(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201301836 A1
(43)公開日： 中華民國 102 (2013) 年 01 月 01 日

(21)申請案號：100121624 (22)申請日： 中華民國 100 (2011) 年 06 月 21 日
(51)Int. Cl.： *H04L9/32 (2006.01)* *H04L9/30 (2006.01)*
H04L9/14 (2006.01)
(71)申請人：國立交通大學 (中華民國) NATIONAL CHIAO TUNG UNIVERSITY (TW)
新竹市大學路 1001 號
(72)發明人：曾建超 TSENG, CHIEN CHAO (TW) ；何姿欣 HO, TZU HSIN (TW)
(74)代理人：林火泉
申請實體審查：有 申請專利範圍項數：18 項 圖式數：3 共 20 頁

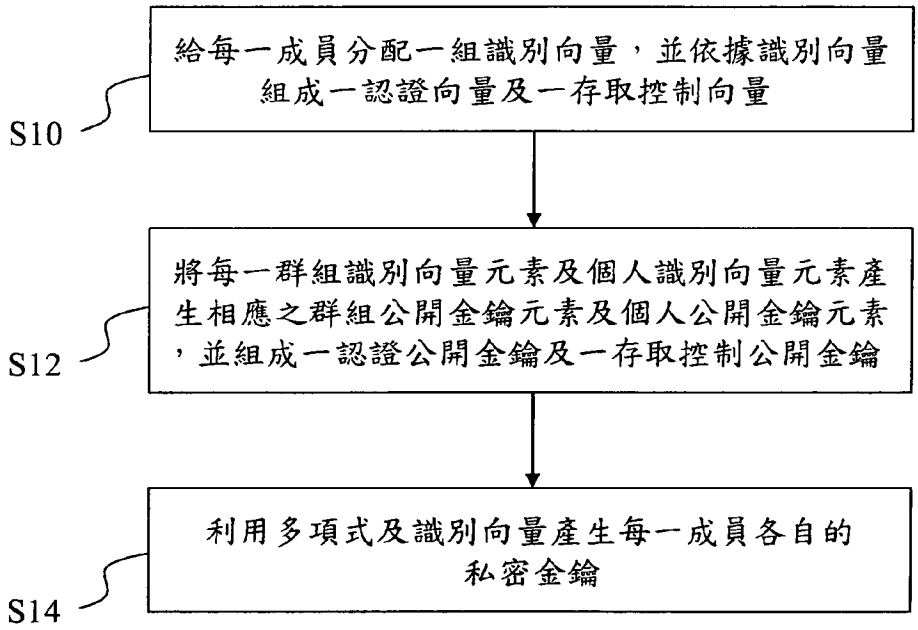
(54)名稱

動態群組中建立金鑰、認證及安全通訊方法

METHOD FOR KEYS GENERATION, MEMBER AUTHENTICATION AND SECURITY COMMUNICATION IN A DYNAMIC GROUP

(57)摘要

本發明提供一種動態群組中建立金鑰、認證及安全通訊方法，其係給群組中每一成員分配一組由共有的群組識別向量元素及獨一無二的個人識別向量元素所組成之識別向量，並依據識別向量可組成一認證向量及一存取控制向量；利用識別向量元素產生相應之公開金鑰元素，以組成一認證公開金鑰及一存取控制公開金鑰，再利用一多項式及識別向量產生一私密金鑰。本發明利用這些由識別向量產生的公開金鑰與私密金鑰進行群組成員間不需伺服器的相互認證及資料存取控制，保護成員身份隱密性並增加通訊安全性。



201301836

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）

※申請案號：100121624

※申請日：100. 6. 21　※IPC分類：H04L 9/32 (2006.01)
H04L 9/30 (2006.01)
H04L 9/14 (2006.01)

一、發明名稱：（中文/英文）

動態群組中建立金鑰、認證及安全通訊方法 / method for keys generation, member authentication and security communication in a dynamic group

二、中文發明摘要：

本發明提供一種動態群組中建立金鑰、認證及安全通訊方法，其係給群組中每一成員分配一組由共有的群組識別向量元素及獨一無二的個人識別向量元素所組成之識別向量，並依據識別向量可組成一認證向量及一存取控制向量；利用識別向量元素產生相應之公開金鑰元素，以組成一認證公開金鑰及一存取控制公開金鑰，再利用一多項式及識別向量產生一私密金鑰。本發明利用這些由識別向量產生的公開金鑰與私密金鑰進行群組成員間不需伺服器的相互認證及資料存取控制，保護成員身份隱密性並增加通訊安全性。

三、英文發明摘要：

The present invention provides a method for keys generation, member authentication and security communication in a dynamic group. Assigned a set of vector including common group vector elements and a unique individual vector element to each member in the group, and assembled an authentication vector and an access control vector according to the vector. The vector elements are used to generate related public key elements, and the public key elements can form an authentication public key and a access control public key. A privacy key is generated using a polynomial and the vector. The present invention uses these public keys and privacy key which generated from the vectors to do serverless mutual member authentication and data access control between group members. This method keeps membership anonymity simultaneously and increases communication security.

四、指定代表圖：

(一)本案指定代表圖為：第（ 一 ）圖。

(二)本代表圖之元件符號簡單說明：

無。

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

本發明係有關一種網路通訊之認證技術，特別是一種動態群組中建立金鑰、認證及安全通訊方法。

【先前技術】

按，目前安全機制分成兩大方向: 對稱式加解密與非對稱式加解密方法。在對稱式密碼方法中，傳送端與接收端雙方均需擁有相同的一把金鑰，當資料加密和解密時採用相同的金鑰，早期最廣泛使用的對稱金鑰演算法為 DES，後來進階加密標準之 AES 演算法取代了 DES 演算法。使用對稱式的優點為速度快，若使用足夠大的金鑰將難以破解，但缺點是在金鑰管理上，若使用者眾多則金鑰的保管安全性會是一個問題，且在群體金鑰的應用上需要較複雜的金鑰管理，必須周期性地更換金鑰。

而非對稱性密碼方法則是每個使用者皆擁有一對金鑰，包含公開金鑰和私密金鑰，資料由發送端之公開金鑰加密後，必須由接收者的私密金鑰予以解密，其中公開金鑰可被廣泛發佈，每個使用者都可得到公開金鑰，但私密金鑰則必須隱密地加以保存。使用非對稱式的優點在於可同時提供私密性、認證與不可否認性等服務，在金鑰管理上較為容易，即是無論與多少人交換資訊，只需保管自己的私密金鑰。迄今為止的所有公開金鑰加密架構中，RSA 公開金鑰加密系統是最著名、最多人使用的一種，其為由 R.Rivest、A.Shamir 和 L.Adleman 利用分解大質數的困難度所提出之非對稱性金鑰演算法。ECC 為新一代的公開金鑰演算法，其係採用離散對數問題的困難度來演算，由於沒有一個有效的演算法可以在有效期間求得離散對

數解，因此ECC的安全性比RSA加密方式高出許多，此外，由於ECC只需使用較短的金鑰長度160位元就可達到與較長金鑰1024位元的RSA演算法強度一般，故非常適合在例如智慧卡等資源有限環境下使用。

