橢圓曲線密碼系統之低成本管線化位元-並列高斯正規基底乘法器

(Low-Cost Bit-Parallel Gaussian Normal Basis Multiplier with Pipeline Structure for Elliptic Curve Cryptosystem)

沈崑賢(Kun-Yin Shen)
健行科技大學資訊工程系
B10013168@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

唐仲儀(Jhong-Yi Tang)
健行科技大學資訊工程系
B10013158@uch.edu.tw

洪士軒(Shih-Syuan Hong)
健行科技大學資訊工程系
B10013131@uch.edu.tw

劉兆平(Jhao-Pian Liu)
健行科技大學資訊工程系
B10013159@uch.edu.tw

陳郭祐(Guo-You Chen)
健行科技大學資訊工程系
B10013147@uch.edu.tw

摘要

智慧型行動裝置如智慧型手機、平板電腦與筆記型電腦成長將遠超過當年個人電腦及網路化的普及率。透過智慧型行動裝置進行行動電子商務的安全付款，將會是非常重要的課題，行動電子商務安全則依賴密碼系統提供的安全。因為需要之鑰匙位元長度極短，橢圓曲線密碼系統非常適合資源受限之智慧型行動裝置。橢圓曲線密碼系統核心運算為乘法器，低硬體成本之乘法器將是資源受限之智慧型行動裝置需要的。本論文將提出新型管線化位元-並列高斯正規乘法器，和現存同類乘法器比較，可再節省約 66% chip area。

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

由於橢圓曲線密碼系統(elliptic curve cryptosystem, ECC)非常適合在智慧型行動裝置(如智慧型手機)等資源有限環境下使用，所以設計橢圓曲線密碼系統的主要運算元件，乘法器，是非常重要的課題。因此如何導出執行速度快速，硬體成本又節省的乘法器，是非常具挑戰又亟需的需求。

在 1985 年，美國華盛頓大學的 Koblitz [1]與 IBM 公司的 Miler [2]各自發表橢圓曲線密碼系統。橢圓曲線密碼系統是植基於解橢圓曲線離散對數問題(Elliptic Curve Discrete Logarithm Problem，ECDLP)上，橢圓曲線是定義在有限場(Finite Field)中，其常見之橢圓曲線方程式型式為 $y^2=x^3+ax+b \bmod p$。若橢圓曲線安全等級係使用 160 位元的模數(moduls)，而 RSA 及 ElGamal 系統卻需使用 1024 位元的模數(moduls)，才能達到足夠的安全等級[3][4]，所以說橢圓曲線運算效率遠較 RSA 及 ElGamal 為高。所以橢圓曲線密碼系統成為新一代的密碼學演算法，已變成國際標準如 ISO 11770-3 [5]、ANSI X9.62 [6]、IEEE P1363-2000 [7] 、FIPS 186-2 [8]等。在相同的安全強度下，由於橢圓曲線密碼系統的金鑰長度可遠較諸如 RSA 等其他密碼系統為小，而且需要較少之頻寬及記憶體，這使得橢圓曲線密碼系統非常適合在智慧型行動裝置等資源有限環境下使用。橢圓曲線密碼系統安全性除了解 DLP(Discrete logarithm problem)問題是 NP-Complete 外，另一個原因是因為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，再跟智慧型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)有三類，二進制延伸場(Binary extension field ($GF(2^m)$)，三進制延伸場($GF(3^m)$和質數場(Prime fields, GF(P))。二進制延伸場數值運算包含了乘法、除法、反元素等運算，其中乘法運算在密碼學的領域中佔有非常重要的地位。如新一代的加密標準 AES (Advanced Encryption Standard)就使用了二進制延伸場乘法運算進行其混合行運算(Mix column operation)。有效率的二進制延伸場乘法運算跟元素的基底表示法息息相關，最常被使用之有限場元素表示法有三種，即多項式基底(Polynomial Basis, PB) [9][10][11][12][13][14][15][16][17][18][19][20][21][22][23][24]， 正規基底(Normal Basis, NB) [11][24][25][26][27][28][29][30][31][32][33][34]，雙重基底(Dual Basis, DB) [24][35][36][37][38][39][40][41][42][43][44]表示法，每種基底表示法都有不同的優點和特性，也因此適合使用於不同應用。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。

