I246298

公告本

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：92109715

※ 申請日期：92-04-25　　※IPC 分類：H04L 9/30

壹、發明名稱：（中文/英文）

加密通信系統，組成該系統之密鑰分佈伺服器及終端裝置，及用於密鑰共享之方法

CRYPTOGRAPHIC COMMUNICATION SYSTEM, KEY DISTRIBUTION SERVER AND TERMINAL DEVICE CONSTITUTING THE SYSTEM, AND METHOD FOR SHARING KEY

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商萬國商業機器公司

INTERNATIONAL BUSINESS MACHINES CORPORATION

代表人：（中文/英文）

傑拉德 羅森賽

GERALD ROSENTHAL

住居所或營業所地址：（中文/英文）

美國紐約州阿蒙市新果園路

NEW ORCHARD ROAD, ARMONK, NEW YORK 10504, U.S.A.

國　籍：（中文/英文）

美國　U.S.A.

參、發明人：（共 2 人）

姓　名：（中文/英文）

1.渡邊 裕治

YUJI WATANABE

2.沼尾 雅之

MASAYUKI NUMAO

住居所地址：（中文/英文）

1.日本國東京都世田谷區上用賀 5-2-8-301

5-2-8-301 KAMIYOUGA, SETAGAYA-KU, TOKYO-TO, JAPAN

2.日本國神奈川縣川崎市麻生區上麻生 3-22-11-1011

3-22-11-1011 KAMI-ASAO, ASAO-KU, KAWASAKI-SHI, KANAGAWA-KEN, JAPAN

國　籍：（中文/英文）

1.2.均日本　JAPAN

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為： 年 月 日。

☑ 本案申請前已向下列國家（地區）申請專利：

1.日本 2002 年 04 月 30 日 特願 2002-129359

2.

3.

4.

5.

☑ 主張國際優先權(專利法第二十四條)：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1.日本 2002 年 04 月 30 日 特願 2002-129359

2.

3.

4.

5.

☐ 主張國內優先權(專利法第二十五條之一)：

【格式請依：申請日；申請案號數 順序註記】

1.

2.

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

本發明係關於一種用以將解密加密之資訊所用的密鑰分佈至一用戶終端之密鑰技術，特定言之係關於一種用於以一安全且快速的方式更新一密鑰之技術。

【先前技術】

在許多狀況中，為建立一系統用以提供資訊給一預先設定之群組，僅將密鑰(群組密鑰)分佈給已登記為該群組之一成員的用戶，然後藉由密鑰以執行密鑰通信。密鑰技術適用於許多應用，如可攜式電話的內容分佈、DVD播放機之解密器/複製器、經由CDROM介面之軟體分佈、警方無線電通信以及P2P(point to point；點對點)服務中群組之間的本地通信等。

在上述系統中，萬一一終端裝置之一部件(解碼器)因諸如遭偷竊等而移除，則群組密鑰將有洩漏給群組成員之外的未授權人員之危險。為此緣故，該舊群組密鑰必須更新以建立一新密鑰，且該新密鑰必須儘快地為群組之成員所共享。

更新密鑰之技術在長期利用一次建立的基礎架構之系統中有極端重要的作用。

假定在包含複數個用戶終端之此類系統(以下稱之為廣播類型密鑰通信系統)中，訊息係分佈給除一單一用戶終端或複數個用戶終端之外的所有用戶終端。請注意，術語「除外」(exclude)意謂將某一用戶終端(或某些用戶終端)自一群

組中除去之操作，且稱該除外之用戶終端為「需除外之終端」(以下稱之為目的除外終端)。一般而言，當除外一目的除外終端時，需將一新群組密鑰分佈給除目的除外終端之外的各個別用戶終端。為此緣故，隨群組之規模的增長，完成使所有用戶終端共享一新群組密鑰之操作所需的通信量及時間延遲量亦隨之增長。

傳統上，為減少上述更新群組密鑰所需之時間延遲量，已構想出多種技術。日本專利申請案2000-196581中所揭示的技術(第一傳統技術)係上述類型之傳統技術的範例。

上述出版物中所揭示之該第一傳統技術所採用的演算法使判定一目的除外終端之後的通信量及時間延遲量與作為群組成員的用戶之數量「n」不成正比。若採用上述演算法且假定需除外的終端之最大數量為「k」，則為計算群組密鑰，各用戶終端必須執行與「k」成正比之一數量的模指數運算。因此，若「k」遠小於「n」(k«n)，則根據此技術之密鑰分佈的執行效率可遠高於一般的群組密鑰分佈。例如，假定一系統(n=10,000)包含10,000用戶終端，且需除外之終端數為100(k=100)，則一般的群組密鑰分佈所需執行處理的次數與數字「10,000」成正比，但依據該出版物中所揭示的該第一傳統技術之密鑰分佈所需執行處理的次數與數字「100」成正比。

然而，在包含多達數百萬用戶終端之一系統(例如，用以向諸如可攜式電話之類的行動終端提供服務之系統)或類似系統中，則需將代表需除外之終端的數量之「k」擴大(例

如，數千至數萬)以符合群組的規模。此即使計算能力不佳的的終端需承受因解密而導致之相當大的計算負載，該負載係與數字「k」成正比。因此，群組密鑰分佈所需執行解密的次數最好係與數字「k」不成正比，或(若可能)為一恆定次數。

日本專利申請案2001-203682為解決上述問題的傳統技術之範例(第二傳統技術)。

該出版物中所揭示之該第二傳統技術僅需執行模指數運算「2」次即實現解密，而非取決於代表用戶終端之總數量的數字「n」及代表需除外之終端的最大數量之數字「k」。因此，第二傳統技術使包含大量用戶終端之系統可快速分佈群組密鑰。

[需本發明解決之問題]

在廣播類型密鑰通信系統中，一協定之成員係界定如下：

密鑰分佈伺服器：用於在設置時決定系統參數及將個人密鑰分佈給個別用戶終端之一可靠機構。當要分佈一群組密鑰時，該伺服器判定哪些終端需除外，然後經由廣播分佈該群組密鑰。密鑰分佈伺服器用「S」表示。

用戶終端：用於自該密鑰分佈伺服器接收一廣播材料之一終端。在設置時，一用戶終端「i」自該密鑰分佈伺服器接收一個人密鑰「s_i」。用戶終端之一集合係定義為集合$\Phi=\{1,\ldots,n\}$($n=|\Phi|$代表用戶終端之總數量)。

除外之用戶終端：藉由該密鑰分佈伺服器所除外之一用戶終端。當該密鑰分佈伺服器在第一輪中分佈一群組密鑰

時，需除外之用戶終端之一集合「d」(<k)係定義為一子集$\Lambda_1(\subset\Phi)$。一旦遭除外，該用戶終端於該終端遭除外之該輪之後即不能解密群組密鑰，因此，即決不會在複數輪中重複遭到除外。即二集合之交集$\Lambda_1\cap\Lambda_{1'}=\{0\}(1\neg 1')$。此外，假定在所有輪中代表除外之用戶終端的總數之數字永不會超過數字「k」(即$|\cup\Lambda_1|\phi$ k)。

有效用戶終端：未除外之一用戶終端。假定在群組密鑰之第一輪分佈中有效用戶終端之一集合係定義為集合$\Omega_1(=\Phi<U^1_{j=1}\Lambda_j)$。

在如此定義的廣播類型密鑰通信系統中，於第一輪中將U_1分佈給全部用戶終端Φ中的有效用戶終端Ω_1。利用U_1加密訊息允許在群組Ω_1中利用該類型的密鑰通信來廣播。即密鑰通信之執行係如下：

1. 設$\Omega_0=\Phi$。密鑰分佈伺服器經由一點對點及密鑰分佈協定連接將一群組密鑰「U_0」及一個人密鑰key_i分佈給各用戶「i」($i\in\Phi$)。
2. 對於各1γ1，重複執行以下程序(以下將稱執行一次以下程序為「1輪」)。

(a) 密鑰分佈伺服器判定Λ_1 Ω_{1-1}。

(b) 若$k\gamma\copyright^1_{j=1}|\Lambda_j|$，則$\Phi:=\Omega_{1-1}$，$U_0:=U_{1-1}$，且然後返回至步驟1。

(c) 密鑰分佈伺服器分佈一標頭H_1至Ω_1，以使Ω_1計算U_1。

(d) v Ω_1利用H_1及key_v計算U_1。

(e) 密鑰分佈伺服器及Ω_1利用U_1執行廣播類型密鑰通信。

此外，在以下所作的說明中會利用以下參數。「p」及「q」係滿足q.∴p-1的大質數，且「g」為有限場(finite field)Z_p上階為「q」之元素。確定「p」及「q」的大小，使群組GF(q)(該群組由作為一生成元素之「g」所組成)上的離散對數問題在計算上變得困難。在以下的解釋中，除非另有說明，否則所有計算皆係利用模p算術進行。請注意，雖然未詳細說明，但除與將階數「p」定義為群組GF(p)上的一質數所使用的定義不同之外，階數「p」可定義在任意群組GF(q)上，使解決離散對數問題在計算上變得困難。例如，一群組之構建係藉由：(1)在階數為「p」的一元素上進行乘法運算，對應於在一任意有限場上的曲線(如橢圓曲線)上的加法運算，或(2)將一質數「p」作為一指數，而非一質數「p」，且然後在一擴展場GF(p')上執行算術運算，而非利用一質數「p'」作為一模數執行其餘運算。