非對稱性密碼方法之缺點在於：計算較複雜，導致加解密速度慢；必須在使用他人的公開金鑰之前先對公開金鑰作認證，確認是否為合法正確的金鑰；藉由一把公開金鑰加密的資料，只能由一把私密金鑰解密，無法達到一把公開金鑰加密的資料，由所有的群組成員用自己的私密金鑰解密；用非對稱性方式做認證的時候，必須對對方的公開金鑰做確認，得知對方的身份，才能達到群組成員相互認證；以及，對於需要保持群組成員身分隱密性的環境，傳統的非對稱性方式（如RSA及ECC）無法達到成員身分隱密性的需求。

因此，本發明即提出一種動態群組中建立金鑰、認證及安全通訊方法，以克服上述該等問題，具體架構及其實施方式將詳述於下。

【發明內容】

本發明之主要目的在提供一種動態群組之金鑰建立方法，其中發起者須儲存一組存取控制公開金鑰，其他每個群組成員只要儲存一組共用的認證公開金鑰與自己的私密金鑰即可，由於只有發起者擁有存取控制公開金鑰，故可避免金鑰被複製，並且發起者可依成員的加入或離開，隨時更換存取控制公開金鑰元素的個人識別部分，以達到存取控制。

本發明之另一目的在提供一種動態群組之安全通訊方法，群組成員使用共用的認證公開金鑰對認證訊息加密，只要是群組成員就可以用他們獨一無二的私密金鑰解開認證訊息，達到無需第三者介入的相互認證，讓兩

個成員間以不需伺服器之方式相互證實群組身份識別，以避免資料被偽造者所傳送。

本發明之再一目的在提供一種動態群組中安全通訊方法，其中群組成員可判別資料是否由發起者起源的，避免真正資料被換過。

本發明之又一目的在提供一種動態群組中安全通訊方法，其中由於發起者利用群組成員的識別向量所產生之存取控制公開金鑰對資料加密，因此只有群組成員可將資料解密，正確的存取資料。

為達上述之目的，本發明提供一種動態群組中建立金鑰之方法，此動態群組中包括一發起者及複數成員，該方法包括下列步驟：給每一成員分配一組識別向量，每一組識別向量包含共同的 d 個群組識別向量元素及獨一無二的一個人識別向量元素，每一成員依據識別向量可組成一認證向量及一存取控制向量；伺服器或發起者將每一群組識別向量元素及個人識別向量元素利用一對應函式產生相應之群組公開金鑰元素及個人公開金鑰元素，並組成一認證公開金鑰及一存取控制公開金鑰；以及伺服器或發起者為每一成員分別產生任意之一 d-1 次多項式，並利用此多項式及識別向量產生一私密金鑰。

本發明另提供一種動態群組之認證方法，其為在動態群組中的第一成員對第二成員進行認證之方法，包括下列步驟：(a)第一成員對第一認證訊息進行加密，傳送給第二成員；(b)第二成員將被加密之第一認證訊息解密為一次解密第一認證訊息，另產生第二認證訊息，並對一次解密第一認證訊息及第二認證訊息進行加密後，傳送給第一成員；(c)第一成員再將被加密之一次解密第一認證訊息及第二認證訊息解密，得到二次解密第一認證

訊息及一次解密第二認證訊息，比對二次解密第一認證訊息與第一認證訊息是否相同，若不同則認證失敗，若相同則第一成員對一次解密第二認證訊息進行加密，再傳送給第二成員；以及(d)第二成員將被加密之一次解密第二認證訊息解密，得到二次解密第二認證訊息，比對二次解密第二認證訊息與第二認證訊息是否相同，若不同則認證失敗，若相同認證成功。

本發明另提供一種動態群組中安全通訊之方法，當動態群組中發起者傳送資料給群組成員中之一接收者時係包括下列步驟：發起者利用存取控制公開金鑰對資料加密後傳送給該成員，接收者接收被加密之該資料後，接收者利用存取控制向量及私密金鑰對資料進行解密，若是其個人的存取控制向量中所包含之個人識別向量元素為存取控制公開金鑰中所依據的那些個人識別向量元素的其中之一，則接收者對資料解密會成功，反之，則解密會失敗，接收者與發起者不屬於同一動態群組。

底下藉由具體實施例詳加說明，當更容易瞭解本發明之目的、技術內容、特點及其所達成之功效。

【實施方式】

本發明提供一種動態群組中建立金鑰、認證及安全通訊方法，其係建立一對多的金鑰，資料可由一個共用的公開金鑰加密，而後可由所有符合條件的群組成員之私密金鑰解密，且群組成員之間相互認證不需透過伺服器，而是利用共同的認證公開金鑰及個人之私密金鑰鑑別身份。

當一發起者建立一動態群組，邀請複數成員加入群組後，發起者為所有成員產生金鑰，並利用安全通道傳送給每一成員，讓成員利用金鑰達到安全的資料傳送之目的。在本發明中，所有的金鑰產生與認證計算皆建構

在循環動態群組（cyclic group）上，此動態群組具有一群組產生器（generator）。

第 1 圖為本發明中建立金鑰之方法的流程圖，首先在步驟 S10 中，每一成員會被分配到一組識別向量 V^{Peer}，其中包括每個成員共有的 d 個群組識別向量元素 $v_{Gr-1}, v_{Gr-2},\ldots,v_{Gr-d}$ 及一獨一無二的個人識別向量元素 v_{Idv}，因此動態群組中第一個成員的識別向量可如下式(1)所示：

$$V^{Peer1} = \{v_{Gr-1}, v_{Gr-2},\ldots,v_{Gr-d}, v_{Idv1}\} \quad (1)$$

而每一成員可依據擁有的識別向量中組成一認證向量 V_{Au} 及一存取控制向量 V_{Ac}，其中認證向量做為認證時所需用到的向量，包含 d 個群組識別向量元素，由於 d 個群組識別向量元素為每個成員共有的，故每一成員所擁有之認證向量皆相同；而存取控制向量做為存取控制時所需用到的向量，則包含 d-1 個群組識別向量元素及一個個人識別向量元素，因此第一個成員的認證向量及存取控制向量又可如下式(2)、(3)所示：

$$V_{Au} = \{v_{Gr-1}, v_{Gr-2},\ldots,v_{Gr-d}\} \quad (2)$$

$$V_{Ac} = \{v_{Gr-1}, v_{Gr-2},\ldots,v_{Gr-d\_1}, v_{Idv1}\} \quad (3)$$

接著在步驟 S12 中建立公開金鑰，此公開金鑰與識別向量的元素為一對一的關係，對於任意群組成員 x 而言，公開金鑰的組成元素是由識別向量元素 v_x 建立相對應的亂數 R_x 與群組產生器 P 以橢圓曲線密碼學（Elliptic Curve Cryptography, ECC）進行乘法運算（multiplication operation）所產生的，因此公開金鑰元素 $q_x = f(v_x) = R_x \cdot P$，其中 R_x 為亂數，將每一個群組識別向量元素及個人識別向量元素計算產生相應之群組公開金鑰元素及個人公開金鑰元素 q_x，並利用群組公開金鑰元素及個人公開金鑰元素組成一認

