玖、發明說明：

【發明所屬之技術領域】

本發明一般係關於密碼學，以及更明確而言，係關於密碼系統的一種同源運用。

【先前技術】

由於數位通訊已極為普遍，因此更增加相關通訊管道之安全需求的重要性。例如，目前的技術容許使用者遠端存取銀行帳戶、醫療記錄以及其他私人和敏感性資料。

密碼學已廣泛被應用於數位通訊的安全上。密碼學一般係關於訊息的加密(或編密)和解密(decrypting)。利用秘密訊息(例如金鑰)加密和解密。在不同加密方法中，可利用單一金鑰或多重金鑰進行加密和解密。

一種常用的多重金鑰密碼系統為公開金鑰編碼系統。在一公開金鑰系統中，傳送者可傳送加密訊息至取得利用私密金鑰產生之已認證公開金鑰的接收者。如名稱所示，公開金鑰可取自公開資源。此外，公開金鑰通常經過認證以避免被偽裝攻擊。可例如利用可信公共檔案、線上可信伺服器或利用離線伺服器和憑證在一可信通道上交換金鑰的技術進行公開金鑰的認證。

在取得認證公開金鑰之後，傳送者以公開金鑰加密原始資料而產生一種密文。特定的接收者則利用公開金鑰解密該密文而取得原始資料。若無私密金鑰則無法解密該密文。因此，僅擁有私密金鑰者可成功解密該密文。

對稱式密碼系統(例如串流式或區塊式加密)使用公開金鑰的優點為在雙方通訊中僅需保密其私密金鑰(同時在對稱式密碼系統中，雙方均保存該私密金鑰)。

一種現代公開金鑰加密系統為利用分佈於有限體上的某種橢圓曲線(ECs)。可利用源自橢圓曲線的一對已發佈值做為公開金鑰(包括分佈於曲線上的點以及藉由曲線上簡單乘法產生(即整數乘法)的相關公開金鑰)。利用曲線上雙線配對進行認證。

一般而言，在維持類似的安全性之下，橢圓曲線和例如 RSA(Rivest、Shamir 和 Adleman 公開金鑰加密技術)的傳統系統比較為具有相當低通訊需求的加密系統。

目前沒有一種公開加密金鑰已被證明為絕對的安全。因此，目前公開金鑰加密系統的安全性為根據一組數論問題的困難度而定。

因此，目前亟需一種更具有安全性的公開金鑰加密系統。

【發明內容】

揭示具有公開金鑰加密系統的技術。更明確而言，為利用同源阿貝爾變數(例如一維實例中的橢圓曲線)於公開金鑰系統。例如，同源運用中可利用多重曲線取代單一曲線以提供更安全的加密法。此技術可運用於電子簽名和/或身份認證加密法(IBE)。此外，同源運用可用於例如盲簽名、層級系統，和其類似物。另外，亦揭示產生同源運用

的解決方案。

在一實施例中，其方法包括公佈一種對應於同源運用的公開金鑰。此方法進一步包括利用對應於同源的解密金鑰(例如，為其雙重同源)進行加密訊息的解密。

【實施方式】

下列討論為假設讀者已熟悉加密技術。密碼學的基本導論請參考 CRC 公司出版由 A.Menezes, P.van Oorschot, 和 S.Vanstone 所著全名為"應用密碼學手冊"第五版(2001年8月)教科書。

下列揭示之改良公開金鑰系統技術為根據多重橢圓曲線(或通稱為阿貝爾變數)。揭示在曲線間產生同源(或排序)的各種技術。公開加密可利用多重曲線取代單一曲線以產生同源。此外，此技術可應用於相當短的數位簽章(例如，使用者鍵入或傳送於短頻寬管道上)和/或身份認證加密法(IBE)解決方案(例如，可記憶公開金鑰)。短數位簽章亦可透過整體的驗證增加其效率。

同源密碼系統之概論

第 1 圖為在一密碼系統中利用同源的一種舉例性方法 100 的說明。一個產生同源(橢圓曲線或通稱為阿貝爾變數)的步驟 102。同源可由接收方或另一方(如參考第 5 圖進一步討論的公信單位)所產生。步驟 102 亦可產生和各產生之同源對應的雙重同源(將於下述進一步討論)。產生同源的各種方法詳述如下。此外，參考第 3 和第 5 圖將更為清楚，

產生之同源可應用於公開金鑰以及已發佈之公開金鑰(104)。傳送方或公信單位可發佈公開金鑰(請看，例如第 3 和第 5 圖之討論)。

傳送方然後利用加密金鑰加密(或簽署)訊息(106)。接收方利用解密金鑰確認/解密步驟 106 之加密訊息以判斷該加密或簽章的可靠性(108)。在一實施例中，利用 Weil 配對確認其加密訊息(如下述之討論)。然而，Weil 配對僅為用於確認或解密之配對的實例之一。例如，亦可利用其他雙線性和/或非退化配對技術如 Tate 配對及平方配對。

同源的概論

第 2 圖舉例性說明兩條曲線(如橢圓曲線)間的同源映射。如所示，曲線 E_1 可藉由同源 φ(當 φ：$E_1 \rightarrow E_2$)被映射至曲線 E_2。第 1 圖亦說明此雙重同源 φ(當 φ：$E_2 \rightarrow E_1$)。

在各種實施例中，密碼系統的同源運用中，當 φ：$E_1 \rightarrow E_2$ 為同源時，可使例如已知曲線 E_1 產生一對(E_1，E_2)同源曲線，而認為極不易構建任何低特異性同源之非零同源 φ：$E_1 \rightarrow E_2$。因此，若總體斷裂(定義為容許任何其後訊息於多項式時間內斷裂的計算法)和按實例斷裂之間存有差異時，則此時同源密碼系統之最佳已知攻擊較總體斷裂之離散對數或"單純"按實例攻擊之其他根據訊息離散對數計算法所需的時間更長。

例如，在一令牌認證系統(token system)下給予各別客戶允許存取某些服務(其可能為低價值)的特殊簽章訊息，代理人可在電話上讀取客戶的令牌，因此其可為相當短的

簽章。其可利用足夠大的參數而使每次訊息攻擊的代價高於可獲得的服務，並同時使總體的斷裂極為昂貴。

同源的詳述

域(field) k可被具q因數之特徵(characteristic) p所固定並且具有一代數收斂$\bar{k}$。設E/k為定義於域k上的橢圓曲線以及$E(k)$為定義於k上的群，並且設$k(E)$表示橢圓曲線的函數域。同理，設$[n]_E$或$[n]$表示E上的映射$P \rightarrow n \cdot P$以及$E[n]$表示映射的核心(kernel)。

同源$\varphi: E_1 \rightarrow E_2$為一種傳送$E_1$之單位元(identity element)至$E_2$的非常數態。當存在該同源時，$E_1$和$E_2$可稱為同源。若$\varphi$為具有係數$k$之定義方程式，則同源被定義於$k$。任何同源亦可變為群同態(group homomorphism)，即$\varphi(P+Q)=\varphi(P)+\varphi(Q)$全部$P,Q \in E_1$，其左手邊之加法為$E_1$的組律以及右手邊的加法為$E_2$的組律。因此$\varphi$之核心為$E_1$的子群。

設$Hom_k(E_1,E_2)$表示從E_1至E_2之定義於k的同源集。$Hom_{\bar{k}}(E_1,E_2)$以$Hom(E_1,E_2)$表示之。任何同源$\varphi: E_1 \rightarrow E_2$，具有雙重同源$\hat{\phi}: E_2 \rightarrow E_1$而使：

$$\hat{\phi} \circ \phi = [n]_{E_1} \quad 及 \quad \phi \circ \hat{\phi} = [n]_{E_2},$$

而$n=\deg(\varphi)$為同源的階。雙重同源滿足標準性質：

$$\hat{\hat{\phi}} = \phi, \widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}, \widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}, [\hat{n}] = [n]$$

在一實施例中，有限映射之φ的階可進一步定義為：

$k(E_1)$於域 kE_2 之回折(pullback)(由 φ)所延伸的階，其 φ 定義於 k。藉由核心的體積(假設函數域延伸為可分開)或上述等式可輕易求得其值。因此，若其階為 B-平滑(即 deg(φ)的質因數小於或等於 B)，則該同源為 B-平滑曲線。橢圓曲線 E 之自同態(endomorphisms)的 $Hom(E,E)$集表示為 $End(E)$；此集合具有下列定義的環構造：

$$(\varphi+\psi)(P)=\varphi(P)+\psi(P),(\varphi\circ\psi)(P)=\varphi(\psi(P))$$

通常，群 $Hom(E_1,E_2)$為一轉矩自由左 $End(E_2)$-模組和右 $End(E_1)$-模組。當 $E_1=E_2=E$ 時，其豐富之代數構造：$Hom(E_1,E_2)=End(E)$為無零因數和具有特徵零的環(非僅為一模組)。

