I889262

(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 I889262 B**

(45)公告日： 中華民國 114 (2025) 年 07 月 01 日

(21)申請案號：113111430 (22)申請日： 中華民國 113 (2024) 年 03 月 27 日

(51)Int. Cl.： ***G06F21/62 (2013.01)*** ***G06F21/79 (2013.01)***

(30)優先權：2023/06/09 美國 18/208,149

(71)申請人：美商萬國商業機器公司 (美國) INTERNATIONAL BUSINESS MACHINES CORPORATION (US)
美國

(72)發明人：傑奎特 格蘭 艾倫 JAQUETTE, GLEN ALAN (US)

(74)代理人：陳長文；黃章典；莊名宇

(56)參考文獻：

TW	200731224A	TW	201203092A
US	11641276B2	US	2022/0191019A1

審查人員：陳奕昌

申請專利範圍項數：24 項 圖式數：7 共 66 頁

(54)名稱

「類型」加密金鑰與每個ＩＯ金鑰致動之電腦實施方法、電腦系統及電腦程式產品

(57)摘要

根據本發明之一個態樣，一種電腦實施方法包括接收具有預定義長度之一位址欄的一命令。該位址欄中之位元的一第一子集識別一特定租戶之一外部金鑰，且該位址欄中之該等位元的一第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者。擷取由位元之該第一子集識別之該外部金鑰。亦擷取對應於位元之該第二子集之該類型金鑰。組合租戶金鑰與該類型金鑰以建立一組合式金鑰以用於加密及/或解密與該命令相關聯之資料。

A device-implemented method, in accordance with one aspect of the present invention, includes receiving a command having an address field of predefined length. A first subset of bits in the address field identify an external key of a particular tenant, and a second subset of the bits in the address field corresponds to one of a plurality of type keys associated with different data types. The external key identified by the first subset of bits is retrieved. The type key corresponding to the second subset of bits is also retrieved. The tenant and type keys are combined to create a combined key for use in encrypting and/or decrypting data associated with the command.

指定代表圖：

符號簡單說明：

300:方法

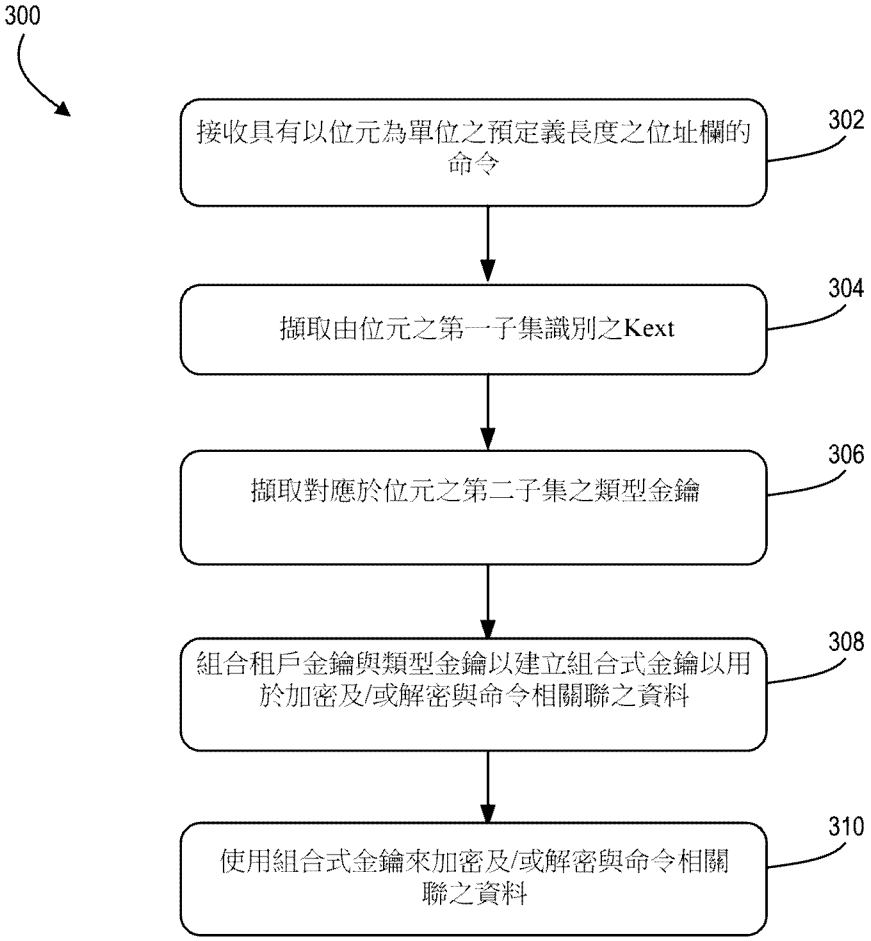
302:操作

304:操作

306:操作

308:操作

310:操作



【圖3】

I889262

【發明摘要】

【中文發明名稱】

「類型」加密金鑰與每個IO金鑰致動之電腦實施方法、電腦系統及電腦程式產品

【英文發明名稱】

COMPUTER-IMPLEMENTED METHOD, COMPUTER SYSTEM, AND COMPUTER PROGRAM PRODUCT OF 'TYPE' ENCRYPTION KEYS WITH KEY PER IO-ENABLED

【中文】

根據本發明之一個態樣，一種電腦實施方法包括接收具有預定義長度之一位址欄的一命令。該位址欄中之位元的一第一子集識別一特定租戶之一外部金鑰，且該位址欄中之該等位元的一第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者。擷取由位元之該第一子集識別之該外部金鑰。亦擷取對應於位元之該第二子集之該類型金鑰。組合租戶金鑰與該類型金鑰以建立一組合式金鑰以用於加密及/或解密與該命令相關聯之資料。

【英文】

A device-implemented method, in accordance with one aspect of the present invention, includes receiving a command having an address field of predefined length. A first subset of bits in the address field identify an external key of a particular tenant, and a second subset of the bits in the address field corresponds to one of a plurality of type keys associated with different data types. The external key identified by the first subset of bits

is retrieved. The type key corresponding to the second subset of bits is also retrieved. The tenant and type keys are combined to create a combined key for use in encrypting and/or decrypting data associated with the command.

【指定代表圖】

圖3

【代表圖之符號簡單說明】

300: 方法

302: 操作

304: 操作

306: 操作

308: 操作

310: 操作

【發明說明書】

【中文發明名稱】

「類型」加密金鑰與每個IO金鑰致動之電腦實施方法、電腦系統及電腦程式產品

【英文發明名稱】

COMPUTER-IMPLEMENTED METHOD, COMPUTER SYSTEM, AND COMPUTER PROGRAM PRODUCT OF 'TYPE' ENCRYPTION KEYS WITH KEY PER IO-ENABLED

【技術領域】

【0001】 本發明係關於每個IO金鑰(Key Per IO)，且更具體言之，本發明係關於能夠指定與每個IO金鑰致動之裝置一起使用之金鑰類型之技術及系統。

【先前技術】

【0002】 現代資料中心可使用能夠加密磁碟(ECD)。無論ECD屬於自加密磁碟(SED)類型，也無論儲存技術如何(例如，固態硬碟(SSD)、硬碟機(HDD)、由固態及硬碟技術構成之混合式硬碟或替代性非揮發性儲存技術磁碟)，ECD均能夠加密。

【0003】 ECD上之資料可使用媒體加密金鑰(MEK)來加密及解密，該媒體加密金鑰可為簡單地為給定租戶建立之唯一金鑰，或藉由組合ECD之加密金鑰與為給定租戶建立之唯一加密金鑰來建立，其中租戶可為個人、伺服器、虛擬機器(VM)、容器等。以此方式，將資料儲存於共用ECD上之各特定租戶無法獲得對其他租戶之資料的存取。

【0004】 術語「密碼抹除」通常指銷毀或永久停用對以某種方式解

密資料所需之加密金鑰的存取。此可例如藉由抹除加密金鑰之所有複本、移除加密金鑰之一部分、停用對產生或解除包裝(unwrap)加密金鑰所需之相關聯金鑰之存取等來進行。藉由永久停用加密金鑰，無法解密運用彼加密金鑰加密之資料；經加密資料實際上顯現為不可加密的。

【0005】 密碼抹除可在磁碟層級執行，例如藉由永久停用磁碟用於儲存於其上之所有資料之加密金鑰的所有複本。密碼抹除可在使用者層級執行，例如藉由永久停用使用者之加密金鑰。然而，停用使用者之加密金鑰會導致與彼使用者相關之所有資料不可讀。

【0006】 問題為加密裝置常常可僅同時處置為所有所要種類之密碼編譯刪除給出足夠粒度所需之金鑰數目之子集。此情形之一個實例為藉由可信賴運算群組之儲存工作群組之每個IO金鑰(KPIO)子群組開發之每個IO金鑰標準。

【0007】 KPIO當前允許16位元NVMe標頭欄指定應該使用哪一金鑰來加密及/或解密給定主機寫入及/或讀取。此可能允許符合KPIO規範的ECD或其他符合KPIO規範的加密裝置同時處置多達2^16 = 65,536個金鑰。此等金鑰中之各者可視為對應租戶之外部金鑰(Kext)，且此處將如此稱呼。然而，大部分符合KPIO規範的ECD (不管HDD抑或SSD)實際上將僅能夠同時容納及/或處置至多幾千個金鑰。舉例而言，估計當前最新技術之符合KPIO規範的ECD可容納至多4,096個不同金鑰。

【0008】 彼等4,096個金鑰可用於同時容納4,096個不同租戶。但設想到，彼等租戶中之各者處置不同資料類型，例如具有不同機密等級之資料，或自隱私觀點看具有不同等級之資料，或與待彼此保持分隔之不同專案相關的資料。

【0009】 對於本實例，假定給定租戶能夠處置16種不同資料類型。為允許所有租戶之所有給定資料類型待獨立地以密碼編譯方式抹除，吾人將必須開始為每個租戶指派多個金鑰。在給定實例中，吾人將需要每個租戶使用至多16個金鑰以允許獨立加密至多16種不同資料類型。多個金鑰之此指派將快速地使用可用金鑰空間。若給定符合KPIO規範的裝置僅可同時容納4,096個不同金鑰，且每個租戶必須容納至多16個金鑰，則彼裝置僅可容納4,096 / 16 = 256個不同租戶。

【0010】 雖然可進行權衡(例如，藉由將資料類型之數目限制降至8，以允許能夠處置4,096個金鑰之裝置容納多達512個租戶)，但所容納之更多資料類型直接減少可由裝置處置之租戶的數目。

【發明內容】

【0011】 根據本發明之一個態樣，一種裝置實施方法包括接收具有預定義長度之一位址欄的一命令。該位址欄中之位元的一第一子集識別一特定租戶之一外部金鑰，且該位址欄中之該等位元的一第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者。擷取由位元之該第一子集識別之該外部金鑰。亦擷取對應於位元之該第二子集之該類型金鑰。組合租戶金鑰與該類型金鑰以建立一組合式金鑰以用於加密及/或解密與該命令相關聯之資料。

【0012】 前述方法使得能夠同時處置較少數目個金鑰之裝置能夠容納約等於較少數目個金鑰之數個租戶，同時亦能夠針對租戶中之各者的不同資料類型使用唯一金鑰，如同裝置能夠處置許多倍之金鑰一樣。該方法亦實現諸如所有租戶之特定資料類型之密碼抹除之類的事情，在下文更詳細地描述。

【0013】 資料類型可包括隱私類型、機密類型等。如上文所提及，方法現使得能夠將特定金鑰用於此等資料類型。

【0014】 在一個較佳途徑中，該命令為一符合非揮發性記憶體高速(NVMe)規範的命令。本方法使得能夠使用NVMe命令來指定類型金鑰。

【0015】 裝置可經組態為每個IO金鑰致動之裝置。本方法為KPIO致動之裝置提供新能力。

【0016】 在一個途徑中，該方法包括：存取儲存於該裝置內之一內部金鑰；使用該內部金鑰及該組合式金鑰來產生一唯一媒體加密金鑰；及使用該媒體加密金鑰來加密及/或解密與該命令相關聯之資料。此特徵添加另外安全層，此係因為將需要內部金鑰來存取儲存於裝置上之資料。此外，可藉由簡單地銷毀內部金鑰及MEK(若儲存於裝置上)來在裝置中執行密碼抹除。此外，若MEK係藉由租戶金鑰、類型金鑰及內部金鑰之組合來建立，則彼MEK可藉由銷毀彼租戶金鑰、或彼類型金鑰或彼內部金鑰而經密碼抹除。因此，在此後一實例中，可以三個不同粒度層級執行密碼抹除，此取決於哪一金鑰被銷毀。

【0017】 較佳地，該裝置經組態以禁止以任何形式將該內部金鑰傳送至該裝置外部。此確保在裝置層級執行之密碼抹除停用使用內部金鑰加密之所有資料。

【0018】 在一個途徑中，該等外部金鑰中之數者個別地與儲存於同一邏輯區塊位址範圍中之不同位置處的唯一資料相關聯。此特徵允許租戶共用同一儲存區域，而無一個租戶能夠存取另一租戶之資料的風險。因此，即使租戶共用一位址空間，在無第一租戶之外部金鑰之情況下，其他租戶無法解密第一租戶之資料。

【0019】 在一個途徑中，藉由銷毀由該租戶使用之該外部金鑰來執行對應於該租戶之所有資料的密碼抹除。此為密碼抹除彼租戶之資料的有效方式。

【0020】 在一個途徑中，藉由銷毀與特定資料類型相關聯之該類型金鑰來執行所有租戶之該特定資料類型之密碼抹除。此為密碼抹除所有特定資料類型之有效方式。此確保彼類型之所有資料的密碼抹除可藉由簡單地明確刪除彼類型金鑰來執行。

【0021】 當使用專用位址位元時，位元之第二子集中之空序列指示給定租戶之外部金鑰之設定(例如，匯入)及/或刪除(例如，移除ECD內之金鑰的所有複本)。此具有能夠設定及/或刪除給定租戶之外部金鑰之效應。

【0022】 在較佳途徑中，類型金鑰係產生於ECD外部。類型金鑰可按需要例如自金鑰管理器基礎結構、金鑰儲存器等提供給ECD。此允許更多地控制向ECD提供哪些類型金鑰，從而增強安全性。應注意，類型金鑰可例如藉由將任何給定IO中之資料分類為資料類型之某一軟體而有效地動態指派。

【0023】 在替代途徑中，該等類型金鑰係產生於該裝置內且僅儲存於該裝置中。此確保密碼抹除可藉由簡單地刪除裝置內之類型金鑰來執行，而無可自裝置外部獲得類型金鑰之任何機會。此提供對類型金鑰之傳播的更多控制。若禁止類型金鑰離開裝置，則自裝置刪除類型金鑰確保用其加密之資料的密碼抹除。

【0024】 根據本發明之另一態樣，一種裝置實施方法包括產生具有預定義長度之一位址欄的一命令，其中該位址欄中之位元的一第一子集識

別一特定租戶之一外部金鑰，其中該位址欄中之該等位元的一第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者。將該命令發送至一每個IO金鑰致動之裝置，該每個IO金鑰致動之裝置經組態以使用自該外部金鑰及與該等位元之該第二子集相關聯之該類型金鑰產生之一組合式金鑰來加密及/或解密與該命令相關聯之資料。

【0025】 前述方法使得能夠同時處置較少數目個金鑰之裝置能夠容納約等於較少數目個金鑰之數個租戶，同時亦能夠針對租戶中之各者的不同資料類型使用唯一金鑰，如同裝置能夠處置許多倍之金鑰一樣。該方法亦實現諸如所有租戶之特定資料類型之密碼抹除之類的事情，在下文更詳細地描述。

【0026】 資料類型可包括隱私類型、機密類型等。方法現使得能夠將特定金鑰用於此等資料類型。

【0027】 在一個較佳途徑中，該命令為一符合非揮發性記憶體高速(NVMe)規範的命令。本方法使得能夠使用NVMe命令來指定類型金鑰。

【0028】 在一個途徑中，藉由請求銷毀儲存於該每個IO金鑰致動之裝置中之該外部金鑰來請求對應於該租戶之所有資料的密碼抹除。此為密碼抹除彼租戶之資料的有效方式。

【0029】 在一個途徑中，藉由請求銷毀用於特定資料類型之類型金鑰來請求所有租戶之彼特定資料類型之密碼抹除。此為密碼抹除所有特定資料類型之有效方式。

【0030】 一種電腦程式產品，其包括具有與其一起體現之程式指令的電腦可讀儲存媒體，程式指令可由經組態以在儲存媒體上執行資料操作之裝置執行以使該裝置執行本文中所呈現之方法中之任一者。