證公開金鑰 PuK_{Au} 及一存取控制公開金鑰 PuK_{Ac}，如下式(4)、(5)所示：

$$PuK_{Au}=\{f(v_{Gr-1}), f(v_{Gr-2}),..., f(v_{Gr-d})\}$$

$$=\{q_{Gr-1}, q_{Gr-2},...,q_{Gr-d}\} \quad (4)$$

$$PuK_{Ac}=\{f(v_{Gr-1}), f(v_{Gr-2}),..., f(v_{Gr-d\_1}), f(v_{Idv1}), f(v_{Idv2}),..., f(v_{Idvn})\}$$

$$=\{q_{Gr-1}, q_{Gr-2},...,q_{Gr-d\_1}, q_{Idv1}, q_{Idv2},..., q_{Idvn}\} \quad (5)$$

由此可知，認證公開金鑰 PuK_{Au} 係由所有的群組公開金鑰元素所組成，而存取控制公開金鑰 PuK_{Ac} 係由 d-1 個群組公開金鑰元素及所有 n 個成員之個人公開金鑰元素所組成，特別的是，只有發起者才有存取控制公開金鑰。

最後如步驟 S14 所述，發起者先隨機產生一值 y，並為每一成員分別產生任意之 d-1 次多項式 $p(x)= a_0+a_1x+a_2x^2+...+ a_{d-1}x^{d-1}$，且此多項式符合 $p(0)=y$，並利用此多項式及識別向量為每個成員製作獨一無二的私密金鑰 Prk^{Peer}，舉例第一個成員之私密金鑰如下式(6)：

$$Prk^{Peer1}=\{f'(v_{Gr-1}), f'(v_{Gr-2}),..., f'(v_{Gr-d}), f'(v_{Idv1})\} \quad (6)$$

其中 $f'(x)=\frac{p(x)}{R_x}\cdot P$，$R_x$ 為由識別向量元素 v_x 所建立相對應的亂數，P 為群組產生器。

當動態群組形成時，由伺服器或發起者分配給成員一組識別向量 V^{Peer}、共用的認證公開金鑰 PuK_{Au} 及成員的私密金鑰 Prk^{Peer}。然而，伺服器或發起者將存取控制公開金鑰 PuK_{Ac} 儲存在發起者端，並不分派給任何群組成員，只有發起者擁有存取控制公開金鑰。

本發明中動態群組的成員相互認證時，假設群組成員中第一成員欲與第二成員做認證時，第一成員會利用認證公開金鑰與亂數將任意訊息做加

密，當作測試第二成員是否為群組成員的認證訊息，若第二成員可以解出訊息，並回傳給第一成員，第一成員就確認第二成員跟他是相同群組的成員。

第二圖為第一成員與第二成員相互認證之流程圖，包含四個步驟，首先，步驟 S20 中第一成員利用認證公開金鑰 PuK_{Au} 與產生的亂數 Rn_1 對任意產生的第一認證訊息 M_1 進行加密，傳送給第二成員；步驟 S22 第二成員收到第一認證訊息 M_1' 後，利用認證向量 V_{Au}^2 與所擁有之第二私密金鑰 PrK^2 解出一次解密第一認證訊息 M_1'，同時第二成員另產生第二認證訊息 M_2，並將 M_1' 與 M_2 串接成 $M_1'||M_2$ 後，用認證公開金鑰 PuK_{Au} 與第二成員產生的亂數 Rn_2 將 $M_1'||M_2$ 加密，回傳給第一成員；步驟 S24，第一成員再將用認證向量 V_{Au}^1 與第一成員所擁有之第一私密金鑰 PrK^1 解出二次解密第一認證訊息 M_1'' 與一次解密第二認證訊息 M_2'，且第一成員比對 M_1'' 與 M_1 是否相同，若相同代表第一成員認證第二成員成功；隨後，第一成員將比對結果 Rslt 與 M_2' 串接成 $Rslt||M_2'$ 後，用 PuK_{Au} 與第一成員產生的亂數 Rn_3 將 $Rslt||M_2'$ 加密，傳送給第二成員；最後，步驟 S26 中第二成員再利用認證向量 V_{Au}^2 與第二私密金鑰 PrK^2 解出二次解密第二認證訊息 M_2''，並將 M_2'' 與 M_2 比對是否相同，如果相同就是第二成員認證第一成員成功，若不同則認證失敗。

因此，群組成員間可利用共用的認證公開金鑰 PuK_{Au} 將認證資料加密，被認證者利用個人的私密金鑰 Prk^{Peer} 與認證向量 V_{Au}^{Peer} 解開認證資料，以確認互相為同一群組關係，達到相互認證。

除此之外，發起者可以利用存取控制公開金鑰 PuK_{Ac} 主控存取資料的成員，只有群組成員可以解開資料，即是達到良好的存取控制。成員亦可

利用個人的私密金鑰 Prk^{Peer} 與存取控制向量 V_{Ac}^{Peer} 解開加密資料，確認資料來源者的身份是發起者，達到資料來源的鑑別性。

本發明中資料鑑別之方法如第三圖之流程圖所示，若發起者要傳送資料給動態群組 n 個成員中的某一成員，則在步驟 S30 中發起者使用存取控制公開金鑰 PuK_{Ac} 對資料加密，再將加密資料傳送給該成員，在上述金鑰產生方法中，已知存取控制公開金鑰 PuK_{Ac} 包含 d-1 個公開金鑰元素 q_{Gr-1}, $q_{Gr-2},\ldots,q_{Gr-d\_1}$ 及所有 n 個成員之個人識別公開金鑰元素 q_{Idv1}, $q_{Idv2},\ldots$, q_{Idvn}；步驟 S32，當群組成員中之接收者接收被加密之資料後，使用存取控制向量與私密金鑰解密，若是其個人的存取控制向量 V_{Au}^{Peer} 中所包含之個人識別向量元素 v_{Idv} ，為存取控制公開金鑰 PuK_{Ac} 中所依據的成員個人識別向量元素 v_{Idv1}, $v_{Idv2},\ldots$, v_{Idvn} 其中之一，則如步驟 S34 所述，成員利用存取控制向量 V_{Ac}^{Peer} 及私密金鑰 Prk^{Peer} 對資料解密成功，反之，若接收者的個人識別向量元素不存在於存取控制公開金鑰所依據的成員個人識別向量元素中，例如接收者的個人識別向量元素為 $v_{Idv(n+1)}$，由於 $Peer_{n+1}$ 不是群組成員，因此如步驟 S36 所述，接收者非動態群組成員，解密會失敗。

舉例而言，假設發起者邀請 $Peer_1, Peer_2,\ldots,Peer_n$ 成為群組成員，當發起者使用 PuK_{Ac} 當公開金鑰對資料加密並欲將加密資料傳送給 $Peer_2$ 時，將 $Peer_2$ 的個人識別向量元素 v_{Idv2} 對應的個人公開金鑰元素 q_{Idv2} 加入到存取控制公開金鑰 PuK_{Ac} 中，故當 $Peer_2$ 接收到加密資料時，使用 V_{Ac}^2 與 $\Pr k^2$ 就有足夠的資訊可以解開資料。又因為 $Peer_2$ 是用 V_{Ac}^2 與 $\Pr k^2$ 解密，代表接到的資料是用存取控制公開金鑰所加密，又存取控制公開金鑰只有發起者擁有，所以 $Peer_2$ 可以確認資料的來源是發起者。

