【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I672932

【45】公告日： 中華民國 108 (2019) 年 09 月 21 日

【51】Int. Cl.：　*H04L9/14　(2006.01)*　　*H04L9/28　(2006.01)*

發明　　全 15 頁

【54】名　稱：基於質數陣列的後量子非對稱密鑰產生方法及系統、加密方法、解密方法及加密通訊系統

【21】申請案號：107134068　　【22】申請日： 中華民國 107 (2018) 年 09 月 27 日

【72】發 明 人： 龐　德沙 (GT) PONTAZA RODAS, RICARDO NEFTALI；林盈達 (TW) LIN, YING-DAR

【71】申 請 人： 國立交通大學　NATIONAL CHIAO TUNG UNIVERSITY

新竹市東區大學路 1001 號

【74】代 理 人： 高玉駿；楊祺雄

【56】參考文獻：

CN　108173651A　　US　2017/0324554A1

I. Gorbenko, O. Kachko, M. Yesina and O. Akolzina, "Post-quantum algorithm of asymmetric encryption and its basic properties," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 265-270, 2018(2018/05/24-27).

Jie-Ren Shih et al., "Securing M2M With Post-Quantum Public-Key Cryptography," in IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 3, no. 1, pp. 106-116, March 2013.

M. S. Alam, "Secure M-commerce data using post quantum cryptography," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 649-654, 2017.

A. J. Gabriel, B. K. Alese, A. O. Adetunmbi and O. S. Adewale, "Post-Quantum Crystography: A combination of Post-Quantum Cryptography and Steganography," 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), pp. 449-452, 2013.

A. Vambol, V. Kharchenko, O. Potii and N. Bardis, "McEliece and Niederreiter Cryptosystems Analysis in the Context of Post-Quantum Network Security," 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), pp. 134-137, 2017.

Xiangdong Li, Lin Leung, Kwan, Xiaowen Zhang, Kahanda and Anshel, "Post-Quantum Diffie-Hellman and Symmetric Key Exchange Protocols", Proceedings of the 2006 IEEE Workshop on Information Assurance, West Point, NY, pp. 382-383, 2006.

審查人員：黃偉倫

【57】申請專利範圍

1. 一種後量子非對稱密鑰產生方法，藉由一處理單元來實施，包含以下步驟：(A)根據作為一亂數種子的一算術函數或一古典字串、及一質數 p，產生一相關於該質數 p 且具有無限個成分的質數向量 $\overrightarrow{f}_p$，該質數向量 $\overrightarrow{f}_p$ 被表示成 $\overrightarrow{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$；(B)根據該質數向量 $\overrightarrow{f}_p$，產生一相關於該質數 p 以及三個均為正整數之參數 m，s，t 的質數陣列 $\overleftrightarrow{f}_p\big|_{s,t}^{m}$，其中該質數 p 及該等參數 s，t 構成一第一參數集 I，且該質數陣列 $\overleftrightarrow{f}_p\big|_{s,t}^{m}$ 被定義為

$$\overleftrightarrow{f}_p\big|_{s,t}^{m} := \sum_{i=0}^{t}\left[f\left(p^{s+im}\right), \ldots, f\left(p^{s+im+(m-1)}\right)\right]$$

，並且當該第一參數集 I 中該質數 p 與該等參數 s，t 之數值被決定時，該質數陣列 $\overleftrightarrow{f}_p\big|_{s,t}^{m}$ 被簡化地表示成 $\overleftrightarrow{f}\big|^{m}$；(C)根據步驟(B)所產生的該質數陣列 $\overleftrightarrow{f}\big|^{m}$，產生一相關矩陣 $\left[\overleftrightarrow{f}\big|^{m}\right]$，該相關矩陣 $\left[\overleftrightarrow{f}\big|^{m}\right]$ 被表示成

$$\left[\overleftrightarrow{f}\big|^{m}\right] = \begin{pmatrix} \overleftrightarrow{f}\big|^{m}(0) & \overleftrightarrow{f}\big|^{m}(1) & \cdots & \overleftrightarrow{f}\big|^{m}(m-1) \\ \overleftrightarrow{f}\big|^{m}(m-1) & \overleftrightarrow{f}\big|^{m}(0) & \cdots & \overleftrightarrow{f}\big|^{m}(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ \overleftrightarrow{f}\big|^{m}(1) & \overleftrightarrow{f}\big|^{m}(2) & \cdots & \overleftrightarrow{f}\big|^{m}(0) \end{pmatrix}$$

，其中 $\overleftrightarrow{f}\big|^{m}$(j)代表該質數陣列 $\overleftrightarrow{f}\big|^{m}$ 的 m 個成分其中的第(j+1)個成分，且 0≤j≤(m-1)；(D)根據步驟(C)所產生的該相關矩陣 $\left[\overleftrightarrow{f}\big|^{m}\right]$、及一為一正整數的模數 l，產生該質數陣列 $\overleftrightarrow{f}\big|^{m}$ 對於該模數 l 的一反質數陣列 $\overleftrightarrow{F}_\ell\big|^{m}$，該反質數陣列 $\overleftrightarrow{F}_\ell\big|^{m}$ 被表示成 $\overleftrightarrow{F}_\ell\big|^{m} := \left(L_\ell[1,0,\cdots,0]\left[\overleftrightarrow{f}\big|^{m}\right]^*\right) \pmod{\ell}$，其中 L_l 代表該相關矩陣 $\left[\overleftrightarrow{f}\big|^{m}\right]$ 的行列式值對於該模數 l 的一模反元素且被表示成 $L_\ell := \left(\det\left[\overleftrightarrow{f}\big|^{m}\right]\right)^{-1} \pmod{\ell}$，及 $\left[\overleftrightarrow{f}\big|^{m}\right]^*$ 代表該相關矩陣 $\left[\overleftrightarrow{f}\big|^{m}\right]$ 的一伴隨矩陣；(E)任意選擇一第一參考質數 p_1，並根據一相關於該第一參考質數 p_1、該質數陣列 $\overleftrightarrow{f}\big|^{m}$ 的該等 m 個成分其中一個最大成分 b、一第一參考正整數 $\tilde{a}$，以及一由該參數 m、一第二參考正整數 $\tilde{b}$ 及一第三參考正整數 r 所構成的第二參數集 S 的預定條件決定出一符合於該預定條件的第二參考質數 p_2，其中該預定條件包含 $p_2>\max(p_1 m_{\tilde{a}}^{\tilde{b}}, mbr)$；(F)藉由分別將該第一參考質數 p_1 及該第二參考質數 p_2 作為該模數 l 代入步驟(D)所產生的該反質數陣列 $\overleftrightarrow{F}_\ell\big|^{m}$，以分別獲得一作為一私鑰 $K_{private}$ 的第一參考反質數陣列 $\overleftrightarrow{F}_{p_1}\big|^{m}$ 及一第二參考反質數陣列 $\overleftrightarrow{F}_{p_2}\big|^{m}$，其中