E(密鑰，訊息)表示利用對稱密鑰加密之訊息加密。「n」表示用戶終端的總數量，且「k」(k<n)表示需除外的終端之最大數量。

根據上述假定，該廣播類型密鑰通信系統在安全及效率方面需滿足以下四項要求：

1. 一有效用戶終端$v \in \Omega_1$能獨立地解密一群組密鑰U_1(在多項式時間內)。
2. 在「k」個用戶終端遭除外之該輪後，即使利用該等除外之用戶終端各自所擁有的個人密鑰，任何人亦無法解密一群組密鑰(在機率性多項式時間內)。

3. 群組密鑰分佈中所使用的標頭之長度及各用戶終端所擁有的個人密鑰之大小不取決於代表用戶終端的總數量之數字。

4. 經過一段時間間隔，用以計算群組密鑰之標頭已接獲且群組密鑰之解密(解密)已完成，在該期間內模指數運算的執行次數不取決於「n」及「k」。

要求1要求一用戶終端能有效地獨立執行解密。在廣播類型密鑰通信系統中，當用戶終端在解密時無需與其他終端通信時，不要在網絡上造成額外的流量很重要。

要求2必須得到滿足，以防止一除外之用戶終端與其他除外之終端合謀試圖解密一會話密鑰。

要求3必須得到滿足，以防止當系統包含非常多的用戶終端時處理量會急劇增加。

當「k」需要很大以與一大群組相稱時，為解密要求一定處理量之一群組密鑰，要求4必須得到滿足，使該處理量並不取決於「n」及「k」。

要求2中包括所謂的「多餘影子攻擊(Spare Shadow Attack)」及「r發佈攻擊(r publish attack)」。利用一時間限值之協定本質上無法解決「秘密發佈攻擊」所引起的問題。請注意，當假定要揭示一秘密的攻擊者之數量為「w」時，若未授權人數不大於「k-w」，則可保持安全。因此，在未授權用戶終端(其與其他未授權用戶終端合謀)的總數量不大於「k」的狀況下評估協定之安全性允許在與要求2相同的領域中說明安全性。

上述傳統技術1滿足上述要求1、2及3。需分佈的加密訊息之長度對應於一恆定時間間隔O(k)，且需分佈的個人密鑰之大小對應於O(l)，意謂該等因素會產生極高的效率。然而，因代表需執行的用以解密群組密鑰之模指數運算的次數之數字等於O(k)，而且該等模指數運算不能先於接收群組密鑰而預先計算，故傳統技術1並不滿足要求4。

傳統技術2致力於要求4的需要提供滿足要求4的演算法。然而，傳統技術2並不滿足要求2(就安全來說，該要求最為重要)，其原因可自以下的分析中獲知。即當將一群組密鑰分佈有限次時，未除外之用戶終端可要求關於整個系統的秘密資訊，且進一步可於有限次數分佈密鑰之後取消需執行的除外運算(例如，若kγ5，則可於群組密鑰分佈三次之後對系統進行攻擊)。

傳統技術2為何不滿足要求2的問題將在下文闡明。首先將解釋傳統技術2用於一廣播類型密鑰通信之演算法。

1. 設置

一密鑰分佈伺服器決定代表需除外的終端之最大數量的數字「k」，且隨機選擇由下列數值表達式1所代表之一k^{th}階多項式Z_q。

[數值表達式1]

$$F(x)=\sum_{j=0}^{k} a_j x^j$$

$$G(x)=\sum_{j=0}^{k} b_j x^j$$

F(0)=S且G(0)=T(mod q)係僅為該密鑰分佈伺服器所知的密鑰。密鑰分佈伺服器經由一秘密通信路徑將

$key_i=(s_i,f_i)=(F(i),g^{G(i)/F(i)})(i=1, \varepsilon\varepsilon\varepsilon, n)$分佈至各用戶終端「i」。此外，密鑰分佈伺服器隨機選擇一元素$U_0 \in GF(q)$且將其廣播出去。

2. 加密群組密鑰

在「l」($\gamma 1$)輪中需分佈的群組密鑰U_l係以下述方式分佈。隨機選擇一元素$r_l \in Z_q$且決定$X_l=g^{rl}$。然後，決定需除外的「d」用戶終端之一集合Λ_l。在「n+k(R-1)」與「n+kR」之間選擇「(k-d)」個整數，且決定由該等「(k-d)」個整數所組成之一集合Θ_l。密鑰分佈伺服器根據下列數值表達式2決定M_{l1}、$\varepsilon\varepsilon\varepsilon$、$M_{lk}$。

[數值表達式2]

$$M_{ij}=r_lF(j)+G(j) \bmod q \ (j \in \Lambda_l Y \Theta_l)$$

最後，密鑰分佈伺服器決定$E(U_{l-1},B_l)=E(U_{l-1},X_l\%[(j,M_{lj}) \therefore j \Lambda_l\Theta_l])$且將其廣播出去。在「l」輪中共享之群組密鑰係$U_l=g^{rlS+T}$。

3. 解密群組密鑰

因有效用戶終端，即一元素v Ω_l在「l」輪中係一元素v Ω_{l-1}，故該用戶終端在「l-1」輪中獲得U_{l-1}。用戶終端「v」利用U_{l-1}解密所接收的加密之訊息$E(U_{l-1},B_l)$中的B_l。然後，利用關於B_l之資訊，該終端根據下列數值表達式3計算該群組密鑰U_l。

[數值表達式3]

$$U_l=(X_lf_v)^{W_{l1}}g^{W_{l2}}$$

其中：

[數值表達式4]

$$W_{l1} = s_v L(v) \mod q$$

$$W_{l2} = \sum_{j \in \Lambda_l \Theta_l} (M_{lj} L(j)) \mod q$$

另外，L(j)係藉由拉格朗日多項式所提供的插值係數，如下列數值表達式5所示：

[數值表達式5]

$$L(j) = \prod_{t \in \Lambda_l \Upsilon \Theta_l \Upsilon \{v\} \setminus \{j\}} t/(t-j) \mod q$$

下面將闡明為何傳統技術2中所採用的演算法未滿足要求2。且將詳細說明在「R」輪中有效且任選的用戶終端$_v$(即一元素$_v \in \Omega_R$)如何計算及決定僅為密鑰分佈伺服器所知的秘密資訊「S」及「T」。在第1至R輪中終端「v」獲得(j, M_{lj})(l=1、εεε、R；j=1、εεε、k)，且所獲得之(j, M_{lj})滿足藉由下列數值表達式6所代表之關係。

[數值表達式6]

$$M_{lj} = r_l \sum_{t=0}^{k} a_t j^t + \sum_{t=0}^{k} b_t j^t \mod q \quad (l = 1, \mathrm{K}, R, \quad j \in \Lambda_l \Upsilon \Theta_l, \quad |\Lambda_l \Upsilon \Theta_l| = k)$$

請注意，因「j」為已知，故對於「2k+2+R」個變數a_0、εεε、a_k、b_0、εεε、b_k、r_1、εεε、r_R可獲得「kR」個等式。即當「R」滿足下列數值表達式7時，則密鑰分佈伺服器所擁有的所有密鑰，即「S」$(=a_0)$及「T」$(=b_{10})$皆可計算出來。

[數值表達式7]

$$2k+2+R \le kR \quad \Leftrightarrow \quad R \ge \frac{2(k+1)}{k-1}$$

例如，若k γ 5，則所有有效的用戶終端可在第3輪中計算出密鑰分佈伺服器所擁有的密鑰(諸如「S」及「T」等)。此即表示傳統技術2並不滿足要求2。

【發明內容】

因此，本發明之一項目的係提供一種用於以一高度安全且足夠迅速的方式更新一群組密鑰之方法，同時該方法滿足上述四項要求。

另外，除上述目的之外，本發明亦要提供一種高度安全且高度有效的廣播類型密鑰通信。

為達成上述目的，本發明係實現為一種密鑰通信系統，其包含一密鑰分佈伺服器用以分佈用於解密加密之資訊的密鑰以及利用該資訊之一具體數量的用戶終端。依據本發明之第一項觀點的密鑰通信系統之特徵在於該密鑰分佈伺服器係構建成用以分佈：用於解密該資訊之一加密的第一群組密鑰；對應於該等具體數量的用戶終端且用於解密該第一群組密鑰之個別解密資訊；以及對應於該等具體數量之用戶終端且用於對一第二群組密鑰執行一部分解密之個別密鑰更新資訊，該第二群組密鑰係於更新一群組密鑰之後予以更新，且該等具體數量的用戶終端係構建成解密該密鑰分佈伺服器所分佈之該第一群組密鑰，解密時利用根據先前所獲得用以解密該第一群組密鑰之密鑰更新資訊所執行的處理操作所獲得之結果，並進一步利用該密鑰分佈伺服器所分佈之該解密資訊。在時間域中，用以解密該群組密鑰之分佈操作減少了更新該群組密鑰時的處理量。