另，$Peer_{n+1}$ 不是群組成員，當發起者使用 PuK_{Ac} 當公開金鑰對資料加密時，並未將 $Peer_{n+1}$ 個人識別向量對應的公開金鑰元素加入 PuK_{Ac}，所以當 $Peer_{n+1}$ 接收到資料時，因為擁有的 $v_{ldv(n+1)}$ 並沒有與加密時所使用的公開金鑰元素相對應，所以無法有足夠的資訊以解開資料。

因此，本發明具有以下優點：1.具有可擴展性，發起者只需產生一組加密資料，就可以發送給所有的群組成員；2.不需伺服器即可相互認證，群組成員使用共用的認證公開金鑰加密認證資料，只要是群組成員就可以用他們獨一無二的私密金鑰解開認證訊息，達到無需第三者介入的相互認證；3.保持群組成員身分隱密性，群組成員不需知道其他成員真實身份，只要確認都是群組成員即可；4.因發起者利用群組成員的個人識別向量元素當依據所產生的存取控制公開金鑰來加密，故只有群組成員可將資料解密並正確的存取資料；5.具資料鑑別性，接收端成員可判別資料是否由發起者起源的，避免真正資料被換過；6.在加密過程加入亂數，所以同一條資料流在每一次加密時都會產生不同的加密資料，增加安全性；以及 7.有效的金鑰管理，發起者須儲存一組存取控制公開金鑰，其他每個群組成員只要儲存一組共用的認證公開金鑰與自己的私密金鑰即可。

綜上所述，本發明所提供之一種動態群組中建立金鑰、認證及安全通訊方法係可應用於一對多資料分享的環境，資料可由一個共用的公開金鑰或是發起者獨有的公開金鑰加密，而後所有符合條件的群組成員之私密金鑰皆可解密；此外，本發明提供群組成員間不需透過伺服器（serverless）相互認證的方法，群組成員間可利用共同的認證公開金鑰與群組成員的私鑰做認證，不再需要經由認證伺服器做認證，此種認證方式同時保護成員

身份隱密性；再者，本發明同時提供資料的存取控制機制，當發起者將資料加密時，由於利用到群組成員的個人識別向量當作加密的依據，故只有群組中的成員可解密，群組成員更可利用解密資料時所用的存取控制向量，查驗資料是由發起者所產生或是由其他人所置換的假資料。

唯以上所述者，僅為本發明之較佳實施例而已，並非用來限定本發明實施之範圍。故即凡依本發明申請範圍所述之特徵及精神所為之均等變化或修飾，均應包括於本發明之申請專利範圍內。

【圖式簡單說明】

第 1 圖為本發明動態群組中建立金鑰之方法之流程圖。

第 2 圖為本發明動態群組中認證方法之流程圖。

第 3 圖為本發明動態群組中安全通訊方法之流程圖。

【主要元件符號說明】

無

七、申請專利範圍：

1. 一種動態群組中建立金鑰之方法，該動態群組中包括一發起者及複數成員，該方法包括下列步驟：

給每一該成員分配一組識別向量，每一組該識別向量包含共同的 d 個群組識別向量元素及不同的一個人識別向量元素，每一該成員依據該識別向量可組成一認證向量及一存取控制向量；

將每一該等群組識別向量元素及該個人識別向量元素計算產生相應之 d 個群組公開金鑰元素及一個人公開金鑰元素，並組成一認證公開金鑰及一存取控制公開金鑰；以及

該發起者為每一該等成員分別產生任意之一 d-1 次多項式，並利用該多項式及該識別向量產生一私密金鑰。

2. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該認證向量係由 d 個該群組識別向量元素所組成，每一該成員所擁有之該認證向量皆相同。

3. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該存取控制向量包含 d-1 個該群組識別向量元素及該個人識別向量元素。

4. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該認證公開金鑰係由該等 d 個群組公開金鑰元素所組成。

5. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該存取控制公開金鑰係由 d-1 個該等群組公開金鑰元素及所有成員之個人識別公開金鑰元素所組成。

6. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該等群組識別向量元素係與該群組產生器以橢圓曲線密碼學（Elliptic Curve Cryptography,

ECC）進行乘法運算，進而產生該等公開金鑰元素。

7. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該發起者隨機產生一值 y，且該多項式 p(x)符合 p(0)=y。

8. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該私密金鑰包括該等成員的 d-1 個群組識別向量元素、一個該個人識別向量元素與該多項式所計算而成之 d 個私密金鑰元素。

9. 一種應用請求項 1 之動態群組之認證方法，該動態群組中一第一成員對一第二成員進行認證之方法係包括下列步驟：

(a)該第一成員對一第一認證訊息進行加密，傳送給該第二成員；

(b)該第二成員將被加密之該第一認證訊息解密為一一次解密第一認證訊息，另產生一第二認證訊息，並對該一次解密第一認證訊息及該第二認證訊息進行加密後，傳送給該第一成員；

(c)該第一成員再將被加密之該一次解密第一認證訊息及該第二認證訊息解密，得到一二次解密第一認證訊息及一一次解密第二認證訊息，比對該二次解密第一認證訊息與該第一認證訊息是否相同，若比對結果不同則認證失敗，若該比對結果相同則進行步驟(d)；

(d)該第一成員對該比對結果及該一次解密第二認證訊息進行加密後，傳送給該第二成員；以及

(e)該第二成員將被加密之該比對結果及該一次解密第二認證訊息解密，得到該比對結果及一二次解密第二認證訊息，比對該二次解密第二認證訊息與該第二認證訊息是否相同，若不同則認證失敗，若相同認證成功。

10.如請求項 9 所述之動態群組之認證方法，其中該步驟(a)中該第一認證訊息係利用一第一亂數與該第一成員所擁有之一認證公開金鑰進行加密。

11.如請求項 9 所述之動態群組之認證方法，其中該步驟(b)中被加密之該第一認證訊息係利用該第二成員所擁有之一第二認證向量與一第二私密金鑰進行解密，得到該一次解密第一認證訊息。

12.如請求項 9 所述之動態群組之認證方法，其中該步驟(b)中係利用一第二亂數與該第二成員所擁有之一認證公開金鑰對該一次解密第一認證訊息及該第二認證訊息加密。

13.如請求項 9 所述之動態群組之認證方法，其中該步驟(c)中被加密之該一次解密第一認證訊息及該第二認證訊息解密係利用該第一成員所擁有之一第一認證向量與一第一私密金鑰進行解密。

