橢圓曲線密碼系統之位元-並列高斯正規基底乘法器的最佳成本×時間設計
(Bit-Parallel Gaussian Normal Basis Multiplier over GF(2^m) with Optimum Area×Time for Elliptic Curve Cryptosystems)

蕭儒珣(Ru-Syun Siao)
健行科技大學資訊工程系
B10013151@uch.edu.tw

邱綺文*(Che Wun Chiou)
健行科技大學資訊工程系
cwchiou@uch.edu.tw
*:corresponding author

呂松諭(J Song-Yu Lyu)
健行科技大學資訊工程系
B10013139@uch.edu.tw

廖柏維(Bo-Wei Liao)
健行科技大學資訊工程系
B10013149@uch.edu.tw

葉耕禔(Keng-Ti Yeh)
健行科技大學資訊工程系
B10013180@uch.edu.tw

徐子峯(Zih-Feng Hsu)
健行科技大學資訊工程系
B10013144@uch.edu.tw

摘要

由於智慧型行動裝置如智慧型手機、筆記型電腦、和平板電腦愈來愈普遍，利用智慧型行動裝置進行電子交易也隨之愈來愈多，所以如何保護電子交易行為安全也成為重要課題。因為橢圓曲線密碼系統使用之鑰匙長度相對 RSA 公開金鑰密碼系統短很多，所以適合在資源有限之智慧型行動裝置使用。乘法器是實現橢圓曲線密碼系統核心元件，如何設計有效率之乘法器是非常重要課題，所以本研究將提出最佳 Chip_Area×Time 之新型位元-並列高斯正規乘法器，有效實現橢圓曲線密碼系統。

關鍵詞：智慧型行動裝置、橢圓曲線密碼系統、乘法器、公開金鑰密碼系統、行動商務、資訊安全

壹、前言

行動商務(M-commerce)市場正逐漸成熟，未來網路與行動商務產業的經濟力將指日可待。由世界各國的購物趨勢，利用行動裝置如手機等進行購物，將會愈來愈普遍，因此行動商務的安全付款，將會是非常重要的課題，行動商務安全則深深依賴密碼系統提供的安全。現代的非對稱金鑰密碼系統或稱公鑰密碼系統(Public-Key Cryptosystem)，是由 Diffie 和 Hellman [1] 首先在 1976 年提出概念，隨後並在 1977 年，由三位美國麻省理工學院學者 Rivest、Shamir、Adleman [2] 提出以指數算法來實現，此演算法即為著名之 RSA 演算法。隨著電腦計算能力愈來愈強，以及雲端運算的推展，為了足夠的安全，RSA 密碼系統使用之金鑰長度位元數必須跟著愈來愈長，這對計算能力受到限制之行動通訊系統是非常不利的。因此後來橢圓曲線密碼系統（Elliptic Curve Cryptosystem, ECC）被提出來後，因為所使用之金鑰長度遠少於 RSA 密碼系統，非常適合在行動通訊系統使用，所以橢圓曲線密碼系統帶領新一波的研究與應用潮流。 橢圓曲線密碼系統是由 Koblitz [3]與 Miler[4]各自推出。若橢圓曲線安全等級係使用 160 位元的模數(moduls)可以和 RSA 系統使用 1024 位元模數達到相同的安全等級[5][6]，使得橢圓曲線密碼系統適合在行動通訊(如手機)等資源有限環境下使用，所以橢圓曲線密碼系統已成為新一代的密碼學演算法，並已被廣泛地制訂在國際標準如 ISO 11770-3 [7]、ANSI X9.62 [8]、IEEE P1363-2000 [9]、FIPS 186-2 [10]等。橢圓曲線密碼系統可由使用者任選曲線方程式而不需要更換硬體，所以如果以晶片方式設計橢圓曲線密碼系統，再跟行動通訊系統結合來執行行動商務的資訊安全，將會是非常有潛力及市場的產品。

在橢圓曲線密碼系統裡最常被使用的有限場(Finite field)有二進制延伸場($GF(2^m)$)、三進制延伸場($GF(3^m)$)和質數場(GF(P))。二進制延伸場數值運算包含了乘法、除法、反元素、指數等運算，其中乘法運算在密碼學的領域中佔有非常重要的地位，因為除法、反元素、指數等運算都可透過乘法來解決。二進制延伸場的元素表示法和乘法運算的效率息息相關，最常被使用之二進制延伸場元素表示法有三種，即多項式基底(Polynomial Basis, PB) [11][12][13][14][15][16][17][18][19][20][21][22][23][24][25][26] 、正規基底(Normal Basis, NB) [13][26][27][28][29][30][31][32][33] [34][35][36]、雙重基底(Dual Basis, DB) [27][37][38][39][40][41][42][43][44][45][46]表示法，每種基底表示法都有它的優點和特性，也因此適合使用於不同運算及應用領域。多項式基底表示法的優點在於硬體架構的低複雜度設計、規則化、簡單性、和模組化，因此非常適合利用 VLSI 的設計。正規基底表示法的優點，是二進制延伸場中元素的平方運算可以利用旋轉位移即可達成，因此在執行平方運算、反元素運算和指數運算上是非常有效率。雙重基底則比其他兩種表示方式更節省硬體成本。另外，目前的研究學者也正透過轉換到不同的數域，使得這三種常用基底表示法能夠同時具有這三種優點。

二進制延伸場乘法器的硬體架構可分為四類，位元-串列(bit-serial) [37][40]、位元-並列(bit-parallel) [13][15][26][38]、位-串列(digit-serial) [19][20][42][43][44][46]、及混合

(hybrid) [16][18][47]。位元-串列乘法器每一時脈周期產生乘法結果之一位元，具有低硬體成本之優點，但需要很長執行時間之缺點。位元-並列乘法器於同一時脈周期產生乘法結果之所有位元，有極短執行時間之優點，卻有很高硬體成本之缺點。混合型乘法器可降低位元-並列乘法器之硬體成本。位-串列乘法器每一時脈周期產生乘法結果之一位，一位為數個位元長度，位-串列乘法器提供硬體成本及執行時間上折衷的彈性設計。