於分佈該群組密鑰之前，該等具體數量的用戶終端對該群組密鑰實施一部分解密。於分佈該群組密鑰之前預先對用戶終端的該群組密鑰實施一部分解密可減少分佈一新群

組密鑰之後執行處理所需的一時間間隔，且在更新群組密鑰時不會喪失安全性。

在該密鑰通信系統中，該密鑰分佈伺服器最好將用以解密該第一群組密鑰之密鑰更新資訊與一第三群組密鑰一起分佈給該等具體數量的用戶終端，該第三群組密鑰係處於更新為該第一群組密鑰之前的一狀態。

另外，萬一該密鑰分佈伺服器更新該群組密鑰，則該密鑰分佈伺服器決定在該等具體數量的用戶終端中哪些用戶終端需除外，且將除該等目的除外用戶終端之外的其餘用戶終端所利用之該解密資訊與得到更新之該群組密鑰一起分佈給該等具體數量的用戶終端，以使該等其餘的用戶終端可解密得到更新之群組密鑰。

為達成上述目的，亦可將本發明實現為一種如下所述構建而成的密鑰分佈伺服器，用以分佈解密加密之資訊所用的一密鑰。該密鑰分佈伺服器之特徵在於其包含：用以產生解密該資訊所用之一第一群組密鑰及加密該第一群組密鑰之構件；用以產生用於解密該第一群組密鑰且對應於用戶終端之個別解密資訊之構件；用以產生用於對一第二群組密鑰執行一部分解密且對應於該等用戶終端之個別密鑰更新資訊之構件，該第二群組密鑰係於更新一群組密鑰之後得到更新；以及用以將該第一群組密鑰、該解密資訊及該密鑰更新資訊分佈給該等用戶終端之構件。

為達成上述目的，亦可將本發明實現為一種如下所述構建而成的終端裝置。該終端裝置之特徵在於其包含：用以

自一具體密鑰分佈伺服器擷取用於解密加密之資訊的一加密之群組密鑰及用於解密該群組密鑰之解密資訊之構件；用以於分佈該群組密鑰之前對該群組密鑰執行一部分解密之構件；以及利用根據對該群組密鑰之一部分解密所執行的處理操作所獲得之結果及自該密鑰分佈伺服器所擷取之解密資訊解密該群組密鑰之構件。

另外，亦可將本發明實現為一種用以控制一電腦，然後使該電腦如同上述密鑰分佈伺服器及/或終端裝置一樣運作之程式。所提供的該程式可儲存於一磁碟、一光碟及/或其他儲存媒體上，如一半導體記憶體，然後經由一網路交遞或分佈該等媒體。

另外，可將本發明實現為一種如下所述構建之密鑰共享方法，用以使利用該資訊之一具體數量的終端共享用於解密加密之資訊的一密鑰。即該密鑰共享方法之特徵在於該方法包含：於分佈該群組密鑰之前使該等具體數量的終端對用於解密該資訊之一加密之群組密鑰執行一部分解密之一步驟；將該群組密鑰及個別解密密鑰(用以執行該群組密鑰之該部分解決以外的其餘解密之一部分，並對應於該等具體數量的端子)分佈給該等具體數量的終端之一步驟；以及使該等具體數量的終端利用所分佈之該解密資訊及藉由對該群組密鑰執行一部分解密，即先前所執行的該部分解密所獲得的結果對該群組密鑰執行解密之一步驟。

【實施方式】

下面將根據附圖中所示的一項具體實施例詳細解釋本發

明。

圖1為依據該具體實施例之一廣播類型密鑰通信系統的一般組態圖。

參考圖1，依據該具體實施例之該廣播類型密鑰通信系統包含：一密鑰分佈伺服器10，用以產生執行密鑰通信所用之一群組密鑰並分佈該密鑰；以及用戶終端20，用以獲得該密鑰分佈伺服器10所分佈之該群組密鑰且利用該密鑰執行密鑰通信。

該密鑰分佈伺服器10係利用一工作站、一個人電腦或其他具有網路功能之計算裝置實現，並在設置時決定系統參數，然後將一個人密鑰分佈給各用戶終端20。當要分佈一群組密鑰時，該伺服器判定哪些用戶終端20需除外，然後解密該群組密鑰，之後將該密鑰作為一廣播材料分佈。該個人密鑰與該群組密鑰的產生、分佈等處理係實現為(例如)一程式控制之CPU的一功能。

用戶終端20係利用一工作站、一個人電腦、一可攜式電話、一個人數位助理(PDA)或其他具有網路功能之資訊終端設備實現，且自密鑰分佈伺服器10接收一廣播材料。用戶終端「i」(第i個用戶終端20)在設置時自密鑰分佈伺服器10接收一個人密鑰s_i。然後，該終端利用該個人密鑰s_i解密該加密之群組密鑰，且進一步利用該群組密鑰解密一具體訊息，然後使用該訊息。該等處理係利用(例如)一程式控制之處理器實現。假定用戶終端20之一集合定義為集合$\Phi=\{1,...,n\}$($n=|\Phi|$代表用戶終端20的總數量)。

全部用戶終端20組成一群組，其利用密鑰分佈伺服器10所分佈之群組密鑰執行密鑰通信。雖然組成該群組之個別用戶終端20最初皆為「有效用戶終端」，可參與密鑰通信，但因故一或多個用戶終端成為「除外之用戶終端」之後，該除外之終端即不能參與密鑰通信。即該除外之終端不能再利用其個人密鑰解密群組密鑰。

該具體實施例中所採用的通信組態可為一用戶端/伺服器系統，其中資訊係在密鑰分佈伺服器10或一具體伺服器與用戶終端20之間交換，或為一點對點系統，其中資訊係在用戶終端20之間交換。即提供用戶終端20所使用的訊息(內容)之一供應者可存在於與密鑰分佈伺服器10相分離的一位置。

利用一群組密鑰在該廣播類型密鑰通信系統中所執行之密鑰通信包含四階段，即群組密鑰設置、利用一群組密鑰加密資訊、利用一群組密鑰解密資訊以及密鑰更新。

圖2為解釋依據本發明如何執行該密鑰通信之流程圖。

在該具體實施例中，於解密加密之群組密鑰期間將一部分計算(該部分取決於代表目的除外終端的最大數量之數字「k」)分離為預計算(密鑰更新)。此舉可以一認證方式保持安全，並進一步允許高速解密群組密鑰(除密鑰更新之外)，其中模指數運算執行兩次。下面將說明依據該具體實施例如何構建一密鑰通信協定。請注意，在以下的解釋中，接收者意謂使用用戶終端20之使用者以及用戶本身。

1. 設置

隨機選擇具有下列數值表達式8所代表的Z_q中之一變數之一「k」階多項式。

[數值表達式8]

$$F(x)=S+\sum_{j=1}^{k}a_j x^j$$

$$G_l(x)=T_l+\sum_{j=1}^{k}b_{lj}x^j$$

$F(0)=S$且$G_l(0)=T_l$係製作為僅為密鑰分佈伺服器10所知的一密鑰。密鑰分佈伺服器10在第一輪中將$key_i=(s_i,f_{li})=(F(i),g^{GI(i)/F(i)})$作為接收者「i」的解密密鑰秘密分佈至各用戶終端$i\in\{1, \varepsilon\varepsilon\varepsilon, n\}$。將一群組密鑰$U_0 \in GF(q)$分佈給所有用戶終端20(步驟201)。

2. 在第l輪中解密群組密鑰

密鑰分佈伺服器10隨機選擇一元素$r_l \in Z_q$且決定$X_l:=g^{rl}$。然後，該伺服器決定需除外的「d」用戶終端20之一集合Λ_l(步驟202)。該伺服器在「n+k(R-1)」與「n+kR」之間選擇「(k-d)」個整數，且決定由該等「(k-d)」個整數所組成之一集合Θ_l。密鑰分佈伺服器10根據下列數值表達式9決定M_{l1}、$\varepsilon\varepsilon\varepsilon$、$M_{lk}$。

[數值表達式9]

$$M_{lj}=r_l F(j)+G_l(j) \mod q \quad (j\in\Lambda_l Y\Theta_l)$$

另外，Ω_l(以下稱之為一用戶終端Ω_l)，其係一有效用戶終端20，利用下列數值表達式10計算為計算第「l」輪中的一分佈密鑰U_l所需的標頭資訊H_l(步驟203)。

