(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 201328279 A1
(43)公開日： 中華民國 102 (2013) 年 07 月 01 日

(21)申請案號：100148211 (22)申請日： 中華民國 100 (2011) 年 12 月 23 日
(51)Int. Cl.： *H04L9/28 (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：葉宏男 YE, HUNG NAN (TW)；王國禎 WANG, KUO CHEN (TW)；簡榮宏 JIAN, RONG HONG (TW)
(74)代理人：李國光；張仲謙
申請實體審查：有 申請專利範圍項數：9 項 圖式數：4 共 20 頁

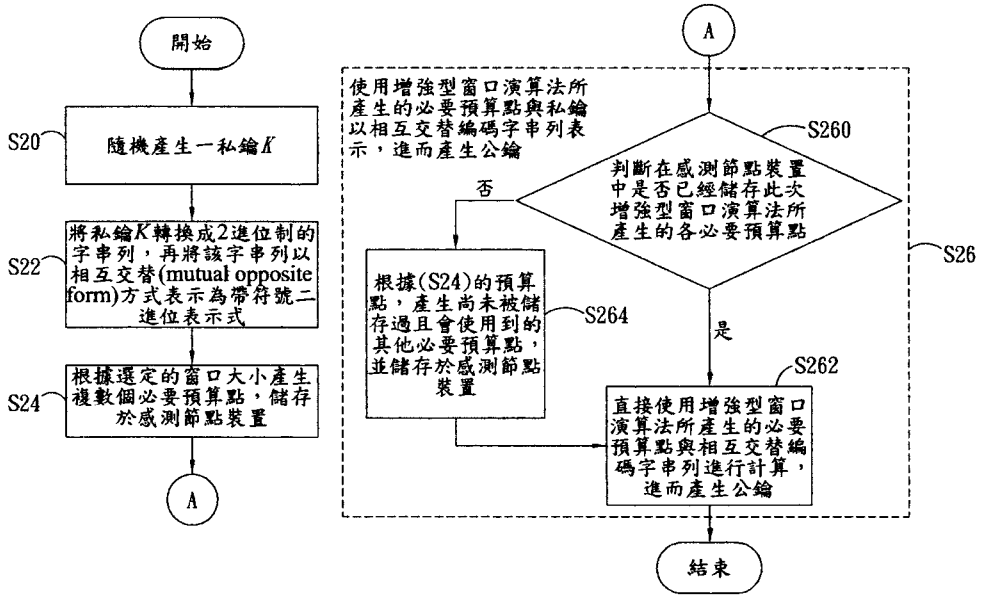
(54)名稱

應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法

METHOD OF USING ENHANCED WINDOW-BASED AND METHOD OF MUTUAL OPPOSITE FORM FOR SCALAR MULTIPLICATION IN ELLIPTIC CURVE CRYPTOGRAPHY

(57)摘要

本發明係一種應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法。首先選定一條橢圓曲線及在其上的基點。接著依選定之窗口大小，計算出必要之預算點。然後隨機產生私鑰，並利用相互交替型式將私鑰之二進位表示式轉換成帶符號二進位表示式。最後利用增強型窗口方法算出公鑰。藉著大量減少預算點，故此方法可以減少公鑰的產生時間（含計算預算點時間）。



S20~S26：步驟

S260~S264：步驟

201328279

專利案號：100148211

智專收字第1002080953-0

日期：100年12月23日

DTD版本：1.0.2

發明專利說明書

※申請案號：100148211　　※ＩＰＣ分類：H04L 9/28 (2006.01)

※申請日：(00.12.23)

一、發明名稱：

應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法

METHOD OF USING ENHANCED WINDOW-BASED AND METHOD OF MUTUAL OPPOSITE FORM FOR SCALAR MULTIPLICATION IN ELLIPTIC CURVE CRYPTOGRAPHY

二、中文發明摘要：

本發明係一種應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法。首先選定一條橢圓曲線及在其上的基點。接著依選定之窗口大小，計算出必要之預算點。然後隨機產生私鑰，並利用相互交替型式將私鑰之二進位表示式轉換成帶符號二進位表示式。最後利用增強型窗口方法算出公鑰。藉著大量減少預算點，故此方法可以減少公鑰的產生時間(含計算預算點時間)。

三、英文發明摘要：

The present invention is an enhanced window-based mutual opposite form (EW-MOF) for scalar multiplication in elliptic curve cryptography (ECC).First, an elliptic curve and a base point on the elliptic curve are selected. Next, essential pre-computed points for a selected window size are calculated. Then, a private key is randomly generated and the MOF is used to convert the private key's binary representation into a signed binary representation. Finally, the public key is calculated using the enhanced window (EW) method. By greatly reducing the number of pre-computed points, the proposed EW-MOF reduces the average key

generation time (including pre-computation time).

