]系統100之一資料處理案例金鑰產生模組118可提供給資料處理案例104用於動態產生特定金鑰 S_j ，及發送所產生的金鑰之盲目版本給虛擬金鑰管理模組P。資料處理案例金鑰產生模組118可由資料擁有者U及/或由虛擬金鑰管理模組P具體實施，但顯示為於圖1之系統100之實例中獨立實施。如此處參考圖4之描述，資料處理案例金鑰產生模
10 組118可具體實施一資料處理案例金鑰產生協定400。

[0034]系統100之一先前儲存物件取回模組120可具體實施自資料儲存庫112取回一先前儲存物件。先前儲存物件取回模組120可由資料擁有者U及/或由虛擬金鑰管理模組P
15 具體實施，但顯示為於圖1之系統100之實例中獨立實施。如此處參考圖5之描述，先前儲存物件取回模組120可具體實施一先前儲存物件取回協定。

[0035]用於該系統100，使用例如透過建立在一既有公鑰基礎架構(PKI)上的安全套接層(SSL)或傳輸層安全性(TLS)所具體實施的通道，不同的實體可在其間安全地通訊。參考圖1-5，金鑰及遮罩元件 K 、 S_j 、 α_j 等可以是具有適當長度的位元-字符串(亦即用於密碼金鑰處理的位元-字符串，其金鑰係藉使用系統100之金鑰分裂協定管理)，及「 $\oplus$ 」
20 可用於互斥或(XOR)。

[0036]圖2例示依據本文揭示之一實施例，用於產生一資料處理案例 A_i 的資料處理案例產生協定200之流程圖。雖然下述方法的執行係參考圖1之系統100描述，但熟諳技藝人士顯然易知其它適合用於執行此等方法的裝置。圖2之流程圖中描述的方法及其它圖式中描述的方法，可以採取儲存於諸如圖8的記憶體806及/或二次資料儲存裝置808之一機器可讀取儲存媒體上的可執行指令之形式，藉由此處描述之一或多個模組來具體實施，及/或以電子電路形式具體實施。

[0037]參考圖2，於方塊202，資料擁有者U可隨機選取主金鑰K(亦即針對主金鑰K選擇一隨機值)。另外，資料擁有者U可從先前產生的金鑰之一選擇中取回主金鑰K。

[0038]於方塊204，資料擁有者U可選取隨機遮罩 γ_i (亦即針對遮罩 γ_i 選擇一隨機值)。

[0039]於方塊206，資料擁有者U可發送主金鑰K互斥或隨機遮罩 γ_i (即 $K \oplus \gamma_i$)給該虛擬金鑰管理模組P。亦即，資料擁有者U可發送呈遮罩形式的隨機遮罩 γ_i 給虛擬金鑰管理模組P。主金鑰K也可由擁有資料114的資料擁有者U選取。

[0040]於方塊208，資料擁有者U可發送隨機遮罩 γ_i 給資料處理案例 A_i 。

[0041]於方塊210，虛擬金鑰管理模組P可儲存主金鑰K互斥或隨機遮罩 γ_i (亦即 $K \oplus \gamma_i$)。換言之，虛擬金鑰管理模組P可儲存由K所遮罩的隨機遮罩 γ_i ，於該處 $K \oplus \gamma_i$ 係由逐位元互斥或運算決定。至於系統100，非暫態儲存媒體可耦合至

虛擬金鑰管理模組P用以儲存與該虛擬金鑰管理模組P相關的任何資訊(例如 $K \oplus \gamma_i$ 、 α_j 等)。

[0042]於方塊212，資料處理案例 A_i 可儲存隨機遮罩 γ_i 。隨機遮罩 γ_i 可由相應的資料處理案例 A_i 之短暫例示用於資料物件加密、解密、或認證、或真實性驗證相關的操作。至於系統100，非暫態儲存媒體可耦合至資料擁有者U用以儲存與該使用者及該資料處理案例 A_i 相關的任何資訊(例如 γ_i 、 S_j 等)。

[0043]至於資料處理案例產生協定200，就資料處理案例 A_i 而言主金鑰K的秘密性可藉所使用的非對稱性加密技術加以確保。就虛擬金鑰管理模組P而言主金鑰K的秘密性可基於遮罩係隨機選取，而非為虛擬金鑰管理模組P所知加以確保。

[0044]圖3例示依據本文揭示之一實施例該資料儲存庫金鑰產生協定300之流程圖。基於主金鑰K的特定案例遮罩 $K \oplus \gamma_i$ 之設定，此種特定案例遮罩可用以保護用於儲存物件的加密、解密、或認證、或真實性驗證的特定金鑰 S_j 。此點可藉由使得資料處理案例 A_i 與虛擬金鑰管理模組P互動進行，於該處虛擬金鑰管理模組P可儲存各種特定金鑰的盲目版本。資料儲存庫金鑰產生協定300可提供第j個特定金鑰 S_j 用以由隨後資料處理案例之不相關例示存取。

[0045]參考圖3，於方塊302，基於資料處理案例產生協定200用於資料處理案例 A_i 之方塊210及212，虛擬金鑰管理模組P可取回或以其它方式接收所儲存的主金鑰K互斥或隨

機遮罩 γ_i (亦即 $K \oplus \gamma_i$)作為輸入，及資料處理案例 A_i 可取回或以其它方式接收所儲存的隨機遮罩 γ_i 作為輸入。

[0046]於方塊304，資料處理案例 A_i 可轉送一請求給虛擬金鑰管理模組P用以產生具有指標j的一新金鑰。如此處描述，具有指標j的新金鑰可根據由虛擬金鑰管理模組P所做隨機選擇而決定。

[0047]於方塊306，虛擬金鑰管理模組P可隨機選擇 α_j ，及決定 $\beta_{ij} = \alpha_j \text{ XOR } (K \text{ XOR } \gamma_i)$ (亦即 $\beta_{ij} = \alpha_j \oplus (K \oplus \gamma_i)$)。針對方塊306， α_j 及 β_{ij} 可表示用於盲目用途的遮罩。

[0048]於方塊308，虛擬金鑰管理模組P可發送 β_{ij} 給資料處理案例 A_i 。

[0049]於方塊310，資料處理案例 A_i 可決定第j個特定金鑰 S_j 為 $\beta_{ij} \text{ XOR } \gamma_i$ (其係等於 $\alpha_j \text{ XOR } K$)。