[數值表達式10]

$$B_l=\langle X_l \| \{(j,M_{lj}) \mid j\in\Lambda_l Y\Theta_l\}\rangle$$

$$H_l=E(U_{l-1},B_l)$$

請注意，在第「l」輪中有效用戶終端「Ω_l」所共享之群組密鑰係由$U_l=g^{rS+Tl}$代表。

然後，為在第「l+1」輪中分佈該群組密鑰，該伺服器產生密鑰更新資訊(即在「l+1」中解密該群組密鑰時用戶終端20利用該資訊在以更新一密鑰)。密鑰分佈伺服器10隨機選擇一元素$b_{l+1,j}\in Z_q(j=0,...,k)$並決定一等式$(u_{l0},...,u_{lk})=(g^{bl+1,0},...,g^{bl+1,k})$，且利用群組密鑰$U_l$根據下列數值表達式11加密該等式以決定$C_l$(步驟204)。

[數值表達式11]

$$C_l = E(U_l, u_{l0} \| K \| u_{lk})$$

然後，密鑰分佈伺服器10將(H_l, C_l)作為一廣播材料分佈給所有用戶終端20(即Φ)(步驟205)。

3. 在第「l」輪中解密群組密鑰

用戶終端「v」，即一元素$v(\in \Omega_l)$，其係能在第「l」輪中執行解密之用戶終端20，根據下列數值表達式12在第「l」輪中執行解密(步驟206)。

[數值表達式12]

$$U = (X_l f_{lv})^{W_{l1}} g^{W_{l2}}$$

$$W_{l1} = s_v L(v) \mod q$$

$$W_{l2} = \sum_{j \in \Lambda Y \Theta} M_{lj} L(j) \mod q$$

其中，

$$L(j) = \prod_{t \in \Lambda Y \Theta Y \{v\} \setminus \{j\}} t/(t-j) \mod q$$

即在此輪中，用戶終端「v」利用f_{lv}(其係根據「l-1」輪中所分佈之資訊預先計算)及「B_l」(其需利用步驟205中所

分佈的H_l解密)解密第「l」輪中之群組密鑰「U_l」。

4. 用於第「l+1」輪的密鑰更新(預計算)

根據下列數值表達式13，用戶終端「v」，即一元素$v \in \Omega_l$，利用C_l中所包含的密鑰更新資訊(其係密鑰分佈伺服器10所分佈)將密鑰更新作為預計算執行(即先於在第「l+1」輪中分佈群組密鑰的處理)(步驟207)。

[數值表達式13]

$$f_{l+1,v} = \left(\prod_{j=0}^{k} u_{lj}^{\ v^j} \right)^{1/s_v}$$

另外，密鑰分佈伺服器10先於在第「l+1」輪中產生群組密鑰執行下列數值表達式14所表示的預計算。

[數值表達式14]

$$T_{l+1} = b_{l+1,0} \mod q$$

$$G_{l+1}(x) = \sum_{j=0}^{k} b_{l+1,j} x^j \mod q$$

密鑰更新(預計算)應藉由用戶終端20以及密鑰分佈伺服器10利用在第「l」中與群組密鑰一起分佈的資訊執行，直至在第「l+1」中分佈群組密鑰之前為止。

下面將確定如上述構建而成之依據本發明之該廣播類型密鑰通信系統在安全及效率方面是否滿足上述四項要求。

首先，很顯然該具體實施例滿足要求1，因在用戶終端20之間無需通信。

另外，該具體實施例之架構使需分佈的加密訊息之長度等於O(k)，且需分佈的個人密鑰之大小等於O(l)，故亦滿足要求3。

另外，該具體實施例之架構使解密係藉由執行模指數運算兩次來完成，故亦滿足要求4。

下面將闡明該具體實施例亦滿足其餘的要求2。

首先，以要求2中所說明的利用「k」個除外之用戶終端所擁有的個人密鑰之一攻擊者為模型。該攻擊者的行為可模擬為一演算法M_1，其根據截至第「R」輪已遭除外之「k」個成員所擁有的解密密鑰以及截至第「R」輪所接收的資訊在第「R」輪中於多項式時間內決定一群組密鑰。不失一般性，假定將(*「k」)個除外之用戶終端20定義為用戶終端「i」(i=1,...,k)。M_1的一輸入為$<g, p, q, k, U_0, (s_1,...,s_k), (f_{11},...,f_{1k}), (H_1, C_1), (H_R, C_R)>$。

當如上所述模擬攻擊者的行為時，可利用決策Diffie-Hellman (DDH)問題將要求2替換為如下所述：

(命題)

「只要不存在於多項式時間內解決DDH問題的演算法，即不會存在M_1。」

DDH問題係一判斷問題：當隨機選擇一集合GF(q)之元素g、h以及元素a、$b \in Z_q$時，存在極大的可能性將$D=<g, h, g^a, h^a>$(此形式稱作「Diffie-Hellman對」)與$R=<g, h, g^a, h^a>$在GF(q)上區別。於多項式時間內解決DDH問題的演算法尚未發現。即此問題係一數學問題，其計算複雜度太大，故可假定該問題很難解決，且根據上述命題可知M_1不存在。因此，該具體實施例滿足要求2。

如上所述，於依據本發明之廣播類型密鑰通信系統中利

用用於共享群組密鑰之方法，當更新一群組密鑰時可以一認證方式保持安全，且可藉由於分佈該群組密鑰之前作為預計算對該群組密鑰實施一部分解密，然後於分佈該更新之群組密鑰之後僅執行模指數運算兩次即完成解密，模指數運算的執行次數並不取決於代表用戶終端的數量之數字「n」以及代表目的除外終端的最大數量之數字「k」。因此，該方法在包含大量用戶終端20於其中的網路系統中特別有效。

下面接著說明藉由將依據本發明之廣播類型密鑰通信系統應用於各種網路系統所構建的範例。

[點對點系統中的群組成員之管理]

該具體實施例可應用於一點對點(P2P)網路系統中，用以於一群組之內以一安全的方式高速執行通信。即網路系統中的一群組內所有對等點(peer)共享一密鑰(群組密鑰)且執行廣播類型密鑰通信。

圖3為說明採用該具體實施例之一點對點網路系統之組態的圖式。如圖3所示，在該網路系統中，問題中的一群組管理者組成該具體實施例之密鑰分佈伺服器10，且該群組內的個別對等點組成用戶終端20。

在上述網路系統中，當一具體的對等點以與一成員利用「leave(離開)」命令離開「jxta」相同的方式離開該群組時，為在該對等點離開該群組之後在該群組內執行安全的通信，即要求其餘的對等點儘快地再次共享一新的群組密鑰。同時，因各種終端皆可成為該點對點網路系統中的一對等

點，故該系統之架構需使：即便是計算能力極其有限的一終端亦可容易地獲得該群組密鑰。在此種點對點網路系統中可採用該具體實施例，用以管理群組內的成員。

當採用該具體實施例時，因群組密鑰之解密可藉由執行模指數乘法2次即全部完成，故群組內的終端並不需要具有很強的計算能力。另外，即使將該具體實施例應用於大規模的網路中，亦可高速更新群組密鑰，而不會喪失需利用的效率。

[即時內容分佈系統]

隨遊戲機變得越來越複雜，藉由設定一點對點網路組態所形成的高級線上遊戲亦隨之出現，其中各遊戲機係界定為一對等點。即對應於一群組管理者之一伺服器將遊戲內容提供給個別遊戲機，然後使用者利用遊戲機執行點對點通信來參與遊戲。

圖4為說明採用該具體實施例之一即時內容分佈系統之組態的圖式。如圖4所示，用於分佈遊戲內容的一伺服器組成該具體實施例之密鑰分佈伺服器10，且個別遊戲機組成用戶終端20。

在此種狀況下，雖然吾人預期廣播類型密鑰通信需在一群組內頻繁地執行，但吾人亦預期放棄群組會員資格的情況亦會頻繁地發生。例如，拖欠會員費之使用者必須與群組斷線。因此，減少用以與其餘成員共享群組密鑰之解密(當一成員退出群組時即要求執行此操作)的執行時間，可保證應用程式的高效率運行。

依據該具體實施例之廣播類型密鑰通信系統具有高速解密能力，且可應用於大規模網路，因此，其可應用於圖4所示之系統中的內容分佈。即該具體實施例之系統允許高速共享群組密鑰，且允許在接收到內容後，即可解密藉由群組密鑰所加密之內容，即即時解密。另外，耗時的密鑰更新可於接收到內容之後利用內容處理時的過剩處理能力執行。請注意，雖然在所說明的範例中通信的執行係用於分佈執行線上遊戲的內容，但毋庸贅述，依據該具體實施例之該廣播類型密鑰通信系統亦可應用於除遊戲內容之外的各種需即時執行的內容之分佈。

[分佈資料至可攜式電話用戶]

近年來，可攜式電話迅速普及，現在本國有超過一半的人口使用及擁有可攜式電話。假定將一項密鑰群組通信服務提供給數百萬可攜式電話用戶的情況。例如，該情況包括將一項具體服務提供給組成一群組之終端的情況。

圖5為顯示應用該具體實施例之用於可攜式電話之一服務提供系統之組態的圖式。如圖5所示，用於提供服務的一伺服器組成一密鑰分佈伺服器10，且註冊使用該服務的可攜式電話組成用戶終端20。