$K_{\text{private}} = \left(\overleftrightarrow{f} \middle|^{m}, p_1, \tilde{a} \right)$；及(G)根據步驟(F)所獲得的該第二參考反質數陣列 $\overleftrightarrow{F}_{p_2} \middle|^{m}$、該第一參考質數 p_1、該第二參考質數 p_2、及一具有 m 個介於 0 到該第一參考正整數$\tilde{a}$的數字成分的密鑰隨機陣列 $\overleftrightarrow{R} \middle|_{(\tilde{a})}^{m}$，產生一相對於該密鑰隨機陣列 $\overleftrightarrow{R} \middle|_{(\tilde{a})}^{m}$且與該私鑰 K_{private} 成對的公鑰 K_{public}，該公鑰 K_{public} 為一具有 m 個數字成分的陣列 $\overleftrightarrow{K}_{\text{public}} \middle|^{m}$ 且被表示成 $K_{\text{public}} = \left(\overleftrightarrow{K}_{\text{public}} \middle|^{m}, p_2 \right)$及 $\overleftrightarrow{K}_{\text{public}} \middle|^{m} := \text{Rand}\left(\overleftrightarrow{F}_{p_2} \middle|^{m}, p_1, \tilde{a} \right) \pmod{p_2}$，其中 Rand($\overleftrightarrow{F}_{p_2} \middle|^{m}$,$p_1$,$\tilde{a}$)被定義為該第二參考反質數陣列 $\overleftrightarrow{F}_{p_2} \middle|^{m}$相關於該密鑰隨機陣列 $\overleftrightarrow{R} \middle|_{(\tilde{a})}^{m}$的密鑰隨機化函數，並被表示成 $\text{Rand}\left(\overleftrightarrow{F}_{p_2} \middle|^{m}, p_1, \tilde{a} \right) = p_1 \left(\overleftrightarrow{F}_{p_2} \middle|^{m} \circledast \overleftrightarrow{R} \middle|_{(\tilde{a})}^{m} \right)$，其中⊛代表一卷積運算子。

2. 一種加密方法，藉由一處理器來實施，包含以下步驟：利用請求項 1 所述的後量子非對稱密鑰產生方法中的該公鑰 K_{public} 與該第二參考質數 p_2 以及一具有 m 個介於 0 到請求項 1 所述的非對稱密鑰產生方法中的該第二參考正整數$\tilde{b}$的數字成分的加密隨機陣列 $\overleftrightarrow{R} \middle|_{(\tilde{b})}^{m}$，對於一對應於一要被傳送的明文訊息且具有 m 個數字成分的資料陣列$\overleftrightarrow{M} \middle|^{m}$進行一加密程序，以獲得一相對於該加密隨機陣列 $\overleftrightarrow{R} \middle|_{(\tilde{b})}^{m}$且具有 m 個加密數字成分的密文陣列$\overleftarrow{Cipher} \middle|^{m}$。

3. 如請求項 2 所述的加密方法，該明文訊息具有 m 個字符，其中，該資料陣列$\overleftrightarrow{M} \middle|^{m}$的該等 m 個數字成分其中每一者係介於 0 到請求項 1 所述的非對稱密鑰產生方法中的該第一參考正整數$\tilde{a}$，並代表該等 m 個字符其中一對應的字符。

4. 如請求項 2 所述的加密方法，其中，該加密程序包含：根據該公鑰 K_{public} 及該加密隨機陣列 $\overleftrightarrow{R} \middle|_{(\tilde{b})}^{m}$，產生該公鑰 K_{public} 相關於該加密隨機陣列 $\overleftrightarrow{R} \middle|_{(\tilde{b})}^{m}$的一加密隨機化函數 $\overleftrightarrow{R} \middle|^{m}$，該加密隨機化函數 $\overleftrightarrow{R} \middle|^{m}$被表示成 $\overleftrightarrow{R} \middle|^{m} := \text{Rand}\left(\overleftrightarrow{K}_{\text{public}} \middle|^{m}, 1, \tilde{b} \right)$；及將該資料陣列 $\overleftrightarrow{M} \middle|^{m}$與該加密隨機化函數 $\overleftrightarrow{R} \middle|^{m}$相加之和模除該第二參考質數 p_2 而獲得該密文陣列 $\overleftarrow{Cipher} \middle|^{m}$，該密文陣列 $\overleftarrow{Cipher} \middle|^{m}$ 被表示成 $\overleftarrow{Cipher} \middle|^{m} := \left(\overleftrightarrow{M} \middle|^{m} + \overleftrightarrow{R} \middle|^{m} \right) \pmod{p_2}$。

5. 一種解密方法，藉由一處理器來實施，包含以下步驟：利用請求項 1 所述的後量子非對稱密鑰產生方法中的該質數陣列 $\overleftrightarrow{f} \middle|^{m}$、該私鑰 K_{private}、該第一參考質數 p_1 及該第二參

考質數 p_2，對於經由請求項 2 所述的加密方法所產生的該密文陣列 $\overleftrightarrow{Cipher}\Big|^m$ 進行一解密程序，以獲得一具有 m 個解密數字成分的明文陣列 $\overleftrightarrow{M_1}\Big|^m$。

6. 如請求項 5 所述的解密方法，其中，該解密程序包含：將該密文陣列 $\overleftrightarrow{Cipher}\Big|^m$ 與該質數陣列 $\overleftrightarrow{f}\Big|^m$ 的一第一卷積運算結果模除該第二參考質數 p_2 而獲得一第一模除結果，並將該第一模除結果模除該第一參考質數 p_1 而獲得一第二模除結果 $\overleftrightarrow{M_0}\Big|^m$，該第二模除結果 $\overleftrightarrow{M_0}\Big|^m$ 被表示成 $\overleftrightarrow{M_0}\Big|^m := \left[\left(\overleftrightarrow{Cipher}\Big|^m \circledast \overleftrightarrow{f}\Big|^m\right) \pmod{p_2}\right] \pmod{p_1}$；及將該第二模除結果 $\overleftrightarrow{M_0}\Big|^m$ 與作為該私鑰 $K_{private}$ 的該第一參考反質數陣列 $\overleftrightarrow{F}_{p_1}\Big|^m$ 的一第二卷積運算結果模除該第一參考質數 p_1 而獲得該明文陣列 $\overleftrightarrow{M_1}\Big|^m$，該明文陣列 $\overleftrightarrow{M_1}\Big|^m$ 被表示成 $\overleftrightarrow{M_1}\Big|^m := \overleftrightarrow{M_0}\Big|^m \circledast \overleftrightarrow{F}_{p_1}\Big|^m \pmod{p_1}$。

7. 一種後量子非對稱密鑰產生系統，包含：一質數向量產生模組，根據作為一亂數種子的一算術函數或一古典字串、及一質數 p，產生一相關於該質數 p 且具有無限個成分的質數向量 $\overrightarrow{f}_p$，該質數向量 $\overrightarrow{f}_p$ 被表示成 $\overrightarrow{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$；一質數陣列產生模組，連接該質數向量產生模組，並根據來自該質數向量產生模組的該質數向量 $\overrightarrow{f}_p$，產生一相關於該質數 p 以及三個均為正整數之參數 m，s，t 的質數陣列 $\overleftrightarrow{f}_p\Big|^m_{s,t}$，其中該質數 p 及該等參數 s，t 構成一第一參數集 I，且該質數陣列 $\overleftrightarrow{f}_p\Big|^m_{s,t}$ 被定義為

$$\overleftrightarrow{f}_p\Big|^m_{s,t} := \sum_{i=0}^{t}\left[f\left(p^{s+im}\right), \ldots, f\left(p^{s+im+(m-1)}\right)\right]$$