在一實施例中，此可被視為一種格子：設 E 為定義於某些域 k 的橢圓曲線。而，$End(E)$和二次方程式假想域之序的 Z 或四元數代數內最大序為同態。對任何兩條橢圓曲線 E_1E_2 而言，群 $Hom(E_1,E_2)$為最多四個秩的的自由 Z 模組。當 $End(E)$大於 Z 時，可認定為 E 具有複數乘法。$End(E)$內對應於 Frobenius 自同態 $(x,y)\rightarrow(x^p,y^p)$的因數被表示為 π，並且其滿足特徵等式 $x^2-tr(E)x+q=0$。橢圓曲線 c 的導體為 $[End(E):Z[\pi]]$。

Weil 配對

Weil 配對 $e_n: E[n]x\ E[n]\rightarrow\mu_n$ 為一種具有 k 內 n^{th} 單位根群之值的雙線性、非退化映射。在一實施例中，利用 Weil 配對執行第 1 圖之步驟 108 的確認/解密。然而，Weil

配對僅為可用於確認或解密的配對實例之一。例如，亦可利用其他雙線性和/或非退化配對技術如 Tate 配對及平方配對。Weil 配對可滿足下述的性質：

$$e_n(S,\hat{\phi}(T))=e_n(\phi(S),T)\text{，其中 }S\in E_1[n],\ T\in E_2[n]$$

此處，$e_n(S,\hat{\phi}(T))$為 E_1 上的配對計算，而 $e_n(\varphi(S),T)$為 E_2 上的配對計算。注意兩條曲線具有 n-扭轉點，其因而使群序受到限制。由於根據 Tate 定理，當且僅當兩組點具有相同序時 $E_1(k)$和 $E_2(k)$在 k 上為同源，故並不會造成困擾。

Weil 配對評估線性相依的全部輸入配對是否相同。因此，其具有確保輸入點非為相互之純量乘積的優點。一種方法為利用定義於有限域 k 上遠大於 n-扭轉點之全群 $E_2[n]\cong(Z/nZ)^2$ 的曲線 E_2 定義於 k 上。此時，在 $1/n$ 的序上可忽略群 $E_2[n]$之兩個隨機元素為線性相依的可能性，故 Weil 配對可獲得高可能性的非無效值。上述等式確保 E_1 上分佈的配對值可符合 E_2。

或者，可利用一種改良配對函數 $\hat{e}(P,Q)=e_n(\lambda(P),Q)$其中 λ為任何非純量自同態，而使 P和 $\lambda(P)$為線性獨立和 $\hat{e}(P,P)\neq 1$。此種映射 λ稱為 E 之扭轉或扭曲。

同源的產生

在各種實施例中，可利用各種方法構建高程度的同源(例如，橢圓曲線或通稱為阿貝爾變數)以及其如參考第 1 圖步驟 102 所討論的雙重同源。此處討論之短數位簽章及 IBE 密碼系統可依習慣發佈成對的值$(P,\varphi(P))$作為公開金

鑰，同時評估構成私密金鑰的雙重 $\hat{\phi}$。

在一具體例中，其構造可摘要為：已知任何 E，其具有一種階(degree)為隨機分佈之構建同源 $E \rightarrow E$ 的演算法，並且具有機率為 $\sim 1/\log(n)$ 的質數；已知任何曲線 E_1，其具有一種從 E_1 至時間之隨機標的 $O(B^3)$ 構建隨機 B-平滑同源的演算法；以及已知 $Hom_k(E_1,E_2)$ 內之 E_1、E_2 和兩條線性獨立同源，其具有一種構建質數冪次同源的演算法(請看，下述有關獨立同源的討論)。

複數乘法同源

若如前所述 $E_1=E_2$ 及假設 E_1 具有以判別式 $D<0$ 之假想二冪次 O_D 的複數乘法(CM)。可利用一種概率演算法產生該曲線 E_1 和一種大質數冪次 E_1 之自同態 φ 以預估 $|D|$ 的時間多項式。

1. 計算判別式 D 的 Hilbert 類多項式 $H_D(X)$。若 K 代表分佈於 Q 上 $H_D(X)$ 的分裂域。

2. 選擇 $H_D(X)$ 的任何根 x 及在具有 j-不變量等於 x 之 C 上構建橢圓曲線 E。應注意 E 為定義於數域 K 上。

3. 藉由 $\sqrt{D}$ 構建具有複數乘法的曲線 E。利用 q-展開式上的線性代數可明確找出具有對應於同源 $\sqrt{D} \in EndE$ 之係數 K 的有理函數 I(X,Y)。

4. 選取隨機整數 a 和 b 直至 a^2-b^2D 為質數。然後，同源 $a+b\sqrt{D}$ 將為具有質數冪次 E 的自同態。

5. 選擇任何 K 之質理想 P 及約化 E 和 I 模數 P 之系數。假定 E_1 代表 E 之歸約及及假定 φ 為 $a+b\sqrt{D}$ 之歸約。

演算法的第 1~3 步驟為$|D|$內的決定性和多項式時間。如第 4 步驟所述，數域的質數定理指出a^2-b^2D的質數機率為 $1/\log(a^2-b^2D)$，故對大小為 n 的整數 a 和 b 在$\log(Dn^2)$冪次試驗後可決定第 4 步驟。

所得自同態 φ 為一種質數冪次 E_1 的自同態。已知 a 和 b 時可僅利用有理函數 $I(X,Y)$以及純量乘法和加法計算 φ 和其雙重 $\hat{\phi}=a-b\sqrt{D}$ 。此類同源 φ 可稱之為一種 CM-同源。

模組化同源

對任何質數 l，模組化曲線 $X_0(l)$可參數化同構類的 l 冪次同源 $E_1\rightarrow E_2$。更明確而言，當且僅當 $\Phi_l(j(E_1),j(E_2))=0$ 時 $X_0(l)$存在具有 E_1 和 E_2 為 l-同源之性質的多項式方程式 $\Phi_l(X,Y)$。

利用多項式 $\Phi_l(X,Y)$，任何 E_1 可計算出其 l-同源曲線 E_2 以及 l 冪次同源 $E_1\rightarrow E_2$ 的一明確多項式方程式。由於具有反 j-不變量之模組化多項式在 X 和 Y 計算中為對稱，故可用於尋找其雙重同源。

操作上，由於這些多項式的系數極大故可不必使用多項式 $\Phi_l(X,Y)$進行實際的運算。具有較小系數之 $X_0(l)$可利用不同但等效的多項式模型代替。估且不論用於此計算之模型的準確度，衍生自此方法的同源可稱之為模組化同源(modular isogeny)。

目前已知計算模組化同源的演算法通常可應用於較小的 l 值。由於已知曲線 E_1 和 E_2 的攻擊者可檢查各 l 值是否為 l-同源曲線並且在確定時將其還原，故利用較小系數的

模組化同源法本身並無法增加其安全性。然而，大平滑冪次 $\mathbf{II}l$ 的同源 φ 可設計出許多模組化同源(例如，選擇不同的 l)，並且可在不顯示中間曲線之下使用 φ 做為其同源。可在任意點上估算 φ 的攻擊者仍可藉由計算 E_1 的全部 l-扭轉點並且觀察任何點是否被 φ 所消除而降低其質數 l。然而，在不易計算雙重同源的假設之下，攻擊者將無法計算其所選擇之點的 φ。為獲得較佳之測定，亦可利用純量同源或 CM 同源將大而非平滑因數導入一執行中之冪次的方法設計其獲得之同源。

線性獨立同源

在一實施例中，從 E_1 至 E_2 的互質冪次可得到線性獨立的同源 φ 和 Ψ。所以，線性組合 $a\varphi+b\Psi$ 為具有 a 和 b 兩個變數的二次式 $a^2\hat{\phi}\phi+ab(\hat{\phi}\psi+\hat{\psi}\phi)+b^2\hat{\psi}\psi$ 。應注意此二次式的系數為整數，因為外系數為 φ 和 Ψ 的冪次並且中項等於 deg(φ+Ψ)-deg(φ)-deg(Ψ)。由於二次式為原始形式，其通常在 a 和 b 變化於全部對 $(a,b)\in Z^2$ 時可獲得無限大的質數值。依此方法，可獲得許多大而非平滑(或偶質數)冪次的同源 $E_1\rightarrow E_2$。亦可估算其結果冪次為非平滑的機率。