四、指定代表圖：

(一)本案指定代表圖為：第 (4) 圖。

(二)本代表圖之元件符號簡單說明：

步驟：S20~S26

步驟：S260~S264

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】

[0001] 本發明是有關於一種橢圓形曲線加密方法，特別是有關於一種應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法。，藉以快速產生橢圓形曲線加密公鑰的方法。

【先前技術】

[0002] 近年來，由於無線(感測)網路廣泛應用在軍事、環境監控及居家照顧上，使得其安全性方面便得越來越重要。而加密機制則是提供一個無線(感測)網路安全服務的基本技術。因為無線(感測)網路中的無線(感測)節點的資源(如：電量)有限，所以在執行加密時必須減少計算、通信和記憶體的負載。

[0003] 基於上述的原因，許多的研究機構或業界的研發單位，乃研發出各種的加密機制，譬如：RSA加密演算法、DSA加密演算法、橢圓曲線加密演算法(Elliptic Curves Cryptography，ECC)…等，其中若比較在相同安全性層次的RSA加密演算法與橢圓曲線加密演算法之保密鑰匙的位元長度，將如下表所示：

[0004]

RSA加密演算法(bits)	橢圓曲線加密演算法(bits)
1024	160
2048	224
3072	256
7680	384
15360	512

[0005] 換言之，在相同的安全強度下，橢圓曲線加密演算法的金鑰長度可遠較其他傳統加密演算法(如：RSA)小且處理速度較快，意即橢圓曲線加密演算法每個金鑰位元所能提供的安全性，係遠超過傳統加密演算法，這使得橢圓曲線加密演算法非常適合利用於無線(感測)網路的各種感測節點裝置，諸如智慧卡或手機無線行動裝置等電量及記憶體有限的環境中。

[0006] 而在橢圓曲線加密演算法中，例如：橢圓曲線數位金鑰交換演算法(Elliptic Curve Diffie-Hellman，簡稱：ECDH)及橢圓曲線數位簽章演算法(Elliptic Curve Digital Signature Algorithm，簡稱：ECDSA)，應用於各種感測節點裝置時，其純量乘法演算法將佔約80%的計算時間，此計算時間將會耗費相當多的電量，這將縮短感測節點裝置使用時間。

[0007] 更進一步以橢圓曲線數位金鑰交換演算法為例，請參閱第1圖所示，在某一無線(感測)網路中包括感測節點裝置A及感測節點裝置B，其中感測節點裝置A之私鑰、公鑰及金鑰分別為K_A、Q_A、R_A，感測節點裝置B之私鑰、公鑰及金鑰分別為K_B、Q_B、R_B，其中R_A及R_B分別如下所示：

[0008] $R_A = K_A \times Q_B$；$R_B = K_B \times Q_A$；且 $R_A = R_B$

[0009] 又進一步定義 $Q = KP$，其中P及Q為橢圓曲線上的兩個點，而K為正整數，且係以下列公式轉換成二進位制的字串列：

[0010] $K=\sum_{i=0}^{l-1} k_i 2^i, where\ k_i \in \{1, 0\}$

[0011]

據上所述，假若 $K=6599=(1100111000111)_2$，Q為取自K的運算過程為P, 2P, 3P, 6P, 12P, 24P, 25P, 50P, 51P, 102P, 103P, 206P, 412P, 824P, 1648P, 1649P, 3298P, 3299P, 6598P, 6599P，需要執行19次。

[0012] 其中私鑰K可用不同的轉換法進行轉換成字串列，若採用符號交替表示式(mutual opposite form)轉換成的字串列則為如下所示：

$$K=6599=\frac{1100111000111}{10\bar{1}0100\bar{1}001001}=(10\bar{1}0100\bar{1}001001)_2$$

[0013] 其中私鑰K若採用互補記錄式(Complementary recoding)則轉換成的字串列則為如下所示：$K=6599=(1100111000111)_2$