在如此設定組態之網路系統中，當一用戶拖欠會員費或其終端丟失或失盜時，即要撤銷其對一群組的存取許可，因該等許可係提供給特定的終端。依據該具體實施例，即便是計算能力很弱的可攜式電話亦可執行該廣播類型密鑰通信，只要將本發明應用於其中。

[多媒體內容分佈系統]

近年來，利用DVD之多媒體內容分佈系統獲得爆炸性推廣。

圖6為顯示依據該具體實施例所構建之一多媒體內容分佈系統之組態圖。如圖6所示，提供多媒體內容之內容提供者組成該密鑰分佈伺服器10，且用於複製該等多媒體內容之複製機組成用戶終端20。

在該系統中，可分佈儲存有加密數位內容(例如電影、音樂及軟體)於其中之DVD媒體。該等加密之內容係利用儲存於該複製機所包含之一解密器/複製器中的一解密密鑰來解密。該解密密鑰依據個別製造者而不同，且係儲存於解密器/複製器之一安全記憶體區域中。然而，解密密鑰有遭洩漏的危險，當駭客分析加密密鑰或一製造者未能正確製作密鑰時，即可看到此種情況。在此狀況下，即需要提供一種使某些加密密鑰不可用的密鑰演算法。

當採用該具體實施例時，可以一認證方式保持安全，且可執行加密密鑰的更新，從而使某些加密密鑰不可用。

[用以解決警方無線電收發器丟失/失盜問題的秘密廣播系統]

警方無線電係於一群組內進行機密通信的典型範例。在此情形中，用於機密通信之一系統需構建成使得：即使利用一無線電接收器(警官所擁有的收發器除外)，亦不能監控該等通信。

圖7為顯示採用該具體實施例之一秘密通信系統之組態

圖。如圖7所示，用於秘密廣播之一廣播台組成該密鑰分佈伺服器10，且個別無線電接收器組成用戶終端20。

如以上所述，執行諸如警方無線電通信等秘密廣播需使得即使利用一無線電接收器(警官所擁有的收發器除外)，亦不能監控通信。然而，萬一一警官的收發器丟失或失盜，該丟失或失盜之收發器即自由用戶終端20所組成之群組中除外，然後其餘的用戶終端依據該具體實施例共享一新群組密鑰，從而使該丟失之收發器不可用。

[本發明之優點]

如以上所述，依據本發明，可提供一種用於以高度可靠的方式高速更新一群組密鑰之方法。

另外，依據本發明，可實現高度安全且高度有效的廣播類型密鑰通信。

【圖式簡單說明】

圖1為說明依據該具體實施例之一廣播類型密鑰通信系統之一般組態的圖式。

圖2為說明依據該具體實施例如何執行密鑰通信之流程圖。

圖3為說明採用該具體實施例之一點對點網路系統之組態的圖式。

圖4為說明採用該具體實施例之一即時內容分佈系統之組態的圖式。

圖5為說明採用該具體實施例、用以向可攜式電話提供服務之一系統之組態的圖式。

圖6為說明採用該具體實施例、用以分佈多媒體內容之一系統之組態的圖式。

圖7為說明採用該具體實施例之一秘密廣播系統之組態的圖式。

【圖式代表符號說明】

10　密鑰分佈伺服器

20　用戶終端

伍、中文發明摘要：

本發明揭示一種用於以高度安全的方式高速更新一群組密鑰之方法。

該方法包含：於分佈該群組密鑰之前使用戶終端對用於解密該資訊之加密群組密鑰進行一部分解密之步驟；將該群組密鑰及用於對該群組密鑰執行不同於該部分解密之一部分其餘的解密，且對應於終端裝置之個別解密資訊分佈給該等用戶終端之步驟；以及使該等用戶終端利用所分佈之該解密資訊及藉由對該群組密鑰實施一部分解密所獲得的結果，對該群組密鑰執行解密之步驟，該部分解密係先前已實施。

陸、英文發明摘要：

[Object] To provide a method for updating a group key in a highly secure manner and at high speed.

[Constitution] A method includes: a step of making subscriber terminals perform a part of decryption of an encrypted group key used to decrypt the information before distribution of the group key; a step of distributing the group key and individual decryption information used to perform a part of remaining decryption other than the part of decryption of the group key and corresponding to terminal devices to the subscriber terminals; and a step of making the subscriber terminals perform decryption of the group key using the decryption information being distributed and results obtained by implementing a part of decryption of the group key, the part of decryption previously being performed.

拾壹、圖式：

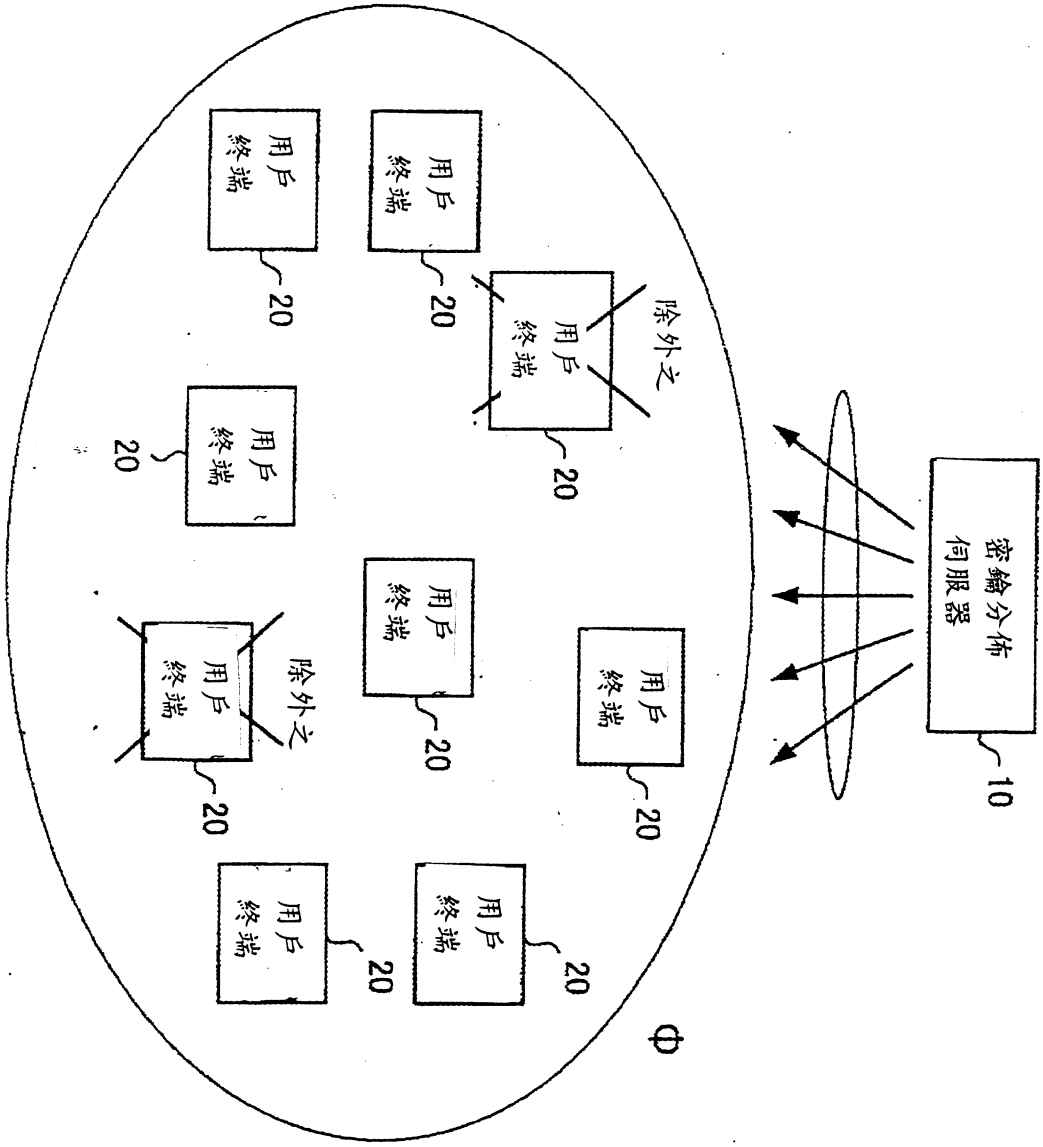
密鑰分佈
伺服器
10
除外之
用戶
終端
20
用戶
終端
20
用戶
終端
20
用戶
終端
20
用戶
終端
20
用戶
終端
20
除外之
用戶
終端
20
用戶
終端
20
用戶
終端
20
Φ