利用同源的短簽章法

在一實施例中，此處討論之技術可應用於極短的簽章法中(例如，使用者鍵入或傳送於短頻寬管道上)。下述將討論兩種簽章法，其部分根據同源以及橢圓曲線上配對的數學性質。

Galois 不變量簽章

假定 F_{q^n}/F_q 為冪次 n 之有限域的擴張。取一定義於 F_q 的橢圓曲線以及定義於 F_{q^n} 的同源 $\varphi: E_1 \rightarrow E_2$，其中 E_2 為定義於 F_{q^n} 的橢圓曲線。在一實施例中，曲線 E_2 為定義於 L 而非定義於 L 的子域(subfield)，但其可使 E_2 僅定義於一子域。然而，基於安全上的理由，同源 φ 不可被定義於 F_{q^n} 的任何適當子域。此外，可根據各種例如上述所討論的技術產生同源 φ。

第 3 圖說明運用同源簽署訊息的舉例性方法 300。此方法包括下列的步驟：

公開金鑰。隨機選擇 $P \in E_1(F_q)$ 以及發佈 (P,Q)，其中 $Q=\varphi(P)$。應注意由於 φ 非定義於 F_q，故 P 定義於 F_q 但 Q 非定義於 F_q。

私密金鑰。φ 之雙重同源 $\hat{\phi}$。

簽章。假定 H 為一來自訊息空間至一組 E_2 上 k-扭轉點的(公開)隨機甲骨文。已知一訊息 m，計算 $S=\sum_{i=0}^{n-1}\pi^i\hat{\phi}H(m)$(步驟 304，其具有利用上述秘密/私密金鑰產生的的簽章)，其 π 為 q^{th} 冪 Frobenius 映射以及其總和表示橢圓曲線在 E_1 上的和。為方便計，我們以 Tr(其代表"微量")表示運算子 $S=\sum_{i=0}^{n-1}\pi^i$。輸出 $S \in E_1(F_q)$ 做為簽章。然後傳送此簽章而被接收方所接收(分別為步驟 306 和 308)。應注意 F_{q^n}/F_q 之 Galois 群為 $\{1,\pi,\cdots,\pi^{n-1}\}$，故 S 為 Galois 不變量並且因此定義於 F_q。

驗證。假定 e_1 和 e_2 分別代表在 $E_1[k]$和 $E_2[k]$上的 Weil

配對。已知一公開金鑰(P,Q)和一訊息-簽章對(m,S)，檢查是否$e_1(P,S)=\prod_{i=1}^{n-1}\pi^i e_2(Q,H(m))$（步驟 310，其利用上述產生的公開金鑰確認接收的簽章）。因此，有效簽章可滿足下列方程式：

$$e_1(P,S)=e_1\left(P,\sum_{i=0}^{n-1}\pi^i\hat{\phi}H(m)\right)=\prod_{i=0}^{n-1}e_1(P,\pi^i\hat{\phi}H(m))$$

$$=\prod_{i=1}^{n-1}e_1(\pi^i P,\pi^i\hat{\phi}H(m))=\prod_{i=0}^{n-1}\pi^i e_1(P,\hat{\phi}H(m))$$

$$=\prod_{i=0}^{n-1}\pi^i e_2(\phi(P),H(m))=\prod_{i=0}^{n-1}\pi^i e_2(Q,H(m))$$

同理，可利用於一基域(base field)之軌跡映射(trace map)，以縮短橢圓曲線(或更廣義而言對任何阿貝爾變數)上的點。換言之，可利用輸出軌跡映射於橢圓曲線上(或更高維阿貝爾變數)，作為藉由利用較低域上資料縮短代表延伸域上之相應點的方法。

多重橢圓曲線之簽章

另一種加強短簽章方案之強度的方法為利用多重公開金鑰並將其加於結果簽章。可利用此改良的本身或結合上述討論的強化 Galois 不變量。

參考第 4 圖，假設同源家族 φ：$E\rightarrow E_i$和隨機甲骨文雜湊函數家族 H_i為分別映射一訊息 m 至橢圓曲線 E_i上的一點。其類似參考第 3 圖所討論的步驟。

公開金鑰。隨機選取 $P \in E$ 並發佈 $P, Q_1, Q_2, \cdots, Q_n$(請看，例如 302)，其中 $Q_i = \varphi_i(P)$。

私密金鑰。同源 φ_i 的家族。

簽章。對各訊息 m，$m(S)$ 簽章為 $\sum_{i=1}^{n} \hat{\phi}_i(H_i(m))$ (請看，例如 304)。然後將簽署訊息傳送至接收方(請看，例如 306)。

驗證。已知一(訊息，簽章)配對 (m, S)，檢查是否 $e(P,S) = \prod_{i=1}^{n} e(Q_i, H_i(m))$ (請看，例如參考第 3 圖討論的步驟 310)。下式成立則屬於有效的簽章：

$$e(P,S) = e\left(P, \sum_{i=1}^{n} \hat{\phi}(H(m))\right) = \prod_{i=1}^{n} e(P, \hat{\phi}(H_i(m))) = \prod_{i=1}^{n} e(Q_i, H_i(m))$$

由於任何能破壞多重同源版本的人可藉由加入其所決定的同源 $\varphi_2, \cdots, \varphi_n$ 將單同源版本轉換成多重同源版本，故此系統被認為至少和僅使用單一同源者具有相同的安全性。此外，對此類系統而言，任何可成功攻擊多重同源版本者需同時破壞 φ_1 至 φ_n 的全部單一同源。

具有同源的身份認證加密(IBE)方案

第 5 圖說明一種利用同源之身份認證加密(IBE)的舉例性方法 500。此橢圓曲線間的單向同源被認為可加強身份認證加密(IBE)方案對抗計算迪菲-赫爾曼(CDH)的安全性。身份認證加密(IBE)方案如下述所定義。

映射至點：定義某些曲線 E 的運算 ID→ $P \in E$。更明確而言，可計算 $H(id)$並利用其定義一點。其可假設 H 具有類似隨機甲骨文的行為。或者，可保存點之列表並將 ID 雜湊入一串隨機權重值然後取其權重和。亦可假設具有一

個公信單位及一有限組的使用者，從各別的 ID 可計算出相應的公開金鑰。在經過公信單位適當的鑑定之後各使用者可獲得其私密金鑰。

公信單位的公開金鑰：$\alpha \in E_1$ ，$\beta = \varphi(\alpha)$。因此，公信單位(或接收方的另一實體)可提供和發佈公開金鑰(502)。若使用一扭曲 λ ，可假設 $\alpha = \lambda(a)$為某個點 a 的扭曲影象。

公信單位的私密金鑰。一種有效的可計算 $\hat{\phi}$ 。

例如，從 Bob 至 Alice 的加密資料可執行如下：

Alice 的公開金鑰：具備 $T \in E_2$ ，例如，由公信單位(或接收方的另一實體)經圖對點(map-to-point)函數 ID→ T(502)。

Alice 的私密金鑰：$S = \hat{\phi}(T)$ 。注意攻擊而迅速得到各客戶的私密金鑰所費時間類似破壞整個簽章系統(如上述)。因此，這些系統亦可稱之為兩層式(two-tier)系統。

由 **Bob** 加密。計算 Alice→ T(步驟 504，其利用公開金鑰的產生加密一訊息)。假定該訊息為 **m**。選取一隨機整數 r。將配對傳送至 Alice(506)：

$$[\mathbf{m} \oplus H(e(\beta, rT)), r\alpha]$$

由 **Alice** 解密。假定密文為 $[e, T]$。在適當鑑定之後利用公信單位(或接收方的另一實體)提供的私密金鑰(510)解密(508)該被傳送的加密訊息。因此，其明文為：

$$[\mathbf{c} \oplus H(e(r\alpha, S))$$

被雜湊入加密步驟的工作量為：

$$e(\beta,rT)=e(\phi(\alpha),rT)=e(\alpha,\hat{\phi}(rT))=e(\alpha,r\hat{\phi}(T))=e(\alpha,rS)=e(r\alpha,S),$$