[0050]於方塊312，資料處理案例 A_i 可儲存第j個特定金鑰 S_j 。

[0051]於方塊314，虛擬金鑰管理模組P可儲存 α_j (其係等於 $S_j \text{ XOR } K$)。

[0052]至於資料儲存庫金鑰產生協定300，由資料處理案例 A_i 輸出的字符串 S_j 可表示第j個特定金鑰 S_j 。於若干實施例中，替代直接使用金鑰 S_j 用於處理資料，可饋入金鑰 S_j 給一金鑰導函數(KDF)作為輸入，其輸出係用作為資料處理金鑰。藉此方式，可避免由虛擬金鑰管理模組P所儲存的資料上的相關金鑰攻擊，於該處該資料包括 $K \oplus S_1$ 、 $K \oplus S_2$ 、...、 $K \oplus S_j$ 等數值。

[0053]圖4例示依據本文揭示之一實施例該資料處理案例金鑰產生協定400之流程圖。

[0054]參考圖4，於方塊402，基於用於資料處理案例 A_i 的資料處理案例產生協定200之方塊210及212，虛擬金鑰管理模組P可取回或以其它方式接收所儲存的主金鑰K互斥或隨機遮罩 γ_i (亦即 $K \oplus \gamma_i$)作為輸入，及資料處理案例 A_i 可取回或以其它方式接收所儲存的隨機遮罩 γ_i 作為輸入。

[0055]於方塊404，資料處理案例 A_i 可轉送一請求給虛擬金鑰管理模組P用於具有指標j的一新金鑰。如此處描述，具有指標j的新金鑰可根據由資料處理案例 A_i 所做隨機選擇而決定。

[0056]於方塊406，資料處理案例 A_i 可隨機選擇第j個特定金鑰 S_j ，及決定 $\beta_{ij}=S_j \text{ XOR } \gamma_i$ ，(亦即 $\beta_{ij}=S_j \oplus \gamma_i$)。

[0057]於方塊408，資料處理案例 A_i 可轉送 β_{ij} 給虛擬金鑰管理模組P。

[0058]於方塊410，虛擬金鑰管理模組P可決定 α_j 為 $\beta_{ij} \text{ XOR } (K \text{ XOR } \gamma_i)$ (亦即 $\alpha_j=\beta_{ij} \oplus (K \oplus \gamma_i)$)。

[0059]於方塊412，資料處理案例 A_i 可儲存第j個特定金鑰 S_j 。

[0060]於方塊414，虛擬金鑰管理模組P可儲存 α_j (其等於 $S_j \text{ XOR } K$)。

[0061]至於資料處理案例金鑰產生協定400，由資料處理案例 A_i 輸出的字符串 S_j 可表示第j個特定金鑰 S_j 。於若干實施例中，替代直接使用金鑰 S_j 用於處理資料，可饋入金鑰

S_j 給一KDF作為輸入，其輸出係用作為資料處理金鑰。藉此方式，可避免由虛擬金鑰管理模組P所儲存的資料上的相關金鑰攻擊，於該處該資料包括 $K \oplus S_1$ 、 $K \oplus S_2$ 、...、 $K \oplus S_j$ 等數值。

5 [0062]圖5例示依據本文揭示之一實施例，先前儲存物件取回協定500之流程圖用以自資料儲存庫112取回一先前(亦即較舊的)儲存物件。

10 [0063]於方塊502，基於用於資料處理案例 A_i 的資料處理案例產生協定200之方塊210及212，虛擬金鑰管理模組P可取回或以其它方式接收所儲存的主金鑰 K 互斥或隨機遮罩 γ_i (亦即 $K \oplus \gamma_i$)作為輸入，及資料處理案例 A_i 可取回或以其它方式接收所儲存的隨機遮罩 γ_i 作為輸入。

15 [0064]於方塊504，虛擬金鑰管理模組P可取回或以其它方式接收 α_j 作為輸入，於該處 α_j 推定係以標示為 A_i 的資料處理案例之一先前例示產生。

20 [0065]於方塊506，資料處理案例 A_i 可轉送一請求給虛擬金鑰管理模組P用以請求具有指標 j 的先前產生的金鑰。如此處描述，具有指標 j 的先前產生的金鑰可根據由資料處理案例 A_i 的一隨機選擇而予決定。

[0066]於方塊508，虛擬金鑰管理模組P可取回 α_j ，及決定 $\beta_{ij} = \alpha_j \text{ XOR } (K \text{ XOR } \gamma_i)$ (亦即 $\beta_{ij} = \alpha_j \oplus (K \oplus \gamma_i)$)。

[0067]於方塊510，虛擬金鑰管理模組P可轉送 β_{ij} 給資料處理案例 A_i 。

[0068]於方塊512，資料處理案例 A_i 可決定第 j 個特定金

鑰 S_j 為 β_{ij} XOR γ_i ，(亦即 $S_j = \beta_{ij} \oplus \gamma_i$)。

[0069]於方塊514，資料處理案例 A_i 可儲存第 j 個特定金鑰 S_j 。於若干實施例中，替代直接使用金鑰 S_j 用於處理資料，可將金鑰 S_j 饋入給一KDF作為輸入，其輸出係用作為資料處理金鑰。藉此方式，可避免由虛擬金鑰管理模組P所儲存的資料上的相關金鑰攻擊，於該處該資料包括 $K \oplus S_1$ 、 $K \oplus S_2$ 、...、 $K \oplus S_j$ 等數值。

[0070]至於資料儲存庫金鑰產生協定300、資料處理案例金鑰產生協定400、及先前儲存物件取回協定500，特定金鑰 S_j 可用以推導多個金鑰，針對該資料114之一集合的資料物件中之各個資料物件各有一個金鑰。所推導的金鑰中之各者可以是對稱性或非對稱性。根據特定金鑰 S_j ，所推導的金鑰可經決定因而形成階層式結構或樹狀結構。以用於信賴平台模組(TPM)，其乃安全密碼處理器的國際標準，之一例的金鑰階層關係為例，各個節點(於該樹)可包括兩個金鑰，一個為對稱性及另一個為非對稱性。

[0071]系統100之該等模組及其它元件可以是儲存於非暫態電腦可讀取媒體上的機器可讀取指令。就此方面而言，系統100可包括或可以是非暫態電腦可讀取媒體。此外或另外，系統100之該等模組及其它元件可以是硬體或機器可讀取指令與硬體的組合。

[0072]圖6及圖7分別為對應金鑰分裂系統100之一實例，其組成容後詳述，用於金鑰分裂的方法600及700之流程圖。方法600及700可參考圖1-5在金鑰分裂系統100具體