Massey 和 Omura [25]在 1986 年第一個提出正規基底(NB)的乘法演算法，隨後，有許多的專家學者陸續提出 Massey 和 Omura 正規基底乘法演算法的變型 [11][26][27][28][29]。Wang et al. [26]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 [30]針對 optimal normal basis(type 2)提出 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 [27]則提出非 systolic array 架構之高斯(Gaussian)正規基底乘法器(type t)。Lidl 和 Niederreiter [45]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 GNB 存在[46]。所以 GNB 也是非常實用的。許多的標準都有包含 GNB，如 ANSI X9.62， FIPS 186-2， 和 IEEE Standard 1363-20000。由於橢圓曲線密碼系統非常適合在行動通訊(如手機)等資源有限環境下使用，所以做為橢圓曲線密碼系統的主要運算元件乘法器，如何導出低硬體成本的 GNB 乘法器，是非常具挑戰又亟需的需求，因此本論文將導出低成本的 GNB 乘法器。

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)、位元-並列(bit-parallel)、混合(hybrid) 、及位-串列(digit-serial)。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，但也需要很長執行時間之缺點。位元-並列乘法器每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。本論文將位元-並列乘法器架構做設計，位元-並列架構又可分為心臟型陣列(systolic array)及非心臟型陣列(non-systolic array)架構，非心臟型陣列架構一般稱為位元-並列架構，本論文將結合心臟型及位元-並列架構，提出管線化位元-並列 GNB 乘法器。Chiou et al. [47]第一個提出管線化位元-並列 GNB 乘法器，Chiou et al.在每一邏輯互斥或(XOR)閘層加一個正反器(D Flip-Flop)，以達到管線化目的，但是一個正反器的硬體成本是互斥或(XOR)閘的 2 到 3 倍，所以每一互斥或閘即加一個正反器，是划不來的，因此本文將提出新的管線化位元-並列 GNB 乘法器，進一步節省 Chiou et al. [47]發表之乘法器的硬體成本。

貳、數學背景

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：

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

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：

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

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 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。

參、傳統位元_並列高斯正規基底乘法器

依據 Chuang et al. [48]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 $\Psi=\left\{\alpha^{2^0},\alpha^{2^1},\alpha^{2^2},...,\alpha^{2^{m-1}}\right\}$ 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 $\Psi'=\left\{\gamma^0,\gamma^1,\gamma^2,\gamma^3,...,\gamma^{mt}\right\}$，轉換的式子如下說明：

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

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：

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

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：

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

根據特性 5，上式可簡化為：

$$C^{'} = \begin{cases} a_0^{'}b_0^{'}\gamma^0 + a_0^{'}b_1^{'}\gamma^1 + a_0^{'}b_2^{'}\gamma^2 + \ldots + a_0^{'}b_{mt-1}^{'}\gamma^{mt-1} + a_0^{'}b_{mt}^{'}\gamma^{mt} + \\ a_1^{'}b_{mt}^{'}\gamma^0 + a_1^{'}b_0^{'}\gamma^1 + a_1^{'}b_1^{'}\gamma^2 + a_1^{'}b_2^{'}\gamma^3 + \ldots + a_1^{'}b_{mt-1}^{'}\gamma^{mt} + \\ \ldots + \\ a_{mt}^{'}b_1^{'}\gamma^0 + a_{mt}^{'}b_2^{'}\gamma^1 + \ldots + a_{mt}^{'}b_{mt-1}^{'}\gamma^{mt-2} + a_{mt}^{'}b_{mt}^{'}\gamma^{mt-1} + a_{mt}^{'}b_0^{'}\gamma^{mt} \end{cases} \quad (2)$$

$$= c_0^{'}\gamma^0 + c_1^{'}\gamma^1 + c_2^{'}\gamma^2 + \ldots + c_k^{'}\gamma^k + \ldots + c_{mt-1}^{'}\gamma^{mt-1} + c_{mt}^{'}\gamma^{mt},$$