在 1986 年，Massey 和 Omura [27]第一個提出正規基底(NB)的乘法演算法，之後陸續有許多的專家學者提出 Massey 和 Omura 正規基底乘法演算法的變型 [13][28][29][30][31]。Wang et al. [32]提出新的 Massey 和 Omura 正規基底乘法演算法，以適合 VLSI 架構。但是 Wang 的架構缺乏規則性及模組化優點，因此 Kwon [32]針對 optimal normal basis(type 2)提出心臟型乘法器(systolic multiplier)，以適合 VLSI 需要的規則性及模組化優點，容易根據不同 m 值擴充。Reyhani-Masoleh [29]則提出非心臟型架構之高斯正規基底乘法器(type t)。Lidl 和 Niederreiter [48]證明對任何正整數都存在一個正規基底乘法，所以正規基底表示法是非常實用的。高斯正規基底表示法(Gaussian normal basis, GNB)是屬於正規基底表示法的一支，它具有低成本的優勢。對所有正整數，除了那些可被 8 除盡外，都有高斯正規基底存在[49]，所以高斯正規基底也是非常實用的。

實現高斯正規基底乘法器主要有兩種架構：心臟型陣列(systolic array)[36]及非心臟型陣列(non-systolic array)架構 [29]，非心臟型陣列架構一般稱為位元-並列架構。位元-並列架構一般會利用二元樹狀邏輯互斥或閘(XOR)架構實現，一個結果位元需要一個二元樹狀邏輯互斥或閘，所以 mt+1 結果位元(GNB with type-t)需要 mt+1 個二元樹狀邏輯互斥或閘，對於資源有限之行動通訊系統而言，硬體成本太高。為了解決此問題，Chiou et al. [50]在每一邏輯互斥或(XOR)閘層加一個 D 型正反器(D Flip-Flop)，以達到管線化目的，這樣只要一個二元樹狀邏輯互斥或閘，就可重覆執行 mt+1 次，得到 mt+1 結果位元。由於管線化二元樹狀邏輯互斥或閘執行此乘法共需要 $\lceil \log_2 mt+1 \rceil + mt$ 時脈周期(clock)，$\lceil x \rceil$ 為上取整函數(ceil(x))，亦即不小於 x 的整數中最小的一個。所以管線化二元樹狀邏輯互斥或閘架構節省許多硬體成本，但會花費較多的執行時間。由於 Chiou et al. [50]的管線化位元-並列高斯正規基底乘法器是在每一層二元樹狀邏輯互斥或閘即加入一層 D 型正反器，我們從 NanGate's Library Creator and the 45-nm FreePDK Based Kit from North Carolina State University (NCSU) [51]發現一個有趣事實，D 型正反器所需要之 chip area (D Flip-flop: 4.522 μm^2)為互斥或閘(XOR gate:1.596μm^2)的 2.8 倍，且 D 型正反器所需要之傳遞延遲時間(D Flip-flop:在 input transition=0.0012ns 和 load capacitance=0.3656fF 情況下 Propagation Delay=0.08ns)為互斥或閘(XOR gate: 在 input transition=0.0012ns 和 load capacitance=0.3656fF 情況下 Propagation Delay=0.05ns)的 1.6 倍，所以 Chiou et al. [50] 的管線化位元-並列高斯正規基底乘法器並不是最佳的架構。本論文將提出較 Chiou et al. [50]的乘法器有更佳之 Area×Time 的管線化位元-並列高斯正規基底乘法器。

貳、數學背景

本章會簡潔地介紹高斯正規基底表示法，若需要更詳細的說明，請參考文獻[48]。在介紹我們採用之方法前，先簡單介紹正規基底乘法。令 $\left\{\alpha^{2^0},\alpha^{2^1},\alpha^{2^2},...,\alpha^{2^{m-1}}\right\}$ 為 GF(2^m) 之一個正規基底，則任何元素 $A,B\in$GF(2^m) 可表示成下列式子：

$$A=a_0\alpha^{2^0}+a_1\alpha^{2^1}+a_2\alpha^{2^2}+...+a_{m-1}\alpha^{2^{m-1}},$$

$$B=b_0\alpha^{2^0}+b_1\alpha^{2^1}+b_2\alpha^{2^2}+...+b_{m-1}\alpha^{2^{m-1}},$$

係數 $a_i,b_i\in\{0,1\}$，i=0,1,2,…, m-1。

一般正規基底具有下列特性：

特性 1： $A^2=a_{m-1}\alpha^{2^0}+a_0\alpha^{2^1}+a_1\alpha^{2^2}+...+a_{m-2}\alpha^{2^{m-1}}$,

特性 2： $(A+B)^2=A^2+B^2$.

如果是具型 t 之高斯正規基底(Gaussian normal basis of type-t)，則除了上述特性外，更具有下列特性：

特性 3： $\alpha=\sum_{i=0}^{t-1}\gamma^{\tau^i}$,

特性 4： $\tau^t=1 \mod mt+1,$

特性 5： $\gamma^{mt+1}=\gamma^{(mt+1) \bmod (mt+1)}=1$,

τ 和 γ 分別是 1 之 primitive t^{th} 和$(mt+1)^{\text{th}}$ 根(primitive t^{th} and $(mt+1)^{\text{th}}$ roots of unity)。

令 $C=A\times B$，且 C 之表示式如下：

$$C=c_0\alpha^{2^0}+c_1\alpha^{2^1}+c_2\alpha^{2^2}+...+c_{m-1}\alpha^{2^{m-1}}\text{ 。}$$

由於正規基底在平方的運算是非常簡單，根據特性 1 只要旋轉位元位置即可，但是正規基底在乘法的運算則是非常困難，主要是因為兩元素相乘後會產生新的權重(weight)位置出來，如下例：

$$\left(a_0\alpha^{2^0}+a_1\alpha^{2^1}+a_2\alpha^{2^2}+\ldots+a_{m-1}\alpha^{2^{m-1}}\right)\times b_1\alpha^{2^1}$$
$$=a_0b_1\alpha^{2^0+2^1}+a_1b_1\alpha^{2^1+2^1}+a_2b_1\alpha^{2^2+2^1}+\ldots+a_{m-1}b_1\alpha^{2^{m-1}+2^1}$$