實施，舉例說明但非限制性。方法600及700可於其它系統實施。

[0073]參考圖6，針對方法600，於方塊602，該方法可包括產生一主金鑰。舉例言之，參考圖1及圖2，於方塊202，資料擁有者U可產生主金鑰K。

[0074]於方塊604，該方法可包括產生一隨機遮罩。舉例言之，參考圖1及圖2，於方塊204，資料擁有者U可產生隨機遮罩 γ_i (亦即產生用於遮罩 γ_i 之一隨機值)。

[0075]於方塊606，該方法可包括藉由使用該隨機遮罩而產生該主金鑰的一經遮罩版本。舉例言之，參考圖1及圖2，資料擁有者U可產生主金鑰K互斥或隨機遮罩 γ_i (亦即 $K \oplus \gamma_i$)。

[0076]於方塊608，該方法可包括轉送該主金鑰的經遮罩版本給一金鑰管理器。舉例言之，參考圖1及圖2，於方塊206，資料擁有者U可產生主金鑰K互斥或隨機遮罩 γ_i (亦即 $K \oplus \gamma_i$)給虛擬金鑰管理模組P。

[0077]於方塊610，回應於轉送該主金鑰的經遮罩版本，該方法可包括自金鑰管理器接收一新遮罩。舉例言之，參考圖1-3，於方塊308，資料處理案例 A_i 可自虛擬金鑰管理模組 P_i 接收 β_{ij} 。

[0078]於方塊612，該方法可包括基於新遮罩及隨機遮罩決定一資料金鑰。舉例言之，參考圖1-3，於方塊310，資料處理案例 A_i 可決定第j個特定金鑰 S_j 為 $\beta_{ij} \text{ XOR } \gamma_i$ (其係等於 $\alpha_j \text{ XOR } K$)。

[0079] 依據一實施例，針對方法600，產生經遮罩版本可包括使用互斥或、加法、或乘法運算以產生主金鑰的經遮罩版本(例如，參考圖2之方塊206)。

5 [0080] 依據一實施例，針對方法600，基於新遮罩及隨機遮罩決定資料金鑰可包括基於新遮罩與隨機遮罩間之互斥或運算而決定資料金鑰(例如，參考圖3之方塊310)。

[0081] 依據一實施例，針對方法600，新遮罩可基於由金鑰管理器對另一遮罩(例如， α_j)之隨機選取及主金鑰的經遮罩版本(例如，參考圖3之方塊306)。

10 [0082] 依據一實施例，方法600可進一步包括產生一資料處理案例，用以運用該資料金鑰而加密、解密、或認證該資料。舉例言之，參考圖1，資料處理案例產生模組102可產生資料處理案例104的一例示i，資料處理案例104的第i個例示標示為 A_i 。

15 [0083] 依據一實施例，針對方法600，產生該資料處理案例可進一步包括產生該資料處理案例之一短暫例示，用以運用該隨機遮罩及該資料金鑰而加密、解密、或認證該資料，且利用該資料處理案例之另一短暫例示，其運用另一隨機遮罩及另一資料金鑰而加密、解密、或認證額外資料。

20

[0084] 依據一實施例，針對方法600，該資料可包括一集合之資料物件，及該方法600可進一步包括使用該資料金鑰用以推導多個資料金鑰，於該處該等多個資料金鑰中之各個資料金鑰對應該集合之資料物件中之一個別資料物

件。舉例言之，參考圖1-5，有關資料儲存庫金鑰產生協定300、資料處理案例金鑰產生協定400、及先前儲存物件取回協定500，該特定金鑰 S_j 可用以推導多個金鑰，於該處該等多個資料金鑰中之各個資料金鑰對應該集合之資料物件中之一個別資料物件。

[0085]參考圖7，針對方法700，於方塊702，該方法可包括於資料相關的一實體產生一主金鑰。舉例言之，參考圖1及圖2，於方塊202，資料擁有者U可產生主金鑰K。

[0086]於方塊704，該方法可包括於資料相關的一實體產生一遮罩。舉例言之，參考圖1及圖2，於方塊204，資料擁有者U可產生遮罩 γ_i 。

[0087]於方塊706，該方法可包括藉使用該遮罩而產生該主金鑰之一經遮罩版本。舉例言之，參考圖1及圖2，資料擁有者U可產生主金鑰K互斥或遮罩 γ_i (亦即 $K \oplus \gamma_i$)。

[0088]於方塊708，該方法可包括轉送該主金鑰之該經遮罩版本給一金鑰管理器。舉例言之，參考圖1及圖2，資料擁有者U可轉送主金鑰K互斥或遮罩 γ_i (亦即 $K \oplus \gamma_i$)給虛擬金鑰管理模組P。

[0089]於方塊710，該方法可包括自該金鑰管理器接收一新遮罩，於該處該新遮罩係與一先前資料金鑰有關。舉例言之，參考圖1、2、及5，於方塊510，資料處理案例 A_i 可自虛擬金鑰管理模組P接收 β_{ij} ，於該處 β_{ij} 係與先前資料金鑰 S_j 有關。

[0090]於方塊712，該方法可包括根據新遮罩及由與資

料相關的實體產生的遮罩而決定該先前資料金鑰。舉例言之，參考圖1、2、及5，於方塊512，資料處理案例 A_i 可決定第 j 個特定金鑰 S_j 為 β_{ij} 互斥或 γ_i (亦即 $S_j = \beta_{ij} \oplus \gamma_i$)。

5 [0091]依據一實施例，針對方法700，該資料可包括一集合之資料物件，及方法700可進一步包括使用該先前資料金鑰用以推導多個資料金鑰，於該處該等多個資料金鑰中之各個資料金鑰對應該集合之資料物件中之一個別資料物件。舉例言之，參考圖1-5，有關資料儲存庫金鑰產生協定300、資料處理案例金鑰產生協定400、及先前儲存物件取
10 回協定500，該特定金鑰 S_j 可用以推導多個金鑰，於該處該等多個資料金鑰中之各個資料金鑰對應該集合之資料物件中之一個別資料物件。

[0092]依據一實施例，方法700可進一步包括產生一資料處理案例，用以運用該資料金鑰而加密、解密、或認證
15 該資料。舉例言之，參考圖1，資料處理案例產生模組102可產生資料處理案例104的一例示 i ，資料處理案例104的第 i 個例示標示為 A_i 。

[0093]依據一實施例，針對方法700，於資料相關的該實體產生該遮罩可進一步包括於資料相關的該實體產生一
20 隨機遮罩。舉例言之，參考圖1及圖2，於方塊204，資料擁有者 U 可產生隨機遮罩 γ_i (亦即產生針對遮罩 γ_i 的一隨機值)。