其等於被雜湊入加密步驟內的數量。以上述中之討論代表其同源(例如，使用具有登入表的機率法)。

同源的指定

若同源為平滑，則其可由代表多項式計算之直線程式獲得之小程度同源的組合表示。對過度延伸的重要曲線而言，在一執行中僅需少數的輸入-輸出配對。

若 $End(E)=End_{\bar{k}}(E)$，可考慮 k 的有限延伸並且需要時可指定該延伸。在一實施例中，藉作用於基域之有限延伸的點群指定其同源。應注意二同源有些一致的延伸，但其較大域內則不同。因此，其足夠在一組產生器 S 上指定 φ。通常，此群為循環，或約為 $|S|=2$。已認為不易找到產生器，但可隨機選取 S。

更明確而言，阿貝爾群 $E(k)$(提示：k 為 q 元素的有限域)和 $Z/mZxZ/nZ$ 為同態，其中 $mn=\#E(k),n|m$ 以及此外 $n|D,D=(mn,q-1)$。可利用 Schoof 演算法計算 $mn=\#E(k)$並且若 D 之因式分解為未知，可利用隨機多項式時間演算法獲得 n。若 $\hat{P}$和 $\hat{Q}$分別 n 和 m 冪次而使任何點可被寫成 $a\hat{P}+b\hat{P}$，其被稱為梯式(echelon form)產生器並且其構建可利用 $O(q^{\frac{1}{2}+\varepsilon})$演算法。

轉而看隨機選擇(Erdos-Renyi)，假定 G 為有限阿貝爾

群以及 $g_1,\cdots,g_k$ 為 G 的隨機元素。存在一小常數 c，若 $k\geq c\cdot\log|G|$ 時，可使其子集和幾乎均勻分佈於 G。更明確而言，g_i 可產生 G。簡約表的大小，當群階為質數時可利用其強化子集和的權重而非子集和。此可在損失小量參數下延伸至任意階。

此外，可利用 $E(k)$ 的構造獲得更詳細的資訊。可選取隨機點 $P_i, i\leq 2$ 並將其寫成 $P_i=a_i\hat{P}+b_i\hat{Q}$。更明確而言，若矩陣 $\begin{bmatrix} a_1 & a_2 \\ b_1 & b_2 \end{bmatrix}$ 為可逆 mod m（注意：$n|m$），則可藉由 P_i 的線性組合表示各個梯形產生器。若此發生時，$\{P_i\}$ 可產生該群。注意落於 $\hat{P}$ 所產生之群內的機率（P_1 和 P_2）為 m^{-2}。同理，$\hat{Q}$ 所產生之群的機率（P_1 和 P_2）為 n^{-2}。因此，機率 $(1-m^{-2})(1-n^{-2})=1+(\#E)^{-2}-(m^{-2}+n^{-2})$ 均不發生上述兩個事件。

硬體的執行

第 6 圖為一般電腦環境 600 的說明，其可用於執行此處所述的技術。例如，可利用電腦環境 600 執行上述圖中討論之工作的有關指令。此外，所述之各實體（例如，第 1、3 和 5 圖所述的公信單位、接收方和/或傳送方）可各自進出此一般電腦環境。

此電腦環境 600 僅為計算環境的實例之一，並且所使

用之電腦及網路架構的使用範圍或功能性並不受到任何的限制。此電腦環境600之執行亦不需依賴在舉例性電腦環境600中結合任何的元件。

電腦環境600包括電腦602內一般用途的計算裝置。此電腦602的元件可包括但不侷限於一種或多種處理器或處理單元604(視需要可包括加密處理器或助理處理器)、系統記憶體606以及連接包括處理器604至系統記憶體606之各種系統元件的系統匯流排608。

系統匯流排608代表一種或多種類型的匯流排構造，包括記憶體匯流排或記憶體控制器、周邊匯流排、繪圖加速埠及一處理器或利用任何各種匯流排架構的區域匯流排。藉由實例，此類架構可包括工業標準架構(ISA)匯流排、微通道架構(MCA)匯流排、加強型工業標準架構(EISA)匯流排、視訊電子標準協會(VESA)區域匯流排及週邊零件連接介面(PCI)匯流排亦稱為整合型(Mezzanine)匯流排。

一般電腦602包括各種的電腦可讀取媒體。此類媒體為任何電腦602可獲得的媒體，其包括揮發和非揮發性媒體及可拭除和不可拭除媒體。

系統記憶體606包括揮發性記憶體形式的電腦可讀取媒體如隨機存取記憶體(RAM)610，和/或非揮發性記憶體如唯讀記憶體(ROM)612。電腦602元件間傳送資訊之基本程序如起動時的基本輸出入系統(BIOS)614為儲存於唯讀記憶體(ROM)612內。隨機存取記憶體(RAM)610一般含處理器單元604立即可及和/或可作業的資料和/或程式模組。

電腦 602 亦可包括其他可拭除/不可拭除、揮發/非揮發性電腦儲存媒體。藉由實施例，第 6 圖說明一種讀取和寫入不可拭除、非揮發性磁性媒體(未顯示)的硬碟驅動器 616；一種讀取和寫入可拭除、非揮發性磁碟 620(如，"軟性磁盤")的磁碟驅動器 618；以及讀取和/或寫入可拭除、非揮發性光碟 624 如 CD-ROM、DVD-ROM 或其他光學媒體的光碟驅動器 622。硬碟驅動器 616、磁碟驅動器 618 及光碟驅動器 622 藉由一種或多種資料媒體介面 626 分別連接至系統匯流排 608。或者，硬碟驅動器 616、磁碟驅動器 618 及光碟驅動器 622 可藉由一種或多種介面(未顯示)連接至系統匯流排 608。

磁碟驅動器和其相關電腦可讀取媒體具有提供電腦 602 的電腦可讀取指令、資料構造、程式模組及其他資料。實施例中雖然以硬碟 616、可拭除磁碟 620 及可拭除光碟 624 做為說明，但是應瞭解其他可儲存電腦存取資料的電腦可讀取媒體類型亦可被用於執行此舉例性計算系統和環境，例如磁性卡匣或其他磁性儲存裝置、快閃記憶卡、CD-ROM、多樣化數位光碟(DVD)或其他光學儲存器、隨機存取記憶體(RAM)、唯讀記憶體(ROM)、可電氣拭除式可改寫唯讀記憶體(EEPROM)等等。

任何數目的程式模組均可儲存於硬碟 616、磁碟 620、光碟 624、ROM 612 和/或 RAM 610，其包括實施例中的操作系統 625、一種或多種的應用程式 628、其他程式模組 630 及程式資料 632。此類操作系統 625、一種或多種應用

程式 628、其他程式模組 630 及程式資料(或其部分組合)可執行全部或部分之支援分散式檔案系統的常駐元件。

使用者可經由例如鍵盤 634 和指向裝置 636(如"滑鼠")之輸入裝置將命令和資料輸入電腦 602。其他輸入裝置 638(未顯示特定裝置)可包括麥克風、搖桿、遊戲控制器、衛星天線、串列埠、掃描器和/或其他等等。這些輸入裝置藉由耦合系統匯流排 608 的輸入/輸出介面 640 連接至處理器單元 604，但亦可藉由其他介面及匯流排構造相連接，例如平行埠、遊戲埠或通用序列匯流排(USB)。

監視器 642 或其他類型顯示裝置亦可經由如視訊轉換器 644 之介面連接至系統匯流排 608。除監視器 642 之外，其他輸出之週邊裝置包括可經由輸入/輸出介面 640 連接至電腦 602 的元件，例如喇叭(未顯示)和印表機 646。

電腦 602 可邏輯連接至一台或多台如遙程計算裝置 648 之遠端電腦而操作於網路環境。實施例之遙程計算裝置 648 可為個人電腦、手提電腦、伺服器、路由器、網路電腦、對等裝置或其他一般網路節點、電視遊戲機等等。以手提電腦說明之遙程計算裝置 648 可包括對應於此處所述之電腦 602 的許多或全部元件及特性。

電腦 602 和遠端電腦 648 之間的邏輯連接稱為區域網路(LAN)650 和通用廣域網路(WAN)652。此類網路環境常見於辦公室、企業內電腦網路、網內網路和網際網路。

當執行於 LAN 網路環境時，電腦 602 經由網路介面或轉接器 654 而連接至區域網路 650。當執行於 WAN 網路環

境時，電腦602通常包括一數據機656或其他在廣域網路652上建立通訊的裝置。內建或外接電腦602的數據機656可經由輸入/輸出介面 640 或其他適當裝置連接至系統匯流排 608。應瞭解此網路連結僅為舉例性說明，可應用建立電腦602和648之間通訊連結的其他方法。