【0031】 根據本發明之各種態樣，一種系統包括一每個IO金鑰致動之裝置，該裝置具有一處理器及與該處理器整合、可由該處理器執行或與該處理器整合且可由該處理器執行之邏輯，該邏輯經組態以使該裝置執行本文中所呈現之方法中之任一者。

【0032】 本文中所描述之各種途徑適用於許多類型之儲存媒體，包括非揮發性記憶體及磁性記錄帶。

【0033】 本發明之其他態樣及途徑將自以下詳細描述變得顯而易見，當結合圖式時，該詳細描述藉助於實例說明本發明之原理。

【圖式簡單說明】

【0034】 圖1為根據本發明之一個態樣的運算環境之圖。

【0035】 圖2為根據本發明之一個態樣的分層資料儲存系統之圖。

【0036】 圖3為根據本發明之一個態樣的方法之流程圖。

【0037】 圖4為根據本發明之一個態樣的方法之流程圖。

【0038】 圖5為根據本發明之一個態樣的方法之流程圖。

【0039】 圖6為根據本發明之一個態樣的方法之流程圖。

【0040】 圖7為根據本發明之一個態樣的方法之流程圖。

【實施方式】

【0041】 出於說明本發明之一般原理的目的而進行以下描述，且以下描述並不意欲限制本文中所主張之本發明概念。此外，本文中所描述之特定特徵可與各種可能組合及排列中之各者中的其他所描述特徵組合使用。

【0042】 除非本文中另外明確定義，否則所有術語應給出其最廣泛可能解釋，包括自說明書暗示之意義以及由熟習此項技術者所理解及/或

在詞典、論文等中所定義之意義。

【0043】 亦必須注意，除非另外規定，否則如本說明書及隨附申請專利範圍中所使用，單數形式「一(a/an)」及「該」包括複數個參考對象。應進一步理解，術語「包含(comprise/comprising)」在用於本說明書中時指定所陳述之特徵、整數、步驟、操作、元件及/或組件之存在，但不排除一或多個其他特徵、整數、步驟、操作、元件、組件及/或其群組之存在或添加。

【0044】 本文中之描述揭示用於顯著地增加每個租戶可藉由每個IO金鑰致動之裝置(例如，ECD、電腦、金鑰伺服器等，該等裝置中之任一者可為如本文中別處所描述之「電腦」)處置之金鑰之數目的系統、方法及電腦程式產品之數種較佳途徑。舉例而言，能夠同時處置僅約4,096個金鑰之裝置可能容納大致4,096個租戶，且又對彼等4,096個租戶中之各者的16種(或大於1之某更少數目)不同資料類型中之各者使用唯一金鑰，如同裝置能夠處置約65,536個金鑰。在較佳態樣中，僅定址所有不同租戶所需之位址位元之數目用於彼目的，且剩餘可用位址位元用於定址『類型』金鑰。因此，由相關規格提供之定址位元的全部數目可用於同時指示租戶及資料之類型。舉例而言，根據允許命令之標頭中之位址欄為16位元之NVMe規格，12位元之位址欄可用於識別租戶，且4位元之位址欄可用於識別命令所請求之基礎讀取或寫入中的資料之類型。

【0045】 根據本發明之一個態樣，一種裝置實施方法包括接收具有預定義長度之位址欄的命令。位址欄中之位元的第一子集識別特定租戶之外部金鑰，且位址欄中之位元的第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者。擷取由位元之第一子集識別之外部金鑰。亦擷

取對應於位元之第二子集之類型金鑰。組合租戶金鑰與類型金鑰以建立組合式金鑰以用於加密及/或解密與命令相關聯之資料。

【0046】 前述方法使得能夠同時處置較少數目個金鑰之裝置能夠容納約等於較少數目個金鑰之數個租戶，同時亦能夠針對租戶中之各者的不同資料類型使用唯一金鑰，如同裝置能夠處置許多倍之金鑰一樣。該方法亦實現諸如所有租戶之特定資料類型之密碼抹除之類的事情，在下文更詳細地描述。

【0047】 資料類型可包括隱私類型、機密類型等。如上文所提及，方法現使得能夠將特定金鑰用於此等資料類型。

【0048】 在一個較佳途徑中，命令為符合非揮發性記憶體高速(NVMe)規範的命令。本方法使得能夠使用NVMe命令來指定類型金鑰。

【0049】 裝置可經組態為每個IO金鑰致動之裝置。本方法為KPIO致動之裝置提供新能力。

【0050】 在一個途徑中，方法包括：存取儲存於裝置內之內部金鑰；使用內部金鑰及組合式金鑰來產生唯一媒體加密金鑰；及使用媒體加密金鑰來加密及/或解密與命令相關聯之資料。此特徵添加另外安全層，此係因為將需要內部金鑰來存取儲存於裝置上之資料。此外，可藉由簡單地銷毀內部金鑰及MEK(若儲存於裝置上)來在裝置中執行密碼抹除。此外，若MEK係藉由租戶金鑰、類型金鑰及內部金鑰之組合來建立，則彼MEK可藉由銷毀彼租戶金鑰、或彼類型金鑰或彼內部金鑰而經密碼抹除。因此，在此後一實例中，可以三個不同粒度層級執行密碼抹除，此取決於哪一金鑰被銷毀。

【0051】 較佳地，裝置經組態以禁止以任何形式將內部金鑰傳送至

裝置外部。此確保在裝置層級執行之密碼抹除停用使用內部金鑰加密之所有資料。

【0052】 在一個途徑中，外部金鑰中之數者個別地與儲存於同一邏輯區塊位址範圍中之不同位置處的唯一資料相關聯。此特徵允許租戶共用同一儲存區域，而無一個租戶能夠存取另一租戶之資料的風險。因此，即使租戶共用一位址空間，在無第一租戶之外部金鑰之情況下，其他租戶無法解密第一租戶之資料。

【0053】 在一個途徑中，藉由銷毀由租戶使用之外部金鑰來執行對應於租戶之所有資料的密碼抹除。此為密碼抹除彼租戶之資料的有效方式。

【0054】 在一個途徑中，藉由銷毀與特定資料類型相關聯之類型金鑰來執行所有租戶之特定資料類型之密碼抹除。此為密碼抹除所有特定資料類型之有效方式。較佳地，類型金鑰僅儲存於裝置上，且裝置經組態以禁止以任何形式將類型金鑰傳送至裝置外部。此確保密碼抹除可藉由簡單地刪除類型金鑰來執行，而無可自裝置外部獲得類型金鑰之任何機會。

【0055】 在一個途徑中，位元之第二子集中之空序列指示給定租戶之外部金鑰之設定(例如，匯入)及/或刪除(例如，移除ECD內之金鑰的所有複本)。此具有能夠設定及/或刪除給定租戶之外部金鑰之效應。

【0056】 在較佳途徑中，類型金鑰係產生於ECD外部。類型金鑰可按需要例如自金鑰儲存器、自租戶等提供給ECD。此允許更多地控制向ECD提供哪些類型金鑰，從而增強安全性。應注意，類型金鑰可例如藉由將任何給定IO中之資料分類為資料類型之某一軟體而有效地動態指派。

【0057】 在替代途徑中，類型金鑰係產生於裝置內且僅儲存於裝置

中。此確保密碼抹除可藉由簡單地刪除類型金鑰來執行，而無可自裝置外部獲得類型金鑰之任何機會。此提供對類型金鑰之傳播的更多控制。若禁止類型金鑰離開裝置，則自裝置刪除類型金鑰確保用其加密之資料的密碼抹除。

【0058】 根據本發明之另一態樣，一種裝置實施方法包括產生具有預定義長度之位址欄的命令，其中位址欄中之位元的第一子集識別特定租戶之外部金鑰，其中位址欄中之位元的第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者。將命令發送至每個IO金鑰致動之裝置，該每個IO金鑰致動之裝置經組態以使用自外部金鑰及與位元之第二子集相關聯之類型金鑰產生之組合式金鑰來加密及/或解密與命令相關聯之資料。

【0059】 前述方法使得能夠同時處置較少數目個金鑰之裝置能夠容納約等於較少數目個金鑰之數個租戶，同時亦能夠針對租戶中之各者的不同資料類型使用唯一金鑰，如同裝置能夠處置許多倍之金鑰一樣。該方法亦實現諸如所有租戶之特定資料類型之密碼抹除之類的事情，在下文更詳細地描述。

【0060】 資料類型可包括隱私類型、機密類型等。方法現使得能夠將特定金鑰用於此等資料類型。

【0061】 在一個較佳途徑中，命令為符合非揮發性記憶體高速(NVMe)規範的命令。本方法使得能夠使用NVMe命令來指定類型金鑰。

【0062】 在一個途徑中，藉由請求銷毀儲存於每個IO金鑰致動之裝置中之外部金鑰來請求對應於租戶之所有資料的密碼抹除。此為密碼抹除彼租戶之資料的有效方式。

【0063】 在一個途徑中，藉由請求銷毀與特定資料類型相關聯之類型金鑰來請求所有租戶之彼特定資料類型的密碼抹除。此為密碼抹除所有特定資料類型之有效方式。

【0064】 一種電腦程式產品，其包括具有與其一起體現之程式指令的電腦可讀儲存媒體，程式指令可由經組態以在儲存媒體上執行資料操作之裝置執行以使該裝置執行本文中所呈現之方法中之任一者。

【0065】 根據本發明之各種態樣，一種系統包括每個IO金鑰致動之裝置，該裝置具有處理器及與處理器整合、可由處理器執行或與處理器整合且可由處理器執行之邏輯，該邏輯經組態以使裝置執行本文中所呈現之方法中之任一者。

【0066】 *說明性運算環境*

【0067】 本揭示之各種態樣由敍述文字、流程圖、電腦系統之方塊圖及/或包括於本發明之電腦程式產品(CPP)態樣中之機器邏輯的方塊圖描述。相對於任何流程圖，取決於所涉及之技術，操作可按與給定流程圖中所展示之次序不同的次序執行。舉例而言，同樣取決於所涉及之技術，連續流程圖區塊中展示之兩個操作可按相反次序執行，作為單一整合步驟執行、並行地執行或以在時間上至少部分地重疊的方式執行。

【0068】 電腦程式產品態樣(「CPP態樣」或「CPP」)為在本揭示中用以描述共同地包括於一或多個儲存裝置之集合中的一或多個儲存媒體(media) (亦稱為「媒體(medium)」)之任何集合的術語，該等儲存裝置共同地包括對應於用於執行給定CPP聲明中指定之電腦操作之指令及/或資料的機器可讀程式碼。「儲存裝置」為可保留及儲存供電腦處理器使用之指令的任何有形裝置。非限制性地，電腦可讀儲存媒體可為電子儲存媒

體、磁性儲存媒體、光學儲存媒體、電磁儲存媒體、半導體儲存媒體、機械儲存媒體或前述各者之任何合適組合。包括此等媒體之一些已知類型之儲存裝置包括：磁片、硬碟、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可抹除可程式化唯讀記憶體(EPROM或快閃記憶體)、靜態隨機存取記憶體(SRAM)、緊密光碟唯讀記憶體(CD-ROM)、數位光碟(DVD)、記憶棒、軟碟、機械編碼裝置(諸如形成於光碟之主表面中的打孔卡片或凹點/焊盤)或前述各者之任何合適組合。本揭示中所使用之術語電腦可讀儲存媒體不應理解為以暫時性信號本身之形式儲存，諸如無線電波或其他自由傳播之電磁波、傳播通過波導之電磁波、傳遞通過光纖電纜之光脈衝、傳達通過導線之電信號及/或其他傳輸媒體。熟習此項技術者將理解，資料通常在儲存裝置之正常操作期間(諸如在存取、去片段化或垃圾收集期間)在一些偶然時間點移動，但此並不使得儲存裝置為暫時性的，此係因為資料在其被儲存時不為暫時性的。

【0069】 運算環境100含用於在執行本發明方法時所涉及之電腦程式碼中的至少一些之環境的實例，諸如區塊150中之用於藉由類型加密金鑰擴展每個IO金鑰之程式碼。除區塊150外，運算環境100包括例如電腦101、廣域網路(WAN) 102、終端使用者裝置(EUD) 103、遠端伺服器104、公共雲端105及私有雲端106。在此途徑中，電腦101包括處理器集110 (包括處理電路系統120及快取記憶體121)、通信網狀架構111、揮發性記憶體112、持久儲存器113 (包括如上文所識別之作業系統122及區塊150)、周邊裝置集114 (包括使用者介面(UI)裝置集123、儲存器124及物聯網(IoT)感測器集125)及網路模組115。遠端伺服器104包括遠端資料庫130。公共雲端105包括閘道器140、雲端協調模組141、主機實體機器集

142、虛擬機器集143及容器集144。

【0070】 電腦101可採取桌上型電腦、膝上型電腦、平板電腦、智慧型手機、智慧型手錶或其他隨身電腦、大型電腦、量子電腦或任何其他形式之電腦或行動裝置的形式，該電腦或行動裝置現在已知或未來要開發，能夠運行程式、存取網路或查詢資料庫，諸如遠端資料庫130。在電腦技術之領域中充分理解，且取決於技術，電腦實施方法之效能可分佈於多個電腦當中及/或多個位置之間。另一方面，在運算環境100之此呈現中，詳細論述集中於單個電腦，具體而言電腦101，以保持呈現儘可能簡單。電腦101可位於雲端中，即使其在圖1中其未展示於雲端中。另一方面，除了可肯定地指示之任何程度之外，電腦101不需要位於雲端中。

【0071】 處理器集110包括現在已知或未來要開發之任何類型的一或多個電腦處理器。處理電路系統120可分佈於多個封裝上，例如多個經協調積體電路晶片上。處理電路系統120可實施多個處理器執行緒及/或多個處理器核心。快取記憶體121為位於一或多個處理器晶片封裝中之記憶體，且通常用於應可用於由在處理器集110上運行之執行緒或核心快速存取之資料或程式碼。快取記憶體通常取決於與處理電路系統之相對接近度來組織成多個層級。替代地，用於處理器集之快取記憶體中之一些或所有可位於「晶片外」。在一些運算環境中，處理器集110可經設計以用於使用量子位元且執行量子運算。

【0072】 電腦可讀程式指令通常載入至電腦101上以使得一系列操作步驟由電腦101之處理器集110執行且藉此影響電腦實施方法，使得如此執行之指令將執行個體化本文中包括之電腦實施方法之流程圖及/或敍述描述中指定之方法(統稱為「本發明方法」)。此等電腦可讀程式指令儲

存於各種類型之電腦可讀儲存媒體中，諸如快取記憶體121及下文論述之另一儲存媒體。程式指令及相關聯資料由處理器集110存取以控制及指導本發明方法之效能。在運算環境100中，用於執行本發明方法之指令中之至少一些可儲存於持久儲存器113中之區塊150中。

【0073】 通信網狀架構111為允許電腦101之各種組件彼此通信的信號傳導路徑。通常，此網狀架構由開關及導電路徑製成，諸如構成匯流排、橋接器、實體輸入/輸出埠及類似者之開關及導電路徑。可使用其他類型之信號通信路徑，諸如光纖通信路徑及/或無線通信路徑。

【0074】 揮發性記憶體112為現在已知或未來要開發之任何類型之揮發性記憶體。實例包括動態型隨機存取記憶體(RAM)或靜態型RAM。通常，揮發性記憶體112之特徵在於隨機存取，但除非肯定指示，否則此並非為必需的。在電腦101中，揮發性記憶體112位於單個封裝中且在電腦101內部，但替代地或另外，揮發性記憶體可分佈於多個封裝上及/或相對於電腦101位於外部。