[0094]依據一實施例，針對方法700，資料可包括一指標。新遮罩可藉該資料之該指標而與先前資料金鑰相關。舉例言之，參考圖1、2、及5，於方塊506，資料處理案例

A_i 可轉送一請求給虛擬金鑰管理模組P用以請求具有指標j的該先前產生的金鑰(亦即該資料之該指標)。新遮罩 β_{ij} 可藉資料的指標j而與先前資料金鑰 S_j 有關。

[0095]依據金鑰分裂方法之另一個實施例，金鑰分裂可包括接收主金鑰K之一經遮罩版本(例如 $K \oplus \gamma_i$)(例如，參考圖2之方塊206)。主金鑰K可由在與資料相關實體(例如資料擁有者U)所產生的一遮罩 γ_i 遮罩(例如參考圖2之方塊204)。金鑰分裂可進一步包括接收一新遮罩 β_{ij} ，其係根據先前資料金鑰 S_j 的選擇及進一步根據在與資料相關實體所產生的該遮罩 γ_i (例如參考圖4之方塊406及408)。又一新遮罩 α_j 可根據新遮罩 β_{ij} 決定，其係根據先前資料金鑰 S_j 的選擇及其係根據主金鑰之經遮罩版本(例如參考圖4之方塊410)。依據一實施例，新遮罩可根據先前資料金鑰 S_j 的隨機選擇(例如參考圖4之方塊406)。依據一實施例，又一新遮罩可根據新遮罩 β_{ij} 與主金鑰之經遮罩版本(例如 $K \oplus \gamma_i$)間之XOR運算決定(例如參考圖4之方塊410)。

[0096]圖8顯示可配合此處描述之實例使用的一電腦系統800。電腦系統800可表示一通用平台，其包括組件其可位於伺服器或另一電腦系統。電腦系統800可用作為系統100之平台。電腦系統800可由處理器(例如單一或多個處理器)或其它硬體處理電路執行此處描述之方法、功能及其它處理。此等方法、功能及其它處理可實施為儲存在一電腦可讀取媒體上的機器可讀取指令，其可以是非暫態，諸如硬體儲存裝置(例如，隨機存取記憶體(RAM)、唯讀記憶體

(ROM)、可抹除可規劃ROM(EPROM)、可電氣抹除可規劃ROM(EEPROM)、硬體驅動裝置、及快閃記憶體)。

[0097] 電腦系統800可包括一處理器802其可實施或執行機器可讀取指令從事部分或全部此處描述之方法、功能及其它處理。來自處理器802的指令及資料可透過通訊匯流排804通訊。電腦系統也可包括一主記憶體806，諸如隨機存取記憶體(RAM)，於執行時間期間處理器802的機器可讀取指令及資料可駐在該處，及一二次資料儲存裝置808，其可以是非依電性及儲存機器可讀取指令及資料。記憶體及資料儲存裝置為電腦可讀取媒體之實例。記憶體806可包括一金鑰分裂模組820，包括於執行時間期間駐在記憶體806且可由處理器802執行的機器可讀取指令。金鑰分裂模組820可包括圖1顯示之系統100之該等模組。

[0098] 電腦系統800可包括一I/O裝置810，諸如鍵盤、滑鼠、顯示器等。電腦系統可包括用於連結至網路的一網路介面812。可增加或取代電腦系統中之其它已知電子組件。

[0099] 前文揭示描述金鑰分裂的多個實例。所揭示的實例可包括用於金鑰分裂的系統、裝置、電腦可讀取儲存媒體、及方法。用於解釋目的，某些實例係參考圖1-8例示的組件描述。然而，例示之組件的功能可能重疊，且可能存在於更少數或更多數元件或組件。又，例示元件之全部或部分功能可並存或分布在數個地理上分散位置。再者，所揭示實例可於各種環境實施而不限於例示實例。

[0100]又，關聯圖1-8描述之操作順序為實例而非意圖為限制性。不背離所揭示實例之範圍可使用或可攻變額外的或更少的操作或操作之組合。又復，符合所揭示實例之具體實施例無需以任何特定順序執行操作順序。如此，本文揭示僅陳述具體實施例之可能實例，及對所描述之實例可做許多變化及修改。全部此等變化及修改意圖皆係含括於本文揭示之範圍且受如下申請專利範圍保護。

【符號說明】

100...金鑰分裂系統	502-514、602-612、
102...資料處理案例產生模組	702-712...方塊
104...資料處理案例	300...資料儲存庫金鑰產生協
106...資料擁有者	定
108...主金鑰	400...資料處理案例金鑰產生
110...虛擬金鑰管理模組	協定
112...資料儲存庫	500...先前儲存物件取回協定
114...資料	600、700...方法
116...資料儲存庫金鑰產生模 組	800...電腦系統
118...資料處理案例金鑰產生 模組	802...處理器
120...先前儲存物件取回模組	804...通訊匯流排
122...隨機遮罩	806...主記憶體
200...資料處理案例產生協定	808...二次資料儲存裝置
202-212、302-314、402-414、	810...I/O裝置
	812...網路介面
	820...金鑰分裂模組