$\overline{K}=(0011000111000)_2$

$K=2^{13}-\overline{K}-1=(100\bar{1}1000\bar{1}\bar{1}\bar{1}00\bar{1})_2$

[0014] 其中私鑰K若採用二元非相鄰式(Non-Adjacent Form，NAF)則轉換成的字串列則為如下所示：

$K=6599=(1100111000111)_2=(10\bar{1}0100\bar{1}001001)_2$

[0015] 在此對前述的三個轉換法進行比較：

[0016]

轉換法	二元非相鄰式(NAF)	符號交替表示式(MOF)	互補記錄式(Complementary recoding)
漢明權重比(Hamming	大	大	小

weight)			
掃瞄方向 (Scanning direction)	由右至左	由右至左 由左至右	由右至左 由左至右
平均執行時間 (Average execution time)	較長(large)	適中 (medium)	較短(small)

又，私鑰K若採用窗口法(Window method)則直接轉換成的字串列則為如下所示：

若窗口大小w為2，則可以下列表示：

$K = 6599 = (1100111000111)_2$

$w = 2 \Rightarrow K = (11\ \ 00\ \ 11\ \ 1\ \ 000\ \ 11\ \ 1)_2$

[0017] 則其預算點為3P。

[0018] 若窗口大小w為3，則可以下列表示：

$K = 6599 = (1100111000111)_2$

$w = 3 \Rightarrow K = (11\ \ 00\ \ 111\ \ 000\ \ 111)_2$

[0019] 則其預算點為3P、5P及7P。

[0020] 由上述可知，窗口法雖需要計算預算點，但可減少執行的次數，再者，將上揭符號交替表示式、互補記錄式及二元非相鄰式輔以窗口法則其可產生的預算點數量分別如下所示：

[0021] A. 符號交替表示式結合窗口法，並以窗口大小w為5為例，其預算點包括3P、5P、7P、9P、11P、13P及15P。

[0022] B. 二元非相鄰式結合窗口法，並以窗口大小w為5為例，其預算點包括3P、5P、7P、9P、11P、13P、15P、17P及21P。

[0023] C. 互補記錄式結合窗口法，並以窗口大小w為5為例，其預算點包括3P、5P、7P、9P、11P、13P、15P、17P、21P、23P、25P、27P、29P及31P。

[0024] 據上所述，在轉換法中二元非相鄰式的平均執行時間較長，且各轉換法結合窗口法又以互補記錄式結合窗口法所需要計算的預算點最多，故若能以符號交替表示式結合窗口法，將可大量減少平均執行時間，並能消減較多的計算和記憶量，將會有效的減少感測節點裝置的電量及記憶體的使用量。

【發明內容】

[0025] 有鑒於上述習知技藝之問題，本發明之目的就是在提供一種應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，以解決習知技術中感測節點裝置耗費較多的電量等問題。

[0026] 根據本發明之目的，提出一種應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，首先我們選定一條橢圓曲線及在其上的基點。接著依選定之窗口大小，計算出必要之預算點(essential pre-computed points)。然後隨機產生私鑰，並利用相互交替型式將私鑰之二進位表示式轉換成帶符號二進位表示式。最後利用增強型窗口方法算出公鑰。藉著大量減少預算點，我們提出的方法可以減少公鑰的產生時間(含

計算預算點的時間）。

[0027] 其中，依選定之窗口大小產生必要預算點係採用下列的公式：

[0028] $\{2P, 4P, 6P\cdots, (3+2S)P, (5+6S)P, (7+10S)P, \cdots\}$

[0029] 在上述公式中S之數值為偶數必要點，且S≧1，又最大必要點加上(2S)P≧最大必要預算點。

其中，在增強型窗口演算法中窗口大小(w)≧4。

[0030] 其中，該方法在隨機產生私鑰後以二進位制的字串列表示，再將該字串列以相互交替(mutual opposite form)方式，轉換成帶符號二進位表示式。