【0075】 持久儲存器113為現在已知或未來要開發之用於電腦的任何形式之非揮發性儲存器。此儲存器之非揮發性意謂不考慮無論向電腦101供電及/或直接向持久儲存器113供電，維護所儲存資料。持久儲存器113可為唯讀記憶體(ROM)，但通常持久儲存器之至少一部分允許寫入資料、刪除資料及重寫資料。持久儲存器之一些熟悉形式包括磁碟及固態儲存裝置。作業系統122可採用數種形式，諸如各種已知專用的作業系統或採用內核之開放原始碼可攜式作業系統介面型作業系統。包括於區塊150中之程式碼通常包括在執行本發明方法時所涉及之電腦程式碼中之至少一些。

【0076】 周邊裝置集114包括電腦101之周邊裝置集。周邊裝置與電腦101之其他組件之間的資料通信連接可以各種方式實施，諸如藍牙連接、近場通信(NFC)連接、由電纜(諸如通用串列匯流排(USB)型電纜)進行之連接、插入型連接(例如，安全數位(SD)卡)、經由區域通信網路進行之連接及甚至經由諸如網際網路之廣域網路進行之連接。在各種態樣中，UI裝置集123可包括諸如顯示螢幕、揚聲器、麥克風、穿戴式裝置(諸如護目鏡及智慧型手錶)、鍵盤、滑鼠、印表機、觸控板、遊戲控制器及觸感裝置之組件。儲存器124為諸如外部硬碟之外部儲存器，或諸如SD卡之可插入儲存器。儲存裝置124可為持久的及/或揮發性的。在一些途徑中，儲存器124可採取量子運算儲存裝置之形式，以用於以量子位形式儲存資料。在要求電腦101具有大量儲存器(例如，電腦101本端儲存及管理大型資料庫)之途徑中，則此儲存器可由經設計以用於儲存極大量資料之周邊儲存裝置提供，諸如由多個地理分佈之電腦共用的儲存區域網路(SAN)。IoT感測器集125由可在物聯網應用中使用之感測器構成。舉例而言，一個感測器可為溫度計，而另一感測器可為運動偵測器。

【0077】 網路模組115為允許電腦101通過WAN 102與其他電腦通信之電腦軟體、硬體及韌體之集合。網路模組115可包括：硬體，諸如數據機或Wi-Fi信號收發器；軟體，其用於對用於通信網路傳輸之資料封包化及/或解封包化；及/或網頁瀏覽器軟體，其用於經由網際網路傳達資料。在一些途徑中，網路模組115之網路控制功能及網路轉發功能在同一實體硬體裝置上執行。在其他途徑(例如，利用軟體定義網路(SDN)之途徑)中，網路模組115之控制功能及轉發功能在實體上分離之裝置上執行，以使得控制功能管理數個不同網路硬體裝置。用於執行本發明方法之電腦

可讀程式指令可通常通過包括於網路模組115中之網路配接器卡或網路介面自外部電腦或外部儲存裝置下載至電腦101。

【0078】 WAN 102為能夠由現在已知或未來要開發之用於傳達電腦資料之任何技術在非本端距離上傳達電腦資料的任何廣域網路(例如，網際網路)。在一些途徑中，WAN 102可由區域網路(LAN)替換及/或補充，該區域網路經設計以在位於諸如Wi-Fi網路之區域中的裝置之間傳達資料。WAN及/或LAN通常包括電腦硬體，諸如銅傳輸電纜、光傳輸光纖、無線傳輸、路由器、防火牆、交換器、閘道器電腦及邊緣伺服器。

【0079】 終端使用者裝置(EUD) 103為由終端使用者(例如，操作電腦101之企業的客戶)使用及控制之任何電腦系統，且可採取上文結合電腦101所論述之形式中的任一者。EUD 103通常自電腦101之操作接收有幫助及有用的資料。舉例而言，在電腦101設計成向終端使用者提供推薦之假設情況下，此推薦將通常通過WAN 102自電腦101之網路模組115傳送至EUD 103。以此方式，EUD 103可向終端使用者顯示或以其他方式呈現推薦。在一些途徑中，EUD 103可為用戶端裝置，諸如瘦用戶端(thin client)、重用戶端(heavy client)、大型電腦、桌上型電腦等等。

【0080】 遠端伺服器104為向電腦101提供至少一些資料及/或功能性之任何電腦系統。遠端伺服器104可由操作電腦101之同一實體控制及使用。遠端伺服器104表示收集及儲存有幫助及有用的資料供諸如電腦101之其他電腦使用的一或多個機器。舉例而言，在電腦101經設計及經程式化以基於歷史資料提供推薦之假設情況下，則可將此歷史資料自遠端伺服器104之遠端資料庫130提供至電腦101。

【0081】 公共雲端105為可供多個實體使用之任何電腦系統，該多

個實體提供電腦系統資源及/或其他電腦能力，尤其資料儲存(雲端儲存)及運算能力之按需可用性，而不需使用者直接主動管理。雲端運算通常利用資源共用來達成同調性及規模經濟。公共雲端105之運算資源的直接及主動管理係由雲端協調模組141之電腦硬體及/或軟體執行。由公共雲端105提供之運算資源通常由在構成主機實體機器集142之電腦的各種電腦上運行之虛擬運算環境來實施，該主機實體機器集為公共雲端105中及/或可供該公共雲端使用之實體電腦的範圍。虛擬運算環境(VCE)通常採取來自虛擬機器集143之虛擬機器及/或來自容器集144之容器的形式。應理解，此等VCE可儲存為影像，且可作為影像抑或在VCE之執行個體化之後在各種實體機器主體當中及之間傳送。雲端協調模組141管理影像之傳送及儲存，部署VCE之新執行個體化且管理VCE部署之主動執行個體化。閘道器140為允許公共雲端105通過WAN 102通信之電腦軟體、硬體及韌體之集合。

【0082】 現將提供對虛擬運算環境(VCE)之一些進一步解釋。VCE可儲存為「影像」。VCE之新主動執行個體可自影像執行個體化。VCE之兩種常見類型為虛擬機器及容器。容器為使用作業系統層級虛擬化之VCE。此係指作業系統特徵，其中內核允許存在多個獨立的使用者空間執行個體，稱為容器。自在其中運行之程式之角度來看，此等獨立的使用者空間執行個體通常表現為真實電腦。在普通作業系統上運行之電腦程式可利用彼電腦之全部資源，諸如連接裝置、檔案及資料夾、網路共用、CPU電源及可定量硬體能力。然而，在容器內部運行之程式僅可使用容器之內容及指派給容器之裝置，此特徵被稱為容器化。

【0083】 除了運算資源僅可供單一企業使用之外，私有雲端106類

似於公共雲端105。雖然私有雲端106經描繪為與WAN 102通信，但在其他途徑中，私有雲端可完全與網際網路斷開連接且僅通過區域/專用網路存取。混合雲端為不同類型之多個雲端(例如，私有、社群或公共雲端類型)之組成，通常分別由不同供應商實施。多個雲端中之各者保持分離及離散實體，但較大混合雲端架構由標準化或專用技術綁在一起，該技術實現多個構成雲端之間的協調、管理及/或資料/應用可攜性。在此途徑中，公共雲端105及私有雲端106均為較大混合雲端之部分。

【0084】 在一些態樣中，根據各種途徑之系統可包括處理器及與處理器整合及/或可由處理器執行之邏輯，該邏輯經組態以執行本文中所列舉之程序步驟中之一或多者。處理器可具有本文中所描述之任何組態，諸如包括許多組件(諸如處理硬體、記憶體、I/O介面等)之離散處理器或處理電路。藉由整合，意謂處理器具有作為硬體邏輯嵌入其中之邏輯，諸如特殊應用積體電路(ASIC)、FPGA等。藉由可由處理器執行，意謂邏輯為硬體邏輯；軟體邏輯，諸如韌體、作業系統之部分、應用程式之部分等；或硬體邏輯與軟體邏輯之某一組合，其可由處理器存取且經組態以使得處理器在由處理器執行時執行某一功能性。軟體邏輯可儲存於任何記憶體類型之區域及/或遠端記憶體上，如此項技術中已知。可使用此項技術中已知之任何處理器，諸如軟體處理器模組及/或硬體處理器，諸如ASIC、FPGA、中央處理單元(CPU)、積體電路(IC)、圖形處理單元(GPU)等。

【0085】 當然，根據本發明之各種態樣，此邏輯可實施為任何裝置及/或系統上之方法或實施為電腦程式產品。

【0086】 現參考圖2，展示根據本發明之一個態樣的儲存系統200。應注意，根據各種途徑，圖2中所展示之元件中之一些可實施為硬體及/或

軟體。儲存系統200可包括儲存系統管理器212，其用於與至少一個較高儲存層202及至少一個較低儲存層206上之複數個媒體及/或磁碟通信。一或多個較高儲存層202較佳可包括一或多個隨機存取及/或直接存取媒體204，例如硬碟機(HDD)中之硬碟、非揮發性記憶體(NVM)、固態硬碟(SSD)中之固態記憶體、快閃記憶體、SSD陣列、快閃記憶體陣列等及/或本文中所提及或此項技術中已知之其他者。一或多個較低儲存層級206可較佳地包括一或多個較低執行儲存媒體208，包括順序存取媒體，諸如磁帶機及/或光學媒體中之磁帶、較慢存取HDD、較慢存取SSD等及/或本文中所提及或此項技術中已知之其他者。一或多個額外儲存層216可包括如系統200之設計者所期望之儲存記憶體媒體之任何組合。此外，較高儲存層202及/或較低儲存層206中之任一者可包括儲存裝置及/或儲存媒體之某一組合。

【0087】 儲存系統管理器212可通過如圖2中所展示之諸如儲存區域網路(SAN)的網路210或一些其他合適之網路類型與一或多個較高儲存層202及一或多個較低儲存層206上之磁碟及/或儲存媒體204、208通信。儲存系統管理器212亦可通過主機介面214與一或多個主機系統(未展示)通信，該主機介面可為或可不為儲存系統管理器212之一部分。儲存系統200之儲存系統管理器212及/或任何其他組件可以硬體及/或軟體實施，且可利用處理器(未展示)來執行此項技術中已知之類型的命令，該處理器為諸如中央處理單元(CPU)、場可程式化閘陣列(FPGA)、特殊應用積體電路(ASIC)等。當然，可使用儲存系統之任何配置，在閱讀本描述後對於熟習此項技術者而言將顯而易見。

【0088】 在更多途徑中，儲存系統200可包括任何數目個資料儲存

層，且可包括各儲存層內之相同或不同儲存記憶體媒體。舉例而言，各資料儲存層可包括相同類型之儲存記憶體媒體，諸如HDD、SSD、順序存取媒體(磁帶機中之帶、光碟機中之光碟等)、直接存取媒體(CD-ROM、DVD-ROM等)或媒體儲存類型之任何組合。在一個此類組態中，較高儲存層202可包括用於在較高執行儲存環境中儲存資料之大多數SSD儲存媒體，且包括較低儲存層206及額外儲存層216之剩餘儲存層可包括用於在較低執行儲存環境中儲存資料之SSD、HDD、磁帶機等的任何組合。以此方式，較頻繁存取之資料、具有較高優先級之資料、需要更快速存取之資料等可儲存至較高儲存層202，而不具有此等屬性中之一者的資料可儲存至額外儲存層216，包括較低儲存層206。當然，熟習此項技術者在閱讀本描述之後可根據本文中所呈現之途徑設計儲存媒體類型之許多其他組合以實施至不同儲存方案中。

【0089】 根據一些途徑，儲存系統(諸如200)可包括經組態以接收打開資料集之邏輯、經組態以判定所請求資料集是否以多個相關聯部分儲存至分層資料儲存系統200之較低儲存層206的邏輯、經組態以將所請求資料集之各相關聯部分移動至分層資料儲存系統200之較高儲存層202的邏輯，及經組態以將所請求資料集自相關聯部分組裝於分層資料儲存系統200之較高儲存層202上的邏輯。

【0090】 *每個IO金鑰原理*

【0091】 在一些情況下，需要允許不同實體使用儲存裝置之中同一位址空間。然而，對此之過分簡單化實施並未向第一實體提供來自第二實體之任何隱私保證，第二實體可以簡單地讀取第一實體寫入儲存裝置之內容。對此之一個解決方案為使各實體(例如，租戶)使用其可在裝置外部管

理之唯一金鑰，該裝置需要加密其寫入資料及解密其經加密密文。彼金鑰在本文中將被稱作外部金鑰、外部MEK及Kext。特別地，各租戶具有唯一Kext，其用以加密各別租戶之資料，且彼Kext不同於其他租戶之Kext。此方案一般稱作每個IO金鑰方案。

【0092】 當每個IO金鑰致動之裝置(例如，ECD、電腦等)通電時，其沒有Kext來執行加密或解密。實情為，Kext以任何所要方式提供給其(例如，按需要結合對讀取或寫入操作之請求等)。舉例而言，租戶可發送Kext以及金鑰標籤(例如，T)，Kext將在將來藉由該金鑰標籤被引用，該裝置將該金鑰標籤儲存於揮發性記憶體中。接著，當裝置接收包括金鑰標籤T作為命令標頭之部分的命令(例如，NVMe命令)時，每個IO金鑰致動之裝置自記憶體擷取相關聯之Kext，且在將密文儲存至非揮發性記憶體之前使用其來加密由主機寫入之明文資料，或在將對應明文發送至主機之前解密自非揮發性記憶體讀取之密文資料。裝置可累積與不同金鑰標籤相關聯之多個Kext。在一些途徑中，若斷電，則僅儲存於揮發性記憶體中之Kext將丟失且因此需要在該揮發性記憶體恢復通電之後重新提供給裝置，隨後可再次使用該等Kext。

【0093】 許多每個IO金鑰方案之目標為允許不同租戶(使用者、應用程式、電腦等)共用同一位址空間。在本文中所呈現之教示之前，租戶之Kext直接用作MEK以加密及解密租戶之資料。理論上，第一租戶之經加密資料對於藉由第二租戶進行之明文存取為安全的，只要其各別Kext彼此為唯一的，且保持安全，不會被其他租戶使用。當第一租戶或負責第一租戶之資料的控制基礎結構想要抹除裝置上之第一租戶之資料時，第一租戶或控制基礎結構銷毀裝置外部之第一租戶之Kext，例如藉由抹除

Kext、覆寫Kext或以其他方式銷毀Kext，不僅包括在裝置外部之Kext的任何剩餘複本，而且包括儲存於裝置內部之揮發性記憶體中的任何一或多個複本。具體言之，若存在自裝置上次功率循環或冷啟動以來第一租戶之Kext已被提供給裝置的任何可能性，則第一租戶應指示裝置抹除用作裝置內部之MEK的Kext。藉由銷毀裝置外部及內部之Kext之所有執行個體，此將有效地密碼抹除用彼MEK加密之資料，該資料仍儲存至彼裝置及可自彼裝置恢復。

【0094】 然而，如上文所提及，銷毀租戶之Kext會使彼租戶之所有資料不可讀。在本文中之本發明之揭示之前，允許租戶儲存不同資料類型之唯一方式為將額外Kext指派給彼租戶。然而，考慮到每個IO金鑰致動之裝置可處置及/或儲存多少金鑰之限制，容納之資料類型愈多，可處置之租戶數目愈少。

【0095】 *有效增加可在每個IO金鑰致動之裝置中使用的數目金鑰之本發明方法*

【0096】 本發明之各種態樣提供一種在不犧牲每個IO金鑰致動之裝置可處置之租戶的數目之情況下有效地增加可在每個IO金鑰致動之裝置中使用的金鑰之數目的方式。以下描述揭示系統、方法及電腦程式產品之數種較佳途徑，用於在如本文所描述修改且在下文中稱為KPIO擴展或簡稱為KPIO-X之KPIO版本中對每個IO金鑰致動之裝置使用『類型』金鑰。

【0097】 雖然本文中大部分描述係結合具有諸如任何類型之SED或ECD的每個IO金鑰致動之裝置的例示性實施來呈現，但此僅藉助於實例來進行，且僅係為了提供上下文作為對讀者之幫助。因此，本文中所呈現之概念及教示同樣適用於利用儲存媒體(諸如，磁性記錄帶、記憶卡、光