申請專利範圍

1. 一種非暫態電腦可讀媒體，其上儲存機器可讀指令用以提供金鑰分裂，該等機器可讀指令當執行時使得至少一個處理器用以：

5 產生一主金鑰；

 產生一隨機遮罩；

 藉由使用該隨機遮罩而產生該主金鑰的一經遮罩版本；

 轉送該主金鑰的該經遮罩版本給一金鑰管理器；

10 響應於轉送該主金鑰的該經遮罩版本，自該金鑰管理器接收一新遮罩；及

 基於該新遮罩及該隨機遮罩而決定用於資料的一資料金鑰。

2. 如請求項1之非暫態電腦可讀媒體，其中用以產生該主金鑰的該經遮罩版本之該等機器可讀指令包含用以進行以下動作之指令：

 使用一互斥或(XOR)、一加法、及一乘法運算中之一者以產生該主金鑰的該經遮罩版本。

3. 如請求項1之非暫態電腦可讀媒體，其中基於該新遮罩及該隨機遮罩而決定該資料金鑰之該等機器可讀指令包含用以進行以下動作之指令：

20 基於該新遮罩與該隨機遮罩間之一互斥或(XOR)運算而決定該資料金鑰。

4. 如請求項1之非暫態電腦可讀媒體，其中該新遮罩係基於該金鑰管理器對另一遮罩的一隨機選擇及該主金鑰的該經遮罩版本。

5. 如請求項1之非暫態電腦可讀媒體，其進一步包含用以進行以下動作之機器可讀指令：

產生一資料處理案例以運用該資料金鑰而加密、解密、或認證該資料。

6. 如請求項5之非暫態電腦可讀媒體，其中用以產生該資料處理案例的該等機器可讀指令包含用以進行以下動作之指令：

產生該資料處理案例之一短暫例示以運用該隨機遮罩及該資料金鑰而加密、解密、或認證該資料；及

利用該資料處理案例之另一短暫例示，其運用另一隨機遮罩及另一資料金鑰，來加密、解密、或認證進一步資料。

7. 如請求項1之非暫態電腦可讀媒體，其中該資料包含一集合之資料物件，及其中該等機器可讀指令進一步包含用以進行以下動作之指令：

使用該資料金鑰以推導多個資料金鑰，其中該等多個資料金鑰中之各個資料金鑰對應於該集合之資料物件中的一個別資料物件。

8. 一種金鑰分裂系統，其包含：

至少一個處理器；及

一記憶體，儲存機器可讀指令，該等指令在由該至

少一個處理器執行時，使得該至少一個處理器用以：

接收一主金鑰的一經遮罩版本，其中該主金鑰係藉使用在與資料相關的一實體所產生的一遮罩而被遮罩；

5 接收一新遮罩，其係基於一先前資料金鑰之選擇及進一步基於在與該資料相關的該實體所產生的該遮罩；及

 基於該新遮罩而決定一進一步新遮罩，而該新遮罩係基於該先前資料金鑰之選擇及基於該主金
10 鑰的該經遮罩版本。

9. 如請求項8之金鑰分裂系統，其中該新遮罩係基於該先前資料金鑰之一隨機選擇。

10. 如請求項8之金鑰分裂系統，其中用以決定該進一步新遮罩的該等機器可讀指令進一步使得該至少一個處理
15 器用以：

 基於該新遮罩與該主金鑰的該經遮罩版本間之一互斥或(XOR)運算而決定該進一步新遮罩。

11. 一種用於金鑰分裂之方法，該方法包含：

 由包含一實體處理器的一電腦系統，在與資料相關
20 的一實體產生一主金鑰；

 由包含該實體處理器的該電腦系統，在與該資料相關的該實體產生一遮罩；

 由包含該實體處理器的該電腦系統，經由使用該遮罩而產生該主金鑰的一經遮罩版本；

由包含該實體處理器的該電腦系統，轉送該主金鑰的該經遮罩版本給一金鑰管理器；

由包含該實體處理器的該電腦系統，自該金鑰管理器接收一新遮罩，其中該新遮罩係與一先前資料金鑰有關；及

由包含該實體處理器的該電腦系統，基於該新遮罩及由與該資料相關的該實體所產生的該遮罩而決定該先前資料金鑰。

12. 如請求項11之方法，其中該資料包含一集合之資料物件，及其中該方法進一步包含：

由包含該實體處理器的該電腦系統，使用該先前資料金鑰以推導多個資料金鑰，其中該等多個資料金鑰中之各個資料金鑰對應該集合之資料物件中之一個別資料物件。

13. 如請求項11之方法，其進一步包含：

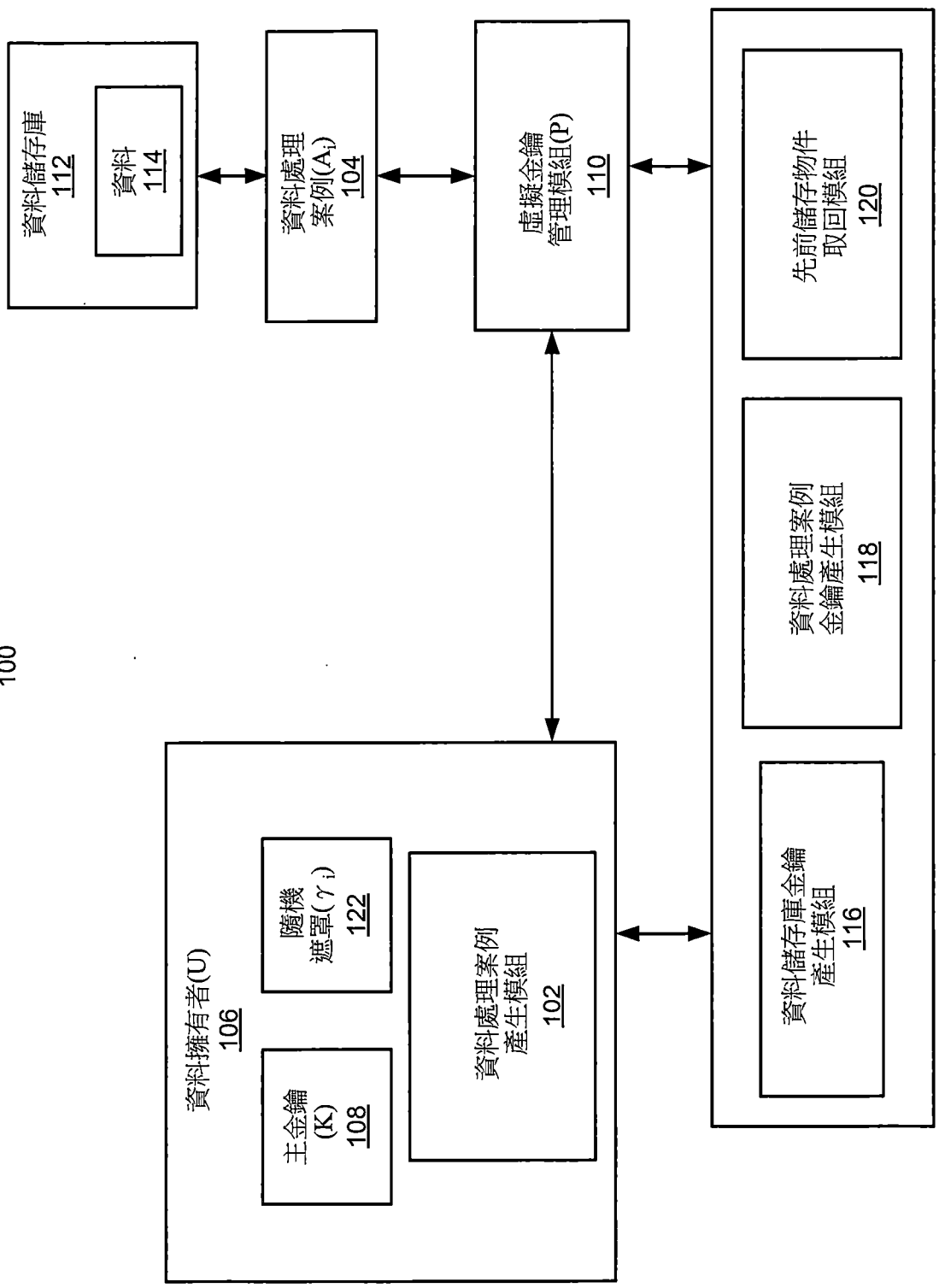
由包含該實體處理器的該電腦系統，產生一資料處理案例以運用一資料金鑰而加密、解密、或認證該資料。