[0031] 綜上所述，由於預先降低預算點之數量，因此只需較少的預算點與私鑰以相互交替編碼字串列表示，即可加快計算橢圓形曲線加密的公鑰所需的時間。

[0032] 為讓本發明之上述和其他目的、特徵和優點能更明顯易懂，下文特舉較佳實施例，並配合所附圖式，作詳細說明如下。

【實施方式】

[0033] 以下將參照相關圖式，說明依本發明之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法之實施例，為使便於理解，下述實施例中之相同元件係以相同之符號標示來說明。其中，所使用之圖式，其主旨僅為示意及輔助說明書之用，未必為本發明實施後之真實比例與精準配置，故不應就所附之圖式的比例與配置關係侷限本發明於實際實施上的專利範圍，合

先敘明。

[0034] 本發明之一種應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，首先選定一條橢圓曲線及在其上的基點。接著依選定之窗口大小，計算出必要之預算點。然後隨機產生私鑰後，以二進位制的字串列表示，再將該字串列以相互交替(mutual opposite form)方式表示為帶符號二進位表示式。

[0035] 在本發明中，增強型窗口演算法產生必要預算點係採用下列的公式：

[0036] $\{2P, 4P, 6P\cdots, (3+2S)P, (5+6S)P, (7+10S)P, \cdots\}$

[0037] 在上述公式中S為偶數必要點的數量，且S≧1，又最大必要點加上(2S)P≧最大必要預算點。更進一步係限定增強型窗口演算法中窗口大小(w)≧4。

[0038] 舉例而言，若在符號交替表示式中使用增強型窗口演算法，且其窗口大小設定為6，且其最大必要預算點為31P，則當S等於1、2或3時，必要點的數量分別如下所示。

[0039] S = 1，必要點為{2P, 5P, 11P, 17P, 23P, 29P}

[0040] (29P + 2P)≧31P，故其必要點的數量為6。

[0041] S = 2，必要點為{2P, 4P, 7P, 17P, 27P}

[0042] (27P + 4P)≧31P，故其必要點的數量為5。

[0043] S = 3，必要點為{2P, 4P, 6P, 9P, 23P, 37P}

[0044] (37P + 6P)≧31P，故其必要點的數量為6。

[0045] 而傳統的窗口演算法所有要預先計算的必要點共計有15個，分別為3P, 5P, 7P, 9P, 11P, 13P, 15P, 17P, 19P, 21P, 23P, 25P, 27P, 29P, 31P，而增強型窗口演算法的必要預算點最少為5個，分別為{2P, 4P, 7P, 17P, 27P}，由此可知，本發明之增強型窗口演算法確實有效減少預算點數量。

[0046] 請參閱第2圖所示，其係增強型窗口演算法與傳統窗口演算法在相同的窗口大小下之預算點數量比較圖。由圖所示可知，增強型窗口演算法較傳統窗口演算法在越大的窗口大小下，前者所產生的必要預算點遠少於後者。其乃是本發明利用增強型窗口演算法作為改善傳統橢圓形曲線加密方法之主因。

[0047] 在本發明中，更進一步將橢圓形曲線加密的私鑰以二進位制的字串列表示，再將該字串列以相互交替(mutual opposite form)方式表示為帶符號二進位表示式。。由於預先降低預算點之數量，因此只需較少的必要預算點與私鑰以相互交替編碼字串列表示，即可減少計算橢圓形曲線加密的公鑰所需的時間。

[0048] 請參閱第3圖，其係為本發明之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法。應用在無線感測網路中的初始參數設定流程圖，其步驟係如下所示：

[0049] (S10)選用一橢圓形曲線。橢圓形曲線採用有限場(如：質數場(prime field，GF(p))，且橢圓形曲線係滿足

下列公式：

[0050] $y^2 = x^3 + ax + b$ ；其中 $a,b \in GF(p)$ ，且 $4a^3 + 27b^2 \neq 0$

[0051] (S12)選擇在橢圓形曲線之一基準點P，且P=(X,Y)，其中X及Y係為基準點P符合橢圓形曲線的座標位置。

[0052] (S14)當無線感測網路中之一感測節點裝置接收到任一訊息時，將選擇一窗口大小，並據以計算出必要預算點。

[0053] (S16)當計算出必要預算點時，將各必要預算點的數值儲存在感測節點裝置中。

[0054] 請參閱第4圖，其係為本發明之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法應用在無線感測網路中的公鑰的產生流程圖。其步驟係如下所示：