學媒體等)及相關裝置之實施。

【0098】 現參考圖3，展示根據本發明之一個態樣的裝置實施方法300之流程圖。根據本發明之方法300可在圖1至圖2中描繪之任何環境中以及以各種途徑來執行。當然，比圖3中具體描述之操作更多或更少的操作可包括於方法300中，如熟習此項技術者在閱讀本描述後將理解。

【0099】 方法300之步驟中之各者可由作業環境之任何合適組件執行。舉例而言，在各種途徑中，方法300可部分或全部由經組態以根據KPIO-X操作之每個IO金鑰致動之裝置、儲存控制器、金鑰伺服器或其中具有一或多個處理器之某一其他裝置執行。處理器(例如，以硬體及/或軟體實施之一或多個處理電路、一或多個晶片及/或一或多個或模組)且較佳地具有至少一個硬體組件可用於任何裝置中以執行方法300之一或多個步驟。說明性處理器包括但不限於中央處理單元(CPU)、特殊應用積體電路(ASIC)、場可程式化閘陣列(FPGA)等、其組合或此項技術中已知之任何其他合適運算裝置。

【0100】 方法300可由每個IO金鑰致動之裝置執行，諸如在儲存媒體上儲存資料之裝置，其可為本文中所揭示之任何類型(例如，磁帶、磁碟、非揮發性隨機存取記憶體(NVRAM)等)。因此，裝置可為任何類型之資料儲存裝置(例如，磁帶機、SSD、HDD、能夠加密之USB磁碟、NVRAM模組等)。此外，裝置可為可移式資料儲存類型之能夠加密磁碟(ECD)，諸如能夠加密之USB磁碟、能夠加密之磁帶機、自加密磁碟(SED)等。

【0101】 如圖3中所展示，方法300可以操作302開始，其中接收具有以位元為單位之預定義長度之位址欄(例如，由規格指定)的命令。應注

意，命令之標頭中或命令中之某其他預定位置處的任何欄位可被視為本文中所使用之位址欄。在一些途徑中，命令為符合NVMe規範的命令。在其他途徑中，命令為另一類型之已知命令，但根據本文中之教示進行修改以包括緊接在下文提及之位元子集。

【0102】 位址欄中之位元的第一子集識別特定租戶之外部金鑰(Kext)。舉例而言，特定位元序列可對應於特定Kext，且識別可(例如，使用此等序列之表及對應於此等序列之Kext)進行。

【0103】 位址欄中之位元的第二(通常不相交)子集對應於與不同資料類型相關聯之複數個類型金鑰中之一者。可指定在閱讀本揭示後對於熟習此項技術者將變得顯而易見之任何資料類型。舉例而言，資料類型可包括隱私及/或機密類型。

【0104】 位元之第一及/或第二子集之長度較佳被預定。在以上實例中，在位址欄規格為16位元之情況下，位元之第一子集為12位元長，且位元之第二子集為4位元長。應注意，相對長度可為任何預定值(例如，8位元及8位元、10位元及6位元、14位元及2位元等)。此外，在一些途徑中，組合式長度可總共等於小於全位址欄規格(例如，在16位元位址空間中使用僅10位元及4位元)。剩餘位址空間位元可被設定成零、一些其他預設空值等。

【0105】 操作302中接收之命令可由裝置自一或多個外部源接收，以用於每個IO金鑰操作。舉例而言，可自租戶之電腦、儲存控制器等接收命令。

【0106】 在操作304中，擷取由位元之第一子集識別之Kext。Kext可儲存於裝置上，自金鑰伺服器擷取等。可使用位元之第一子集查詢使

Kext與預定義位元序列關聯之查找表。

【0107】 在操作306中，擷取對應於位元之第二子集之類型金鑰。類型金鑰可儲存於裝置上，自金鑰伺服器擷取等。可使用位元之第二子集查詢使類型金鑰與預定義位元序列關聯之查找表。

【0108】 在操作308中，以某一方式組合租戶金鑰與類型金鑰以建立組合式金鑰以用於加密及/或解密與命令相關聯之資料。組合可為兩個金鑰之直接組合，或如下文所描述，可需要組合金鑰中之一者與另一金鑰之衍生物(例如，使用另一金鑰建立之經包裝金鑰，或兩個金鑰之導數的組合)。所有此類變體均應視為等效物。

【0109】 如操作310中所指出，可接著使用組合式金鑰來加密及/或解密與命令相關聯之資料。

【0110】 在一個途徑中，若該等金鑰有效地為獨立金鑰，則簡單互斥或(XOR)可令人滿意。在其他途徑中，可使用此項技術中已知之更複雜金鑰衍生演算法。

【0111】 繼續上文給定之實例，在裝置僅能夠處置至多4,096個金鑰且位址欄規格為16位元之情況下，則16位元中僅12位元需要用於指定(例如，定址)彼等數千個金鑰中之哪一者將用於加密(及/或解密)與給定輸入/輸出(IO)相關聯之資料。因此，在此實例中，可定址至多4096個金鑰而無需多於12個位元之定址。若標頭欄之僅12位元用於定址裝置中之同時Kext之數目，則4位元可用於其他目的。

【0112】 因此，本發明之各種態樣使用另外不需要的及/或未使用的位址位元來指定在本文中被稱作「類型金鑰」之其他金鑰。類型金鑰亦用於加密(及/或解密)主機寫入(及/或讀取)。繼續16位元位址規格實例，瞭

解本揭示之人可以理解，若需要僅12位元來定址所支援之所有Kext，則存在設定成定址類型金鑰之4個另外未使用的位址位元。藉由使用彼等四個位址位元，若使用此整個額外位址空間，則可能指定至多16個類型金鑰。此外，可將16個位址值中之一者(例如，0000b)保留以指定待『使用』之空類型金鑰(例如，實際上全零)，留下15個可設定或指定之其他(非空)類型金鑰。

【0113】 作為使用之一個實例，假定使用15個非空類型金鑰位址值，如下：

0000b =空(例如，全零)金鑰

0001b = COc =租戶之公司(CO)機密資料

0010b = COp =私有租戶資料(例如，個人識別資訊(PII))

0011b = COo =既非PII亦非獨立公司機密之租戶一般資料

0100b = ProjXr =公司機密受限之專案X (ProjX)資料

0101b = ProjXc =公司機密之租戶ProjX相關資料

0110b = ProjXp =私有(例如，含有PII)之租戶ProjX相關資料

0111b = ProjXo =既非PII亦非獨立公司機密之租戶ProjX資料

1000b = ProjYr =公司機密受限之專案Y (ProjY)資料

1001b = ProjYc =公司機密之租戶ProjY相關資料

1010b = ProjYp =私有(例如，含有PII)之租戶ProjY相關資料

1011b = ProjYo =既非PII亦非獨立公司機密之租戶ProjY資料

1100b = ProjZr = 公司機密受限之專案Z (ProjZ)資料

1101b = ProjZc =公司機密之租戶ProjZ相關資料

1110b = ProjZp =私有(例如，含有PII)之租戶ProjZ相關資料

1111b = ProjZo =既非PII亦非獨立公司機密之租戶ProjZ資料

【0114】 由於16位元標頭欄之低12位元用於識別至多4096個『租戶』金鑰。若由給定租戶(Ten_X)寫入之資料始終具有正確的較低12位元，則彼資料與至多4096個Kext中之一者相關聯。若各記錄由某個軟體標記為正由租戶寫入之公司機密資料，則KeyID欄位之高4位元被設定成0001b。淨結果為，與Ten_X相關聯之一個金鑰及與COc相關聯之另一金鑰經提取且以某種方式組合，例如簡單互斥或或另一已知金鑰衍生演算法，以建立用於加密(及/或解密)彼主機寫入(及/或讀取)之組合式金鑰。

【0115】 *媒體加密金鑰*

【0116】 在一些途徑中，使用組合式金鑰建立之媒體加密金鑰(MEK)可用於加密及/或解密資料。MEK可以本文別處所描述之各種方式使用。舉例而言，MEK可藉由存取儲存於裝置內之內部金鑰建立。使用上文提及之內部金鑰及組合式金鑰，例如藉由將該等金鑰一起進行互斥或，藉由使用已知金鑰衍生技術等，建立唯一MEK。在另一途徑中，MEK可藉由組合租戶金鑰與類型金鑰來形成。在又一途徑中，MEK可藉由組合租戶金鑰、類型金鑰與裝置之內部金鑰來形成。

【0117】 由此形成之MEK接著用於加密及/或解密與命令相關聯之資料。此特徵添加另外安全層，此係因為將需要內部金鑰來存取儲存於裝置上之資料。此外，可藉由簡單地銷毀內部金鑰及儲存於裝置上之MEK之任何揮發性複本來在裝置中執行密碼抹除。

【0118】 較佳地，裝置經組態以禁止以任何形式將內部金鑰傳送至裝置外部。此確保在磁碟層級執行之密碼抹除停用使用內部金鑰加密之所有資料，例如在下文更詳細地描述。

【0119】 在一些態樣中，由於類型金鑰與租戶之特定Kext組合以建立組合金鑰，該組合金鑰接著用於寫入及讀取0個彼租戶，即使租戶共用位址空間，在無第一租戶之Kext的情況下，其他租戶無法解密第一租戶之資料。因此，數個不同租戶之Kext可個別地與儲存於同一邏輯區塊位址範圍(儲存媒體之邏輯區塊的所允許範圍(例如，在NVMe名稱空間中))內之不同位置處的唯一資料相關聯，該邏輯區塊位址範圍可為數百萬扇區長。應注意，通常藉由ECD上方之一些邏輯上(logic up)將金鑰ID指派給金鑰有效地在ECD之邊界外部進行。以上之彼邏輯上應該在其無法被黑客攻擊之部署中完美地運行，從而使得不會向ECD發出命令，其中金鑰ID指定除其應為外之位址位元。

【0120】 *使用類型金鑰之密碼抹除*

【0121】 藉由使用組合式金鑰加密及/或解密主機寫入扇區，用彼組合式金鑰加密之資料現可有效地以兩種基本方式中之一者進行密碼抹除。Kext (例如，Ten_X)抑或類型金鑰(例如，COc)可自其儲存之所有位置(例如，金鑰儲存器)抹除，包括自裝置自身。因此，對應於租戶之所有資料的密碼抹除可藉由銷毀Kext之所有執行個體及(若適用)裝置中之使用彼Kext建立之所有相關聯媒體加密金鑰來執行。

【0122】 應注意，給定Ten_X Kext可與任何類型金鑰(對應於由彼租戶寫入之任何資料類型)一起使用。若如此，則刪除Ten_X金鑰密碼抹除由給定租戶寫入之所有資料，而不管類型如何。

【0123】 但亦應注意，ProjXr類型金鑰可能由其他或所有租戶使用。若如此，刪除類型金鑰ProjXr同時密碼抹除與由任何租戶寫入之ProjX相關聯之所有公司機密受限資料。若吾人另外刪除與ProjXc、

ProjXp及ProjX0相關聯之類型金鑰，則與專案X相關聯之所有資料將以密碼編譯方式。因此，藉由銷毀對應於彼資料類型之類型金鑰的所有執行個體及(若適用)使用彼類型金鑰建立之所有相關聯MEK，可密碼抹除所有租戶之特定資料類型。較佳地，類型金鑰僅儲存於裝置上，且裝置經組態以禁止以任何形式將類型金鑰傳送至裝置外部。

【0124】 可使用、修改此等密碼抹除方法中之任一者，及/或可與下文關於用於密碼抹除之額外途徑所描述之特徵組合。

【0125】 使用類型金鑰之裝置組態

【0126】 以下描述描述調適任何類型之KPIO致動之裝置以如本文所描述操作之一種可能方式，如上文所提及，該裝置在本文中被稱為KPIO擴展，或簡稱為KPIO-X。應注意，在本揭示中詳述之大多數情況下，存在調適該裝置及KPIO命令以達成相同目標之可行替代等效方法，在閱讀本揭示之後對於熟習此項技術者而言將顯而易見。

【0127】 *多模式操作*

【0128】 調適該裝置以能夠進行KPIO-X操作之直接方式係以能夠按KPIO操作之裝置開始，且接著擴展彼裝置以使其能夠在不同操作模式中操作，具體地能夠進行KPIO-X操作。此裝置可經擴展以能夠按以下方式中之任一者操作。

【0129】 第一種方式嚴格符合現有KPIO規格(亦即，在無任何類型金鑰之情況下)，且第二種方式(該磁碟可經組態以替代地使用)將以支援類型金鑰之方式操作，因此符合此處所描述之KPIO-X操作。裝置接著藉由預定義命令組態以控制裝置在一個模式或另一模式(例如，KPIO抑或KPIO-X)中操作。

【0130】 *指定外部金鑰之數目及類型金鑰之數目*

【0131】 當前KPIO規格允許使用者查詢裝置(例如，磁碟)關於可支援之加密金鑰之總數目及每個NVMe名稱空間之加密金鑰之數目。此允許磁碟報告所支援之Kext之數目，且應為報告在KPIO-X模式中操作時所支援之Kext之數目的最簡單方式。

【0132】 在磁碟能夠報告總共支援之類型金鑰之數目及每個NVMe名稱空間支援之類型金鑰之數目的一個途徑中，建立供應商唯一命令，其使用許多相同命令建構來允許此報告。

【0133】 應注意，在一些途徑中，當裝置在KPIO-X模式中操作時，所報告之兩個數字(例如，對於給定NVMe名稱空間)應彼此一致，使得租戶及類型金鑰可獨立地用不同位址位元定址。作為一實例，為了支援多達4,096個Kext (儘管其不一定必須為恰好2^N數目)，需要在NVMe命令中使用低12位址位元。此僅留下至多4個剩餘高位址位元以用於類型金鑰定址。若彼等類型金鑰位址中之一者經保留以用作空金鑰(例如，如下文更詳細地描述)，則所支援之類型金鑰之數目可達到但不超過(2^4) - 1 = 15 (但不需要恰好(2^M) - 1，且可為零(但在後一情況下，除了支援供應商唯一命令之可能性之外，其實際上變得類似於常規KPIO而非KPIO-X)。

【0134】 在一些途徑中，本文中所描述之類型/租戶分段可以不需要儲存任何額外金鑰之方式管理。舉例而言，假定一給定SSD可容納4096個金鑰，且因此將消耗16位址位元中之12位址位元。目標為允許使用由剩餘4位址位元定址之15個唯一類型金鑰加上一個空類型金鑰。然而，假定不存在儲存此等類型金鑰之額外位置。此可藉由將指派給租戶之金鑰之數目自4096減少至4080來處置。因此，至少在KPIO-X模式中，4080將為就

可用外部金鑰位置而言報告之數字。在KPIO模式中時，裝置可報告4080(與在KPIO-X模式中一致)或4096，假定彼等最後金鑰可用於租戶。最簡單實施(自ASIC設計觀點及易於使用者理解觀點兩者)將始終報告4080個外部金鑰。在KPIO-X模式中時，裝置將接著例如經由供應商唯一查詢命令報告15個類型金鑰設定。應注意，4080個外部金鑰中之各者可能與15個類型金鑰設定中之各者一起使用，此允許4080 × 15 =61,200個金鑰組合，其接近16位元可定址之64K數字。

【0135】 *設定及刪除外部金鑰之例示性技術*

【0136】 在一些途徑中，位元之第二子集(高位元)中之空序列指示Kext之設定及/或刪除。空序列可為全零，如在以上實例中。然而，在其他途徑中，空序列可替代地為全一，或不用於指定類型金鑰之一些預定之零及一之序列。

【0137】 在一個說明性途徑中，租戶Kext (或MEK)金鑰可被設定標準KPIO方式，但經調適以用於此目的，例如藉由在高「類型金鑰」位址位元上設定全零。

【0138】 類似地，租戶Kext (或MEK)金鑰可自裝置刪除標準KPIO方式，但經調適以用於此目的，例如藉由在高「類型金鑰」位址位元上設定全零。

【0139】 *設定類型金鑰之例示性技術*

【0140】 在一些途徑中，類型金鑰通常可被設定標準KPIO方式，經調適以用於此目的，但在高「類型金鑰」位址位元中具有非零值。應注意，在低「外部金鑰」位址位元中發送之值可設定成全零(若彼為所需的)，或若彼為較佳的，可允許為任何值。