圖 1

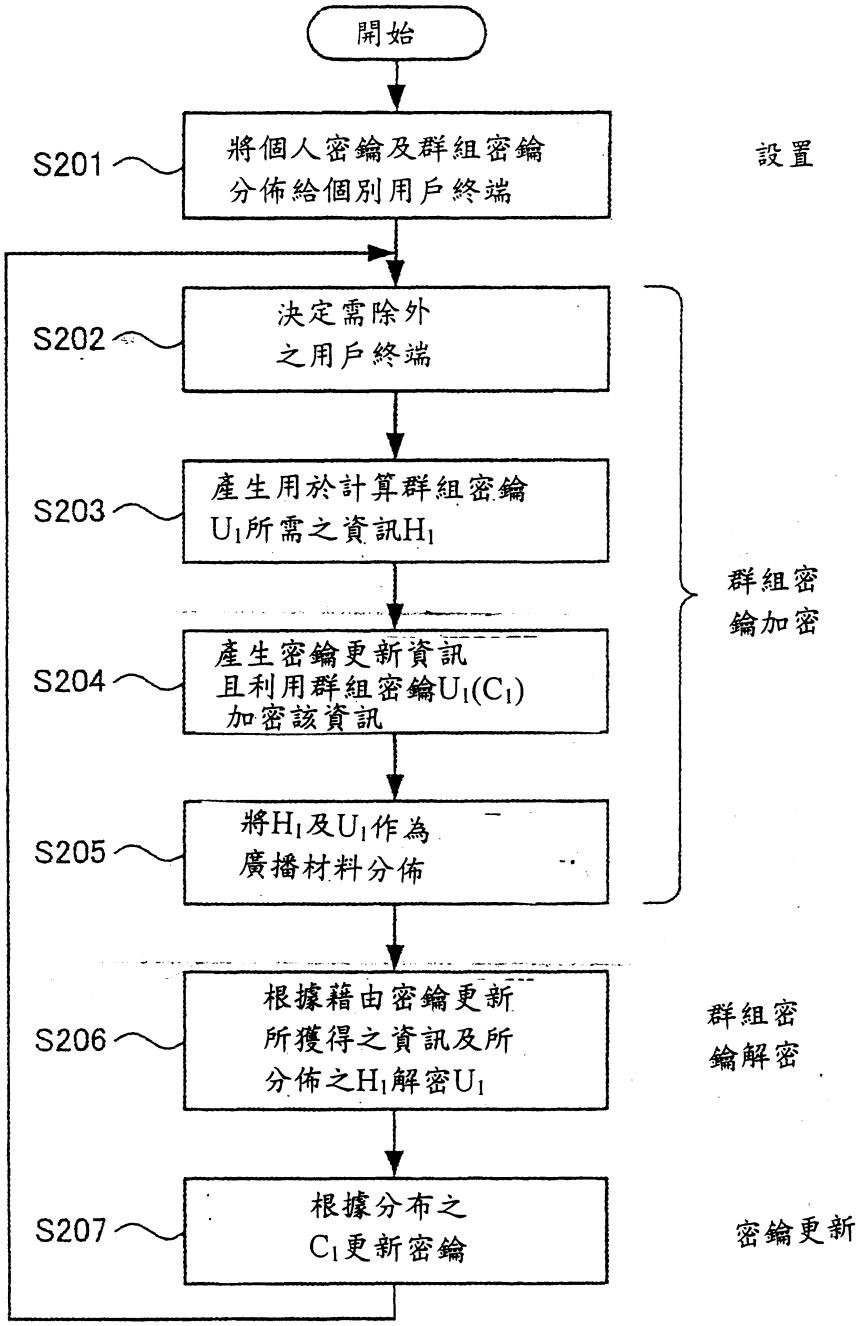
開始
S201
將個人密鑰及群組密鑰
分佈給個別用戶終端
設置
S202
決定需除外
之用戶終端
S203
產生用於計算群組密鑰
U_1所需之資訊H_1
S204
產生密鑰更新資訊
且利用群組密鑰$U_1(C_1)$
加密該資訊
S205
將H_1及U_1作為
廣播材料分佈
群組密
鑰加密
S206
根據藉由密鑰更新
所獲得之資訊及所
分佈之H_1解密U_1
群組密
鑰解密
S207
根據分布之
C_1更新密鑰
密鑰更新