以 $a_0b_1\alpha^{2^0+2^1}$ 而言，其權重 $\alpha^{2^0+2^1}=\alpha^3$ 並不在正規基底內，所以會多出很多權重位置出來，使得硬體成本增加許多或軟體演算法變得很複雜。因此比較好的方法是將其轉為多項式基底，但是要轉成多項式基底，只有正規基底是具型 t 之高斯正規基底或具型 1 或型 2 之最佳正規基底(Optimal basis of type-1 or type-2)才有辦法轉換(根據特性 5)。很幸運的，如前所述，對任何 m 值，具型 t 之高斯正規基底幾乎都存在，所以具型 t 之高斯正規基底是很實用的，譬如美國 NIST(National Institute of Standards and Technology)建議的 m 值：163、233、283、409、及 571，都有具型 t 之高斯正規基底可運用。當執行乘法運算時，高斯正規基底表示法能夠很容易轉換成多項式基底表示法來做乘法運算。

參、傳統位元_並列高斯正規基底乘法器

就如前所述，在執行高斯正規基底乘法時，必須將元素的高斯正規基底表示法轉換成多項式基底表示法，做完多項式基底乘法後，再將結果轉換成高斯正規基底表示法。轉換過程請參考文獻[52]，本論文將不再贅述。依據 Chuang et al. [52]對傳統位元_並列高斯正規基底乘法的推導，對於上述屬於具型 t 之高斯正規基底 $\Psi=\left\{\alpha^{2^0},\alpha^{2^1},\alpha^{2^2},\ldots,\alpha^{2^{m-1}}\right\}$ 的兩元素 A 和 B 及其相乘後之結果 C ，由於高斯正規基底乘法相當困難，所以必須先轉換成多項式基底 $\Psi'=\left\{\gamma^0,\gamma^1,\gamma^2,\gamma^3,\ldots,\gamma^{mt}\right\}$，轉換的式子如下說明：

$$A=a_0\alpha^{2^0}+a_1\alpha^{2^1}+\ldots+a_i\alpha^{2^i}+\ldots+a_{m-1}\alpha^{2^{m-1}}=\begin{cases}a_0\left(\gamma^{2^0\tau^0}+\gamma^{2^0\tau^1}+\ldots+\gamma^{2^0\tau^{t-1}}\right)+\\ a_1\left(\gamma^{2^1\tau^0}+\gamma^{2^1\tau^1}+\ldots+\gamma^{2^1\tau^{t-1}}\right)+\\ \ldots+\\ a_{m-1}\left(\gamma^{2^{m-1}\tau^0}+\gamma^{2^{m-1}\tau^1}+\ldots+\gamma^{2^{m-1}\tau^{t-1}}\right)\end{cases}$$
$$=a_0'\gamma^0+a_1'\gamma^1+a_2'\gamma^2+\ldots+a_{mt}'\gamma^{mt},$$

如果 $k=2^i\tau^j \bmod mt+1$ 則 $a_k'=a_i$ $(0\le i\le m-1, 0\le j\le t-1,\ 0\le k\le mt)$，且 $a_0'=0$. 相同的，元素 B 亦可轉成多項式基底 Ψ' 如下：

$$B=b_0\alpha^{2^0}+b_1\alpha^{2^1}+\ldots+b_i\alpha^{2^i}+\ldots+b_{m-1}\alpha^{2^{m-1}}=b_0'\gamma^0+b_1'\gamma^1+b_2'\gamma^2+\ldots+b_{mt}'\gamma^{mt},$$

如果 $k=2^i\tau^j \bmod mt+1$ 則 $b_k'=b_i$ $(0\le i\le m-1, 0\le j\le t-1,\ 0\le k\le mt)$，且 $b_0'=0$.

因此，乘法 $C'=A'\times B'$ 計算如下：

$$C^{'}$$
$$= (a_0^{'}\gamma^0 + a_1^{'}\gamma^1 + a_2^{'}\gamma^2 + ... + a_{mt-1}^{'}\gamma^{mt-1} + a_{mt}^{'}\gamma^{mt}) \times (b_0^{'}\gamma^0 + b_1^{'}\gamma^1 + b_2^{'}\gamma^2 + ... + b_{mt-1}^{'}\gamma^{mt-1} + b_{mt}^{'}\gamma^{mt}) \quad (1)$$
$$= \begin{cases} a_0^{'}\gamma^0 b_0^{'}\gamma^0 + a_0^{'}\gamma^0 b_1^{'}\gamma^1 + a_0^{'}\gamma^0 b_2^{'}\gamma^2 + ... + a_0^{'}\gamma^0 b_{mt-1}^{'}\gamma^{mt-1} + a_0^{'}\gamma^0 b_{mt}^{'}\gamma^{mt} + \\ a_1^{'}\gamma^1 b_0^{'}\gamma^0 + a_1^{'}\gamma^1 b_1^{'}\gamma^1 + a_1^{'}\gamma^1 b_2^{'}\gamma^2 + ... + a_1^{'}\gamma^1 b_{mt-1}^{'}\gamma^{mt-1} + a_1^{'}\gamma^1 b_{mt}^{'}\gamma^{mt} + \\ ... + \\ a_{mt}^{'}\gamma^{mt} b_0^{'}\gamma^0 + a_{mt}^{'}\gamma^{mt} b_1^{'}\gamma^1 + a_{mt}^{'}\gamma^{mt} b_2^{'}\gamma^2 + ... + a_{mt}^{'}\gamma^{mt} b_{mt-1}^{'}\gamma^{mt-1} + a_{mt}^{'}\gamma^{mt} b_{mt}^{'}\gamma^{mt}. \end{cases}$$

根據特性 5，上式可簡化為：

$$C^{'}$$
$$= \begin{cases} a_0^{'}b_0^{'}\gamma^0 + a_0^{'}b_1^{'}\gamma^1 + a_0^{'}b_2^{'}\gamma^2 + ... + a_0^{'}b_{mt-1}^{'}\gamma^{mt-1} + a_0^{'}b_{mt}^{'}\gamma^{mt} + \\ a_1^{'}b_{mt}^{'}\gamma^0 + a_1^{'}b_0^{'}\gamma^1 + a_1^{'}b_1^{'}\gamma^2 + a_1^{'}b_2^{'}\gamma^3 + ... + a_1^{'}b_{mt-1}^{'}\gamma^{mt} + \\ ... + \\ a_{mt}^{'}b_1^{'}\gamma^0 + a_{mt}^{'}b_2^{'}\gamma^1 + ... + a_{mt}^{'}b_{mt-1}^{'}\gamma^{mt-2} + a_{mt}^{'}b_{mt}^{'}\gamma^{mt-1} + a_{mt}^{'}b_0^{'}\gamma^{mt} \end{cases} \quad (2)$$
$$= c_0^{'}\gamma^0 + c_1^{'}\gamma^1 + c_2^{'}\gamma^2 + ... + c_k^{'}\gamma^k + ... + c_{mt-1}^{'}\gamma^{mt-1} + c_{mt}^{'}\gamma^{mt},$$