，並且當該第一參數集 I 中該質數 p 與該等參數 s，t 之數值被決定時，該質數陣列 $\overleftrightarrow{f}_p\Big|^m_{s,t}$ 被簡化地表示成 $\overleftrightarrow{f}\Big|^m$；一相關矩陣產生模組，連接該質數陣列產生模組，並根據來自於該質數陣列產生模組的該質數陣列 $\overleftrightarrow{f}\Big|^m$，產生一相關矩陣 $\left[\overleftrightarrow{f}\Big|^m\right]$，該相關矩陣 $\left[\overleftrightarrow{f}\Big|^m\right]$ 被表示成

$$\left[\overleftrightarrow{f}\Big|^m\right] = \begin{pmatrix} \overleftrightarrow{f}\Big|^m(0) & \overleftrightarrow{f}\Big|^m(1) & \cdots & \overleftrightarrow{f}\Big|^m(m-1) \\ \overleftrightarrow{f}\Big|^m(m-1) & \overleftrightarrow{f}\Big|^m(0) & \cdots & \overleftrightarrow{f}\Big|^m(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ \overleftrightarrow{f}\Big|^m(1) & \overleftrightarrow{f}\Big|^m(2) & \cdots & \overleftrightarrow{f}\Big|^m(0) \end{pmatrix}$$

，其中 $\overleftrightarrow{f}\Big|^m(j)$ 代表該質數陣列 $\overleftrightarrow{f}\Big|^m$ 的 m 個成分其中的第(j+1)個成分，且 $0 \le j \le (m-1)$；一反質數陣列產生模組，連接該相關矩陣產生模組，並根據來自於該相關矩陣產生模組的

該相關矩陣$\left[\overleftrightarrow{f}\Big|^{m}\right]$、及一為一正整數的模數 *l*，產生該質數陣列$\overleftrightarrow{f}\Big|^{m}$對於該模數 *l* 的一反質數陣列$\overleftrightarrow{F}_{\ell}\Big|^{m}$，該反質數陣列$\overleftrightarrow{F}_{\ell}\Big|^{m}$被表示成

$\overleftrightarrow{F}_{\ell}\Big|^{m} := \left(L_{\ell}[1,0,\cdots,0]\left[\overleftrightarrow{f}\Big|^{m}\right]^{*}\right) \pmod{\ell}$，其中 L_l 代表該相關矩陣$\left[\overleftrightarrow{f}\Big|^{m}\right]$的行列式值對於該模數*l* 的一模反元素且被表示成$L_{\ell} := \left(\det\left[\overleftrightarrow{f}\Big|^{m}\right]\right)^{-1} \pmod{\ell}$，及$\left[\overleftrightarrow{f}\Big|^{m}\right]^{*}$代表該相關矩陣$\left[\overleftrightarrow{f}\Big|^{m}\right]$的一伴隨矩陣；一參考質數決定模組，用來先任意選擇一第一參考質數 p_1，然後並根據一相關於該第一參考質數 p_1、該質數陣列$\overleftrightarrow{f}\Big|^{m}$的該等 m 個成分其中一個最大成分 b，以及一由該參數 m、一第一參考正整數$\tilde{a}$、一第二參考正整數$\tilde{b}$及一第三參考正整數 r 所構成的第二參數集 S 的預定條件決定出一符合於該預定條件的第二參考質數 p_2，其中該預定條件包含 $p_2>\max(p_1 m\tilde{a}\tilde{b}, mbr)$；一私鑰產生模組，連接該反質數陣列產生模組及該參考質數決定模組，並將來自於該參考質數決定模組的該第一參考質數 p_1 作為該模數 *l* 代入來自於該反質數陣列產生模組的該反質數陣列$\overleftrightarrow{F}_{\ell}\Big|^{m}$以獲得一作為一私鑰 $K_{private}$ 的第一參考反質數陣列$\overleftrightarrow{F}_{p_1}\Big|^{m}$，其中$K_{private} = \left(\overleftrightarrow{f}\Big|^{m}, p_1, \tilde{a}\right)$；及一公鑰產生模組，連接該反質數陣列產生模組及該參考質數決定模組，且將來自於該參考質數決定模組的該第二參考質數 p_2 作為該模數 *l* 代入來自於該反質數陣列產生模組的該反質數陣列$\overleftrightarrow{F}_{\ell}\Big|^{m}$以獲得一第二參考反質數陣列$\overleftrightarrow{F}_{p_2}\Big|^{m}$，並根據所獲得的該第二參考反質數陣列$\overleftrightarrow{F}_{p_2}\Big|^{m}$、來自於該參考質數決定模組的該第一參考質數 p_1 與該第二參考質數 p_2、及一具有 m 個介於 0 到該第一參考正整數$\tilde{a}$的數字成分的密鑰隨機陣列$\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$，產生一相對於該密鑰隨機陣列$\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$且與該私鑰 $K_{private}$ 成對的公鑰 K_{public}，該公鑰 K_{public} 為一具有 m 個數字成分的陣列$\overleftrightarrow{K}_{public}\Big|^{m}$且被表示成

$$K_{public} = \left(\overleftrightarrow{K}_{public}\Big|^{m}, p_2\right) \text{ 且 } \overleftrightarrow{K}_{public}\Big|^{m} := \text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) \pmod{p_2},$$

其中 Rand($\overleftrightarrow{F}_{p_2}\Big|^{m}$,$p_1$,$\tilde{a}$)被定義為該第二參考反質數陣列$\overleftrightarrow{F}_{p_2}\Big|^{m}$相關於該密鑰隨機陣列$\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$的密鑰隨機化函數，並被表示成 $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) = p_1\left(\overleftrightarrow{F}_{p_2}\Big|^{m} \circledast \overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}\right)$，其中⊛代表一卷積運算子。

8. 如請求項 7 所述的後量子非對稱密鑰產生系統，還包含一儲存模組，該儲存模組連接該質數陣列產生模組、該參考質數決定模組、該私鑰產生模組及該公鑰產生模組，並儲存來自於該質數陣列產生模組的該質數陣列$\overleftrightarrow{f}\Big|^{m}$、來自該參考質數決定模組的該第一參

考質數 p_1 與該第二參考質數 p_2、來自該私鑰產生模組的該第一參考反質數陣列 $\overleftrightarrow{F}_{p_1}\Big|^{m}$、及來自該公鑰產生模組的該第二參考反質數陣列 $\overleftrightarrow{F}_{p_2}\Big|^{m}$。

9. 如請求項 8 所述的後量子非對稱密鑰產生系統，其中，該公鑰產生模組根據該儲存模組所儲存的該第二參考反質數陣列 $\overleftrightarrow{F}_{p_2}\Big|^{m}$、該第一參考質數 p_1、該第二參考質數 p_2、及另一具有 m 個介於 0 到該第一參考正整數$\tilde{a}$的數字成分且不同於該密鑰隨機陣列 $\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$ 的隨機陣列 $\overleftrightarrow{R^*}\Big|^{m}_{(\tilde{a})}$，產生一相對於該隨機陣列 $\overleftrightarrow{R^*}\Big|^{m}_{(\tilde{a})}$ 且與該私鑰 $K_{private}$ 成對的更新公鑰 K^*_{public}，該更新公鑰 K^*_{public} 被表示成 $K^*_{\text{public}} = \left(\overleftrightarrow{K^*}_{\text{public}}\Big|^{m}, p_2\right)$ 且 $\overleftrightarrow{K^*}_{\text{public}}\Big|^{m} = \text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) \pmod{p_2} = p_1\left(\overleftrightarrow{F}_{p_2}\Big|^{m} \circledast \overleftrightarrow{R^*}\Big|^{m}_{(\tilde{a})}\right) \pmod{p_2}$。