圖 2

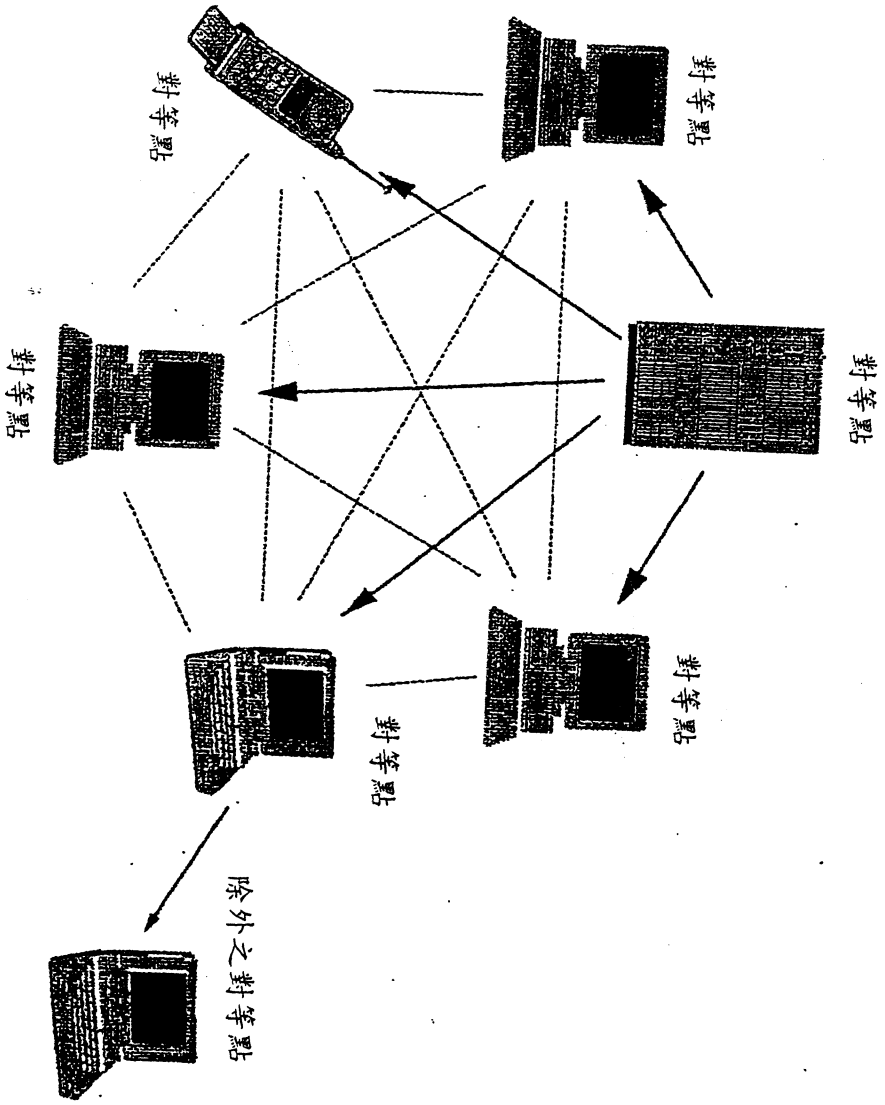

圖 3

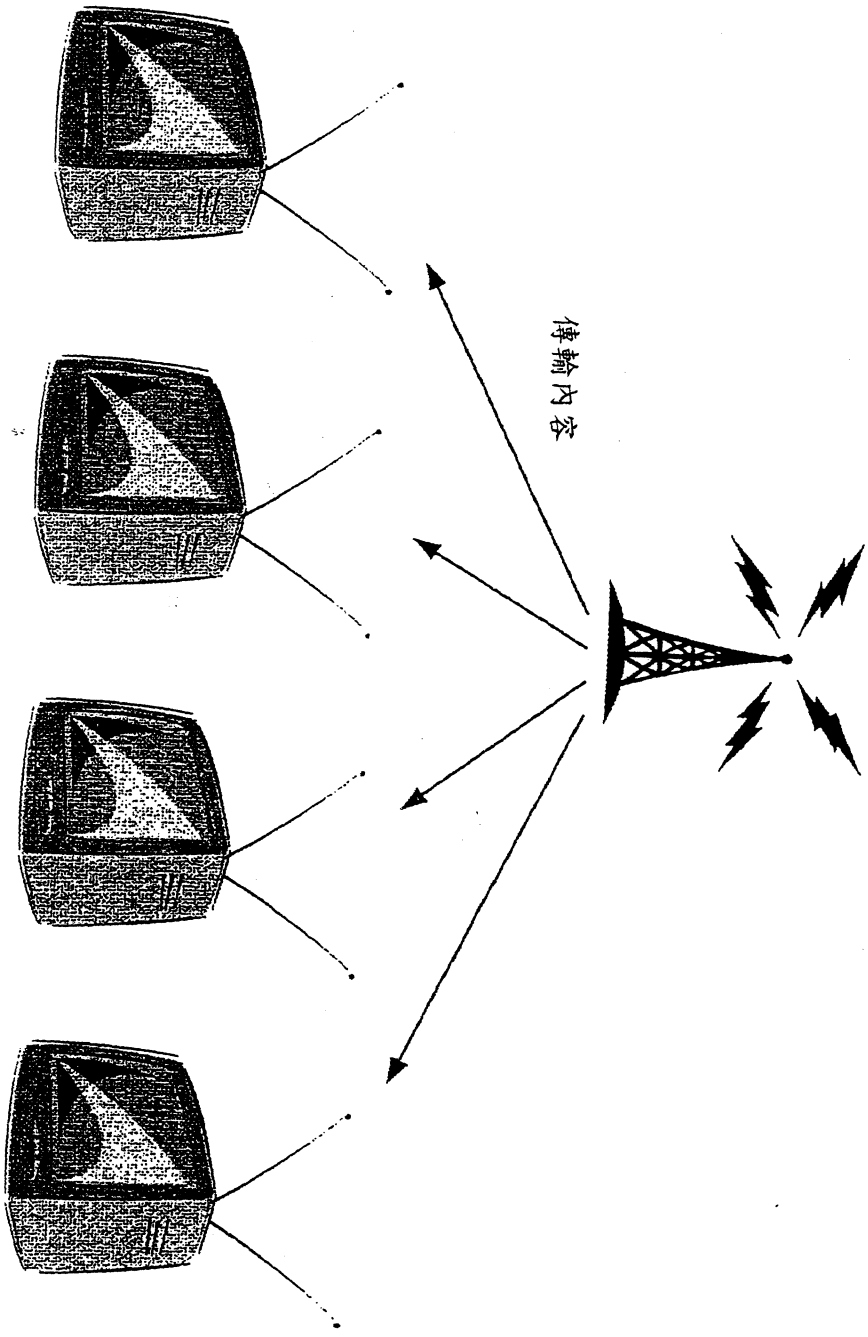

圖4

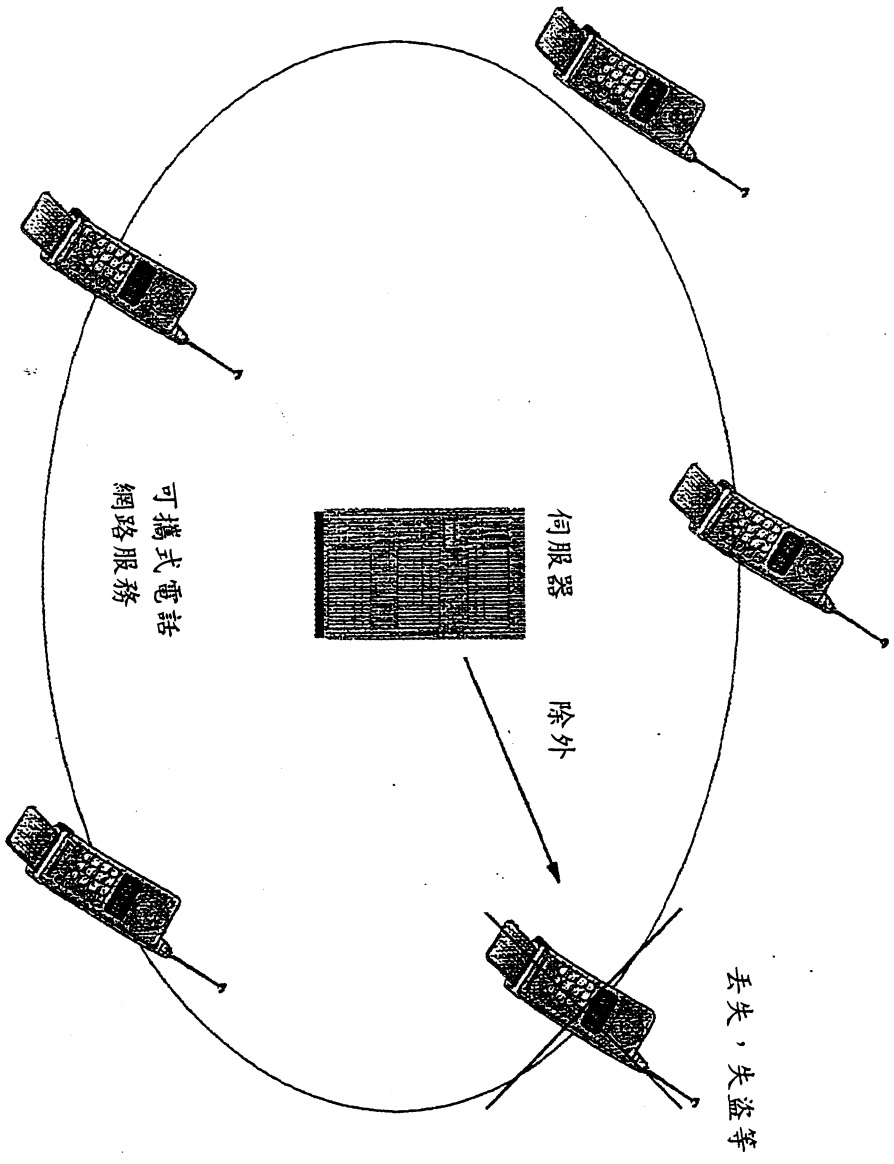

圖 5

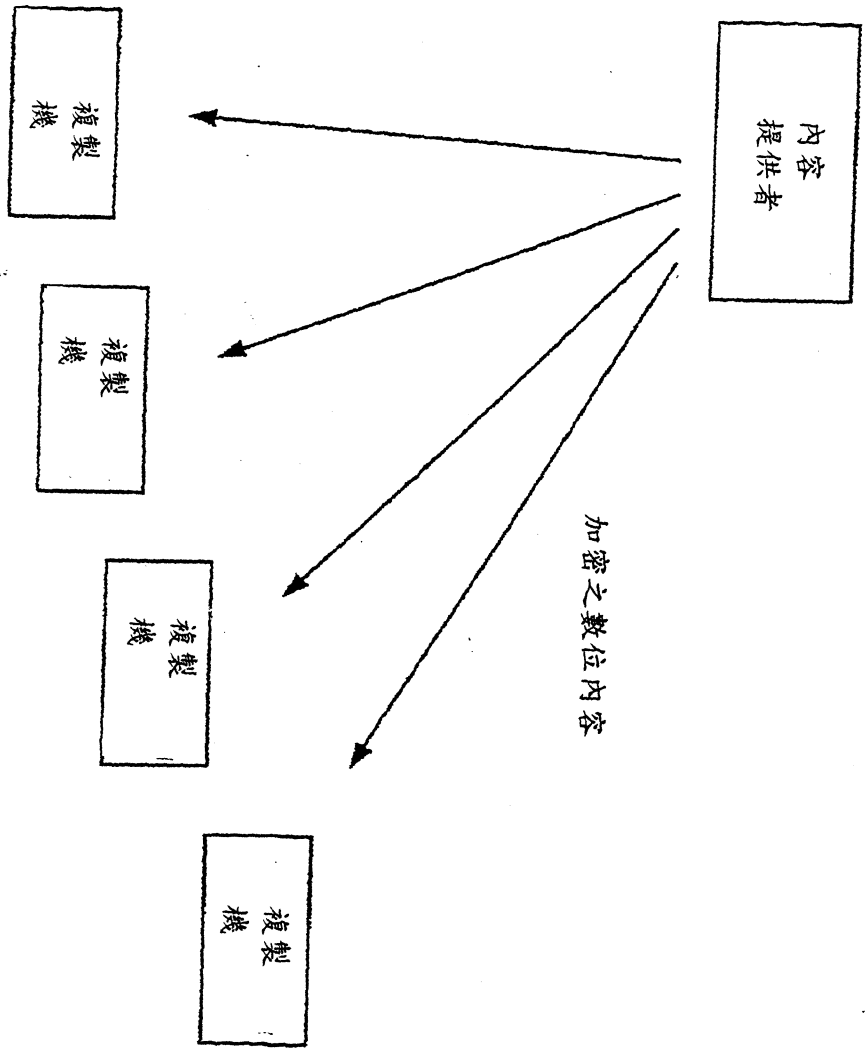

圖 6

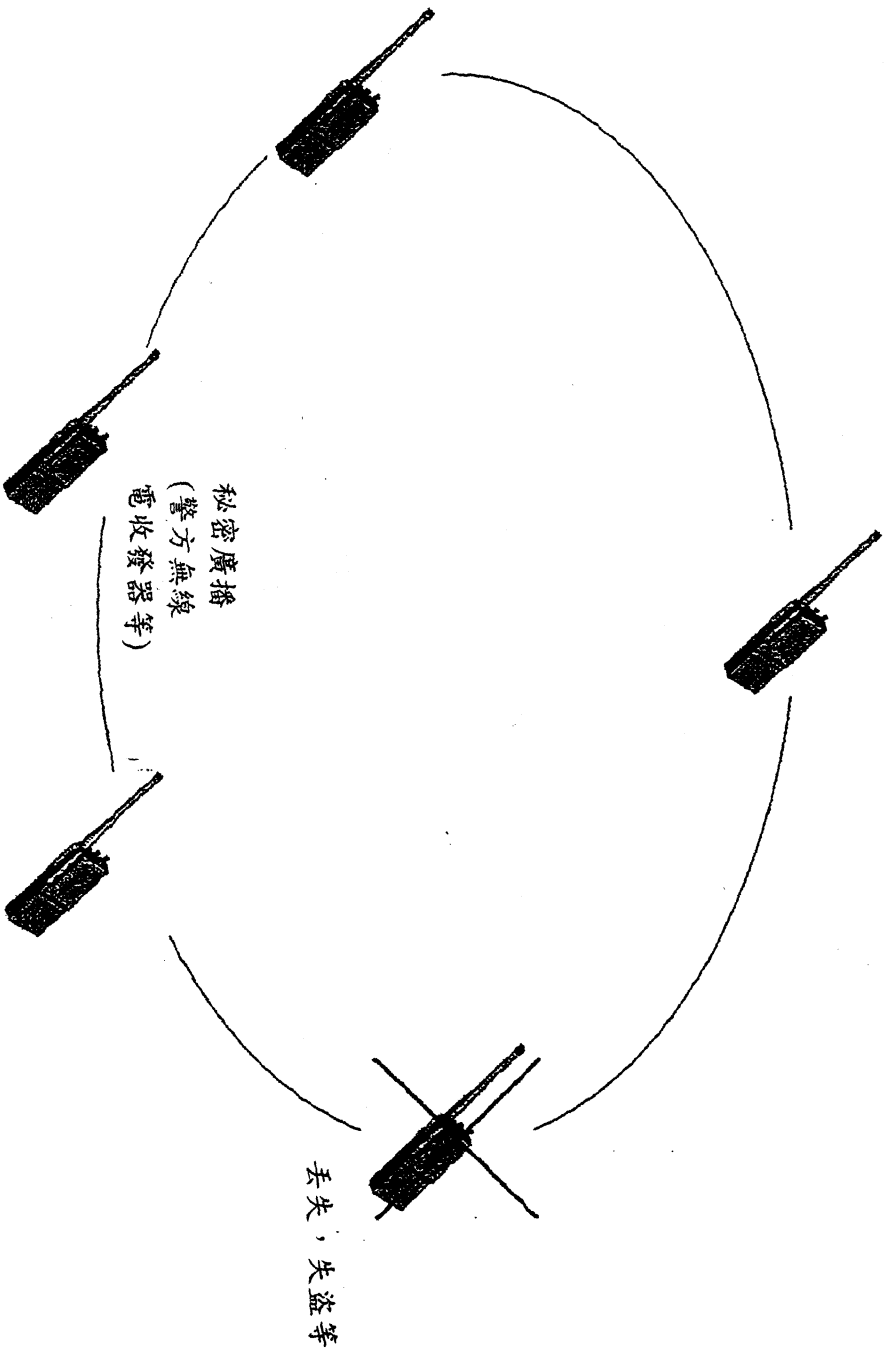

圖 7

柒、指定代表圖：

(一)本案指定代表圖為：第(2)圖。

(二)本代表圖之元件代表符號簡單說明：

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

拾、申請專利範圍：

1. 一種加密通信系統，其包含：

一密鑰分佈伺服器，用以分佈用於解密加密之資訊之一密鑰；以及

利用該資訊之一具體數量的用戶終端，

其中該密鑰分佈伺服器分佈：

一加密之第一群組密鑰，其用於解密該資訊；

個別解密資訊，其對應於該等具體數量的用戶終端且用於解密該第一群組密鑰；以及

個別密鑰更新資訊，其對應於該等具體數量的用戶終端且用於對一第二群組密鑰執行一部分解密，該第二群組密鑰係於更新一群組密鑰之後得到更新，且其中該等具體數量的用戶終端利用根據先前所獲得用以解密該第一群組密鑰之該密鑰更新資訊所執行的處理操作所獲得之結果，並利用該密鑰分佈伺服器所分佈之該解密資訊解密該密鑰分佈伺服器所分佈之該第一群組密鑰。

2. 如申請專利範圍第1項之加密通信系統，其中於分佈該群組密鑰之前，該等具體數量的用戶終端對該群組密鑰實施一部分解密，該解密係利用該個別密鑰更新資訊執行。

3. 如申請專利範圍第1項之加密通信系統，其中該密鑰分佈伺服器將用以解密該第一群組密鑰之密鑰更新資訊與一第三群組密鑰一起分佈給該等具體數量的用戶終端，該第三群組密鑰係處於更新成為該第一群組密鑰之前的一狀態。

4. 如申請專利範圍第1項之加密通信系統，其中當該密鑰分佈

伺服器更新該群組密鑰，則該密鑰分佈伺服器決定在該等具體數量的用戶終端中哪些用戶終端需除外，且將該等需除外用戶終端之外的其餘用戶終端所用之該解密資訊與得到更新之該群組密鑰一起分佈給該等具體數量的用戶終端，以使該等其餘的用戶終端可解密得到更新之該群組密鑰。

5. 一種用以分佈用於解密加密之資訊的一密鑰之密鑰分佈伺服器，其包含：

用以產生用於解密該資訊之一第一群組密鑰及加密該第一群組密鑰之構件；

用以產生用於解密該第一群組密鑰且對應於用戶終端之個別解密資訊之構件；

用以產生用於對一第二群組密鑰執行一部分解密且對應於該等用戶終端之個別密鑰更新資訊，該第二群組密鑰係於更新一群組密鑰之後得到更新之構件；以及

用以將該第一群組密鑰、該解密資訊及該密鑰更新資訊分佈給該等用戶終端之構件。