【0141】 *刪除類型金鑰之例示性技術*

【0142】 在一些途徑中，類型金鑰可自裝置刪除標準KPIO方式，經調適以用於此目的，但在高「類型金鑰」位址位元中具有非零值。如上所述，在低「外部金鑰」位址位元中發送之值可設定成全零(若彼為所需的)，或若彼為較佳的，可允許為任何值。

【0143】 保留「空金鑰」設定之益處

【0144】 前幾段中之描述明確使用高「類型金鑰」位址位元中之全零設定來指定對Kext之操作(例如，設定或刪除)而不影響任何類型金鑰。類似地，在結合設定及刪除金鑰之命令使用時，高「類型金鑰」位址位元中之非零設定指示將對特定類型金鑰進行操作，且較佳不影響外部金鑰中之任一者。

【0145】 保留空金鑰設定之代價為其消耗「類型金鑰」位址位元設定中之一者，例如導致15個類型金鑰設定可用，而非16個。然而，可能需要允許僅藉由外部金鑰加密而無需使用任何類型金鑰(其可被視為已知預設類型金鑰，例如，全零金鑰)。若如此，此第16類型金鑰設定實際上用於指定已知預設『類型』金鑰之使用。

【0146】 關於保留一個空「類型」金鑰設定，應注意，在其他途徑中，可類似地保留一個空「租戶」金鑰設定，以在設定或刪除類型金鑰時使用。此為可選的，而非嚴格需要的，此係因為邏輯可簡單地偵測類型金鑰中之非零值，且回應於此偵測，裝置辨識設定金鑰或刪除金鑰僅意欲用於所定址之類型金鑰。若需要空「租戶」金鑰設定，則此設定應較佳地為與外部金鑰相關聯之低位址位元之全一設定，此係因為彼將為所使用之最後外部金鑰位址，且因此在大部分使用案例中很可能不會使用。保留一個

空「租戶」金鑰設定之結果將為少了一個可用租戶Kext (例如，若為外部金鑰使用保留12位元，則吾人可僅支援4095個租戶而非4096個)。

【0147】 可與本文中所呈現之方法一起使用之額外安全性特徵

【0148】 在一些途徑中，本文中所描述之KPIO-X組態可經組態以允許僅在裝置處儲存金鑰，且因此可在裝置處刪除金鑰。此類組態在本文中別處論述。

【0149】 在一個途徑中，類型金鑰係產生於裝置外部。類型金鑰可自一些外部金鑰管理實體提供至裝置，例如以租戶金鑰可提供至裝置之類似方式。

【0150】 在另一途徑中，所有類型金鑰均可由裝置內部產生且儲存於裝置內。舉例而言，類型金鑰產生於裝置內且僅儲存於裝置中。此提供對類型金鑰之傳播的更多控制。若禁止類型金鑰離開裝置，則自裝置刪除類型金鑰確保用彼類型金鑰加密之資料的密碼抹除。

【0151】 在又一途徑中，明文形式之任何金鑰(例如，未經包裝的)Kext及(若適用) MEK僅儲存於裝置中，理想地儲存於揮發性記憶體中。因此，裝置之功率循環或功率損失自裝置清除此等金鑰。類型金鑰可以未加密(in the clear)及/或經包裝形式儲存於裝置中之非揮發性記憶體中。在一個途徑中，外部提供之Kext與內部產生之類型金鑰組合，且所得組合式金鑰用於實際大量加密。

【0152】 在又其他途徑中，該等類型之金鑰中之一或多者(Kext、類型金鑰、組合式金鑰、MEK)可儲存於裝置內，例如儲存於裝置之非揮發性記憶體中。彼非揮發性記憶體可在諸如NAND快閃之專用IC上，或可嵌入於諸如FPGA、ASIC、CPU等之一些較大IC中。在一些途徑中，該

等類型之金鑰中之至少一者以原始(未經加密)形式儲存於裝置中。在其他途徑中，該等類型之金鑰中之一或多者以經包裝形式(例如，經加密形式、密碼保護形式、模糊形式等)儲存於裝置中。在該等類型之金鑰中之一或多者以經包裝形式儲存之情況下，用於解除包裝一或多個金鑰之資訊(諸如另一金鑰、密碼等)可被擷取及/或接收且用於解除包裝一或多個金鑰。舉例而言，管理裝置所需之PIN或密碼可用作用於包裝內部金鑰之包裝金鑰。替代地，金鑰加密金鑰(KEK)可用作包裝金鑰以包裝一或多個金鑰。較佳地，僅非揮發性儲存器之該等類型之金鑰中之一或多者呈經包裝形式。

【0153】 如上文所提及，組合式金鑰可使用在閱讀本揭示之後對於熟習此項技術者將變得顯而易見之任何合適的技術自多個金鑰建立。舉例而言，可使用簡單互斥或。在本文所使用之途徑中之任一者中，國家標準與技術研究院(NIST)批准之金鑰衍生函式(KDF)可用於計算實際上使用之大量加密金鑰。此為對KPIO現今使用之直接金鑰模型的改良，此係因為其保證了在磁碟上進行密碼抹除之能力，且使用外部提供之熵。

【0154】 根據本發明之一個態樣，一種系統包括每個IO金鑰致動之裝置，該裝置具有處理器及與處理器整合、可由處理器執行或與處理器整合且可由處理器執行之邏輯。邏輯經組態以使得裝置執行本文中所呈現之方法中的任一者，包括圖3之方法。

【0155】 利用KPIO-X之租戶裝置操作

【0156】 現參考圖4，展示根據本發明之一個態樣的方法400之流程圖。根據本發明之方法400可在圖1至圖3中描繪之任何環境中以及以各種途徑來執行。當然，比圖4中具體描述之操作更多或更少的操作可包括於

方法400中，如熟習此項技術者在閱讀本描述後將理解。

【0157】 方法400之步驟中之各者可由作業環境之任何合適組件執行。舉例而言，在各種途徑中，方法400可部分或完全由租戶之電腦或其中具有一或多個處理器之某一其他裝置執行。處理器(例如，以硬體及/或軟體實施之一或多個處理電路、一或多個晶片及/或一或多個模組，且較佳地具有至少一個硬體組件)可用於任何裝置中以執行方法400之一或多個步驟。說明性處理器包括但不限於中央處理單元(CPU)、特殊應用積體電路(ASIC)、場可程式化閘陣列(FPGA)等、其組合或此項技術中已知之任何其他合適運算裝置。

【0158】 如圖4中所展示，方法400可以操作402開始，其中產生具有預定義長度之位址欄的命令。在一個途徑中，命令為符合NVMe規範的命令，但根據本發明之各種態樣，此項技術中已知之其他類型之命令可經調適以供使用。位址欄中之位元的第一子集識別特定租戶之Kext，且位址欄中之位元的第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者。

【0159】 在操作404中，將命令發送至每個IO金鑰致動之裝置，該每個IO金鑰致動之裝置經組態以使用自Kext及與位元之第二子集相關聯之類型金鑰產生之組合式金鑰來加密及/或解密與命令相關聯之資料。如上文所提及，組合可為兩個金鑰之直接組合，或如下文所描述，可需要組合金鑰中之一者與另一金鑰之衍生物(例如，使用另一金鑰建立之經包裝金鑰)。所有此類變體均應視為等效物。

【0160】 亦如上文所提及，資料類型可包括隱私類型及/或機密類型。

【0161】 在一個途徑中，藉由請求銷毀儲存於每個IO金鑰致動之裝置中之Kext及(若適用)裝置中之使用彼Kext建立之所有相關聯媒體加密金鑰來請求對應於租戶之所有資料的密碼抹除。若在裝置上存在Kext之多於一個執行個體，則請求較佳地引起其所有執行個體之銷毀。

【0162】 在另一途徑中，藉由請求銷毀類型金鑰之所有執行個體及(若適用)裝置中之使用彼類型金鑰建立之所有相關聯媒體加密金鑰來密碼抹除所有租戶之特定資料類型。

每個IO金鑰致動之裝置中之密碼抹除的額外實例

【0163】 以下描述揭示用於使得本端加密之資料能夠藉由經組態用於KPIO-X之每個IO金鑰致動之裝置(諸如ECD)中的內部動作被密碼抹除之系統、方法及電腦程式產品之數種較佳途徑。一般而言，使用自上文所提及之組合式金鑰及儲存於儲存裝置(例如，ECD、SED、帶匣、可攜式記憶體等)內之內部金鑰(Kint)建立之MEK來加密及/或解密資料。在銷毀Kint及自其建立之所有MEK後，僅用彼MEK加密儲存之所有資料經密碼抹除，因此變得不可恢復。類似地，組合式金鑰及用於建立組合式金鑰之Kext之所有複本的銷毀密碼抹除對應於彼Kext之資料。同樣地，組合式金鑰及用於建立彼組合式金鑰之類型金鑰之所有複本的銷毀密碼抹除對應於彼類型金鑰之資料。

【0164】 此外，由於Kint與使用租戶之特定Kext建立之組合式金鑰組合以建立接著用於寫入及讀取彼租戶之資料之MEK，即使租戶共用位址空間，在無第一租戶之Kext或相關聯組合式金鑰之情況下，其他租無法解密第一租戶之資料。因此，數個Kext可個別地與儲存於同一邏輯區塊位址範圍(邏輯區塊之所允許範圍(例如，在NVMe名稱空間中))內之不同位

置處的唯一資料相關聯，該邏輯區塊位址範圍可為數百萬扇區長。此並不與個別寫入命令之範圍混淆，所有寫入命令將利用每個IO金鑰使用由到達彼寫入命令頭之標頭之金鑰標籤指定的單一Kext來寫入。

【0165】 *ECD及SED中之密碼抹除*

【0166】 雖然本文中大部分描述係結合具有任何類型之SED或ECD的例示性實施來呈現，但此僅藉助於實例來進行，且僅係為了提供上下文作為對讀者之幫助。因此，本文中所呈現之概念及教示同樣適用於利用儲存媒體(諸如，磁性記錄帶、記憶卡、光學媒體等)及相關裝置之實施。

【0167】 現參考圖5，展示根據一個途徑之方法500的流程圖。根據本發明之方法500可在本文中所描述之其他圖中描繪的任何環境中以及以各種途徑來執行。當然，比圖5中具體描述之操作更多或更少的操作可包括於方法500中，如熟習此項技術者在閱讀本描述後將理解。

【0168】 方法500之步驟中之各者可由作業環境之任何合適組件執行。舉例而言，在各種途徑中，方法500可部分或完全由諸如電腦、磁碟或其中具有一或多個處理器之某一其他裝置之裝置執行。處理器，例如以硬體及/或軟體實施之一或多個處理電路、一或多個晶片及/或一或多個模組，及較佳地具有至少一個硬體組件可用於任何裝置中以執行方法500之一或多個步驟。說明性處理器包括但不限於中央處理單元(CPU)、特殊應用積體電路(ASIC)、場可程式化閘陣列(FPGA)等、其組合或此項技術中已知之任何其他合適運算裝置。

【0169】 如圖5中所展示，方法500可以操作502開始，其中經組態以在儲存媒體上執行資料操作(諸如自儲存媒體讀取資料及/或將資料寫入至儲存媒體)之裝置接收一或多個唯一外部加密金鑰(Kext)。一或多個

Kext自一或多個外部源提供至裝置以用於每個IO金鑰操作。外部源可為任何外部源。舉例而言，外部源可為在虛擬機器或容器中運行之應用程式，或本身在正寫入或讀取資料之主機伺服器上運行之應用程式，或透明地處置彼等應用程式、虛擬機器、容器或主機伺服器之所有金鑰佈建的控制基礎結構。外部源亦可為金鑰儲存器、金鑰伺服器、由使用者輸入之金鑰(例如，經由鍵盤、藉由插入快閃隨身碟等)。

【0170】 一或多個Kext與命令標頭中指定之一或多個類型金鑰一起使用以產生一或多個組合式金鑰，例如在上文更詳細地描述。注意操作503。

【0171】 一或多個Kext及一或多個組合式金鑰較佳僅儲存於裝置中之揮發性記憶體中，使得其在裝置之斷電或重啟動後銷毀。一或多個Kext可以任何合適方式接收，諸如：按需要，回應於對Kext之請求(例如，來自裝置)，一次全部接收等。舉例而言，Kext可結合讀取或寫入以經加密形式儲存於或待儲存於儲存媒體上之資料的請求來接收。

【0172】 儲存媒體可為本文中所揭示之任何類型，例如磁帶、磁碟、非揮發性隨機存取記憶體(NVRAM)等等。因此，裝置可為任何類型之資料儲存裝置(例如，磁帶機、SSD、HDD、能夠加密之USB磁碟、NVRAM模組等)。此外，裝置可為可移式資料儲存類型之能夠加密磁碟(ECD)，諸如能夠加密之USB磁碟、能夠加密之磁帶機、自加密磁碟(SED)等。

【0173】 在操作504中，例如自裝置之非揮發性記憶體存取儲存於裝置內之Kint。彼非揮發性記憶體可在諸如NAND快閃之專用IC上，或可嵌入於諸如FPGA、ASIC、CPU等之一些較大IC中。在一些途徑中，Kint

以原始(未經加密)形式儲存於裝置中。在其他途徑中，Kint以經包裝形式(例如，經加密形式、密碼保護形式、模糊形式等)儲存於裝置中。在Kint以經包裝形式儲存之情況下，用於解除包裝Kint之資訊(諸如另一金鑰、PIN、密碼等)可被擷取及/或接收且用於解除包裝Kint。舉例而言，管理裝置所需之PIN或密碼可用作用於包裝內部金鑰之包裝金鑰。替代地，金鑰加密金鑰(KEK)可用作包裝金鑰以包裝內部金鑰。較佳地，僅非揮發性儲存器之內部金鑰通常應呈經包裝形式。

【0174】 在較佳態樣中，裝置經組態以禁止以任何形式將Kint傳送至裝置外部。然而，在裝置內部之微處理器或控制器可存取裝置內之Kint。

【0175】 在操作506中，使用Kint及一或多個組合式金鑰中之相關聯一者為Kext中之至少一些中的各者產生唯一MEK。換言之，與用於產生其之給定Kext相關聯之MEK不同於任何其他MEK。任何已知技術均可用於自組合式金鑰及Kint建立MEK，例如藉由將組合式金鑰及Kint一起進行XOR，藉由應用另一已知金鑰衍生或雜湊演算法，藉由將兩個金鑰附加在一起以建立較大MEK等。

【0176】 用於給定資料集之MEK可在任何所需時間建立。在一個途徑中，MEK係回應於組合式金鑰之建立而產生。在另一途徑中，MEK回應於接收對與Kext相關聯之資料執行資料操作的請求而建立。

【0177】 無論MEK何時建立，MEK可揮發性地儲存於裝置內以供使用及/或再用，可用於資料操作且丟棄等。較佳地，呈明文形式之MEK僅儲存於裝置內之揮發性記憶體中，使得其在裝置斷電或重設時丟失。此有助於確保MEK不可自裝置外部存取，亦不能在裝置被停用且因此斷電

且自儲存系統移除之情況下存取。

【0178】 在操作508中，回應於接收對與組合式金鑰中之一者相關聯的資料執行資料操作之請求，與彼組合式金鑰相關聯之MEK用於加密及/或解密資料，例如使用另外傳統式加密/解密技術。舉例而言，在操作508中，回應於接收到讀取請求，使用適當MEK來解密所請求之資料的密文，以得到未經加密(亦即，明文)形式之所請求資料，其接著可輸出至請求者。所請求之資料的密文可複製至緩衝器中，且接著經解密，可在讀取期間「即時」解密等。經解密資料例如經由主機介面輸出至資料之請求者等。

【0179】 在一些途徑中，MEK在完成相關聯請求後刪除。在其他途徑中，MEK可保留於某一形式之揮發性記憶體或暫存器中以供再用。在兩種情況下，儲存裝置可保留Kext、組合式金鑰及/或相關聯MEK，直至藉由顯式命令或重設被告知忘記其，或斷電導致其被忘記。

【0180】 圖5之各種操作的態樣提供於下文中。此等態樣僅藉助於實例呈現，且並不意欲為限制性的。如上文所提及，當前大部分論述係指ECD；此已僅藉助於實例進行。此外，此等態樣可根據多個可能態樣及途徑以任何方式組合以實踐本發明。