$c_k^{'} \in GF(2)$ 且 $0 \le k \le mt$ 。

所以 $c_k^{'}$ 可由下式得到：

$$c_k^{'} = \sum_{x=0}^{mt} a_x^{'} b_{\langle k-x \rangle}^{'}, \quad (3)$$

$\langle s \rangle$ 表示 $s \bmod mt+1$。

因此，

$$c_0^{'} = a_0^{'}b_0^{'} + a_1^{'}b_{mt}^{'} + a_2^{'}b_{mt-1}^{'} + ... + a_{mt-1}^{'}b_2^{'} + a_{mt}^{'}b_1^{'},$$

$$c_1^{'} = a_0^{'}b_1^{'} + a_1^{'}b_0^{'} + a_2^{'}b_{mt}^{'} + ... + a_{mt-1}^{'}b_3^{'} + a_{mt}^{'}b_2^{'},$$

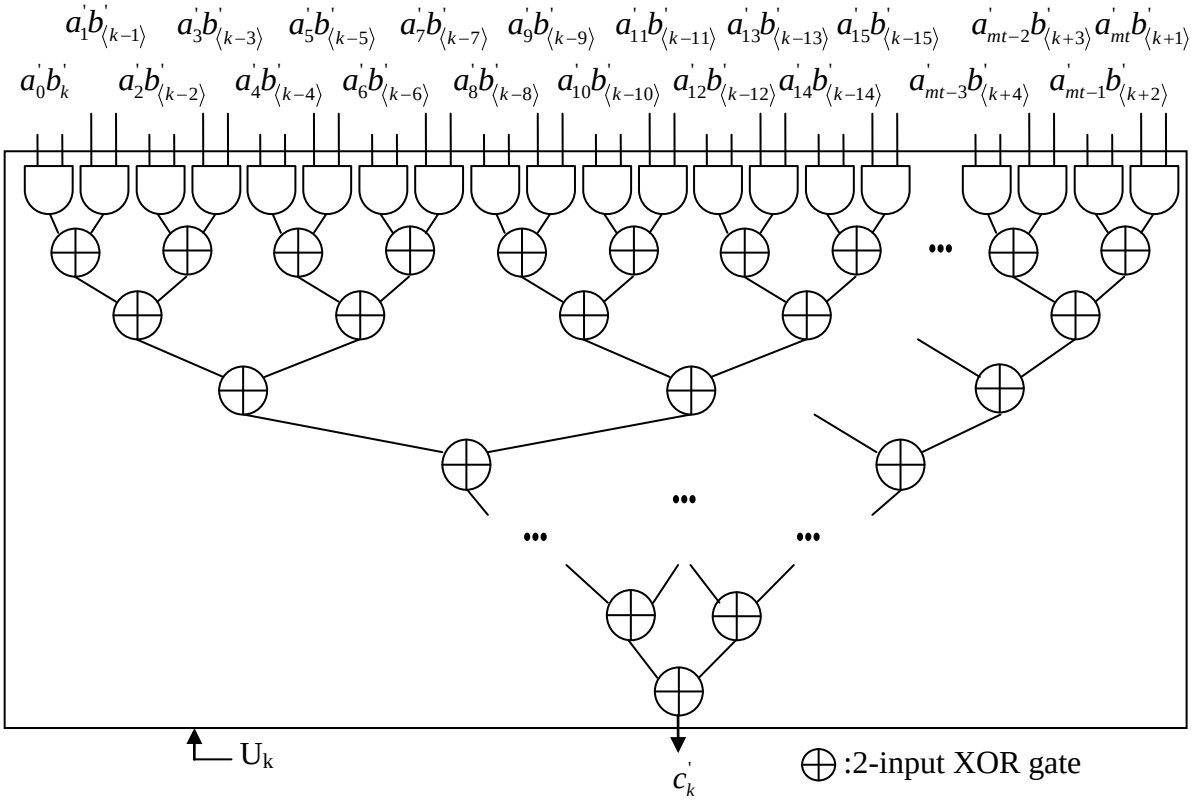
$$c_2^{'} = a_0^{'}b_2^{'} + a_1^{'}b_1^{'} + a_2^{'}b_0^{'} + ... + a_{mt-1}^{'}b_4^{'} + a_{mt}^{'}b_3^{'},$$

…

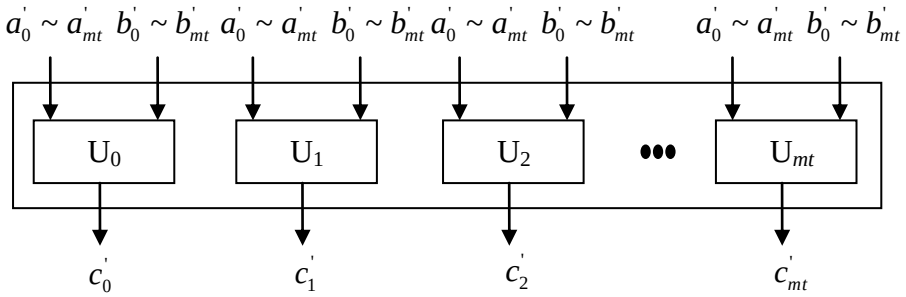
$$c_{mt}^{'} = a_0^{'}b_{mt}^{'} + a_1^{'}b_{mt-1}^{'} + a_2^{'}b_{mt-2}^{'} + ... + a_{mt-1}^{'}b_1^{'} + a_{mt}^{'}b_0^{'}.$$

根據式(3)，傳統二元樹狀互斥或閘架構產生結果位元 $c_k^{'}$ 如圖一所示。利用圖一，傳統高斯正規基底乘法器如圖二所示。傳統高斯正規基底乘法器需要 $mt+1$ 個圖一之樹狀架構，所需要之硬體成本相當高，另外觀察圖一及式(3)，高斯正規基底乘法器之 $mt+1$ 個圖一