14.如請求項 10 所述之動態群組之認證方法，其中該步驟(d)中該比對結果及該一次解密第二認證訊息係利用一第三亂數與該認證公開金鑰進行加密。

15.如請求項 11 所述之動態群組之認證方法，其中該步驟(e)中被加密之該比對結果及該一次解密第二認證訊息係利用該第二認證向量與該第二私密金鑰進行解密。

16.一種應用請求項 1 之動態群組中安全通訊之方法，該動態群組中一發起者傳送資料給群組成員中之一接收者時之通訊方法係包括下列步驟：

該發起者利用一存取控制公開金鑰對該資料加密，該存取控制公開金鑰中包括 d-1 個群組公開金鑰元素及所有成員對應之該等個人公開金鑰元素；

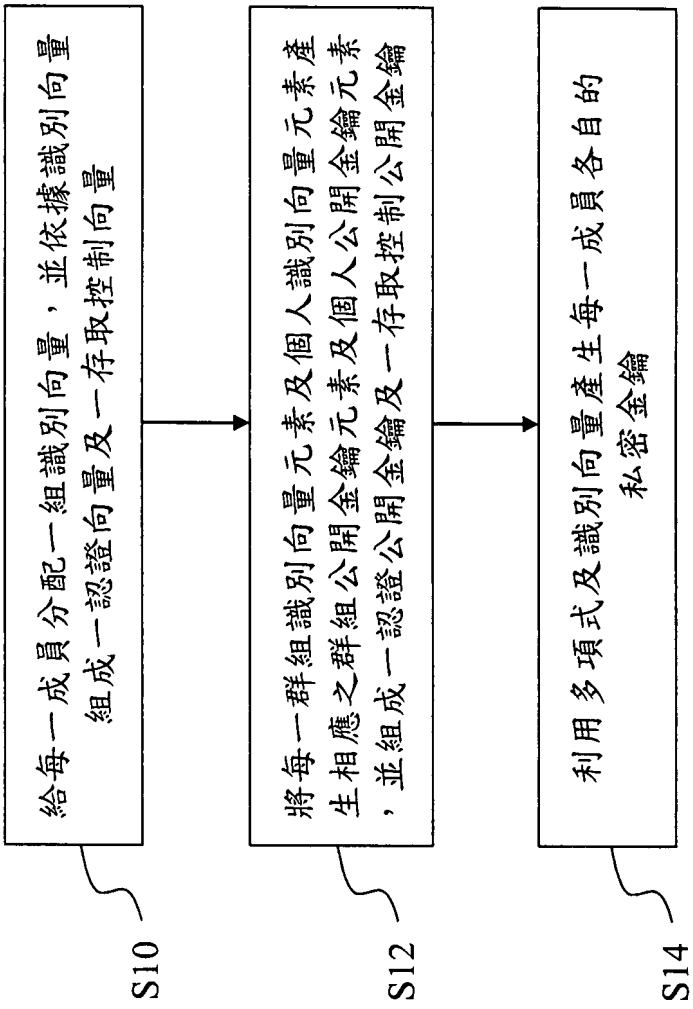
該接收者接收被加密之該資料後，使用該存取控制向量與該私密金鑰解密；以及

若該接收者的該個人識別向量與該存取控制公開金鑰中所依據的該等個人識別向量元素其中之一相同，則對該資料進行解密會成功，反之，若該接收者的該個人識別向量不存在於該存取控制公開金鑰所依據的該等個人識別向量元素中，則該資料進行解密會失敗，該接收者與該發起者不為同一動態群組之成員。

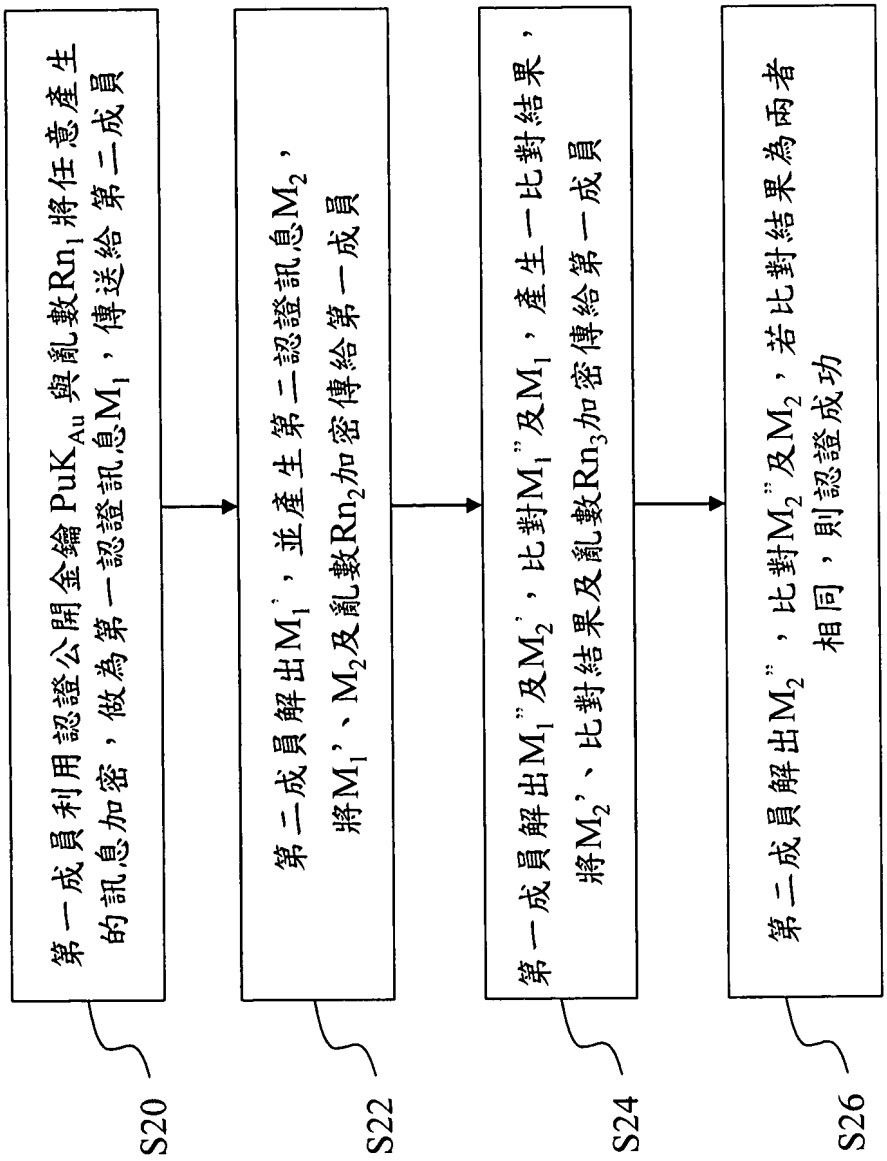
17.如請求項16所述之動態群組中安全通訊之方法，其中該成員係利用該存取控制向量及一私密金鑰對該資料解密。