例如所說明之計算環境600的網路環境中，電腦602的程式模組或其部分可儲存於遠端記憶體儲存裝置內。實施例中的遠端應用程式658被儲存於遠端電腦648的記憶裝置內。為說明之便，應用程式和其他如操作系統之可執行程式元件以不同區塊進行說明，但是已知該程式和元件為於不同時間被置於電腦裝置602的不同儲存元件內，並且由電腦的資料處理器進行執行工作。

此處說明電腦可執行指令之一般內容的各種模組及技術，例如可被一種或多種電腦或其他裝置執行的程式模組。通常，程式模組包括常規程式、一般程式、物件、元件、資料結構等，其可執行特定的工作或執行特定的抽象化資料形態。一般而言，在各種實作中可視需要結合或分配該程式模組的功能。

這些模組和技術在實作時可儲存於或被傳送通過某種形式的電腦可讀取媒體。電腦可讀取媒體可為任何電腦可存取之可用媒體。在非限制性電腦可讀取媒體的實例中包括”電腦儲存媒體”及”傳輸媒體”。

”電腦儲存媒體”包括以任何方法或技術儲存如電腦可讀取指令、資料結構、程式模組或其他資料之資訊的揮發

性和非揮發性、可拭除及不可拭除媒體。電腦儲存媒體包括但不侷限於 RAM、ROM、EEPROM、快閃記憶體或其他記憶體技術、CD-ROM、多樣化數位光碟(DVD)或其他光學儲存器、磁性卡匣、磁帶、磁碟儲存器或其他磁性儲存裝置、或任何其他可用於儲存所需資訊並且可被電腦存取的媒體。

"傳輸媒體"一般包括電腦可讀取指令、資料結構、程式模組或其他在調變資料信號內的資料，例如載波或其他傳輸機制。傳輸媒體亦包括任何資料傳送媒體。"調變資料信號"一詞意指具有一或多組其特性的信號或以該方法改變信號內之編碼資訊的信號。實施例中的傳輸媒體包括但不侷限於有線媒體如有線網路或直接連線的媒體，以及無線媒體如聲頻、射頻(RF)、紅外線(IR)、標準無線區域網路(例如，IEEE 802.11b 無線網路)(Wi-Fi)、行動電話、藍芽功能及其他無線媒體。電腦可讀取媒體亦包括上述任何形式媒體的結合。

結　論

雖然本發明以文字說明其構造上的特性及執行的方法，但是應瞭解附件申請專利範圍內所定義的本發明並非僅侷限於上述特定的特性或實例。反之，所揭示之特定特性和實例僅為執行本發明的舉例性型式。例如，此處討論的橢圓曲線為一維阿貝爾變數。同理，同源亦可使用於其他運用中如盲簽章、分層系統等。同樣地，此處所述之技術亦可被運用於較高維的阿貝爾變數。

【圖式簡單說明】

參考附圖進行詳細說明。在圖中，最先出現於圖中的元件符號以元件符號最左邊的數字做為識別。不同圖中的相同元件符號代表類似或相同的元件。

第 1 圖舉例說明密碼系統之同源運用的方法。

第 2 圖舉例性說明兩條曲線間的同源映射。

第 3 圖舉例說明同源簽署訊息的利用。

第 4 圖舉例說明多重曲線間的同源映射。

第 5 圖說明利用同源之身份認證加密法(IBE)的舉例性方法。

第 6 圖說明可用於執行此處所述之技術的一般電腦環境 600。

【主要元件符號說明】

100 同源加密公開金鑰

102 產生同源

104 發佈利用同源產生的公開金鑰

106 加密/簽署訊息

108 確認/解密加密訊息

200 同源映射

300 多重曲線同源映射

300 以同源簽署

302 發佈公開金鑰

304 提供簽章

306 傳送簽章

308 接收簽章

310 確認簽章

500 以同源身份認證加密

502 發佈公開金鑰

504 加密訊息

506 傳送加密訊息

508 解密傳送訊息

510 提供私密金鑰

600 電腦環境

602 電腦

604 處理器

606 系統記憶體

608 系統匯流排

610 隨機存取記憶體

612 唯讀記憶體(ROM)