之樹狀架構都是相同的架構，只是輸入值不同，所以如果只用一個硬體樹狀架構 U_k，重覆執行 mt+1 次，也能得到 mt+1 個結果位元，只是需要非常長之執行時間，即原來時間之 mt+1 倍。所以如何設計具有最佳成本×時間之高斯正規基底乘法器將是本論文之目的。



圖一：傳統高斯正規基底乘法器產生一結果位元之互斥或閘二元樹電路



圖二：傳統位元-並列高斯正規基底乘法器

肆、新位元_並列高斯正規基底乘法器

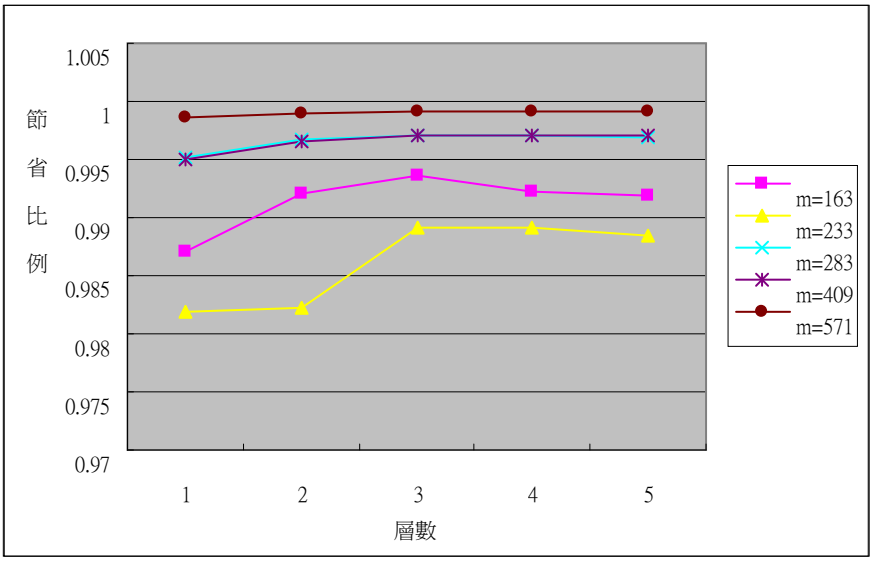
在傳統位元_並列高斯正規基底乘法器，每一結果位元需要一個互斥或閘二元樹，所以 *mt*+1 結果位元就需要 *mt*+1 個互斥或閘二元樹，硬體成本非常龐大。為了改善此問題，Chiou et al. [50]把 D 型正反器加在互斥或閘二元樹的每一層上，達到管線化架構的目的，因此只需要一個互斥或閘二元樹，就可讓 *mt*+1 結果位元重覆使用，節省相當多的硬體成本。在 Chiou et al. [50]提出的架構中一個互斥或閘會配上一個 D 型正反器，但從 NanGate's Library Creator and the 45-nm FreePDK Based Kit from North Carolina State University (NCSU) [51]數據上知道 D 型正反器所需要之 chip area 和傳輸時間都遠大於互斥或閘，所以一個互斥或閘配上一個 D 型正反器的架構並不是最佳的架構。為了探討此問題，我們利用多層互斥或閘加一層 D 型正反器的架構，計算其 Chip Area×Time 的最佳值，找出最佳層數來做為我們設計新型乘法器的參考。計算中之 Time 為 Input Transition=0.0012ns 及 Load Capacitance=0.3556fF 情況下之 Propagation Delay。表一列出傳統架構及各種互斥或閘層數在 NIST 建議 *m* 值(163、233、283、409、571)下之 Chip Area×Time 數值。當層數=1 即為 Chiou et al. [50]提出的架構。表二則秀出各種不同層數和傳統架構比較，節省之 Chip Area×Time 比例。圖三為表二之圖形表示，從圖三可知層數為 3 有最佳的結果。因此，為了有最佳的 Chip Area×Time，我們的新型位元_並列高斯正規基底乘法器採用每三層互斥或閘會加一層 D 型正反器如圖四所示，利用圖四之乘法器，即可完成完整之乘法，以 GF(2^{409})為例，輸入及輸出結果如圖五所示。在圖五，每組輸入隔一個時脈周期，所以每隔一個時脈周期即能產生一結果位元。新型位元_並列高斯正規基底乘法器比傳統乘法器節省 99.55% Chip_Area×Time，和 Chiou et al. [50]架構比較則節省 42.45%，請參考表三。

表一： Chip Area×Time 需求

m	163	233	283	409	571
層數	unit: $\mu m^2 \times ns$				
傳統	51009885	18476384	903701584	813314760	34606458621
1	656352	333426	4436139	4101096	49736400
2	408044	326844	2955489	2739665	33345774
3	324000	199584	2635458	2438813	29651724
4	391437	200037	2635136	2447094	29792568
5	417744	212212	2808927	2435328	31747284
6	453840				