10. 一種加密通訊系統，包含：一密鑰伺服器，包括一質數向量產生模組，根據作為一亂數種子的一算術函數或一古典字串，產生一相關於一質數 p 且具有無限個成分的質數向量 $\overrightarrow{f}_p$，該質數向量 $\overrightarrow{f}_p$ 被表示成 $\overrightarrow{f}_p := [f(p^0), f(p^1), f(p^2), f(p^3), \ldots]$，一質數陣列產生模組，連接該質數向量產生模組，並根據來自該質數向量產生模組的該質數向量 $\overrightarrow{f}_p$，產生一相關於該質數 p 以及三個均為正整數之參數 m，s，t 的質數陣列 $\overleftrightarrow{f}_p\Big|^{m}_{s,t}$，其中該質數 p 及該等參數 s，t 構成一第一參數集 I，且該質數陣列 $\overleftrightarrow{f}_p\Big|^{m}_{s,t}$ 被定義為

$$\overleftrightarrow{f}_p\Big|^{m}_{s,t} := \sum_{i=0}^{t}\left[f\left(p^{s+im}\right), \ldots, f\left(p^{s+im+(m-1)}\right)\right]$$

，並且當該第一參數集 I 中該質數 p 與該等參數 s，t 之數值被決定時，該質數陣列 $\overleftrightarrow{f}_p\Big|^{m}_{s,t}$ 被簡化地表示成 $\overleftrightarrow{f}\Big|^{m}$，一相關矩陣產生模組，連接該質數陣列產生模組，並根據來自於該質數陣列產生模組的該質數陣列 $\overleftrightarrow{f}\Big|^{m}$，產生一相關矩陣 $\left[\overleftrightarrow{f}\Big|^{m}\right]$，該相關矩陣 $\left[\overleftrightarrow{f}\Big|^{m}\right]$ 被表示成

$$\left[\overleftrightarrow{f}\Big|^{m}\right] = \begin{pmatrix} \overleftrightarrow{f}\Big|^{m}(0) & \overleftrightarrow{f}\Big|^{m}(1) & \cdots & \overleftrightarrow{f}\Big|^{m}(m-1) \\ \overleftrightarrow{f}\Big|^{m}(m-1) & \overleftrightarrow{f}\Big|^{m}(0) & \cdots & \overleftrightarrow{f}\Big|^{m}(m-2) \\ \vdots & \vdots & \ddots & \vdots \\ \overleftrightarrow{f}\Big|^{m}(1) & \overleftrightarrow{f}\Big|^{m}(2) & \cdots & \overleftrightarrow{f}\Big|^{m}(0) \end{pmatrix}$$

，其中 $\overleftrightarrow{f}\Big|^{m}$(j)代表該質數陣列 $\overleftrightarrow{f}\Big|^{m}$ 的 m 個成分其中的第(j+1)個成分，且 0≤j≤(m-1)，一反質數陣列產生模組，連接該相關矩陣產生模組，並根據來自於該相關矩陣產生模組的該相關矩陣 $\left[\overleftrightarrow{f}\Big|^{m}\right]$、及一為一正整數的模數 *l*，產生該質數陣列 $\overleftrightarrow{f}\Big|^{m}$ 對於該模數 *l* 的一反質數陣列 $\overleftrightarrow{F}_{\ell}\Big|^{m}$，該反質數陣列 $\overleftrightarrow{F}_{\ell}\Big|^{m}$ 被表示成

$\overleftrightarrow{F}_{\ell}\Big|^{m} := \left(L_{\ell}[1,0,\cdots,0]\left[\overleftrightarrow{f}\Big|^{m}\right]^{*}\right) \pmod{\ell}$，其中 L_l 代表該相關矩陣$\left[\overleftrightarrow{f}\Big|^{m}\right]$的行列式值對於該模數 l 的一模反元素且被表示成 $L_{\ell} := \left(\det\left[\overleftrightarrow{f}\Big|^{m}\right]\right)^{-1} \pmod{\ell}$，及$\left[\overleftrightarrow{f}\Big|^{m}\right]^{*}$代表該相關矩陣$\left[\overleftrightarrow{f}\Big|^{m}\right]$的一伴隨矩陣，一參考質數決定模組，用來先任意選擇一第一參考質數 p_1，然後並根據一相關於該第一參考質數 p_1、該質數陣列$\overleftrightarrow{f}\Big|^{m}$的該等 m 個成分其中一個最大成分 b、一第一參考正整數 $\tilde{a}$，以及一由該參數 m、一第二參考正整數 $\tilde{b}$及一第三參考正整數 r 所構成的第二參數集 S 的預定條件決定出一符合於該預定條件的第二參考質數 p_2，其中該預定條件包含 $p_2>\max(p_1 m\tilde{a}\tilde{b}, mbr)$，一私鑰產生模組，連接該反質數陣列產生模組及該參考質數決定模組，並將來自於該參考質數決定模組的該第一參考質數 p_1 作為該模數 l 代入來自於該反質數陣列產生模組的該反質數陣列$\overleftrightarrow{F}_{\ell}\Big|^{m}$以獲得一作為一私鑰 $K_{private}$ 的第一參考反質數陣列 $\overleftrightarrow{F}_{p_1}\Big|^{m}$，其中 $K_{private} = \left(\overleftrightarrow{f}\Big|^{m}, p_1, \tilde{a}\right)$，及一公鑰產生模組，連接該反質數陣列產生模組及該參考質數決定模組，且用來將來自於該參考質數決定模組的該第二參考質數 p_2 作為該模數 l 代入來自於該反質數陣列產生模組的該反質數陣列 $\overleftrightarrow{F}_{\ell}\Big|^{m}$以獲得一第二參考反質數陣列 $\overleftrightarrow{F}_{p_2}\Big|^{m}$，並根據所獲得的該第二參考反質數陣列 $\overleftrightarrow{F}_{p_2}\Big|^{m}$、來自於該參考質數決定模組的該第一參考質數 p_1 與該第二參考質數 p_2、及一具有 m 個介於 0 到該第一參考正整數$\tilde{a}$的數字成分的密鑰隨機陣列 $\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$，產生一相對於該密鑰隨機陣列 $\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$且與該私鑰 $K_{private}$ 成對的公鑰 K_{public}，該公鑰 K_{public} 為一具有 m 個數字成分的陣列 $\overleftrightarrow{K}_{public}\Big|^{m}$且被表示成

$$K_{public} = \left(\overleftrightarrow{K}_{public}\Big|^{m}, p_2\right) \quad \text{且} \quad \overleftrightarrow{K}_{public}\Big|^{m} := \text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) \pmod{p_2},$$