[0055] (S20)隨機產生一私鑰K。

[0056] (S22)將私鑰K轉換成二進位制的字串列，再將該字串列以相互交替(mutual opposite form)方式表示為帶符號二進位表示式。

[0057] (S24)根據選定的窗口大小產生複數個必要預算點，儲存於感測節點裝置。

[0058] (S26)使用增強型窗口演算法所產生的必要預算點與私鑰以相互交替編碼字串列表示，進而產生公鑰。

[0059] 據上所述，由於只需較少的必要預算點與私鑰以相互交替編碼字串列表示，即可減少計算橢圓形曲線加密的公

鑰所需的時間。

[0060] 在本發明中，其中步驟(S26)係更進一步包括下列步驟：

[0061] (S260)判斷在感測節點裝置中是否已經儲存此次增強型窗口演算法所產生的各必要預算點。若是進行下列步驟，否則進行步驟(S264)

[0062] (S262)直接使用增強型窗口演算法所產生的必要預算點與相互交替編碼字串列進行計算，進而產生公鑰

[0063] (S264)根據(S24)的預算點，產生尚未被儲存過且會使用到的其他必要預算點，並儲存於感測節點裝置，再進行步驟(S262)。

[0064] 據上所述，感測節點裝置儲存其已產生的必要預算點，而僅再產生未被儲存的必要預算點，將使得感測節點裝置更為節省電量。

[0065] 綜上所述，因依本發明之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，其可具有一或多個下述優點：

[0066] (1)此發明之增強型窗口演算法係有效地減少預算點數目。

[0067] (2)此發明之純量乘法演算法係更進一步只需較少的必要預算點與相互交替編碼字串列的計算次數，即可減少計算橢圓形曲線加密的公鑰所需的時間。

[0068] 雖然前述的描述及圖式已揭示本發明之較佳實施例，必須瞭解到各種增添、許多修改和取代可能使用於本發明

較佳實施例，而不會脫離如所附申請專利範圍所界定的本發明原理之精神及範圍。熟悉該技藝者將可體會本發明可能使用於很多形式、結構、佈置、比例、材料、元件和組件的修改。

[0069] 因此，本文於此所揭示的實施例於所有觀點，應被視為用以說明本發明，而非用以限制本發明。本發明的範圍應由後附申請專利範圍所界定，並涵蓋其合法均等物，並不限於先前的描述。

【圖式簡單說明】

[0070] 第1圖係無線(感測)網路示意圖。

第2圖係增強型窗口演算法與傳統窗口演算法在相同的窗口大小下之預算點數量比較圖。

第3圖係為本發明應用在無線感測網路中的初始參數設定流程圖。

第4圖係本發明應用在無線感測網路中的公鑰的產生流程圖。

【主要元件符號說明】

[0071] 感測節點裝置：A

感測節點裝置B

步驟：S10~S16

步驟：S20~S26

步驟：S260~S264

七、申請專利範圍：

1．一種應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，係使用一增強型窗口演算法，依選定的窗口大小，產生數個必要預算點。

2．如申請專利範圍第1項所述之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，其中該增強型窗口演算法產生必要預算點係採用下列的公式：

$\{2P, 4P, 6P\cdots,(3+2S)P,(5+6S)P,(7+10S)P,\cdots\}$ ；

該公式中S為偶數必要點的數量，且S≧1，又最大必要點加上(2S)P≧最大必要預算點。

3．如申請專利範圍第2項所述之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，其中更進一步係限定增強型窗口演算法中窗口大小(w)≧4。

4．如申請專利範圍第3項所述之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，其中更進一步將該私鑰轉換成二進位制的字串列，再將該字串列依相互交替編碼方式，以帶符號二進位制的字串列表示。

5．如申請專利範圍第4項所述之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，其中更進一步使用各該必要預算點與相互交替編碼字串列計算產生一公鑰。

6．一種應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，其包括：

選用一橢圓形曲線；

選擇在該橢圓形曲線之一基準點P，且P=(X,Y)，其中X及Y係為該基準點P符合該橢圓形曲線的一座標位置；

當該無線感測網路中之一感測節點裝置接收到任一訊息時，將選擇一窗口大小，並據以計算出複數個必要預算點；以及

當計算出各該必要預算點時，將各該必要預算點的數值儲存在該感測節點裝置中。

7．如申請專利範圍第6項所述之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，其中該橢圓形曲線採用有限場，且橢圓形曲線係滿足下列公式：