【0181】 MEK可使用此項技術中已知及/或在閱讀本描述後對於熟習此項技術者將變得顯而易見之任何技術自兩個分離金鑰建立。舉例而言，建立需要使用Kint及組合式金鑰兩者來計算之MEK的一種方式為使Kint為經產生之隨機數，且接著執行需要Kint及組合式金鑰兩者之計算，諸如兩者一起之逐位元互斥或，或此等兩個值之串聯，以計算MEK。

【0182】 Kint可來源於任何可設想來源。Kint較佳地建立於ECD內

部，此為最安全途徑，此係因為Kint之複本將永不需要存在於ECD外部，除非有意地自其複製。舉例而言，使用來自ECD內之隨機數產生器的輸出以已知方式產生Kint。

【0183】 在其他途徑中，Kint可建立於ECD外部且提供至ECD。舉例而言，Kint可在製造建置期間經程式化至裝置中，可由管理員程式化至裝置中，可在裝置之組態或格式化期間插入至裝置中等。

【0184】 在一個態樣中，Kint可特定針對於特定資料集，且因此裝置可儲存多個唯一Kint，該等唯一Kint各自與唯一資料集相關聯。

【0185】 較佳地，ECD經組態以不允許Kint之任何外部可見性或自ECD傳送或複製Kint。

【0186】 在一個說明性途徑中，組合式金鑰及僅經包裝形式之Kint儲存於ECD中之非揮發性記憶體中。Kext僅以非揮發性形式儲存於ECD外部，且因此必須在功率循環及/或冷啟動之後提供至ECD (或由ECD存取)至少一次以允許計算MEK。MEK可僅在ECD具有Kint及Kext兩者時經計算。因此，Kext必須以某種形式提供至ECD (或由ECD存取)以計算組合式金鑰。根據各種態樣，存在可進行此之許多方式。一種方式為使Kext注入至用金鑰加密金鑰(KEK)包裝之ECD中。替代地，若ECD支援金鑰管理互操作性協定(KMIP)用戶端，則其可經由安全通道(諸如由TLS或IPsec保護)自此項技術中已知之類型的外部金鑰管理器請求及接收Kext。交替地，Kext可經由針對安全協定輸入及安全協定輸出命令等設立之安全隧道以類似於個人識別碼(PIN)之方式的方式(例如，以明文形式)提供至ECD。

【0187】 Kint較佳以經包裝形式儲存於ECD中，且在提供包裝金鑰

(其可為KEK或可替代地取決於一或多個密碼或一或多個PIN，經提供至ECD以鑑別ECD支援之一或多個不同角色(例如，Admin1))之前為不可包裝的。因此，自ECD外部提供之包裝函式金鑰的任何部分皆經提供至ECD以允許解除包裝Kint。一旦ECD已被提供或已存取計算MEK必需之所有所需資訊(包括Kext)，ECD就計算MEK，且接著能夠解密現有密文以產生所得明文(例如，回應於主機讀取)，或將呈明文形式之新接收到之客戶資料加密為密文(例如，回應於主機寫入)。

【0188】 在一個途徑中，Kint係在內部產生且用KEK抑或用與某個管理安全提供者(下文「AdminSP」)角色(例如，Admin1)相關聯之PIN包裝。因此，一旦將KEK注入至ECD中，或諸如Admin1之實體已用其密碼或PIN鑑別，就可存取Kint。

【0189】 可允許包裝Kint之KEK或PIN作為(包裝金鑰之)重設金鑰操作之部分而改變。Kint本身亦可被重設金鑰，但此將導致對由MEK加密之資料的密碼抹除，該等MEK在Kint被重設金鑰之前自在使用之Kint建立。

【0190】 一個實施包括在一些或所有情況下使用例如由隨機命令調用之相同類型之內部隨機數產生能力使ECD成為Kint之產生源。

【0191】 現參考圖6，展示根據一個途徑之用於在每個IO金鑰方案中寫入可密碼抹除資料之例示性方法600的流程圖。根據本發明之方法600可在本文中所描述之其他圖(尤其圖5)中描繪的任何環境中以及以各種途徑來執行。當然，比圖6中具體描述之操作更多或更少的操作可包括於方法600中，如熟習此項技術者在閱讀本描述後將理解。

【0192】 方法600之步驟中之各者可藉由作業環境之任何合適組件

執行。舉例而言，在各種途徑中，方法600可部分或完全由諸如電腦、磁碟或其中具有一或多個處理器之某一其他裝置之裝置執行。處理器(例如，以硬體及/或軟體實施之一或多個處理電路、一或多個晶片及/或一或多個模組，且較佳地具有至少一個硬體組件)可用於任何裝置中以執行方法600之一或多個步驟。說明性處理器包括但不限於中央處理單元(CPU)、特殊應用積體電路(ASIC)、場可程式化閘陣列(FPGA)等、其組合或此項技術中已知之任何其他合適運算裝置。

【0193】 在操作602中，在經組態以對儲存媒體執行KPIO-X操作之裝置處接收請求。該請求為使用與第一資料相關聯之第一Kint以經加密形式將第一資料寫入至儲存媒體。

【0194】 在操作604中，存取儲存於裝置內之Kint。

【0195】 在操作606中，使用Kint及自Kext及類型金鑰建立之組合式金鑰產生第一MEK。

【0196】 在操作608中，使用第一MEK來加密第一資料。

【0197】 在操作610中，將經加密第一資料在儲存媒體之第一邏輯區塊位址範圍中寫入至儲存媒體。第一邏輯區塊位址範圍較佳為儲存媒體之邏輯區塊之所允許範圍(例如，在NVMe名稱空間中)，其可為數百萬扇區長。此並不與全部與單一Kext相關聯之特定寫入命令的有限範圍混淆。

【0198】 在操作612中，在裝置處接收第二請求。第二請求為使用與第二資料相關聯之第二外部金鑰以經加密形式將第二資料寫入至儲存媒體的請求，其中第二外部金鑰不同於第一外部金鑰。

【0199】 在操作614中，存取儲存於裝置內之內部金鑰。

【0200】 在操作616中，使用內部金鑰及使用Kext及類型金鑰建立

之第二組合式金鑰產生第二MEK。

【0201】 在操作618中，使用第二MEK來加密第二資料。

【0202】 在操作620中，將經加密第二資料在儲存媒體之第一邏輯區塊位址範圍中寫入至儲存媒體。第二寫入可至可或可不與由第一寫入命令寫入之邏輯區塊範圍重疊的在所允許邏輯區塊範圍(例如，在NVMe名稱空間中)內之任何邏輯區塊位址範圍。

【0203】 可在此方法600中執行額外操作，且可在方法600中實施本文中所描述之特徵中之任一者。

【0204】 現參考圖7，展示根據一個途徑之用於在每個IO金鑰方案中對資料執行密碼抹除之例示性方法700的流程圖。根據本發明之方法700可在本文中所描述之其他圖(尤其圖4至圖5)中描繪的任何環境中以及以各種途徑來執行。當然，比圖7中具體描述之操作更多或更少的操作可包括於方法700中，如熟習此項技術者在閱讀本描述後將理解。

【0205】 方法700之步驟中之各者可由作業環境之任何合適組件執行。舉例而言，在各種途徑中，方法700可部分或完全由諸如電腦、磁碟或其中具有一或多個處理器之某一其他裝置之裝置執行。處理器(例如，以硬體及/或軟體實施之一或多個處理電路、一或多個晶片及/或一或多個模組，且較佳地具有至少一個硬體組件)可用於任何裝置中以執行方法700之一或多個步驟。說明性處理器包括但不限於中央處理單元(CPU)、特殊應用積體電路(ASIC)、場可程式化閘陣列(FPGA)等、其組合或此項技術中已知之任何其他合適運算裝置。

【0206】 在操作702中，在經組態以使用每個IO金鑰操作在儲存媒體上執行資料操作之裝置處接收引起處於儲存媒體之至少一個邏輯區塊位

址範圍中之所有資料之密碼抹除的請求。至少一個邏輯區塊位址範圍中之資料的個別部分各自與唯一Kext相關聯，例如對應於唯一租戶及/或唯一類型金鑰，例如對應於唯一資料類型。資料之個別部分各自使用利用Kint建立之唯一MEK及與資料之部分相關聯之唯一組合式金鑰加密。

【0207】 在操作704中，藉由銷毀Kint (例如，藉由抹除Kint、覆寫Kint及/或實體上銷毀儲存Kint之記憶體)及裝置中之自彼Kint建立之任何一或多個MEK來達成密碼抹除。

【0208】 *金鑰類型及對應參數之實例*

【0209】 以下描述提供本文中提及之各種類型之金鑰之例示性組態及參數。以下特徵之任何組合可結合上文所描述之對應金鑰中之任一者使用及/或應用於上文所描述之對應金鑰中之任一者。

【0210】 租戶金鑰(或Kext)

【0211】 在一些途徑中，位址位元之第一集合允許每個租戶一個金鑰，可能減去一個以允許空設定(例如，若位址位元之彼第一集合中存在12位元，則支援4095個租戶)。

【0212】 在一些途徑中，在通電之後，所需的所有租戶金鑰始終自某個外部金鑰管理器提供至符合KPIO-X規範的ECD，且從不以明文形式儲存於非揮發性記憶體中。作為一選項，租戶金鑰可以經包裝形式發送。

【0213】 在一些途徑中，外部(ECD外部之)金鑰管理實體負責能夠藉由使得在ECD中(藉由向其發出命令)及在所有外部金鑰儲存器中銷毀與給定租戶相關聯之所有資料來密碼抹除其。

【0214】 在一些途徑中，給定租戶金鑰並不與位址位元之第一集合之任何給定設定持久地相關聯。作為一實例，外部(ECD外部之)金鑰管理

實體(例如，金鑰管理器)可首先將給定租戶金鑰(例如，對於TenantX)提供至ECD作為第五金鑰(且因此，其可與KeyID設定的前12位元000000000101相關聯)。但接著，若TenantX之金鑰在一段時間內沒有被使用(例如，隔夜，當租戶不工作時)，則彼金鑰管理器可用TenantY之金鑰覆寫彼金鑰位置，且隨後，當TenantX回來工作且想要存取TenantX之資料時，將TenantX之金鑰發送至完全不同的金鑰位置(例如，與KeyID設定000101100010相關聯)。

【0215】 在一些途徑中，給定租戶之資料並不靜態地指派給共同名稱空間中之任何給定位址範圍。每次租戶寫入資料時，可動態地分配寫入。舉例而言，假定TenantY最近刪除映射至共同名稱空間之位址範圍內的一組扇區之某一邏輯實體(例如，一檔案)，該TenantY仍將TenantY之密文寫入至該組扇區。現在，TenantX想要寫入某一邏輯實體。空間經動態地分配至TenantX之資料，且因此TenantX密文可覆寫先前容納TenantY密文且回應TenantY刪除檔案而經釋放之扇區中的一些或全部。ECD外部之處理程序可管理哪個租戶及類型金鑰與哪組扇區相關聯，使得當需要讀取彼等扇區時，租戶及類型金鑰兩者之正確KeyID與主機讀取命令一起發送，以允許解密彼密文。

【0216】 類型金鑰

【0217】 在一些途徑中，位址位元之第二集合允許每個類型一個金鑰，可能減去一個以允許空設定(例如，若位址位元之彼第二集合中存在4位元，則支援15種類型)。

【0218】 在一些途徑中，在通電之後，所需的所有類型金鑰始終自某個外部金鑰管理器提供至符合KPIO-X規範的ECD，且從不以明文形式

儲存於非揮發性記憶體中(此將違反KPIO規格，且亦可能違反KPIO-X規格)。較佳地，類型金鑰以經包裝形式發送至ECD。

【0219】 在一些途徑中，外部(ECD外部之)金鑰管理實體負責能夠藉由使得在ECD中(藉由向其發出命令)及在所有外部金鑰儲存器中銷毀與給定類型相關聯之所有資料來密碼抹除其。

【0220】 在一些途徑中，給定類型金鑰並不與位址位元之第二集合之任何給定設定持久地相關聯。作為一實例，外部(ECD外部之)金鑰管理實體(例如，金鑰管理器)可首先將給定類型金鑰(例如，對於TypeX)提供至ECD作為第五金鑰(且因此，其可與KeyID設定之第二4位元0101相關聯)。但接著，若TypeX之金鑰在一段時間內沒有被使用(例如，已終止專案)，則彼金鑰管理器可用TypeY之金鑰覆寫彼金鑰位置，且隨後，若恢復專案且因此再次需要TypeX且想要存取資料，則可將TypeX之金鑰發送至某一完全不同的金鑰位置(例如，與KeyID設定0010相關聯)。

【0221】 在一些途徑中，給定類型之資料可或可不靜態地指派給共同名稱空間中之給定位址範圍。每次租戶寫入資料時，可假定其被動態地分配。舉例而言，假定TenantY已寫入TypeA之某內容，但從那時起已刪除映射至共同名稱空間之位址範圍內的某一組扇區之某一邏輯實體(例如，一檔案)，該TenantY仍將TenantY之密文寫入至該組扇區。現在，TenantY想要寫入例如TypeB之某一其他邏輯實體。空間經動態地分配至TenantY之TypeB資料，且因此TenantY TypeB密文可覆寫先前容納TenantY TypeA密文、在TenantY刪除TypeA資料之彼檔案時經釋放之扇區中的一些或全部。ECD外部之處理程序可管理哪個租戶及類型金鑰與哪組扇區相關聯，使得當需要讀取彼等扇區時，租戶及類型金鑰兩者之正確

KeyID與主機讀取命令一起發送，以允許解密彼密文。

【0222】 內部金鑰

【0223】 在一些途徑中，每個名稱空間可分配一個內部金鑰。替代地，一個共同內部金鑰可與由給定ECD支援之所有名稱空間一起使用。

【0224】 在一些途徑中，在各次通電之後接著解鎖ECD之後，經包裝內部金鑰被解除包裝，且因此然後為可存取的。較佳地，內部金鑰從不以明文形式非揮發性地儲存。

【0225】 在一些途徑中，負責管理ECD之狀態的外部(ECD外部之)實體在一些情況下可發出使ECD將其自身恢復至其原始工廠狀態(OFS)必需之命令，且當ECD恢復到其原始工廠狀態時，ECD經組態以覆寫或以其他方式主動刪除含有內部金鑰以及可位於揮發性記憶體中之內部金鑰之任何明文版本的任何經包裝金鑰結構。

【0226】 在一些途徑中，每次建立名稱空間時，在ECD內內部產生新的內部金鑰(或可能在磁碟恢復回OFS之後初始化磁碟之後僅一次，而不管此後建立多少名稱空間(例如，若ECD能夠維護多於一個名稱空間))。

【0227】 將清楚，可以任何方式組合前述系統及/或方法之各種特徵，從而自上文所呈現之描述建立複數個組合。

【0228】 應進一步瞭解，本發明之態樣可以代表客戶部署之服務的形式提供，以按需要供應服務。

【0229】 已出於說明之目的呈現本發明之各種態樣之描述，但該等描述並不意欲為詳盡的或限於所揭示之途徑。在不脫離所描述態樣之範疇及精神的情況下，許多修改及變化對於一般熟習此項技術者而言將顯而易