表二： 比傳統架構節省 Chip Area×Time 之比例

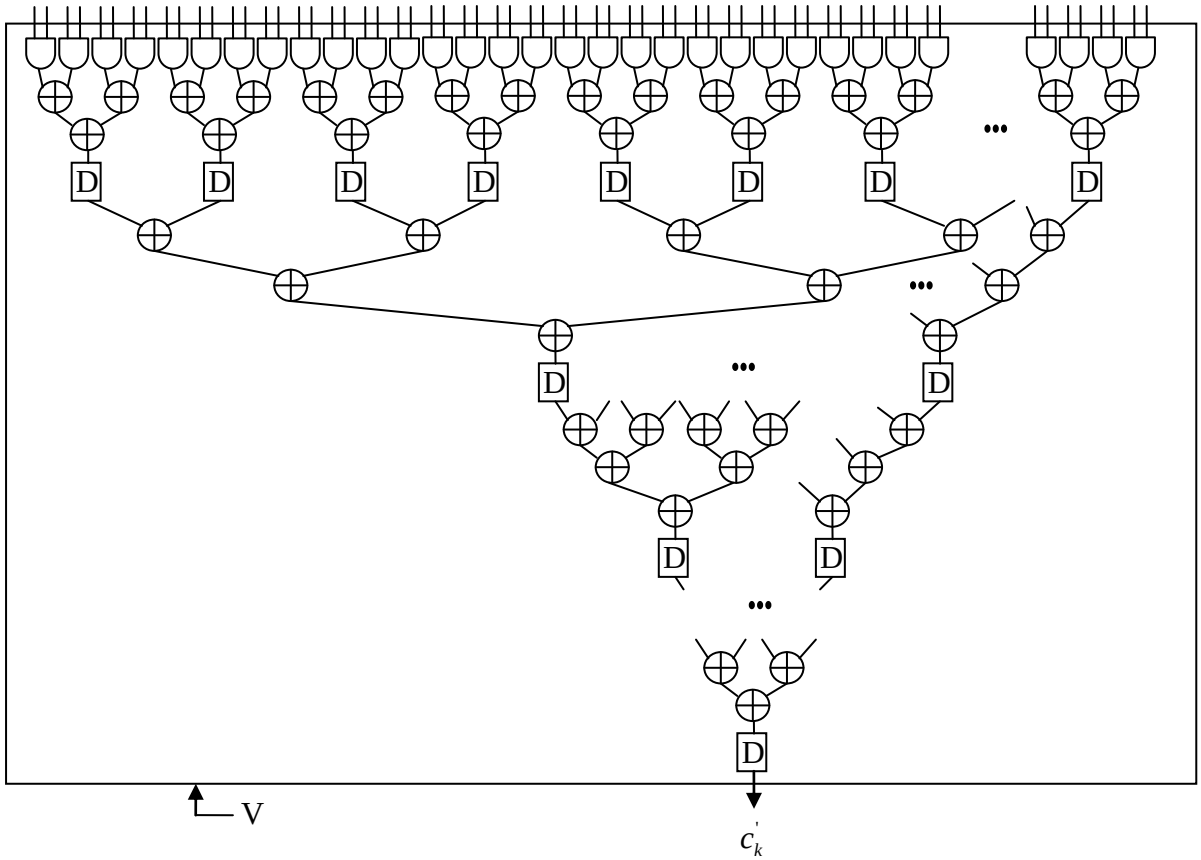
m 層數	163	233	283	409	571	平均
1	0.987133	0.981954	0.995091	0.994958	0.998563	0.99154
2	0.992001	0.98231	0.99673	0.996631	0.999036	0.993342
3	0.993648	0.989198	0.997084	0.997001	0.999143	0.995215
4	0.992326	0.989173	0.997084	0.996991	0.999139	0.994943
5	0.991811	0.988514	0.996892	0.997006	0.999083	0.994661
6	0.991103					



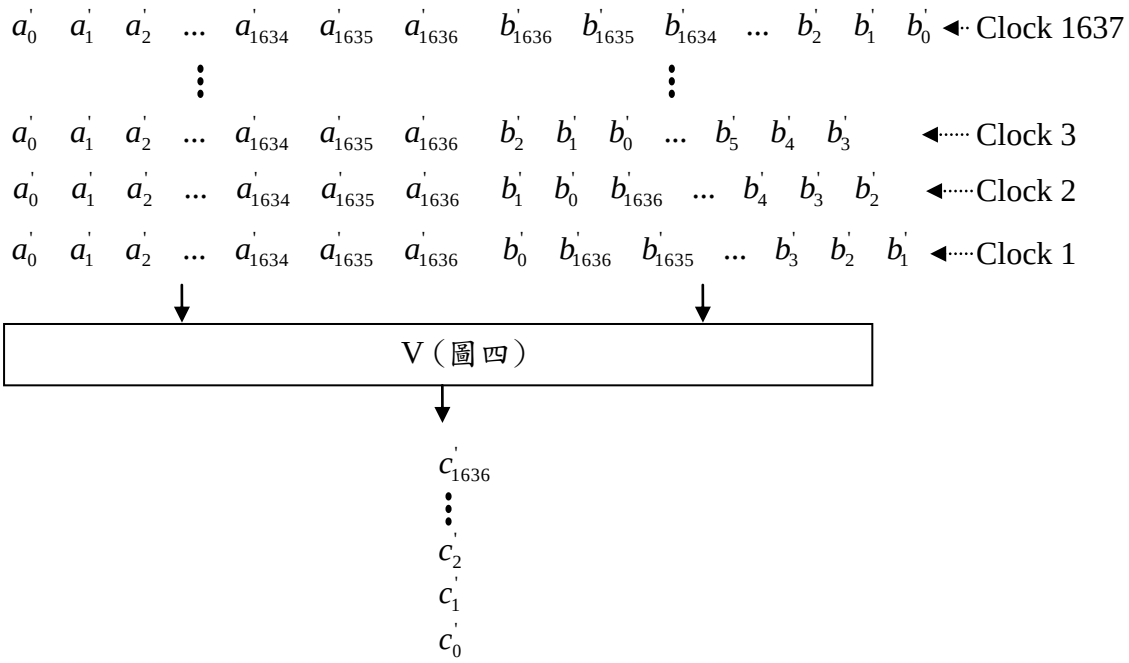
圖三：不同層數節省之比例

表三：不同位元_並列高斯正規基底乘法器之 Chip Area×Time 比較

乘法器 m	傳統乘法器 (圖二) (a)	Chiou et al. [50] (b)	新型乘法器 (圖五) (c)	節省之 Chip Area×Time 1-(c)/(a)	 1-(c)/(b)
163	51009885	656352	324000	0.993648	0.506362
233	18476384	333426	199584	0.989198	0.401414
283	903701584	4436139	2635458	0.997084	0.405912
409	813314760	4101096	2438813	0.997001	0.405327
571	34606458621	49736400	29651724	0.999143	0.403822
平均				0.9952148	0.4245674



圖四：新高斯正規基底乘法器之管線化互斥或閘二元樹電路



圖五：新位元-並列高斯正規基底乘法器執行乘法(以 GF(2^{409})為例)

伍、結論

世界上持有智慧型手機或平板電腦民眾愈來愈多，利用此類智慧型行動裝置進行電子商務行為也愈來愈普遍，因此適合行動電子商務交易安全之橢圓曲線密碼系統變得非常重要。實現橢圓曲線密碼系統核心元件-乘法器，引起許多專家學者注意及研究。針對橢圓曲線密碼系統，本研究提出具有最佳 Chip_Area×Time 之新型位元-並列高斯正規乘法器，採用每三層互斥或閘會加一層 D 型正反器架構。新型位元_並列高斯正規基底乘法器比傳統類似乘法器節省 99.55% Chip_Area×Time，和 Chiou et al. [50]架構比較則可節省 42.45% Chip_Area×Time。

[誌謝]

作者感謝健行科技大學資訊工程系『資訊工程實務專題』經費及中華民國國科會計畫(NSC 101-2221-E-231-024 及 NSC 102-2221-E-231-008)部份經費的支持，才能順利完成本論文之模擬及撰寫。

參考文獻

[1] W. Diffie and M.E. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, Vol.IT-22, No.6, pp.644-654, Nov. 1976.