$y^2 = x^3 + ax + b$ ；其中 $a,b \in GF(p)$ ，且 $4a^3 + 27b^2 \neq 0$ 。

8．如申請專利範圍第7項所述之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，其中更包括公鑰的產生步驟：

隨機產生一私鑰；

將該私鑰轉換成二進位制的一字串列，再將該字串列以一符號交替表示，並轉換成一相互交替編碼字串列；

根據選擇的窗口大小產生複數個必要預算點，並儲存於一感測節點裝置，並將以相互交替編碼字串列表示之私鑰切成複數個區塊；以及

使用各該必要預算點與該相互交替編碼字串列進行計算，進而產生該公鑰。

9．如申請專利範圍第8項所述之應用增強型窗口方法和相互交替型式於純量乘法演算法之橢圓形曲線加密方法，其中使用增強型窗口演算法所產生的必要預算點與相互交替編

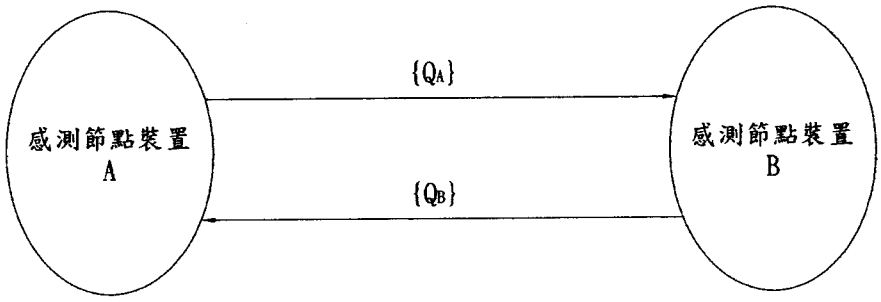
碼字串列進行計算，進而產生公鑰的步驟，更包括：

判斷在該感測節點裝置中是否已經儲存此次產生的各該必要預算點；

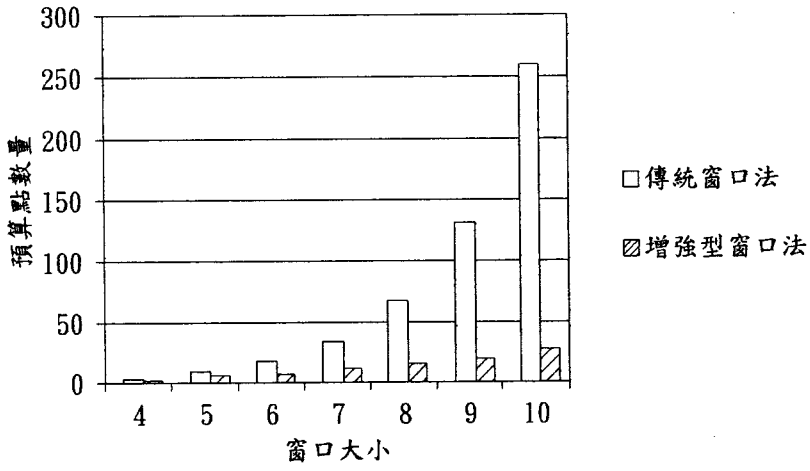
當該感測節點裝置已經儲存此次產生的各該必要預算點，則直接使用各該必要預算點與該相互交替編碼字串列進行計算，進而產生該公鑰；以及

當該感測節點裝置未儲存此次產生的各該必要預算點，根據被選擇一窗口大小，將相互交替編碼字串列切成複數個區塊，產生尚未被儲存過的必要預算點，並儲存於感測節點裝置，再使用各該必要預算點與該相互交替編碼字串列進行計算，進而產生該公鑰。