614 基本輸出入系統

616 硬碟驅動器

618 磁碟驅動器

620 磁碟片

622 光碟驅動器

624 光碟片

625 操作系統

626 資料媒體介面

628 應用程式

630 程式模組

632 程式資料

634 鍵盤

636 滑鼠

638 其他輸入裝置

640 輸入/輸出介面

642 監視器

644 視訊轉換器

646 印表機

648 遠端電腦

650 區域網路

652 網際網路

654 網路轉接器

656 數據機

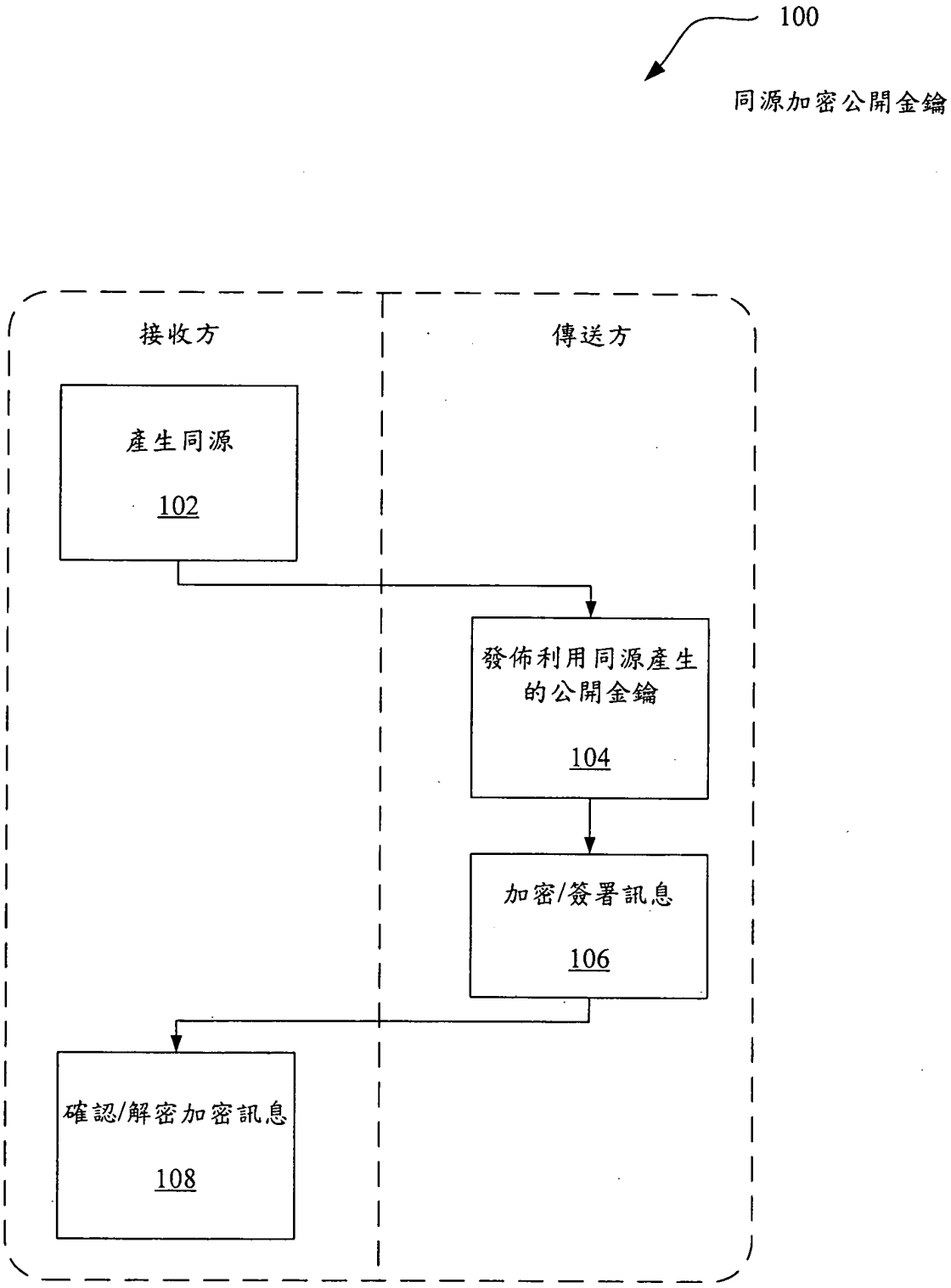
658 遠端應用程式

伍、中文發明摘要：

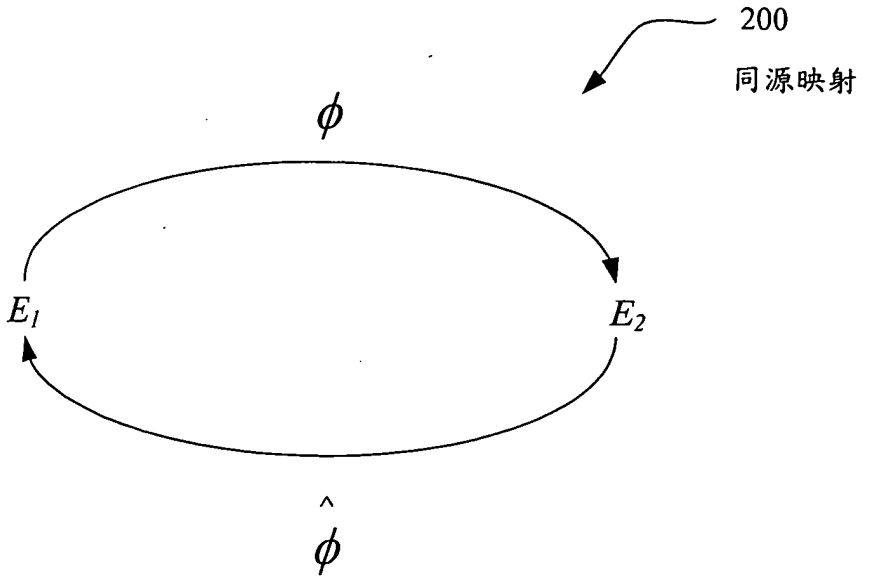
本發明揭示一種提供公開金鑰加密系統的技術。更明確而言，利用同源(isogenies)阿貝爾(Abelian)變數(如一維之橢圓曲線)以提供公開金鑰加密系統。例如，該同源允許利用多重曲線代替單一曲線以提供更安全的加密法。此技術可運用於數位簽章和/或身份認證加密法(IBE)解決方案。並且，此同源可用於其他的運用如盲簽章(blind signatures)、分層系統(hierarchical systems)等。此外，本發明亦揭示產生同源的方法。

陸、英文發明摘要：

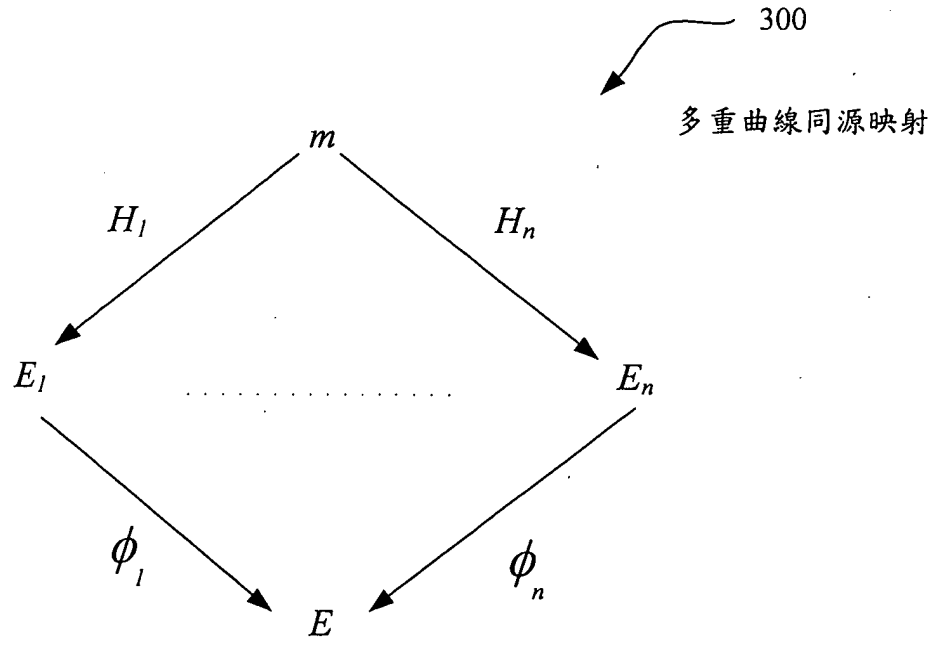
Techniques are disclosed to provide public-key encryption systems. More particularly, isogenies of Abelian varieties (e.g., elliptic curves in one-dimensional cases) are utilized to provide public-key encryption systems. For example, the isogenies permit the use of multiple curves instead of a single curve to provide more secure encryption. The techniques may be applied to digital signatures and/or identity based encryption (IBE) solutions. Furthermore, the isogenies may be used in other applications such as blind signatures, hierarchical systems, and the like. Additionally, solutions are disclosed for generating the isogenies.