其中 Rand($\overleftrightarrow{F}_{p_2}\Big|^{m}$,$p_1$,$\tilde{a}$)被定義為該第二參考反質數陣列$\overleftrightarrow{F}_{p_2}\Big|^{m}$相關於該密鑰隨機陣列 $\overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}$的密鑰隨機化函數，並被表示成 $\text{Rand}\left(\overleftrightarrow{F}_{p_2}\Big|^{m}, p_1, \tilde{a}\right) = p_1\left(\overleftrightarrow{F}_{p_2}\Big|^{m} \circledast \overleftrightarrow{R}\Big|^{m}_{(\tilde{a})}\right)$，其中⊛代表一卷積運算子；一發送端，包含一儲存有該公鑰 K_{public}、該第二參考質數 p_2 及該第二參考正整數$\tilde{b}$的儲存單元，及一電連接該儲存單元的處理器；及一接收端，包含一儲存有儲存有該私鑰 $K_{private}$、該質數陣列 $\overleftrightarrow{f}\Big|^{m}$、該第一參考質數 p_1 及該第二參考質數 p_2 的儲存單元，及一電連接該接收端的該儲存單元的處理器；其中，對於一對應於一要被發送至該接收端的明文訊息且具有 m 個數字成分的資料陣列 $\overleftrightarrow{M}\Big|^{m}$，該發送端的該處理器利用該儲存單元所儲存的該公鑰 K_{public} 與該第二參考質數 p_2、及一具有 m 個介於 0 到該第二參考正整數 $\tilde{b}$的數字成分的加密隨機陣列 $\overleftrightarrow{R}\Big|^{m}_{(\tilde{b})}$，對於該資料陣列$\overleftrightarrow{M}\Big|^{m}$進行一

加密程序，以獲得一相對於該加密隨機陣列 $\overleftrightarrow{R}\Big|_{(\tilde{b})}^{m}$ 且具有 m 個加密數字成分的密文陣列 $\overleftarrow{Cipher}\Big|^{m}$，該發送端經由一第一通訊通道，將該密文陣列 $\overleftarrow{Cipher}\Big|^{m}$ 發送至該接收端；及其中，在該接收端，該處理器在接收到來自該發送端的該密文陣列 $\overleftarrow{Cipher}\Big|^{m}$ 時，利用該儲存單元所儲存的該質數陣列 $\overleftrightarrow{f}\Big|^{m}$、該私鑰 $K_{private}$、該第一參考質數 p_1 及該第二參考質數 p_2，對於該密文陣列 $\overleftarrow{Cipher}\Big|^{m}$ 進行一解密程序，以獲得一具有 m 個解密數字成分的明文陣列 $\overleftrightarrow{M_1}\Big|^{m}$，該明文陣列 $\overleftrightarrow{M_1}\Big|^{m}$ 係完全相同於該資料陣列 $\overleftrightarrow{M}\Big|^{m}$。

11. 如請求項 10 所述的加密通訊系統，該明文訊息具有 m 個字符，其中，該發送端的該處理器係配置有一訊息轉換模組，該訊息轉換模組利用一預定字符轉數字技術，將該明文訊息轉換成該資料陣列 $\overleftrightarrow{M}\Big|^{m}$，且該資料陣列 $\overleftrightarrow{M}\Big|^{m}$ 的該等 m 個數字成分其中每一者係介於 0 到該第一參考正整數 $\tilde{a}$，並代表該等 m 個字符其中一個對應的字符。

12. 如請求項 11 所述的加密通訊系統，其中：該發送端的該處理器還配置有一加密隨機化函數產生模組、及一連接該訊息轉換模組與該加密隨機化函數產生模組的密文陣列產生模組；及在該加密程序中，該加密隨機化函數產生模組根該公鑰 K_{public}、及該加密隨機陣列 $\overleftrightarrow{R}\Big|_{(\tilde{b})}^{m}$，產生該公鑰 K_{public} 相關於該加密隨機陣列 $\overleftrightarrow{R}\Big|_{(\tilde{b})}^{m}$ 的一加密隨機化函數 $\overleftrightarrow{R}\Big|^{m}$，該加密隨機化函數 $\overleftrightarrow{R}\Big|^{m}$ 被表示成 $\overleftrightarrow{R}\Big|^{m} := \mathrm{Rand}\left(\overleftrightarrow{K}_{\mathrm{public}}\Big|^{m}, 1, \tilde{b}\right)$，並且將該資料陣列 $\overleftrightarrow{M}\Big|^{m}$ 與該加密隨機化函數 $\overleftrightarrow{R}\Big|^{m}$ 相加之和模除該第二參考質數 p_2 而獲得該密文陣列 $\overleftarrow{Cipher}\Big|^{m}$，該密文陣列 $\overleftarrow{Cipher}\Big|^{m}$ 被表示成 $\overleftarrow{Cipher}\Big|^{m} := \left(\overleftrightarrow{M}\Big|^{m} + \overleftrightarrow{R}\Big|^{m}\right) \pmod{p_2}$。

13. 如請求項 10 所述的加密通訊系統，其中：該接收端的該處理器配置有一第一卷積運算模組、及一連接該第一卷積運算模組的第二卷積運算模組；及在該解密程序中，該第一卷積運算模組計算出該密文陣列 $\overleftarrow{Cipher}\Big|^{m}$ 與該質數陣列 $\overleftrightarrow{f}\Big|^{m}$ 的一第一卷積運算結果，並將該第一卷積運算結果模除該第二參考質數 p_2 而獲得一第一模除結果，且將該第一模除結果模除該第一參考質數 p_1 而獲得一第二模除結果 $\overleftrightarrow{M_0}\Big|^{m}$，該第二模除結果 $\overleftrightarrow{M_0}\Big|^{m}$ 被表示成 $\overleftrightarrow{M_0}\Big|^{m} := \left[\left(\overleftarrow{Cipher}\Big|^{m} \circledast \overleftrightarrow{f}\Big|^{m}\right) \pmod{p_2}\right] \pmod{p_1}$，及該第二卷積運算模組計算出來自於該第一卷積運算模組的該第二模除結果 $\overleftrightarrow{M_0}\Big|^{m}$ 與該儲存單元所儲存並作為該私鑰 $K_{private}$ 的該第一參考反質數陣列 $\overleftrightarrow{F}_{p_1}\Big|^{m}$ 的一第二卷積運算結果，並將該第二卷積運算結果模除該第一參考質數 p_1 而獲得該明文陣列 $\overleftrightarrow{M_1}\Big|^{m}$，該明文陣列 $\overleftrightarrow{M_1}\Big|^{m}$ 被表示成 $\overleftrightarrow{M_1}\Big|^{m} := \overleftrightarrow{M_0}\Big|^{m} \circledast \overleftrightarrow{F}_{p_1}\Big|^{m} \pmod{p_1}$。

14. 如請求項 10 所述的加密通訊系統，其中：在該公鑰 K_{public}、第二參考質數 p_2 及該第二參考正整數 $\tilde{b}$ 被儲存於該發送端的該儲存單元之前，該密鑰伺服器將該公鑰 K_{public}、該第二參考質數 p_2 及該第二參考正整數 $\tilde{b}$ 經由一第二通訊通道傳送至該發送端，以致該發送端的該處理器將接收自該密鑰伺服器的該公鑰 K_{public}、該第二參考質數 p_2 及該第二參考正整數 $\tilde{b}$ 儲存於該發送端的該儲存單元；及在該私鑰 $K_{private}$、該質數陣列 $\left|\overleftrightarrow{f}\right|^{m}$、該第一參考質數 p_1 及該第二參考質數 p_2 被儲存於該接收端的該儲存單元之前，該密鑰伺服器將該私鑰 $K_{private}$、該質數陣列 $\left|\overleftrightarrow{f}\right|^{m}$、該第一參考質數 p_1 及該第二參考質數 p_2 經由一第三通訊通道傳送至該接收端，以致該接收端的該處理器將接收自該密鑰伺服器的該私鑰 $K_{private}$、該質數陣列 $\left|\overleftrightarrow{f}\right|^{m}$、該第一參考質數 p_1 及該第二參考質數 p_2 儲存於該接收端的該儲存單元。