18.如請求項16所述之動態群組中安全通訊之方法，其中該動態群組中僅有該發起者擁有該存取控制公開金鑰。

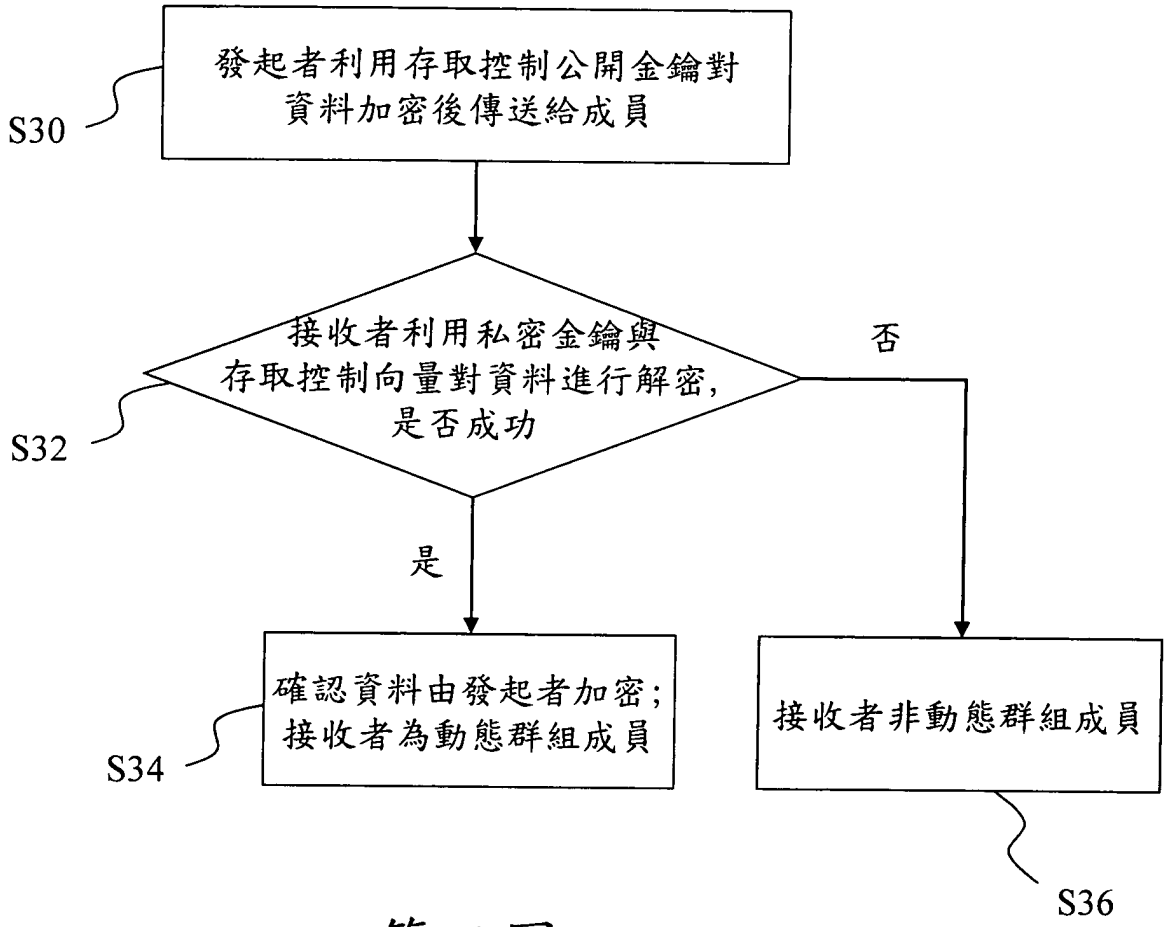
六、圖式：


給每一成員分配一組識別向量，並依據識別向量組成一認證向量及一存取控制向量
將每一群組識別向量元素及個人識別向量元素產生相應之群組公開金鑰元素及個人公開金鑰元素，並組成一認證公開金鑰及一存取控制公開金鑰
利用多項式及識別向量產生每一成員各自的私密金鑰
S10
S12
S14

第一圖


第一成員利用認證公開金鑰 PuK_{Au} 與亂數 Rn_1 將任意產生的訊息加密，做為第一認證訊息 M_1，傳送給 第二成員
S20
第二成員解出 M_1'，並產生第二認證訊息 M_2，將 M_1'、M_2及亂數 Rn_2 加密傳給第一成員
S22
第一成員解出 M_1" 及 M_2'，比對 M_1" 及 M_1，產生一比對結果，將 M_2'、比對結果及亂數 Rn_3 加密傳給第一成員
S24
第二成員解出 M_2"，比對 M_2" 及 M_2，若比對結果為兩者相同，則認證成功
S26

第二圖



第三圖

201301836

在循環動態群組（cyclic group）上，此動態群組具有一群組產生器（generator）。

第 1 圖為本發明中建立金鑰之方法的流程圖，首先在步驟 S10 中，每一成員會被分配到一組識別向量 V^{Peer}，其中包括每個成員共有的 d 個群組識別向量元素 $v_{Gr-1}, v_{Gr-2},\ldots,v_{Gr-d}$ 及一獨一無二的個人識別向量元素 v_{Idv}，因此動態群組中第一個成員的識別向量可如下式(1)所示：

$$V^{Peer1} = \{v_{Gr-1}, v_{Gr-2},\ldots,v_{Gr-d}, v_{Idv1}\} \quad (1)$$

而每一成員可依據擁有的識別向量中組成一認證向量 V_{Au} 及一存取控制向量 V_{Ac}，其中認證向量做為認證時所需用到的向量，包含 d 個群組識別向量元素，由於 d 個群組識別向量元素為每個成員共有的，故每一成員所擁有之認證向量皆相同；而存取控制向量做為存取控制時所需用到的向量，則包含 d-1 個群組識別向量元素及一個個人識別向量元素，因此第一個成員的認證向量及存取控制向量又可如下式(2)、(3)所示：

$$V_{Au} = \{v_{Gr-1}, v_{Gr-2},\ldots,v_{Gr-d}\} \quad (2)$$

$$V_{Ac} = \{v_{Gr-1}, v_{Gr-2},\ldots,v_{Gr-d\_1}, v_{Idv1}\} \quad (3)$$

接著在步驟 S12 中建立公開金鑰，此公開金鑰與識別向量的元素為一對一的關係，公開金鑰的組成元素是由識別向量元素 v_x 建立相對應的亂數 R_x 與群組產生器 P 以橢圓曲線密碼學（Elliptic Curve Cryptography, ECC）進行乘法運算（multiplication operation）所產生的，因此公開金鑰元素 $q_x = f(v_x) = R_x \cdot P$，其中 R_x 為亂數，將每一個群組識別向量元素及個人識別向量元素計算產生相應之群組公開金鑰元素及個人公開金鑰元素 q_x，並利用群組公開金鑰元素及個人公開金鑰元素組成一認證公開金鑰 PuK_{Au} 及一存取

控制公開金鑰 PuK_{Ac}，如下式(4)、(5)所示：

$$PuK_{Au}=\{f(v_{Gr-1}), f(v_{Gr-2}),..., f(v_{Gr-d})\}$$
$$=\{q_{Gr-1}, q_{Gr-2},...,q_{Gr-d}\} \quad (4)$$

$$PuK_{Ac}=\{f(v_{Gr-1}), f(v_{Gr-2}),..., f(v_{Gr-d\_1}), f(v_{Idv1}), f(v_{Idv2}),..., f(v_{Idvn})\}$$
$$=\{q_{Gr-1}, q_{Gr-2},...,q_{Gr-d\_1}, q_{Idv1}, q_{Idv2},..., q_{Idvn}\} \quad (5)$$

由此可知，認證公開金鑰 PuK_{Au} 係由所有的群組公開金鑰元素所組成，而存取控制公開金鑰 PuK_{Ac} 係由 d-1 個群組公開金鑰元素及所有 n 個成員之個人公開金鑰元素所組成，特別的是，只有發起者才有存取控制公開金鑰。

最後如步驟 S14 所述，發起者先隨機產生一值 y，並為每一成員分別產生任意之 d-1 次多項式 $p(x)= a_0+a_1x+a_2x^2+...+ a_{d-1}x^{d-1}$，且此多項式符合 $p(0)=y$，並利用此多項式及識別向量為每個成員製作獨一無二的私密金鑰 Prk^{Peer}，舉例第一個成員之私密金鑰如下式(6)：

$$Prk^{Peer1}=\{f'(v_{Gr-1}), f'(v_{Gr-2}),..., f'(v_{Gr-d}), f'(v_{Idv1})\} \quad (6)$$