[2] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, Vol.21, No.2, pp.120-126, Feb.1978.

[3] N. Koblitz, “Elliptic curve cryptosystems,” Math. Computal., Vol. 48, pp.203-209, 1987.

[4] V. S. Miller, “Use of elliptic curves in cryptography,” Advances in Cryptology Crypto’85, LNCS 218, Springer-Verlag, pp.417-426, 1986.

[5] W. Caelli, E. Dawson and S. Rea, “PKI, Elliptic curve cryptography and digital signatures,” Computer & Security, Vol.18, No.1, pp.47-66, 1999.

[6] S. Vanstone, “Elliptic curve cryptosystem – the answer to strong, fast public-key cryptography for securing constrained environments,” Information Security Technical Report, Vol.2, No.2, Elsevier, pp.78-87, 1997.

[7] ISO/IEC 11770-3:2008, “Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques,” 2008.

[8] ANSI X9.62-2005, “Public Key Cryptography for the Financial Services Industry : The Elliptic Curve Digital Signature Algorithm (ECDSA),” American National Standards Institute (ANSI), Nov. 2005.

[9] IEEE Standard 1363-2000, “IEEE standard specifications for public-key cryptography,”

Jan. 2000.

[10] FIPS 186-2, "Digital Signature Standard (DSS)," Federal Information Processing Standards Publication 186-2, Nat'l Inst. of Standards and Technology, 2000.

[11] T.C. Bartee and D. J. Schneider, "Computation with finite fields," Information and Computing, Vol.6, pp.79-98, Mar. 1963.

[12] E.D. Mastrovito, "VLSI architectures for multiplication over finite field GF(2^m)," Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Proc. Sixth Int'l Conf., AAECC-6, T. Mora, ed., Rome, pp.297-309, July 1988.

[13] Ç. K. Koç and B. Sunar, "Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields," IEEE Trans. Computers, Vol.47, No.3, pp.353-356, March 1998.

[14] T. Itoh and S. Tsujii, "Structure of parallel multipliers for a class of fields GF(2^m)," Information and Computation, Vol. 83, pp.21-40, 1989.

[15] C. Y. Lee, E. H. Lu, and J. Y. Lee, "Bit-parallel systolic multipliers for GF(2^m) fields defined by all-one and equally-spaced polynomials," IEEE Trans. Computers, Vol.50, No.5, pp.385-393, May 2001.

[16] C. Paar, P. Fleischmann, and P. Roelse, "Efficient multiplier architectures for Galois Fields GF(2^{4n})," IEEE Trans. Computers, Vol.47, No.2, pp.162-170, Feb. 1998.

[17] H. Wu, "Bit-parallel finite field multiplier and squarer using polynomial basis", IEEE Trans. Computers, Vol.51, No.7, pp.750-758, July 2002.

[18] H. Fan, M.A. Hasan, "A new approach to subquadratic space complexity parallel multipliers for extended binary fields," IEEE Trans. Computers, Vol.56, No.2, pp.224-233, Feb. 2007.

[19] J.-H. Guo and C.-L. Wang, "Digit-serial systolic multiplier for finite fields GF(2^m)," IEE Proc. Comput. Digit.Tech., Vol.145, No.2, pp.143-148, May 1998.

[20] C.H. Kim, C.P. Hong, and S. Kwon, "A digit-serial multiplier for finite field GF(2^m)," IEEE Trans. Very Large Scale Integration (VLSI) Systems, Vol.13, No.4, pp.476-483, April 2005.

[21] S. Kumar, T. Wollinger, and C. Paar, "Optimum digit-serial GF(2^m) multipliers for curve-based cryptography," IEEE Trans. Computers, Vol.55, No.10, pp.1306-1311, Oct. 2006.

[22] S. Talapatra, H. Rahaman, and J. Mathew, "Low complexity digit serial systolic Montgomery multipliers for special class of GF(2^m)," IEEE Trans. Very Large Scale Integration (VLSI) Systems, Vol.18, No.5, pp.847-852, May 2010.

[23] W.-T. Huang, C. H. Chang, C. W. Chiou, S.-Y. Tan, "Non-XOR approach for low-cost bit-parallel polynomial basis multiplier over GF(2^m)," IET Information Security, Vol.5,

No.3, pp.152-162, Sep. 2011.

[24] J. Xie, P.K. Meher, J. He, "Low-latency area-delay-efficient systolic multiplier over GF(2^m) for a wider class of trinomials using parallel register sharing," IEEE International Symposium on Circuits and Systems, (ISCAS'12), Seoul, Korea, pp.89-92, 20-23 May, 2012.

[25] J. Xie, J.J. He, P.K. Meher, "Low latency systolic Montgomery multiplier for finite field GF(2^m) based on pentanomials," IEEE Trans. VLSI Systems, Vol.21, No.2, pp.385-389, Feb. 2013.

[26] C.Y. Lee and C.W. Chiou, "Efficient design of low-complexity bit-parallel systolic Hankel multipliers to implement multiplication in normal and dual bases of GF(2^m)," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, Vol.E88-A, No.11, pp.3169-3179, Nov. 2005.

[27] J. L. Massey and J. K. Omura, "Computational method and apparatus for finite field arithmetic," U.S. Patent Number 4,587,627, May 1986.

[28] C. C. Wang, T. K. Truong, H. M. Shao, L. J. Deutsch, J. K. Omura, and I. S. Reed, "VLSI architectures for computing multiplications and inverses in GF(2^m)," IEEE Trans. Computers, Vol.C-34, No.8, pp.709-717, Aug. 1985.