6. 如申請專利範圍第5項之密鑰分佈伺服器，其中用以產生該解密資訊之該構件決定在該等用戶終端中哪些終端需除外，且產生該等需除外之用戶終端之外的其餘用戶終端所用之該解密資訊，以使該等其餘用戶終端能解密該群組密鑰。

7. 一種終端裝置，其包含：

用以自一具體密鑰分佈伺服器擷取用於解密加密之資

訊的一加密之群組密鑰及用於解密該群組密鑰之解密資訊之構件；

用以於分佈該群組密鑰之前對該群組密鑰執行一部分解密之構件；以及

利用根據對該群組密鑰之一部分解密所執行的處理操作所獲得之結果及自該密鑰分佈伺服器所擷取之該解密資訊解密該群組密鑰之構件。

8. 一種將用以控制一電腦及然後分佈用於解密加密之資訊的一密鑰之一程式記錄於其上之記錄媒體，該程式係製成為可藉由該電腦讀取，從而使該電腦具有藉由使用該程式所實現之能力，該程式包含：

產生用於解密該資訊之一第一群組密鑰及加密該第一群組密鑰之功能；

產生用於解密該第一群組密鑰且對應於用戶終端之個別解密資訊之功能；

產生用於對一第二群組密鑰執行一部分解密且對應於該等用戶終端之個別密鑰更新資訊，該第二密鑰係於更新一群組密鑰之後得到更新之功能；以及

將該第一群組密鑰、該解密資訊及該密鑰更新資訊經由具體的通信構件分佈給該等用戶終端之功能。

9. 如申請專利範圍第8項之記錄媒體，其中產生個別解密資訊之該功能決定在該等用戶終端中哪些用戶終端需除外，且產生該等需除外之用戶終端外的其餘用戶終端所用之該解密資訊，以使該等其餘用戶終端能解密該群組密鑰。

10.一種將用以控制一電腦及然後實現一具體功能之一程式記錄於其上之記錄媒體，該程式係製成為可藉由該電腦讀取，從而使該電腦具有藉由使用該程式所實現之能力，該程式包含：

經由具體的通信構件自一具體的密鑰分佈伺服器擷取用於解密加密之資訊的一加密之群組密鑰及用於解密該群組密鑰之解密資訊之功能；

於分佈該群組密鑰之前對該群組密鑰執行一部分解密之功能；以及

利用根據對該群組密鑰之一部分解密所執行的處理操作所獲得之結果及自該密鑰分佈伺服器所擷取之該解密資訊解密該群組密鑰之功能。

11.一種用以使一具體數量的用戶終端共享用於解密加密之資訊的一密鑰之密鑰共享方法，該等具體數量之終端使用該資訊，該方法包含：

於分佈該群組密鑰之前使該等具體數量的終端對用於解密該資訊之一加密之群組密鑰執行一部分解密之步驟；

將該群組密鑰及用於對該群組密鑰執行不同於該部分解密之一部分其餘的解密且對應於該等具體數量的終端之個別解密資訊分佈給該等具體數量的終端之步驟；以及

使該等具體數量的終端利用所分佈之該解密資訊及藉由對該群組密鑰執行一部分解密，即先前所執行的該部分解密所獲得的結果對該群組密鑰執行解密之步驟。

12.如申請專利範圍第11項之密鑰共享方法，其中用於執行該部分解密之資訊係於分佈該群組密鑰之前與該群組密鑰一

起分佈給該等具體數量的終端，該群組密鑰係處於獲更新前的一狀態。