100
同源加密公開金鑰
接收方
傳送方
產生同源
102
發佈利用同源產生的公開金鑰
104
加密/簽署訊息
106
確認/解密加密訊息
108

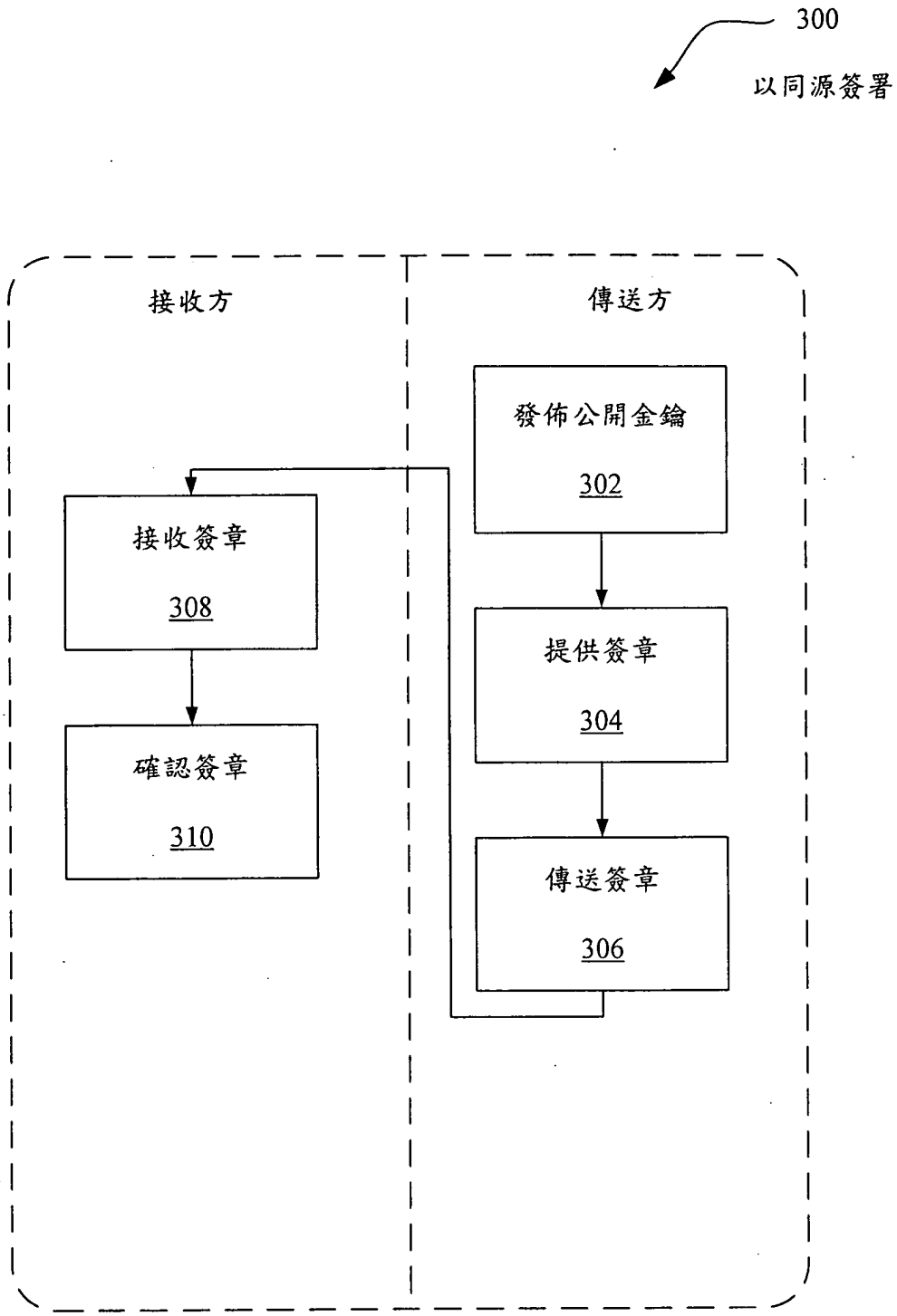
第 1 圖



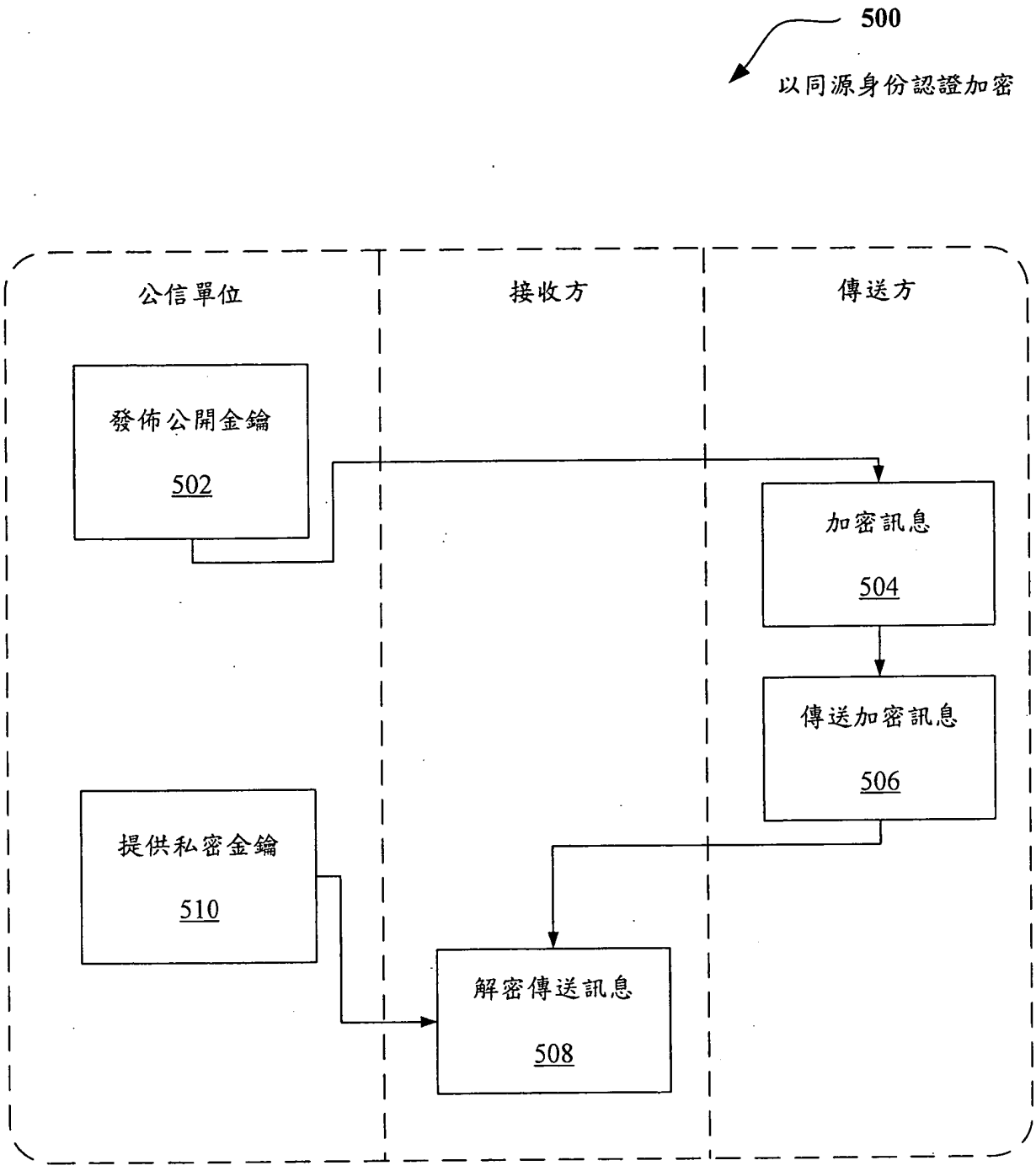
第 2 圖



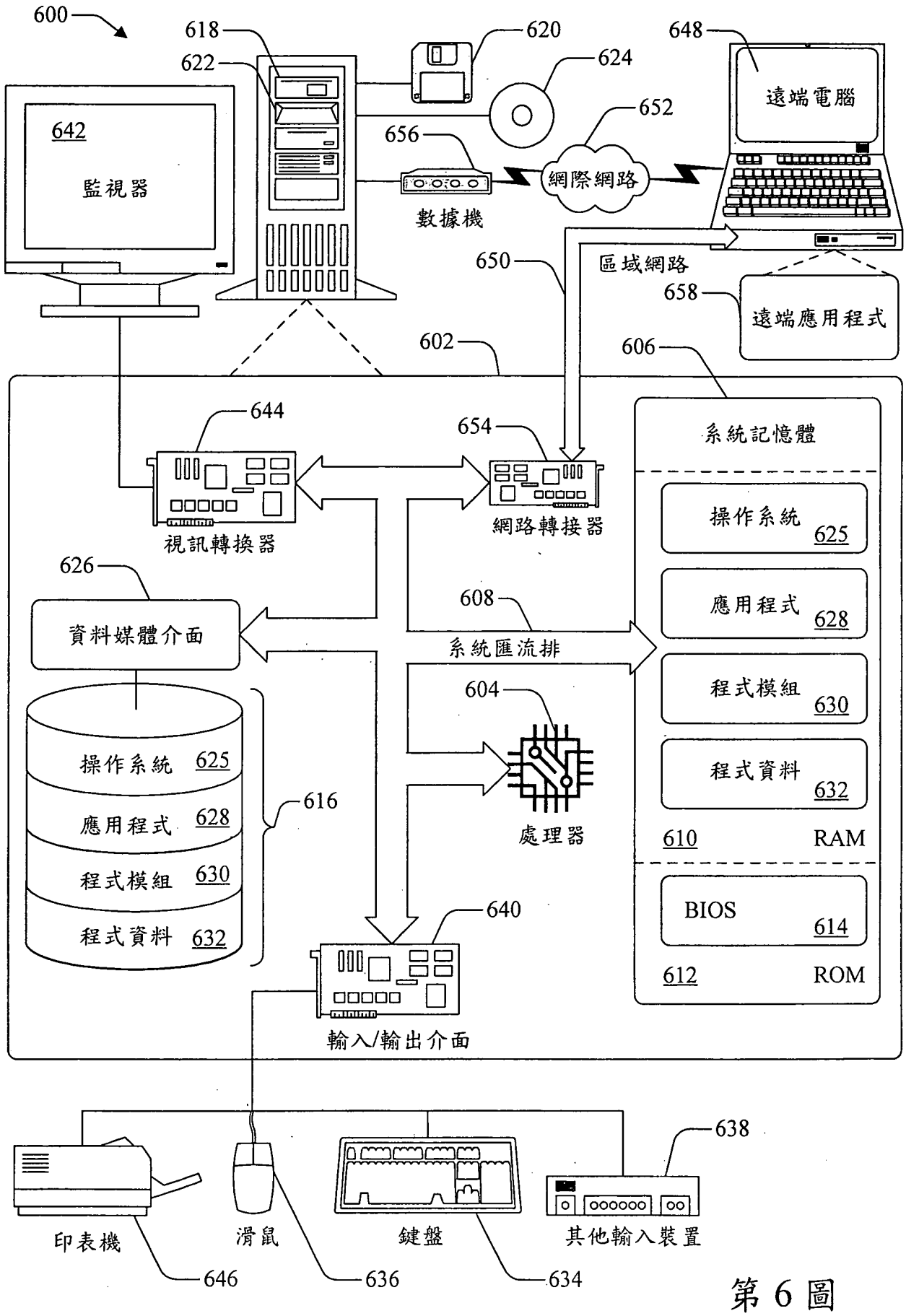
第 4 圖


300
以同源簽署
接收方
傳送方
發佈公開金鑰
302
接收簽章
308
提供簽章
304
確認簽章
310
傳送簽章
306

第 3 圖


500
以同源身份認證加密
公信單位
接收方
傳送方
發佈公開金鑰
502
加密訊息
504
傳送加密訊息
506
提供私密金鑰
510
解密傳送訊息
508

第 5 圖


600
618
622
620
624
648
遠端電腦
642
監視器
652
656
網際網路
數據機
650
區域網路
658
遠端應用程式
602
606
644
654
系統記憶體
視訊轉換器
網路轉接器
操作系統 625
626
應用程式 628
608
資料媒體介面
系統匯流排
程式模組 630
604
程式資料 632
處理器
610 RAM
616
操作系統 625
應用程式 628
程式模組 630
程式資料 632
640
BIOS 614
612 ROM
輸入/輸出介面
638
印表機
滑鼠
鍵盤
其他輸入裝置
646
636
634