[29] A. Reyhani-Masoleh, "Efficient algorithms and architectures for field multiplication using Gaussian normal bases," IEEE Trans. Computers, Vol. 55, No.1, pp.34-47, Jan. 2006.

[30] G.B. Agnew, R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone, "An implementation for a fast public-key cryptosystem," Journal of Cryptology, Vol.3, pp.63-79, 1991.

[31] M.A. Hasan, M.Z. Wang, V.K. Bhargava, "A modified Massey-Omura parallel multiplier for a class of finite fields," IEEE Trans. Computers, Vol.42, No.10, pp.1278-1280, Oct. 1993.

[32] S. Kwon, "A low complexity and a low latency bit parallel systolic multiplier over GF(2^m) using an optimal normal basis of type II," Proc. of the 16th IEEE Symposium on Computer Arithmetic, Santiago de Compostela, Spain, pp.196-202, 15-18 June 2003.

[33] H. Fan, M.A. Hasan, "Subquadratic computational complexity schemes for extended binary field multiplication using optimal normal bases," IEEE Trans. Computers, Vol.56, No.10, pp.1435-1437, Oct. 2007.

[34] C.-Y. Lee and C. W. Chiou, "Scalable Gaussian normal basis multipliers over GF(2^m) using Hankel matrix-vector representation," Journal of Signal Processing Systems for Signal Image and Video Technology, Vol.69, No.2, pp.197-211, Nov. 2012.

[35] C.W. Chiou, T.-P. Chuang, S.-S. Lin, C.-Y. Lee, J.-M. Lin, Y.-C. Yeh, "Palindromic-like representation for Gaussian normal basis multiplier over GF(2^m) with odd type-t," IET

Information Security, Vol.6, Iss.4, pp.318-323, Dec. 2012.

[36] C.W. Chiou, H.W. Chang, W.-Y. Liang, C.-Y. Lee, J.-M. Lin, Y.-C. Yeh, "Low-complexity Gaussian normal basis multiplier over GF(2^m)," IET Information Security, Vol.6, Iss.4, pp.310-317, Dec. 2012.

[37] E.R. Berlekamp, "Bit-serial reed-solomon encoder", IEEE Trans. Inf. Theory, Vol.IT-28, pp. 869-874, 1982.

[38] H. Wu, M. A. Hasan, and I. F. Blake, "New low-complexity bit-parallel finite field multipliers using weakly dual bases," IEEE Trans. Computers, Vol.47, No.11, pp.1223-1234, Nov. 1998.

[39] S. T. J. Fenn, M. Benaissa, and D. Taylor, "GF(2^m) multiplication and division over the dual basis," IEEE Trans. Computers, Vol.45, No.3, pp.319-327, March 1996.

[40] M. Wang and I.F Blake, "Bit serial multiplication in finite fields," SIAM J. Disc. Math., Vol.3, No.1, pp.140-148, Feb. 1990.

[41] J.-H. Wang, H.W. Chang, C.W. Chiou, W.-Y. Liang, "Low-complexity design of bit-parallel dual basis multiplier over GF(2^m)," IET Information Security, Vol.6, Iss.4, pp.324-328, Dec. 2012.

[42] M.K. Ibrahim and A. Aggoun, "Dual basis digit serial GF(2^m) multiplier," International Journal of Electronics, Vol.89, No.7, pp.517-523, July 2002.

[43] P.-L. Chang, L.-H. Chen, C.-Y. Lee, "Low-complexity dual basis digit serial GF(2^m) multiplier," ICIC Express Letters, Vol.3, No.4, pp.1113-1118, Dec. 2009.

[44] P.-L. Chang, F.-H. Hsieh, L.-H. Chen, C.-Y. Lee, "Efficient digit serial dual basis GF(2^m) multiplier," Proc. of the 2010 5th IEEE Conference on Industrial Electronics and Applications, ICIEA 2010, pp.166-170, Taichung, Taiwan, 15 June 2010.

[45] L.-H. Chen, P.-L. Chang, C.-Y. Lee, Y.-K. Yang, "Scalable and systolic dual basis multiplier over GF(2^m)," International Journal of Innovative Computing, Information and Control, Vol.7, No.3, pp.1193-1208, March 2011.

[46] Y.Y. Hua, J.-M. Lin, C.W. Chiou, C.-Y. Lee, Y.H. Liu, "A novel digit-serial dual basis Karatsuba multiplier over GF(2^m)," Journal of Computers, Vol.23, No.2, pp.80-94, July 2012.

[47] C. Paar, P. Fleischmann, and P. Roelse, "Efficient multiplier architectures for Galois Fields GF(2^{4n})," IEEE Trans. Computers, Vol.47, No.2, pp.162-170, Feb. 1998.

[48] R. Lidl and H. Niederreiter, Introduction to Finite Fields and Their Applications, New York: Cambridge Univ. Press, 1994.

[49] D.W. Ash, I.F. Blake, and S.A. Vanstone, "Low complexity normal bases," Discrete Applied Math., Vol.25, pp.191-210, 1989.

[50] C. W. Chiou, J.-M. Lin, Y.-K. Li, C.-Y. Lee, T.-P. Chuang, Y.-C. Yeh, "Pipeline Design of

Bit-Parallel Gaussian Normal Basis Multiplier over GF(2^m)," The Seventh International Conference on Genetic and Evolutionary Computing, Prague, Czech Republic, August 25-27, 2013. Full text also in Advances in Intelligent Systems and Computing, Vol.238, pp. 369-377, Aug. 2013.

[51] NanGate Standard Cell Library [Online]. Available: http://www.si2.org/openeda.si2.org/projects/nangatelib/.

[52] T.-P. Chuang, C.W. Chiou, S.-S. Lin, "Self-checking alternating logic bit-parallel Gaussian normal basis multiplier with type-t", IET Information Security, Vol.5, Iss.1, pp.33-42, March 2011.

[作者簡介]

蕭儒珣、呂松諭、廖柏維、葉耕禔、和徐子峯目前就讀於健行科技大學資訊工程系。邱綺文現為健行科技大學資訊工程系教授，邱教授於 2013 年 8 月榮獲英國 IET Fellow (Fellow of Institution of Engineering and Technology, UK)。