其中 $f'(x)=\frac{p(x)}{R_x}\cdot P$，$R_x$ 為由識別向量元素 v_x 所建立相對應的亂數，P 為群組產生器。

當動態群組形成時，由伺服器或發起者分配給成員一組識別向量 V^{Peer}、共用的認證公開金鑰 PuK_{Au} 及成員的私密金鑰 Prk^{Peer}。然而，伺服器或發起者將存取控制公開金鑰 PuK_{Ac} 儲存在發起者端，並不分派給任何群組成員，只有發起者擁有存取控制公開金鑰。

在加密解密過程中，採方法一發起者直接用存取控制公開金鑰對資料加密，或者採方法二發起者隨機選取一對稱資料編碼金鑰，並利用對稱資

料編碼金鑰將資料加密，之後再利用存取控制公開金鑰對對稱資料編碼金鑰進行加密。而接收者接收被加密之資料後，若採方法一則直接用存取控制向量與私密金鑰對資料解密，若採方法二則接收者先使用存取控制向量與私密金鑰解開對稱資料編碼金鑰，接著再利用對稱資料編碼金鑰對資料進行解密。

本發明中動態群組的成員相互認證時，假設群組成員中第一成員欲與第二成員做認證時，第一成員會利用認證公開金鑰與亂數將任意訊息做加密，當作測試第二成員是否為群組成員的認證訊息，若第二成員可以解出訊息，並回傳給第一成員，第一成員就確認第二成員跟他是相同群組的成員。

第二圖為第一成員與第二成員相互認證之流程圖，包含四個步驟，首先，步驟 S20 中第一成員利用認證公開金鑰 PuK_{Au} 與產生的亂數 Rn_1 對任意產生的第一認證訊息 M_1 進行加密，傳送給第二成員；步驟 S22 第二成員收到第一認證訊息 M_1' 後，利用認證向量 V_{Au}^2 與所擁有之第二私密金鑰 PrK^2 解出一次解密第一認證訊息 M_1'，同時第二成員另產生第二認證訊息 M_2，並將 M_1' 與 M_2 串接成 $M_1'||M_2$ 後，用認證公開金鑰 PuK_{Au} 與第二成員產生的亂數 Rn_2 將 $M_1'||M_2$ 加密，回傳給第一成員；步驟 S24，第一成員再將用認證向量 V_{Au}^1 與第一成員所擁有之第一私密金鑰 PrK^1 解出二次解密第一認證訊息 M_1'' 與一次解密第二認證訊息 M_2'，且第一成員比對 M_1'' 與 M_1 是否相同，若相同代表第一成員認證第二成員成功；隨後，第一成員將比對結果 Rslt 與 M_2' 串接成 $Rslt||M_2'$ 後，用 PuK_{Au} 與第一成員產生的亂數 Rn_3 將 $Rslt||M_2'$ 加密，傳送給第二成員；最後，步驟 S26 中第二成員再利用認證向量 V_{Au}^2 與

第二私密金鑰 PrK^2 解出二次解密第二認證訊息 M_2''，並將 M_2'' 與 M_2 比對是否相同，如果相同就是第二成員認證第一成員成功，若不同則認證失敗。

因此，群組成員間可利用共用的認證公開金鑰 PuK_{Au} 將認證資料加密，被認證者利用個人的私密金鑰 Prk^{Peer} 與認證向量 V_{Au}^{Peer} 解開認證資料，以確認互相為同一群組關係，達到相互認證。

除此之外，發起者可以利用存取控制公開金鑰 PuK_{Ac} 主控存取資料的成員，只有群組成員可以解開資料，即是達到良好的存取控制。成員亦可利用個人的私密金鑰 Prk^{Peer} 與存取控制向量 V_{Ac}^{Peer} 解開加密資料，確認資料來源者的身份是發起者，達到資料來源的鑑別性。

本發明中資料鑑別之方法如第三圖之流程圖所示，若發起者要傳送資料給動態群組 n 個成員中的某一成員，則在步驟 S30 中發起者使用存取控制公開金鑰 PuK_{Ac} 對資料加密，再將加密資料傳送給該成員，在上述金鑰產生方法中，已知存取控制公開金鑰 PuK_{Ac} 包含 d-1 個公開金鑰元素 q_{Gr-1}, $q_{Gr-2},\cdots,q_{Gr-d\_1}$ 及所有 n 個成員之個人識別公開金鑰元素 q_{Idv1}, $q_{Idv2},\cdots$, q_{Idvn}；步驟 S32，當群組成員中之接收者接收被加密之資料後，使用存取控制向量與私密金鑰解密，若是其個人的存取控制向量 V_{Au}^{Peer} 中所包含之個人識別向量元素 v_{Idv}，為存取控制公開金鑰 PuK_{Ac} 中所依據的成員個人識別向量元素 $v_{Idv1}, v_{Idv2},\cdots, v_{Idvn}$ 其中之一，則如步驟 S34 所述，成員利用存取控制向量 V_{Ac}^{Peer} 及私密金鑰 Prk^{Peer} 對資料解密成功，反之，若接收者的個人識別向量元素不存在於存取控制公開金鑰所依據的成員個人識別向量元素中，例如接收者的個人識別向量元素為 $v_{Idv(n+1)}$，由於 $Peer_{n+1}$ 不是群組成員，因此如步驟 S36 所述，接收者非動態群組成員，解密會失敗。

舉例而言，假設發起者邀請 $Peer_1, Peer_2, \ldots, Peer_n$ 成為群組成員，當發起者使用 PuK_{Ac} 當公開金鑰對資料加密並欲將加密資料傳送給 $Peer_2$ 時，將 $Peer_2$ 的個人識別向量元素 v_{Idv2} 對應的個人公開金鑰元素 q_{Idv2} 加入到存取控制公開金鑰 PuK_{Ac} 中，故當 $Peer_2$ 接收到加密資料時，使用 V_{Ac}^2 與 $\Pr k^2$ 就有足夠的資訊可以解開資料。又因為 $Peer_2$ 是用 V_{Ac}^2 與 $\Pr k^2$ 解密，代表接到的資料是用存取控制公開金鑰所加密，又存取控制公開金鑰只有發起者擁有，所以 $Peer_2$ 可以確認資料的來源是發起者。

另，$Peer_{n+1}$ 不是群組成員，當發起者使用 PuK_{Ac} 當公開金鑰對資料加密時，並未將 $Peer_{n+1}$ 個人識別向量對應的公開金鑰元素加入 PuK_{Ac}，所以當 $Peer_{n+1}$ 接收到資料時，因為擁有的 $v_{Idv(n+1)}$ 並沒有與加密時所使用的公開金鑰元素相對應，所以無法有足夠的資訊以解開資料。

因此，本發明具有以下優點：1.具有可擴展性，發起者只需產生一組加密資料，就可以發送給所有的群組成員；2.不需伺服器即可相互認證，群組成員使用共用的認證公開金鑰加密認證資料，只要是群組成員就可以用他們獨一無二的私密金鑰解開認證訊息，達到無需第三者介入的相互認證；3.保持群組成員身分隱密性，群組成員不需知道其他成員真實身份，只要確認都是群組成員即可；4.因發起者利用群組成員的個人識別向量元素當依據所產生的存取控制公開金鑰來加密，故只有群組成員可將資料解密並正確的存取資料；5.具資料鑑別性，接收端成員可判別資料是否由發起者起源的，避免真正資料被換過；6.在加密過程加入亂數，所以同一條資料流在每一次加密時都會產生不同的加密資料，增加安全性；以及 7.有效的金鑰管理，發起者須儲存一組存取控制公開金鑰，其他每個群組成員只要儲存一