15. 如請求項 14 所述的加密通訊系統，其中，該密鑰伺服器還包括一儲存模組，該儲存模組連接該質數陣列產生模組、該參考質數決定模組、該私鑰產生模組及該公鑰產生模組，並儲存分別來自於該質數陣列產生模組、該參考質數決定模組、該私鑰產生模組及該公鑰產生模組的該質數陣列 $\left|\overleftrightarrow{f}\right|^{m}$、該第一參考質數 p_1 與該第二參考質數 p_2、該第一參考反質數陣列 $\left|\overleftrightarrow{F}_{p_1}\right|^{m}$ 及該第二參考反質數陣列 $\left|\overleftrightarrow{F}_{p_2}\right|^{m}$。

16. 如請求項 15 所述的加密通訊系統，其中：該密鑰伺服器的該公鑰產生模組根據該儲存模組所儲存的該第二參考反質數陣列 $\left|\overleftrightarrow{F}_{p_2}\right|^{m}$、該第一參考質數 p_1、該第二參考質數 p_2、及另一具有 m 個介於 0 到該第一參考正整數 $\tilde{a}$ 的數字成分且不同於該密鑰隨機陣列 $\left|\overleftrightarrow{R}\right|^{m}_{(\tilde{a})}$ 的隨機陣列 $\left|\overleftrightarrow{R^*}\right|^{m}_{(\tilde{a})}$，產生一相對於該隨機陣列 $\left|\overleftrightarrow{R^*}\right|^{m}_{(\tilde{a})}$ 且與該私鑰 $K_{private}$ 成對的更新公鑰 K^*_{public}，該更新公鑰 K^*_{public} 被表示為 $K^*_{\text{public}} = \left(\left|\overleftrightarrow{K^*}_{\text{public}}\right|^{m}, p_2\right)$，其中 $\left|\overleftrightarrow{K^*}_{\text{public}}\right|^{m} = \text{Rand}\left(\left|\overleftrightarrow{F}_{p_2}\right|^{m}, p_1, \tilde{a}\right) \pmod{p_2} = p_1\left(\left|\overleftrightarrow{F}_{p_2}\right|^{m} \circledast \left|\overleftrightarrow{R^*}\right|^{m}_{(\tilde{a})}\right) \pmod{p_2}$，該密鑰伺服器經由該第二通訊通道將該更新公鑰 K^*_{public} 傳送至該發送端；該發送端的該處理器在接收到來自該密鑰伺服器的該更新公鑰 K^*_{public} 時，以該更新公鑰 K^*_{public} 更新該發送端的該儲存單元所儲存的該公鑰 K_{public}；該發送端的該處理器在利用該公鑰 K^*_{public}、該第二參考質數 p_2、及該加密隨機陣列 $\left|\overleftrightarrow{R}\right|^{m}_{(\tilde{b})}$，對該資料陣列 $\left|\overleftrightarrow{M}\right|^{m}$ 進行該加密程序後，獲得另一相對於該公鑰 K^*_{public} 與該加密隨機陣列 $\left|\overleftrightarrow{R}\right|^{m}_{(\tilde{b})}$ 且具有 m 個加密數字成分的密文陣列 $\left|\overleftrightarrow{Cipher^*}\right|^{m}$，並經由該第一通訊通道將該密文陣列 $\left|\overleftrightarrow{Cipher^*}\right|^{m}$ 發送至該接收端；及該接收端的該處理器在接收到來自該發送端的該密文陣列 $\left|\overleftrightarrow{Cipher^*}\right|^{m}$ 時，利用該質數陣列

$\overleftrightarrow{f}\Big|^m$、該私鑰 $K_{private}$、該第一參考質數 p_1 及該第二參考質數 p_2，對於該密文陣列 $\overleftrightarrow{Cipher}\Big|^m$進行該解密程序而獲得該明文陣列 $\overleftrightarrow{M_1}\Big|^m$。

圖式簡單說明

本發明的其他的特徵及功效，將於參照圖式的實施方式中清楚地呈現，其中：圖 1 是一方塊圖，示例地說明本發明加密通訊系統的一實施例；圖 2 是一方塊圖，示例地繪示出一配置於該實施例的一密鑰伺服器的後量子非對稱密鑰產生系統的組成；圖 3 及圖 4 是流程圖，示例地說明該實施例的該後量子非對稱密鑰產生系統如何執行一非對稱密鑰產生程序；圖 5 是一方塊圖，示例地繪示出該實施例的一發送端；圖 6 是一方塊圖，示例地繪示出該實施例的一接收端；圖 7 是一流程圖，示例地說明該實施例中一發送端如何對於一要被傳送的明文訊息執行一加密程序；及圖 8 是一流程圖，示例地說明該實施例中的一接收端如何對於一接收自該發送端的密文執行一解密程序。