第 6 圖

柒、指定代表圖：

(一)、本案指定代表圖為：第 1 圖。

(二)、本代表圖之元件代表符號簡單說明：

100 同源加密公開金鑰

102 產生同源

104 發佈利用同源產生的公開金鑰

106 加密/簽署訊息

108 確認/解密加密訊息

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

I360920
公告本
100年4月19日修正替換頁 第93127553號專利案100年4月修正

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：93127553

※ 申請日期：2004 年 9 月 10 日　　※IPC 分類：H04L 9/08
(2006.01)

一、發明名稱：（中文/英文）

在密碼系統中使用同源之方法、設備及電腦可讀取媒體

METHOD, APPARATUS, AND COMPUTER-READABLE MEDIUM FOR USING ISOGENIES IN A CRYPTOSYSTEM

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商．微軟公司

Microsoft Corporation

代表人：（中文/英文）

艾苹那諾爾 D 巴特萊

EPPENAUER, D. BARTLEY

住居所或營業所地址：（中文/英文）

美國華盛頓州列德蒙微軟路 1 號

One Microsoft Way, Building 8, Redmond, WA 98052-6399, U.S.A.

國　籍：（中文/英文）

美國/USA

三、發明人：（共 2 人）

姓　名：（中文/英文）

1.趙大衛 Y/JAO, DAIVD Y.

2.凡卡特珊拉馬拉南/VENKATESAN, RAMARATHNAM

國　籍：（中文/英文）

1.美國/USA

2.印度/India

100年4月19日修正替換頁

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1.美國；2003 年 11 月 3 日；60/517,142

2.美國；2004 年 3 月 31 日；10/816,083

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

拾、申請專利範圍：

1. 一種在密碼系統中使用同源(isogenies)之方法，其包含以下動作：

產生一同源，其從一第一橢圓曲線映射多數點至一第二橢圓曲線，其中該同源的產生為利用選自一群包括複數(complex)乘法生成、模組生成、線性獨立生成及其組合的技術；

發佈對應於該同源的一公開金鑰；

利用對應於該同源之一加密金鑰加密一訊息；

利用對應於該同源之一解密金鑰解密該加密過之訊息，其中該解密係藉由雙線性配對(bilinear pairing)而執行，且該雙線性配對為選自一群包括 Weil 配對、Tate 配對及平方配對的配對；以及

利用一軌跡映射以縮短在一阿貝爾變數(Abelian variety)上的點。

2. 如申請專利範圍第 1 項所述之方法，其中該加密金鑰或解密金鑰之至少一者為一私密金鑰，該私密金鑰為該同源的一雙重同源。

3. 如申請專利範圍第 1 項所述之方法，其中該產生動作從一第一橢圓曲線映射多數點至多數條橢圓曲線。

4. 如申請專利範圍第 1 項所述之方法，其中係利用阿貝爾

(Abelian)變數來運用該方法。

5. 如申請專利範圍第 1 項所述之方法，其中該方法可簽署該訊息。

6. 如申請專利範圍第 1 項所述之方法，其中該方法提供以身份認證為基礎之加密。

7. 如申請專利範圍第 1 項所述之方法，其另包括構成多數模組之同源之動作，以提供該同源而不顯示任何中間曲線。

8. 如申請專利範圍第 1 項所述之方法，其另包括利用於一基域(base field)之一軌跡映射(trace map)之動作，以縮短被該同源映射於一橢圓曲線上的點。

9. 一種在密碼系統中使用同源(isogenies)之方法，其包括以下動作：

發佈對應於一同源的一公開金鑰，其從一第一橢圓曲線映射多數點至一第二橢圓曲線，其中該同源的產生為利用選自一群包括複數乘法生成、模組生成、線性獨立生成及其組合的技術；以及

利用對應於該同源之一解密金鑰，解密一加密過的訊息，其中該解密係藉由雙線性配對(bilinear pairing)而執

行，且該雙線性配對為選自一群包括 Weil 配對、Tate 配對及平方配對的配對。

10. 如申請專利範圍第 9 項所述之方法，其中該解密金鑰為該同源的一雙重同源。

11. 如申請專利範圍第 9 項所述之方法，其中該同源從一第一橢圓曲線映射多數點至多數橢圓曲線。

12. 如申請專利範圍第 9 項所述之方法，其中係利用阿貝爾變數來運用該方法。

13. 如申請專利範圍第 9 項所述之方法，其中該方法可簽署該訊息。

14. 如申請專利範圍第 9 項所述之方法，其中該方法提供以身份認證為基礎之加密。

15. 如申請專利範圍第 9 項所述之方法，其另包括利用於一基域之軌跡映射之動作，以縮短被該同源映射於一橢圓曲線上的點。

16. 一種在密碼系統中使用同源(isogenies)之設備，其包

括：

一第一處理器；

一第一系統記憶體，其連接至該第一處理器，該第一系統記憶體儲存對應於一同源之一公開金鑰，該同源從一第一橢圓曲線映射多數點至一第二橢圓曲線；

一第二處理器；

一第二系統記憶體，其連接至該第二處理器，該第二系統記憶體儲存一加密過之訊息及一解密金鑰，其對應於解密該加密過之訊息之同源，其中該解密係藉由雙線性配對(bilinear pairing)而執行，且該雙線性配對為選自一群包括 Weil 配對、Tate 配對及平方配對的配對；

其中該加密過之訊息係利用一加密金鑰進行加密。

17. 如申請專利範圍第 16 項所述之設備，其中該加密金鑰或解密金鑰之至少一者為一私密金鑰，該私密金鑰為該同源的一雙重同源。

18. 如申請專利範圍第 16 項所述之設備，其中該同源從一第一橢圓曲線映射多數點至多數橢圓曲線。

19. 一種其上儲存有指令之電腦可讀取媒體，當該等指令被執行時係可引導一機器執行包括以下之動作：

發佈對應於一同源(isogeny)的公開金鑰，該同源從一

第一橢圓曲線映射多數點至一第二橢圓曲線，其中該同源的產生為利用選自一群包括複數乘法生成、模組生成、線性獨立生成及其組合的技術；以及

利用對應於該同源之一解密金鑰，解密一加密過的訊息，其中該解密係藉由雙線性配對(bilinear pairing)而執行，且該雙線性配對為選自一群包括 Weil 配對、Tate 配對及平方配對的配對。

20. 如申請專利範圍第 19 項所述之電腦可讀取媒體，其中該解密金鑰為一私密金鑰，此私密金鑰為該同源的一雙重同源。

21. 如申請專利範圍第 19 項所述之電腦可讀取媒體，其中該同源從一第一橢圓曲線映射多數點至多數橢圓曲線。

22. 如申請專利範圍第 19 項所述之電腦可讀取媒體，其中係利用阿貝爾變數來運用該動作。

23. 如申請專利範圍第 19 項所述之電腦可讀取媒體，其中該等動作另包括利用於一基域之軌跡映射，以縮短被該同源映射於一橢圓曲線上的點。

24. 如申請專利範圍第 19 項所述之電腦可讀取媒體，其中

該等動作另包括構成多數模組同源，以提供該同源而不顯示任何中間曲線。

25. 如申請專利範圍第 19 項所述之電腦可讀取媒體，其中該等動作另包括利用一軌跡映射以縮短阿貝爾變數上的點。

26. 如申請專利範圍第 19 項所述之電腦可讀取媒體，其中該等動作為簽署該訊息。

27. 如申請專利範圍第 19 項所述之電腦可讀取媒體，其中該等動作提供以身份認證為基礎之加密。