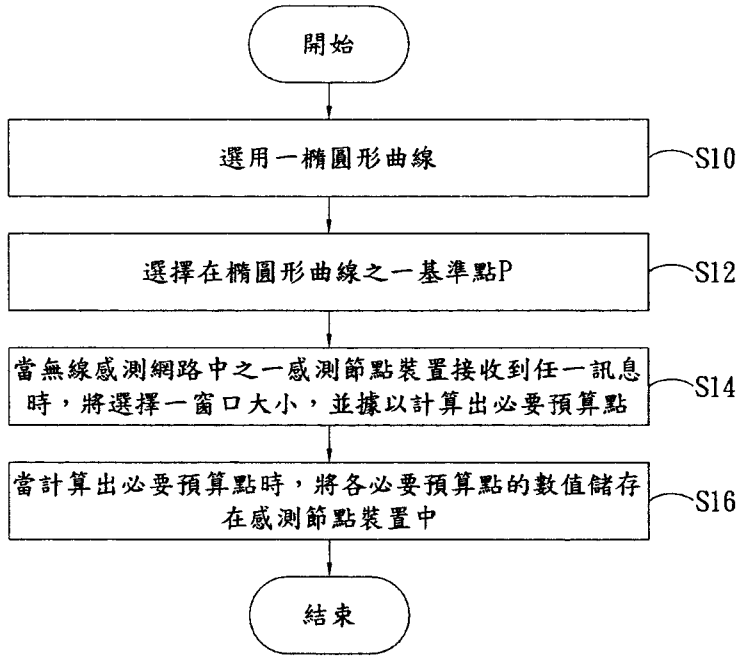
八、圖式：


感測節點裝置
A
{QA}
{QB}
感測節點裝置
B

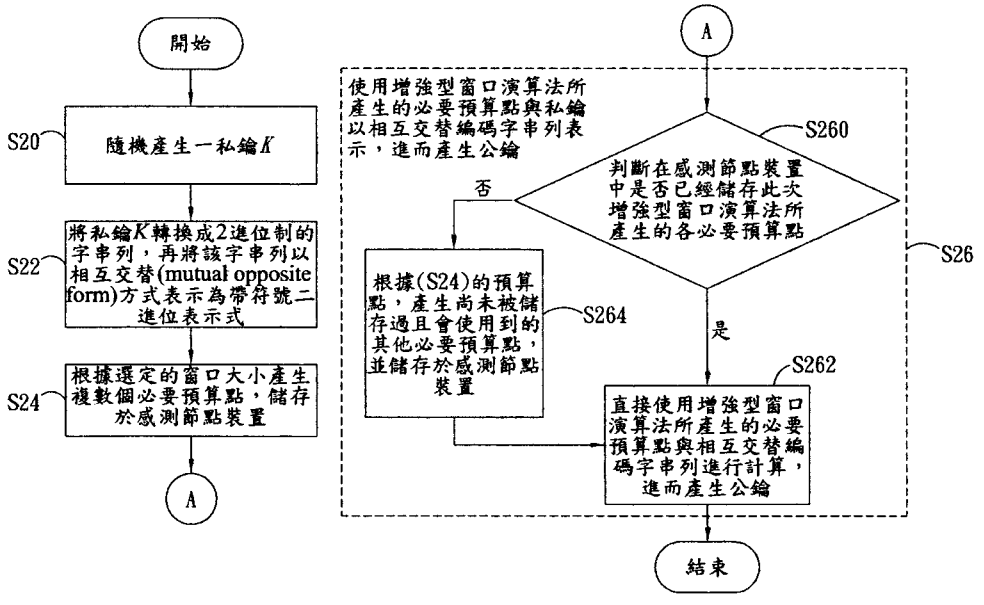
第1圖


300
250
200
150
100
50
0
預算點數量
4
5
6
7
8
9
10
窗口大小
□傳統窗口法
▨增強型窗口法

第2圖


開始
選用一橢圓形曲線
S10
選擇在橢圓形曲線之一基準點P
S12
當無線感測網路中之一感測節點裝置接收到任一訊息時，將選擇一窗口大小，並據以計算出必要預算點
S14
當計算出必要預算點時，將各必要預算點的數值儲存在感測節點裝置中
S16
結束

第3圖


開始
S20
隨機產生一私鑰K
S22
將私鑰K轉換成2進位制的字串列，再將該字串列以相互交替(mutual opposite form)方式表示為帶符號二進位表示式
S24
根據選定的窗口大小產生複數個必要預算點，儲存於感測節點裝置
A
A
使用增強型窗口演算法所產生的必要預算點與私鑰以相互交替編碼字串列表示，進而產生公鑰
S260
判斷在感測節點裝置中是否已經儲存此次增強型窗口演算法所產生的各必要預算點
否
是
S26
根據(S24)的預算點，產生尚未被儲存過且會使用到的其他必要預算點，並儲存於感測節點裝置
S264
S262
直接使用增強型窗口演算法所產生的必要預算點與相互交替編碼字串列進行計算，進而產生公鑰
結束

第4圖