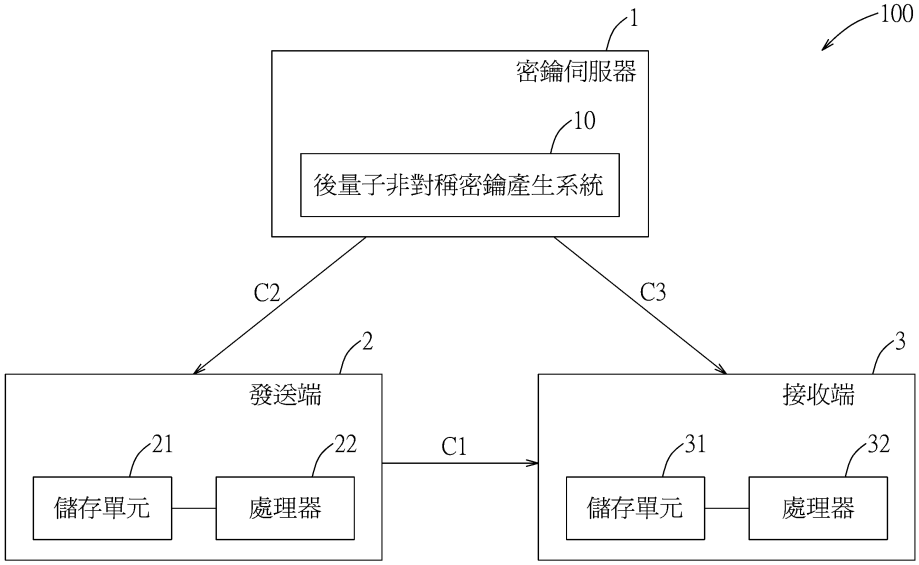

圖 1

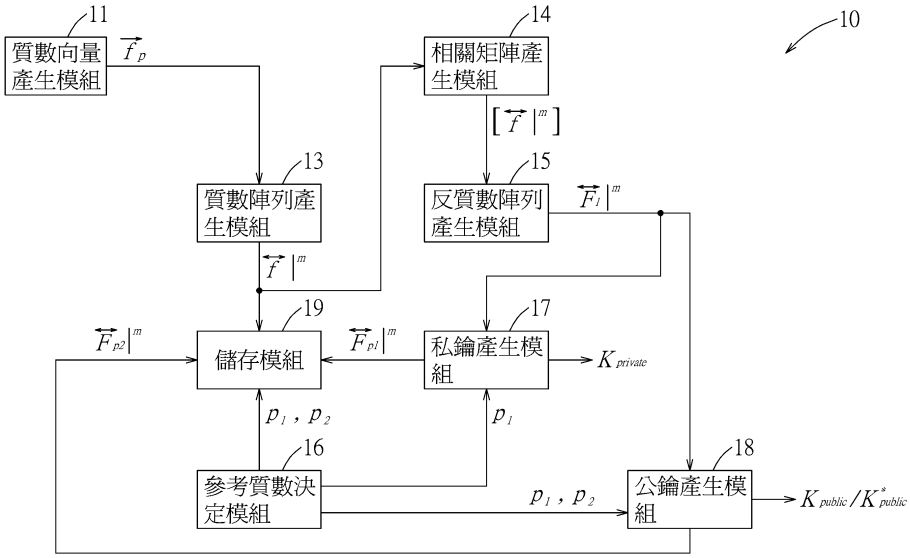
11
質數向量產生模組
$\vec{f}_p$
14
相關矩陣產生模組
10
$[\overleftarrow{f}|^m]$
13
質數陣列產生模組
15
反質數陣列產生模組
$\overleftarrow{F}_1|^m$
$\overleftarrow{f}|^m$
19
17
$\overleftarrow{F}_{p2}|^m$
儲存模組
$\overleftarrow{F}_{p1}|^m$
私鑰產生模組
$K_{private}$
p_1，p_2
p_1
16
18
參考質數決定模組
p_1，p_2
公鑰產生模組
K_{public}/K^*_{public}

圖 2

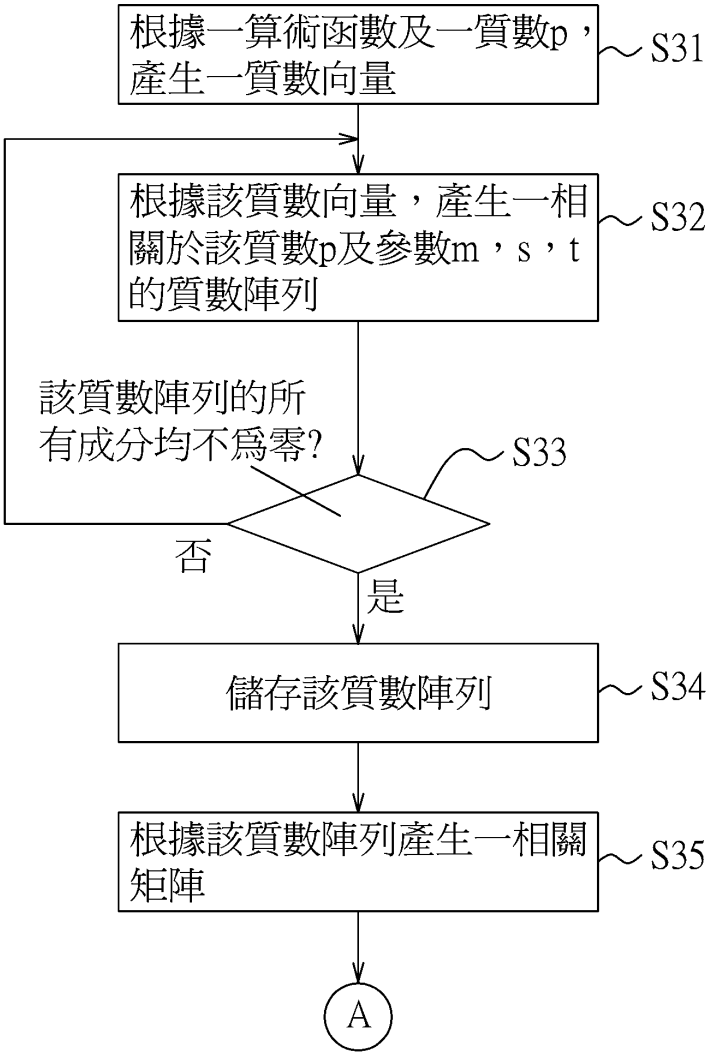
根據一算術函數及一質數p，產生一質數向量
S31
根據該質數向量，產生一相關於該質數p及參數m，s，t的質數陣列
S32
該質數陣列的所有成分均不爲零?
S33
否
是
儲存該質數陣列
S34
根據該質數陣列產生一相關矩陣
S35
A

圖 3

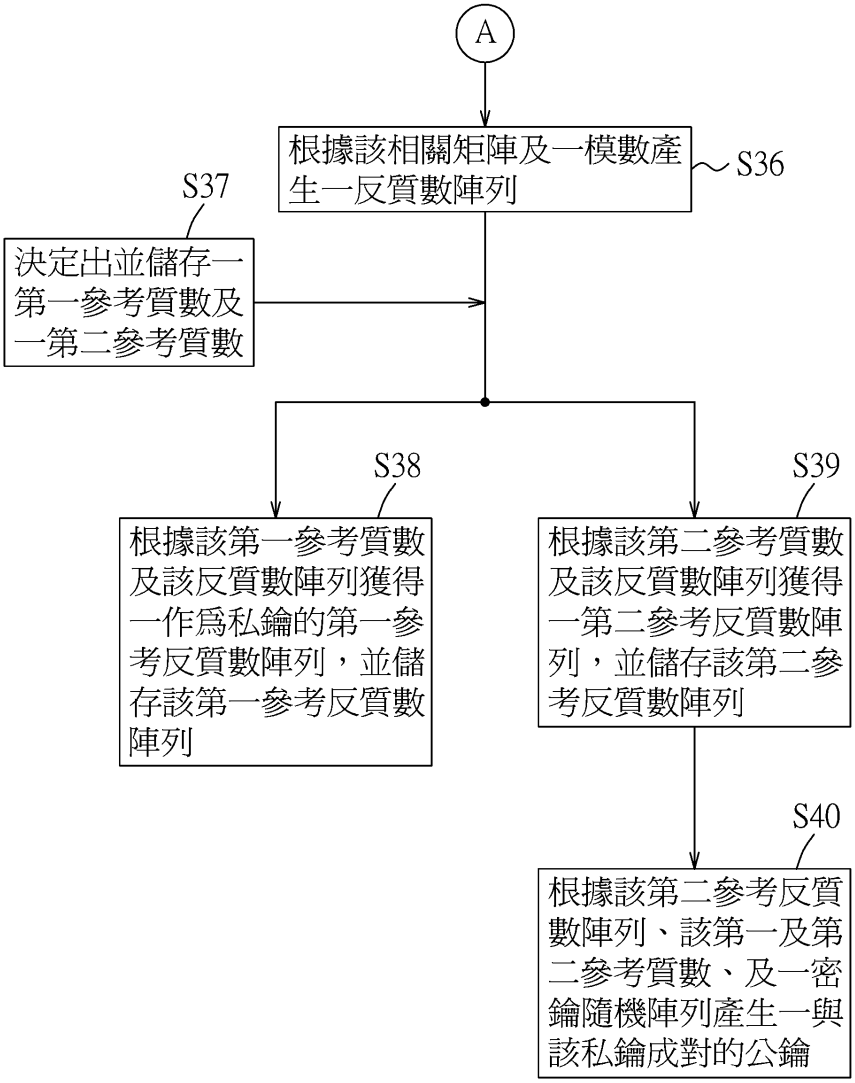
A
根據該相關矩陣及一模數產生一反質數陣列
S36
S37
決定出並儲存一第一參考質數及一第二參考質數
S38
根據該第一參考質數及該反質數陣列獲得一作爲私鑰的第一參考反質數陣列，並儲存該第一參考反質數陣列
S39
根據該第二參考質數及該反質數陣列獲得一第二參考反質數陣列，並儲存該第二參考反質數陣列
S40
根據該第二參考反質數陣列、該第一及第二參考質數、及一密鑰隨機陣列產生一與該私鑰成對的公鑰