組共用的認證公開金鑰與自己的私密金鑰即可。

綜上所述，本發明所提供之一種動態群組中建立金鑰、認證及安全通訊方法係可應用於一對多資料分享的環境，資料可由一個共用的公開金鑰或是發起者獨有的公開金鑰加密，而後所有符合條件的群組成員之私密金鑰皆可解密；此外，本發明提供群組成員間不需透過伺服器（serverless）相互認證的方法，群組成員間可利用共同的認證公開金鑰與群組成員的私鑰做認證，不再需要經由認證伺服器做認證，此種認證方式同時保護成員身份隱密性；再者，本發明同時提供資料的存取控制機制，當發起者將資料加密時，由於利用到群組成員的個人識別向量當作加密的依據，故只有群組中的成員可解密，群組成員更可利用解密資料時所用的存取控制向量，查驗資料是由發起者所產生或是由其他人所置換的假資料。

唯以上所述者，僅為本發明之較佳實施例而已，並非用來限定本發明實施之範圍。故即凡依本發明申請範圍所述之特徵及精神所為之均等變化或修飾，均應包括於本發明之申請專利範圍內。

【圖式簡單說明】

第 1 圖為本發明動態群組中建立金鑰之方法之流程圖。

第 2 圖為本發明動態群組中認證方法之流程圖。

第 3 圖為本發明動態群組中安全通訊方法之流程圖。

【主要元件符號說明】

無

七、申請專利範圍：

1. 一種動態群組中建立金鑰之方法，該動態群組中包括一發起者及複數成員，該方法包括下列步驟：

給每一該成員分配一組識別向量，每一組該識別向量包含共同的 d 個群組識別向量元素及不同的一個人識別向量元素，每一該成員依據該識別向量可組成一認證向量及一存取控制向量；

將每一該等群組識別向量元素及該個人識別向量元素計算產生相應之 d 個群組公開金鑰元素及一個人公開金鑰元素，並組成一認證公開金鑰及一存取控制公開金鑰；以及

該發起者為每一該等成員分別產生任意之一 d-1 次多項式，並利用該多項式及該識別向量產生一私密金鑰。

2. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該認證向量係由 d 個該群組識別向量元素所組成，每一該成員所擁有之該認證向量皆相同。

3. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該存取控制向量包含 d-1 個該群組識別向量元素及該個人識別向量元素。

4. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該認證公開金鑰係由該等 d 個群組公開金鑰元素所組成。

5. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該存取控制公開金鑰係由 d-1 個該等群組公開金鑰元素及所有成員之個人識別公開金鑰元素所組成。

6. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該等群組識別向量元素係與該群組產生器以橢圓曲線密碼學（Elliptic Curve Cryptography,

ECC）進行乘法運算，進而產生該等公開金鑰元素。

7. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該發起者隨機產生一值 y，且該多項式 p(x)符合 p(0)=y。

8. 如請求項 1 所述之動態群組中建立金鑰之方法，其中該私密金鑰包括該等成員的 d 個群組識別向量元素、一個該個人識別向量元素與該多項式所計算而成之 d+1 個私密金鑰元素。

9. 一種應用請求項 1 之動態群組之認證方法，該動態群組中一第一成員對一第二成員進行認證之方法係包括下列步驟：

(a)該第一成員對一第一認證訊息進行加密，傳送給該第二成員；

(b)該第二成員將被加密之該第一認證訊息解密為一一次解密第一認證訊息，另產生一第二認證訊息，並對該一次解密第一認證訊息及該第二認證訊息進行加密後，傳送給該第一成員；

(c)該第一成員再將被加密之該一次解密第一認證訊息及該第二認證訊息解密，得到一二次解密第一認證訊息及一一次解密第二認證訊息，比對該二次解密第一認證訊息與該第一認證訊息是否相同，若比對結果不同則認證失敗，若該比對結果相同則進行步驟(d)；

(d)該第一成員對該比對結果及該一次解密第二認證訊息進行加密後，傳送給該第二成員；以及

(e)該第二成員將被加密之該比對結果及該一次解密第二認證訊息解密，得到該比對結果及一二次解密第二認證訊息，比對該二次解密第二認證訊息與該第二認證訊息是否相同，若不同則認證失敗，若相同認證成功。

10.如請求項 9 所述之動態群組之認證方法，其中該步驟(a)中該第一認證訊息係利用一第一亂數與該第一成員所擁有之一認證公開金鑰進行加密。

11.如請求項 9 所述之動態群組之認證方法，其中該步驟(b)中被加密之該第一認證訊息係利用該第二成員所擁有之一第二認證向量與一第二私密金鑰進行解密，得到該一次解密第一認證訊息。

12.如請求項 9 所述之動態群組之認證方法，其中該步驟(b)中係利用一第二亂數與該第二成員所擁有之一認證公開金鑰對該一次解密第一認證訊息及該第二認證訊息加密。

13.如請求項 9 所述之動態群組之認證方法，其中該步驟(c)中被加密之該一次解密第一認證訊息及該第二認證訊息解密係利用該第一成員所擁有之一第一認證向量與一第一私密金鑰進行解密。

14.如請求項 10 所述之動態群組之認證方法，其中該步驟(d)中該比對結果及該一次解密第二認證訊息係利用一第三亂數與該認證公開金鑰進行加密。

15.如請求項 11 所述之動態群組之認證方法，其中該步驟(e)中被加密之該比對結果及該一次解密第二認證訊息係利用該第二認證向量與該第二私密金鑰進行解密。

16.一種應用請求項 1 之動態群組中安全通訊之方法，該動態群組中一發起者傳送資料給群組成員中之一接收者時之通訊方法係包括下列步驟：

該發起者利用一存取控制公開金鑰對該資料加密，該存取控制公開金鑰中包括 d-1 個群組公開金鑰元素及所有成員對應之該等個人公開金鑰元素；

該接收者接收被加密之該資料後，使用該存取控制向量與該私密金鑰解密；以及

若該接收者的該個人識別向量與該存取控制公開金鑰中所依據的該等個人識別向量元素其中之一相同，則對該資料進行解密會成功，反之，若該接收者的該個人識別向量不存在於該存取控制公開金鑰所依據的該等個人識別向量元素中，則該資料進行解密會失敗，該接收者與該發起者不為同一動態群組之成員。

17.如請求項 16 所述之動態群組中安全通訊之方法，其中該成員係利用該存取控制向量及一私密金鑰對該資料解密。

18.如請求項 16 所述之動態群組中安全通訊之方法，其中該動態群組中僅有該發起者擁有該存取控制公開金鑰。

19. 如請求項 16 所述之動態群組中安全通訊之方法，其中該發起者隨機選取一對稱資料編碼金鑰，並利用該對稱資料編碼金鑰將該資料加密，再利用該存取控制公開金鑰對該對稱資料編碼金鑰進行加密，而該接收者接收被加密之該資料後，使用該存取控制向量與該私密金鑰解開該對稱資料編碼金鑰，再利用該對稱資料編碼金鑰解密該資料。