14. 如請求項11之方法，其中在與該資料相關的該實體產生該遮罩進一步包含：

由包含該實體處理器的該電腦系統，在與該資料相關的該實體產生一隨機遮罩。

15. 如請求項11之方法，其中該資料包含一指標，及其中該新遮罩係藉該資料之該指標而與該先前資料金鑰相關。

金鑰分裂系統
100



圖式
1/8

雙面影印

圖1

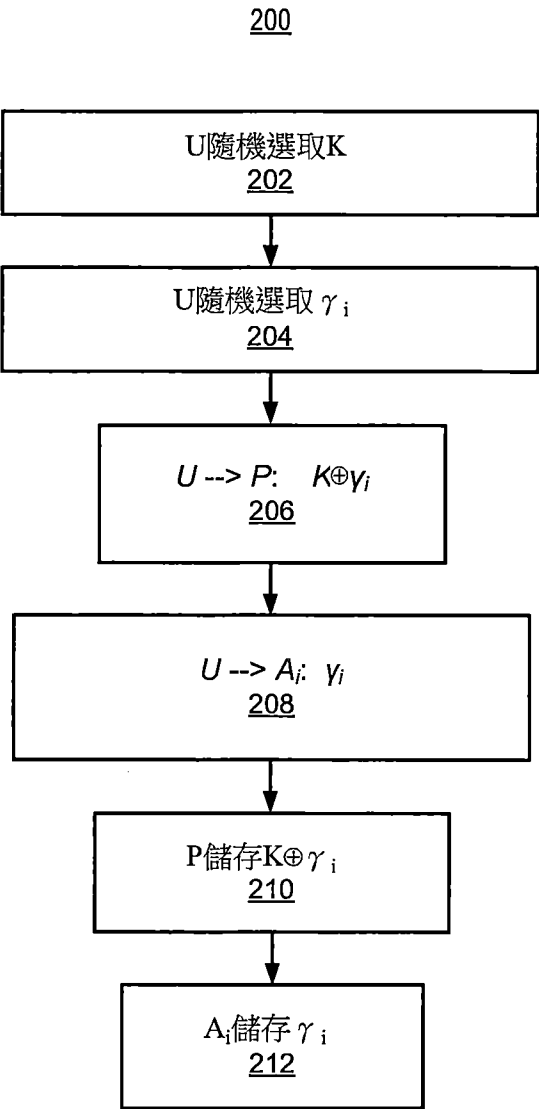


圖2

3/8
300

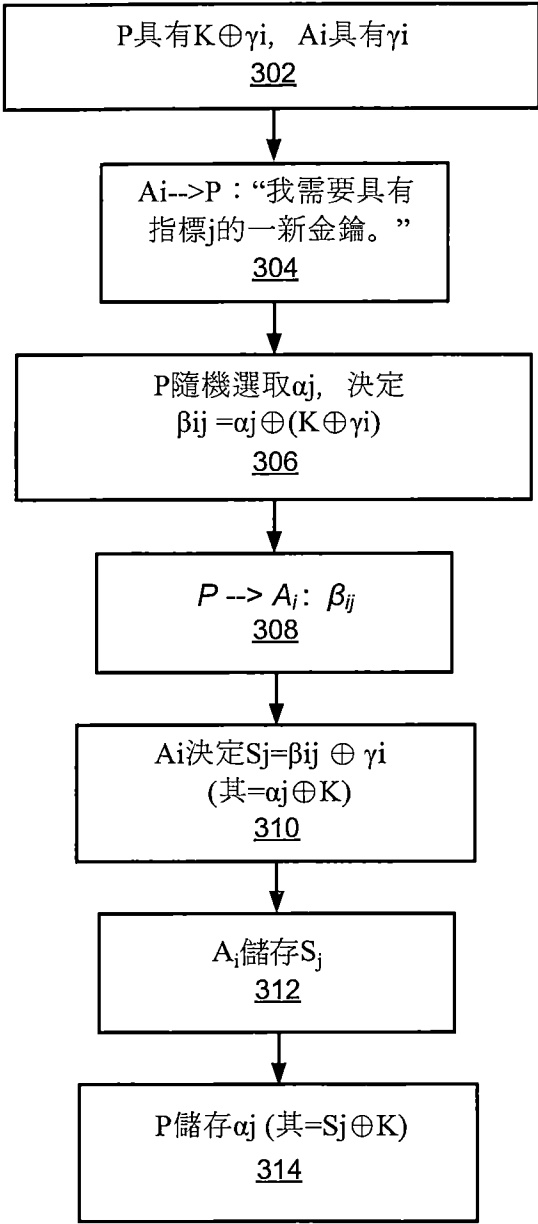


圖3

4/8
400

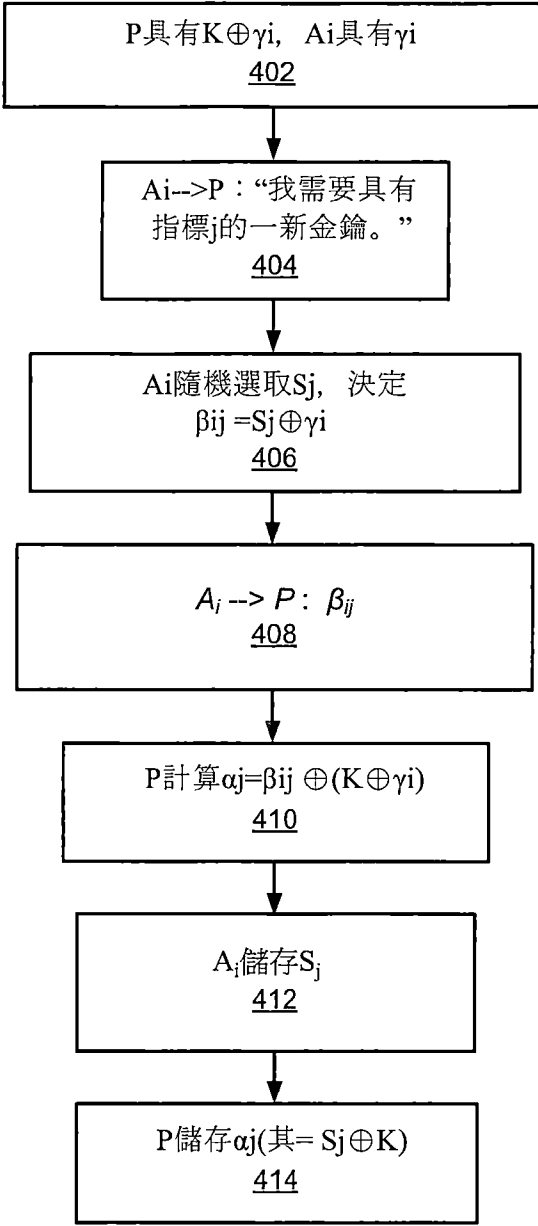


圖4

5/8

500

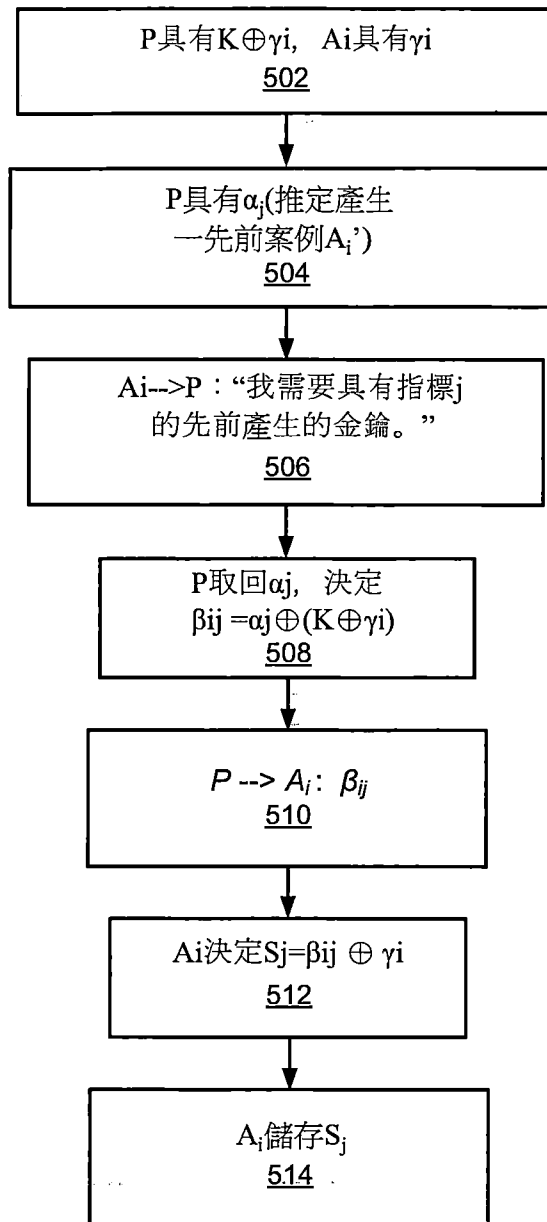