圖 4

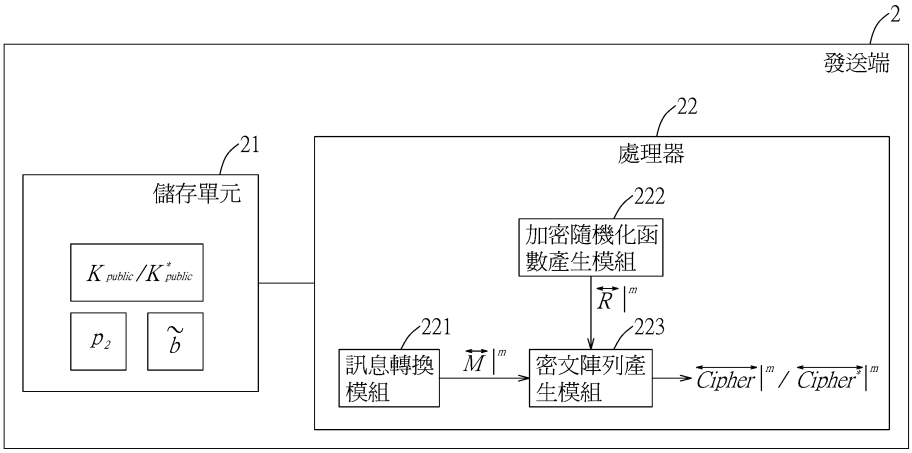
2
發送端
22
處理器
21
儲存單元
222
加密隨機化函數產生模組
$K_{public}/K^{*}_{public}$
p_2
$\tilde{b}$
$\overleftrightarrow{R}|^m$
221
訊息轉換模組
$\overleftrightarrow{M}|^m$
223
密文陣列產生模組
$\overleftrightarrow{Cipher}|^m / \overleftrightarrow{Cipher^*}|^m$

圖5

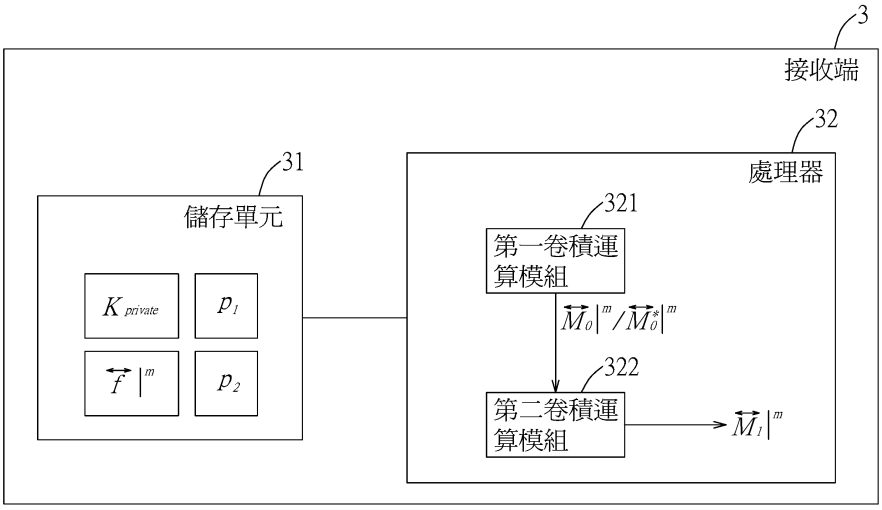
3
接收端
32
處理器
31
儲存單元
321
第一卷積運算模組
$K_{private}$
p_1
$\overleftrightarrow{f}|^m$
p_2
$\overleftrightarrow{M_0}|^m / \overleftrightarrow{M_0^*}|^m$
322
第二卷積運算模組
$\overleftrightarrow{M_1}|^m$

圖6

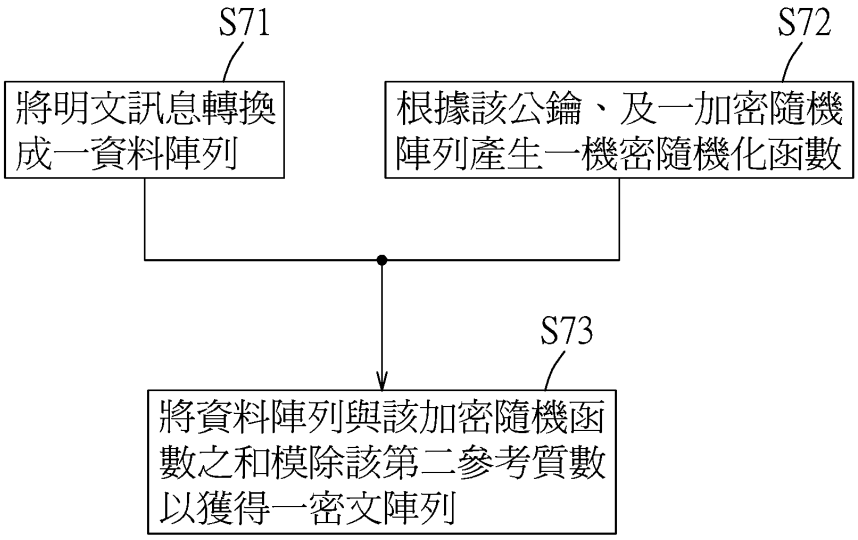
S71
S72
將明文訊息轉換成一資料陣列
根據該公鑰、及一加密隨機陣列產生一機密隨機化函數
S73
將資料陣列與該加密隨機函數之和模除該第二參考質數以獲得一密文陣列

圖7

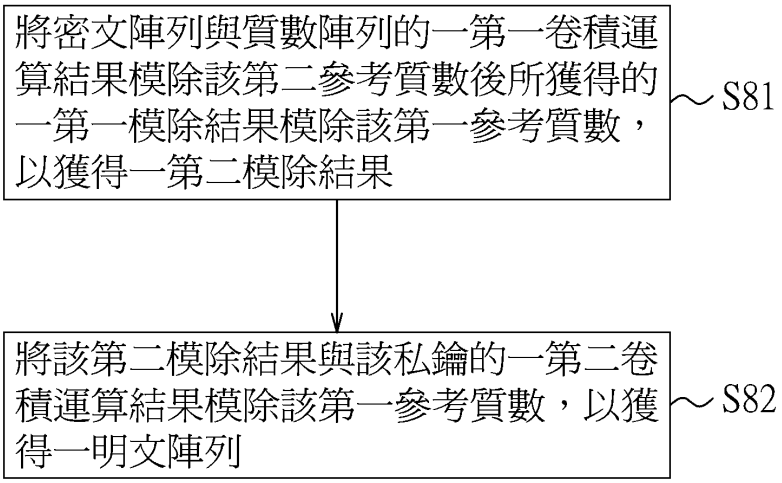
將密文陣列與質數陣列的一第一卷積運算結果模除該第二參考質數後所獲得的一第一模除結果模除該第一參考質數，以獲得一第二模除結果
S81
將該第二模除結果與該私鑰的一第二卷積運算結果模除該第一參考質數，以獲得一明文陣列
S82

圖8