見。本文中所使用之術語經選擇以最佳解釋各種途徑之原理、實際應用或對市場中發現之技術的技術改良，或使得其他一般熟習此項技術者能夠理解本文中所揭示之途徑。

【符號說明】

【0230】

100: 運算環境

101: 電腦

102: 廣域網路

103: 終端使用者裝置

104: 遠端伺服器

105: 公共雲端

106: 私有雲端

110: 處理器集

111: 通信網狀架構

112: 揮發性記憶體

113: 持久儲存器

114: 周邊裝置集

115: 網路模組

120: 處理電路系統

121: 快取記憶體

122: 作業系統

123: 使用者介面裝置集

124: 儲存器

125: 物聯網感測器集

130: 遠端資料庫

140: 閘道器

141: 雲端協調模組

142: 主機實體機器集

143: 虛擬機器集

144: 容器集

150: 區塊

200: 儲存系統

202: 較高儲存層

204: 隨機存取媒體/直接存取媒體

206: 較低儲存層

208: 較低執行儲存媒體

212: 儲存系統管理器

214: 主機介面

216: 額外儲存層

300: 方法

302: 操作

304: 操作

306: 操作

308: 操作

310: 操作

400: 方法

402: 操作

404: 操作

500: 方法

502: 操作

503: 操作

504: 操作

506: 操作

508: 操作

600: 方法

602: 操作

604: 操作

606: 操作

608: 操作

610: 方法

612: 方法

614: 方法

616: 方法

618: 方法

620: 方法

700: 方法

702: 操作

704: 操作

【發明申請專利範圍】

【請求項1】

一種電腦實施方法，其包含：

接收具有預定義長度之一位址欄的一命令，其中該位址欄中之位元的一第一子集識別一特定租戶之一外部金鑰，其中該位址欄中之該等位元的一第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者；

擷取由位元之該第一子集識別之該外部金鑰；

擷取對應於位元之該第二子集之該類型金鑰；及

組合租戶金鑰與該類型金鑰以建立一組合式金鑰以用於加密及/或解密與該命令相關聯之資料；

存取儲存於該電腦內之一內部金鑰；

使用該內部金鑰及該組合式金鑰來產生一唯一媒體加密金鑰；及

使用該媒體加密金鑰來加密及/或解密與該命令相關聯之資料。

【請求項2】

如請求項1之電腦實施方法，其中該等資料類型包括隱私類型。

【請求項3】

如請求項1之電腦實施方法，其中該等資料類型包括機密類型。

【請求項4】

如請求項1之電腦實施方法，其中該命令為一符合非揮發性記憶體高速(NVMe)規範的命令。

【請求項5】

如請求項1之電腦實施方法，其中該電腦經組態為一每個IO金鑰致動之電腦。

【請求項6】

如請求項1之電腦實施方法，其中該電腦經組態以禁止以任何形式將該內部金鑰傳送至該電腦外部。

【請求項7】

如請求項1之電腦實施方法，其中該等外部金鑰中之數者個別地與儲存於同一邏輯區塊位址範圍中之不同位置處的唯一資料相關聯。

【請求項8】

如請求項1之電腦實施方法，其包含藉由銷毀由該租戶使用之該外部金鑰來執行對應於該租戶之所有資料的密碼抹除。

【請求項9】

如請求項1之電腦實施方法，其包含藉由銷毀與特定資料類型相關聯之該類型金鑰來執行所有租戶之該特定資料類型之密碼抹除。

【請求項10】

如請求項9之電腦實施方法，其中該類型金鑰僅儲存於該電腦上，其中該電腦經組態以禁止以任何形式將該類型金鑰傳送至該電腦外部。

【請求項11】

如請求項1之電腦實施方法，其中位元之該第二子集中之一空序列指示該外部金鑰之設定及/或刪除。

【請求項12】

如請求項1之電腦實施方法，其中該等類型金鑰係產生於該電腦外部。

【請求項13】

如請求項1之電腦實施方法，其中該等類型金鑰係產生於該電腦內且

僅儲存於該電腦中。

【請求項14】

一種電腦系統，其包含：

一每個IO金鑰致動之電腦，該電腦具有一處理器及與該處理器整合、可由該處理器執行或與該處理器整合且可由該處理器執行之邏輯，該邏輯經組態以使該電腦：

藉由該電腦接收具有預定義長度之一位址欄的一命令，其中該位址欄中之位元的一第一子集識別一特定租戶之一外部金鑰，其中該位址欄中之該等位元的一第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者；

藉由該電腦擷取由位元之該第一子集識別之該外部金鑰；

藉由該電腦擷取對應於位元之該第二子集之該類型金鑰；及

藉由該電腦組合租戶金鑰與該類型金鑰以建立一組合式金鑰以用於加密及/或解密與該命令相關聯之資料；

藉由該電腦存取儲存於該電腦內之一內部金鑰；

藉由該電腦使用該內部金鑰及該組合式金鑰來產生一唯一媒體加密金鑰；及

藉由該電腦使用該媒體加密金鑰來加密及/或解密與該命令相關聯之資料。

【請求項15】

一種電腦程式產品，該電腦程式產品包含一或多個電腦可讀儲存媒體及共同儲存於該一或多個電腦可讀儲存媒體上之程式指令，該等程式指令包含：

接收具有預定義長度之一位址欄的一命令之程式指令，其中該位址欄中之位元的一第一子集識別一特定租戶之一外部金鑰，其中該位址欄中之該等位元的一第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者；

擷取由位元之該第一子集識別之該外部金鑰的程式指令；

擷取對應於位元之該第二子集之該類型金鑰的程式指令；及

組合租戶金鑰與該類型金鑰以建立一組合式金鑰以用於加密及/或解密與該命令相關聯之資料的程式指令；

存取儲存於該電腦內之一內部金鑰的程式指令；

使用該內部金鑰及該組合式金鑰來產生一唯一媒體加密金鑰的程式指令；及

使用該媒體加密金鑰來加密及/或解密與該命令相關聯之資料的程式指令。

【請求項16】

如請求項15之電腦程式產品，其中該等資料類型包括選自由隱私類型及機密類型組成之群的資料類型。

【請求項17】

如請求項15之電腦程式產品，其中該命令為一符合非揮發性記憶體高速(NVMe)規範的命令。

【請求項18】

如請求項15之電腦程式產品，其中執行該等程式指令之一電腦經組態為一每個IO金鑰致動之電腦。

【請求項19】

一種電腦實施方法，其包含：

產生具有預定義長度之一位址欄的一命令，其中該位址欄中之位元的一第一子集識別一特定租戶之一外部金鑰，其中該位址欄中之該等位元的一第二子集對應於與不同資料類型相關聯之複數個類型金鑰中的一者；

將該命令發送至一每個IO金鑰致動之電腦，該每個IO金鑰致動之電腦經組態以使用自該外部金鑰及與該等位元之該第二子集相關聯之該類型金鑰產生之一組合式金鑰來加密及/或解密與該命令相關聯之資料；