圖5

6/8
600

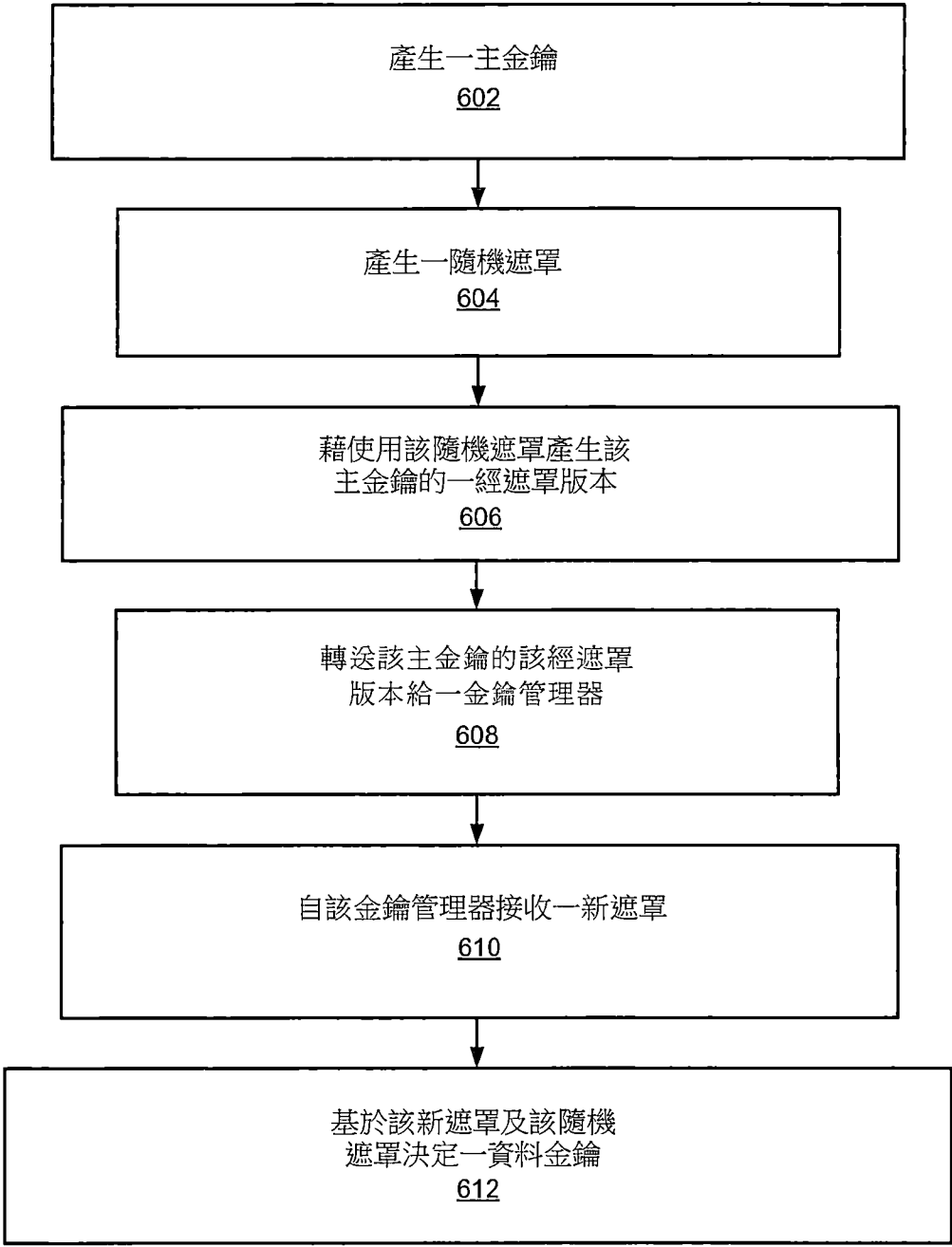


圖6

7/8

700

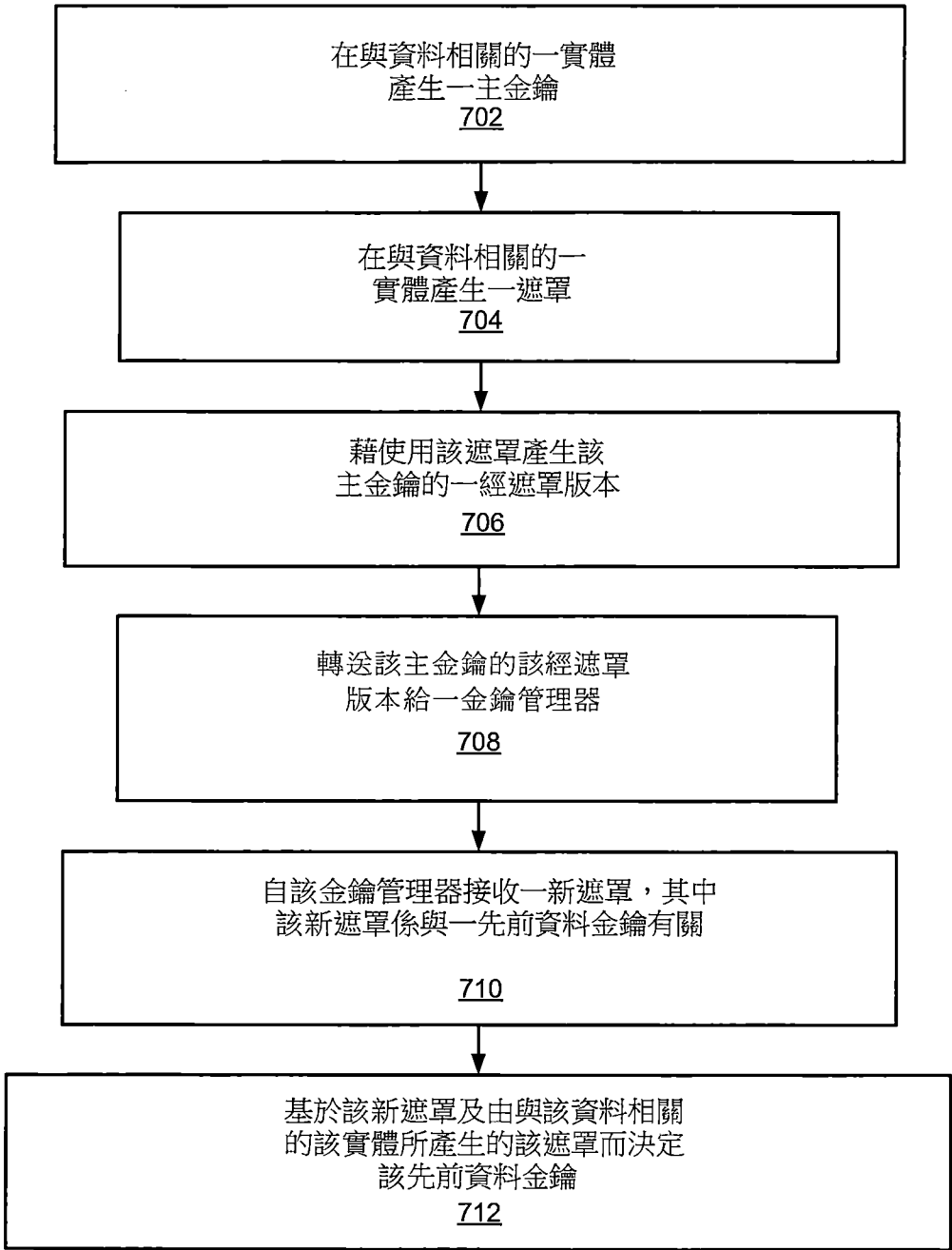


圖7

800

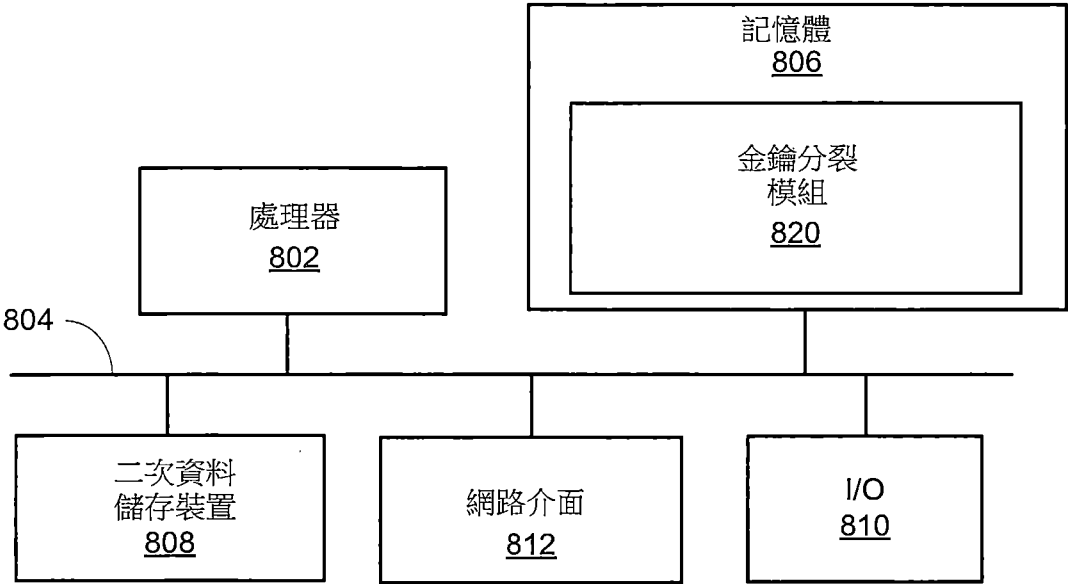


圖8