接收儲存於每個IO金鑰致動之電腦內之一內部金鑰；

使用該內部金鑰及該組合式金鑰來產生一唯一媒體加密金鑰；及

使用該媒體加密金鑰來加密及/或解密與該命令相關聯之資料。

【請求項20】

如請求項19之電腦實施方法，其中該等資料類型包括隱私類型。

【請求項21】

如請求項19之電腦實施方法，其中該等資料類型包括機密類型。

【請求項22】

如請求項19之電腦實施方法，其中該命令為一符合非揮發性記憶體高速(NVMe)規範的命令。

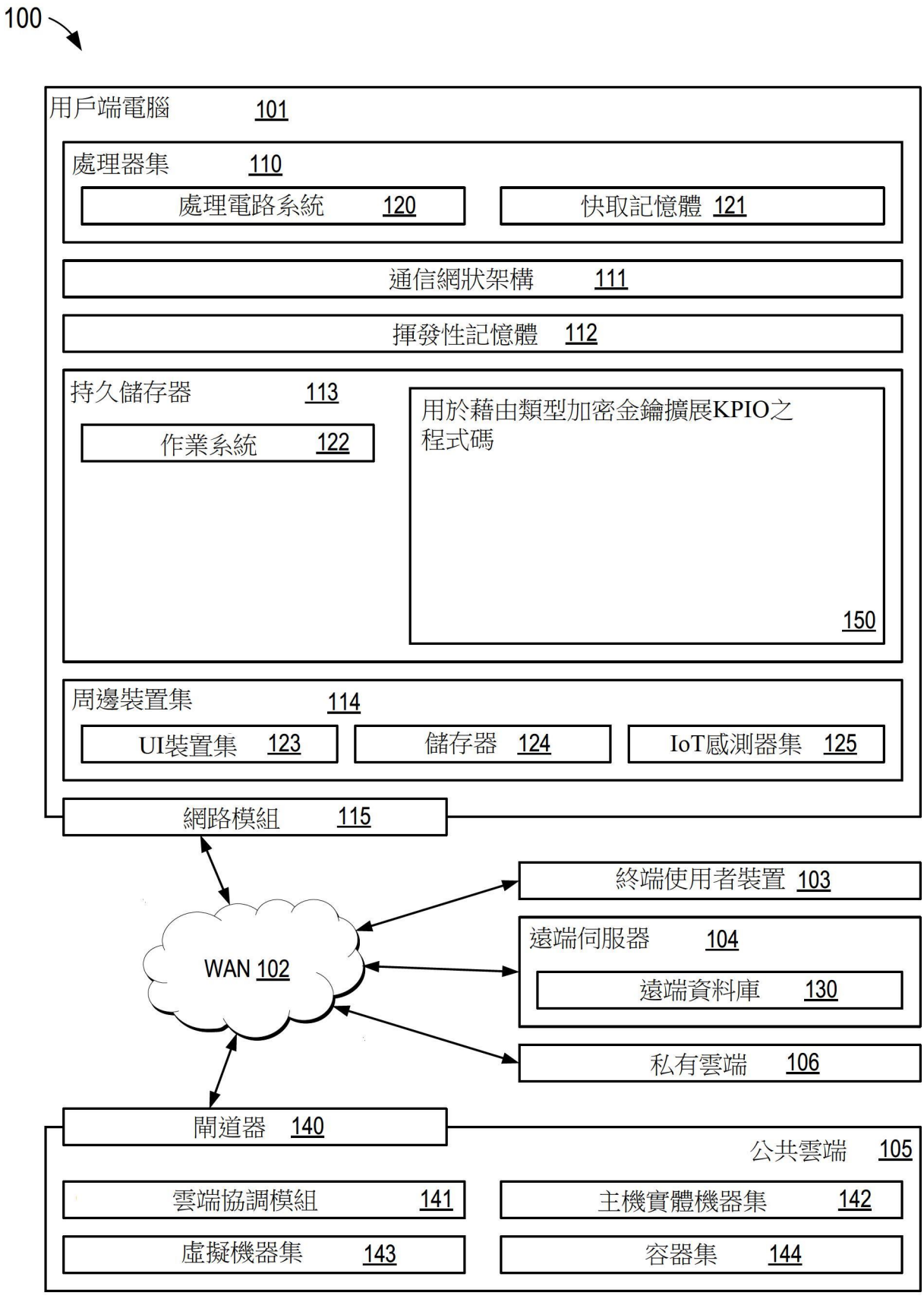
【請求項23】

如請求項19之電腦實施方法，其包含藉由請求銷毀儲存於該每個IO金鑰致動之電腦中之該外部金鑰來請求對應於該租戶之所有資料的密碼抹除。

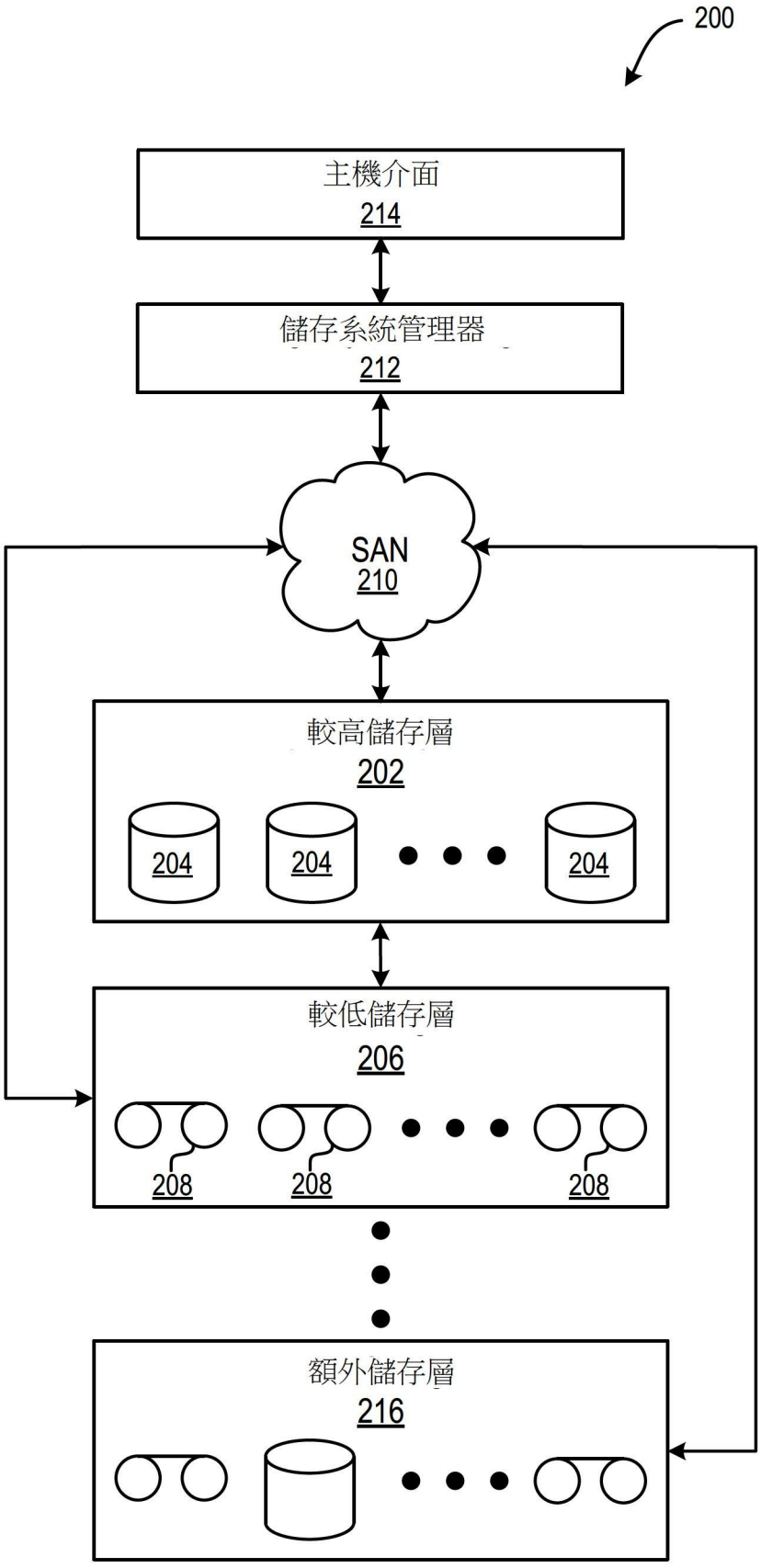
【請求項24】

如請求項19之電腦實施方法，其包含藉由請求銷毀與特定資料類型相關聯之該類型金鑰來請求所有租戶之該特定資料類型之密碼抹除。

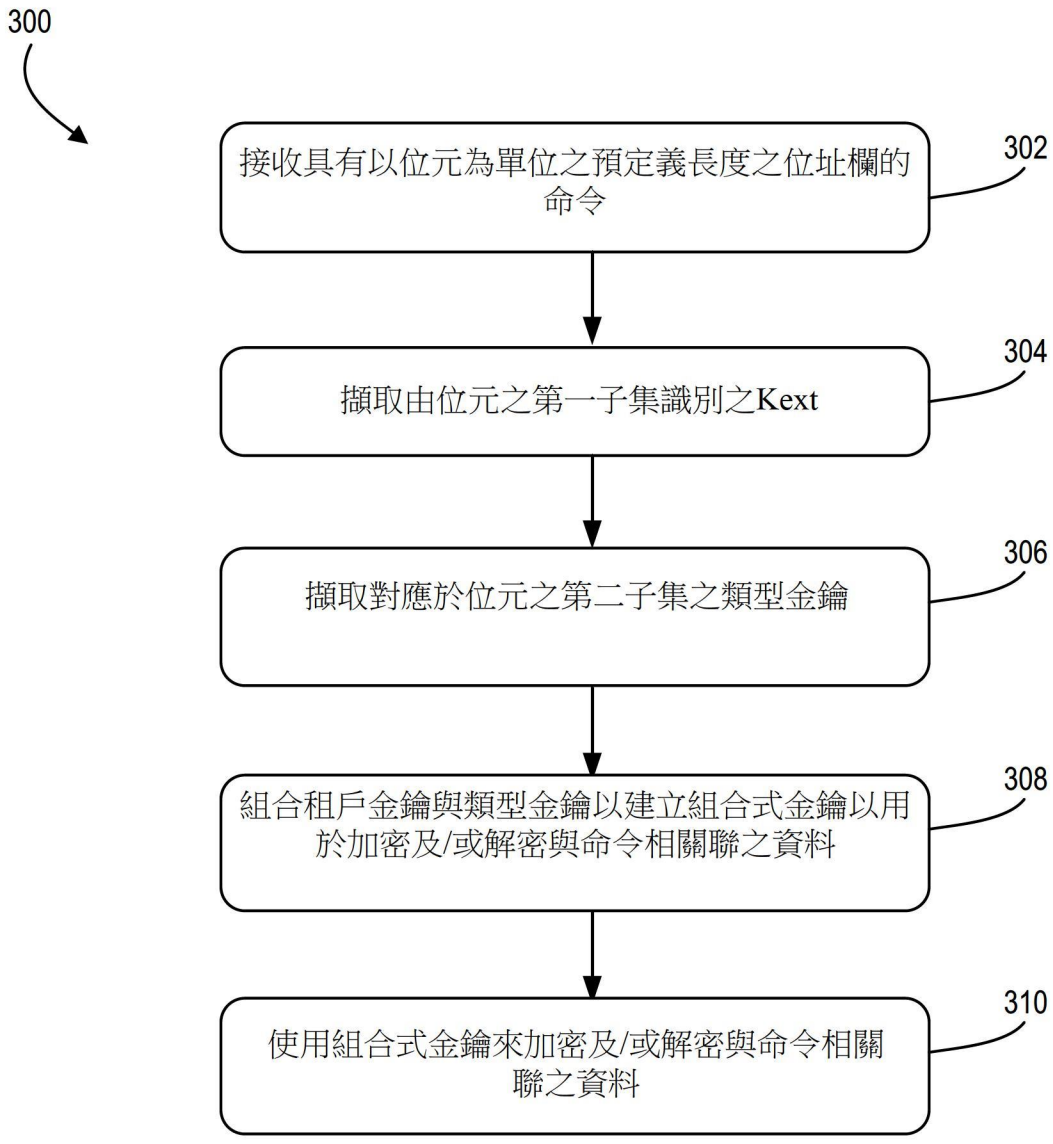
【發明圖式】


100
用戶端電腦 101
處理器集 110
處理電路系統 120
快取記憶體 121
通信網狀架構 111
揮發性記憶體 112
持久儲存器 113
作業系統 122
用於藉由類型加密金鑰擴展KPIO之程式碼
150
周邊裝置集 114
UI裝置集 123
儲存器 124
IoT感測器集 125
網路模組 115
WAN 102
終端使用者裝置 103
遠端伺服器 104
遠端資料庫 130
私有雲端 106
閘道器 140
公共雲端 105
雲端協調模組 141
主機實體機器集 142
虛擬機器集 143
容器集 144

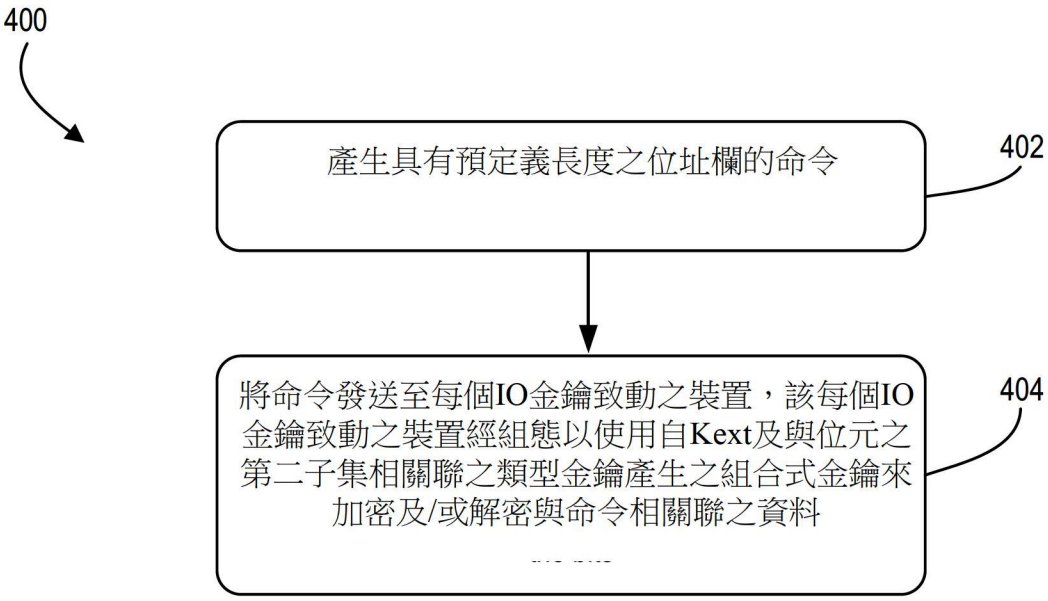
【圖1】


200
主機介面
214
儲存系統管理器
212
SAN
210
較高儲存層
202
204
204
204
較低儲存層
206
208
208
208
額外儲存層
216

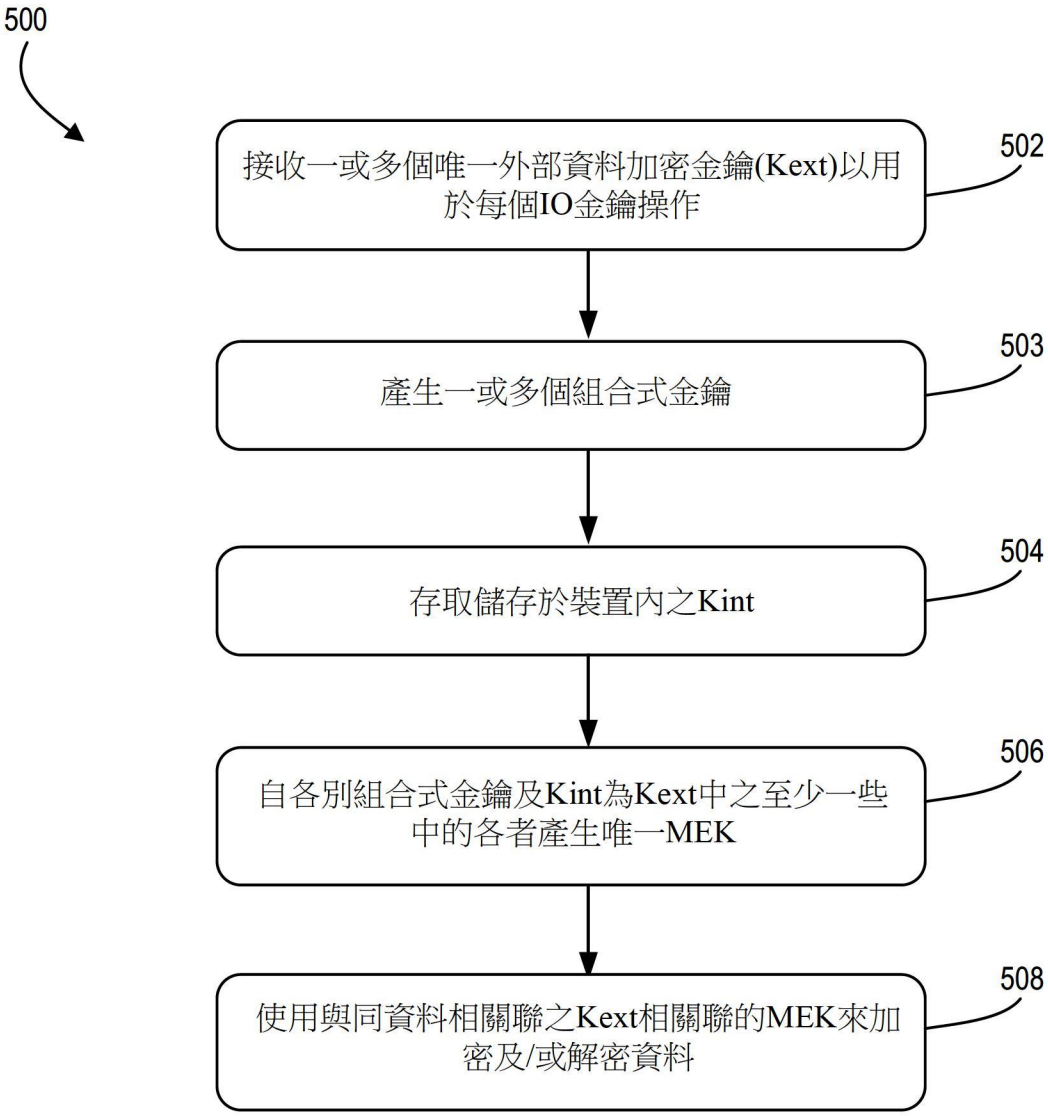
【圖2】


300
接收具有以位元為單位之預定義長度之位址欄的命令
302
擷取由位元之第一子集識別之Kext
304
擷取對應於位元之第二子集之類型金鑰
306
組合租戶金鑰與類型金鑰以建立組合式金鑰以用於加密及/或解密與命令相關聯之資料
308
使用組合式金鑰來加密及/或解密與命令相關聯之資料
310

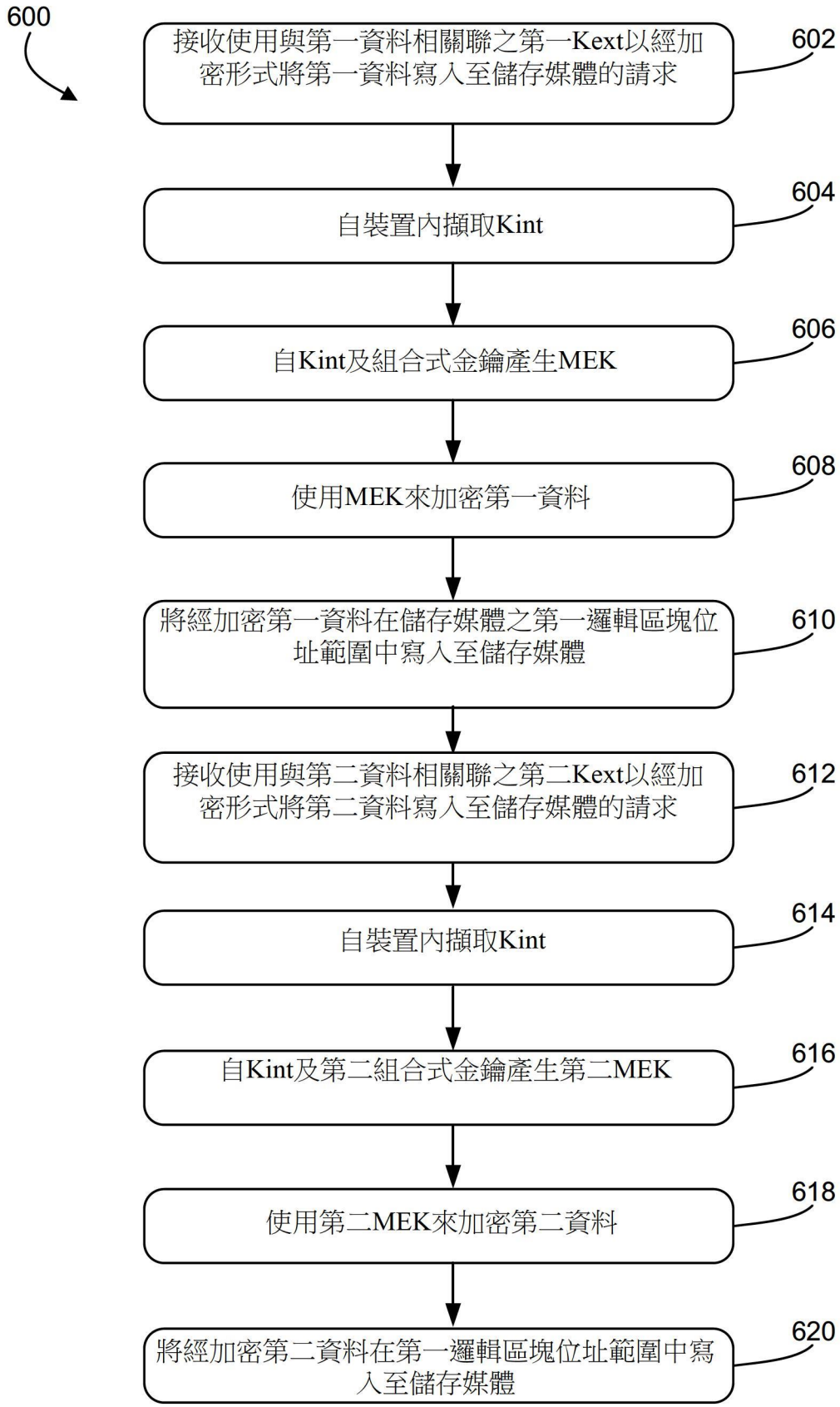
【圖3】


400
產生具有預定義長度之位址欄的命令
402
將命令發送至每個IO金鑰致動之裝置，該每個IO金鑰致動之裝置經組態以使用自Kext及與位元之第二子集相關聯之類型金鑰產生之組合式金鑰來加密及/或解密與命令相關聯之資料
404

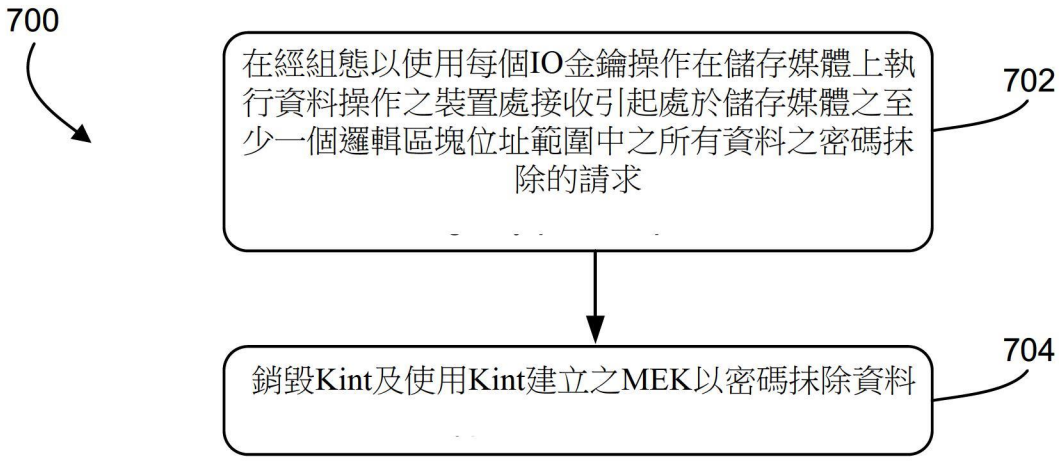
【圖4】


500
接收一或多個唯一外部資料加密金鑰(Kext)以用於每個IO金鑰操作
502
產生一或多個組合式金鑰
503
存取儲存於裝置內之Kint
504
自各別組合式金鑰及Kint為Kext中之至少一些中的各者產生唯一MEK
506
使用與同資料相關聯之Kext相關聯的MEK來加密及/或解密資料
508

【圖5】


600
接收使用與第一資料相關聯之第一Kext以經加密形式將第一資料寫入至儲存媒體的請求
602
自裝置內擷取Kint
604
自Kint及組合式金鑰產生MEK
606
使用MEK來加密第一資料
608
將經加密第一資料在儲存媒體之第一邏輯區塊位址範圍中寫入至儲存媒體
610
接收使用與第二資料相關聯之第二Kext以經加密形式將第二資料寫入至儲存媒體的請求
612
自裝置內擷取Kint
614
自Kint及第二組合式金鑰產生第二MEK
616
使用第二MEK來加密第二資料
618
將經加密第二資料在第一邏輯區塊位址範圍中寫入至儲存媒體
620

【圖6】


700
在經組態以使用每個IO金鑰操作在儲存媒體上執行資料操作之裝置處接收引起處於儲存媒體之至少一個邏輯區塊位址範圍中之所有資料之密碼抹除的請求
702
銷毀Kint及使用Kint建立之MEK以密碼抹除資料
704

【圖7】