$c_k^{'} \in GF(2)$ 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 mod mt+1。

因此，

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

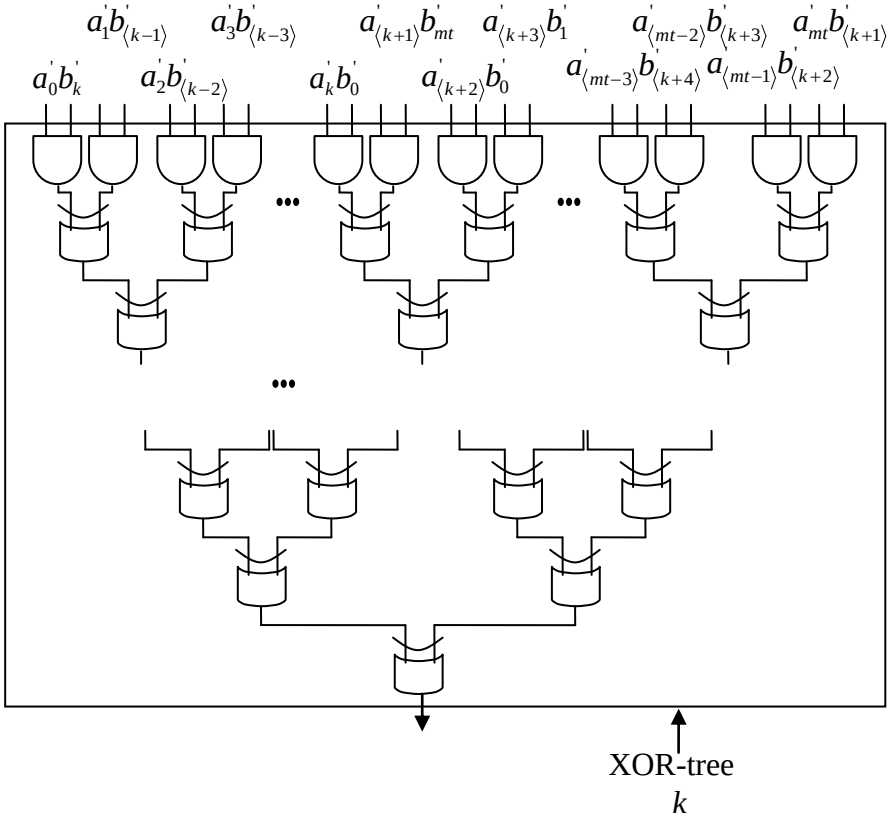
$$c_1^{'} = a_0^{'}b_1^{'} + a_1^{'}b_0^{'} + a_2^{'}b_{mt}^{'} + \ldots + a_{mt-1}^{'}b_3^{'} + a_{mt}^{'}b_2^{'},$$

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

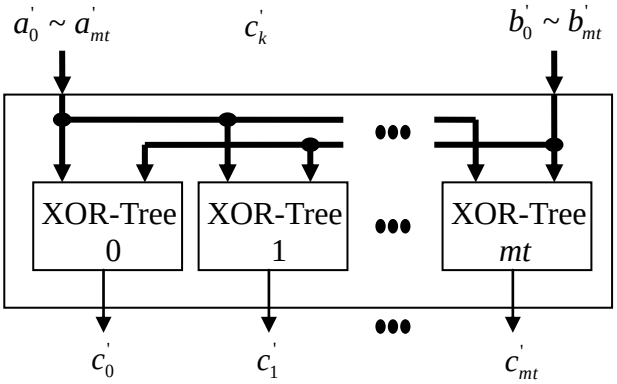
…

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

根據式(3)，傳統 XOR-tree 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。



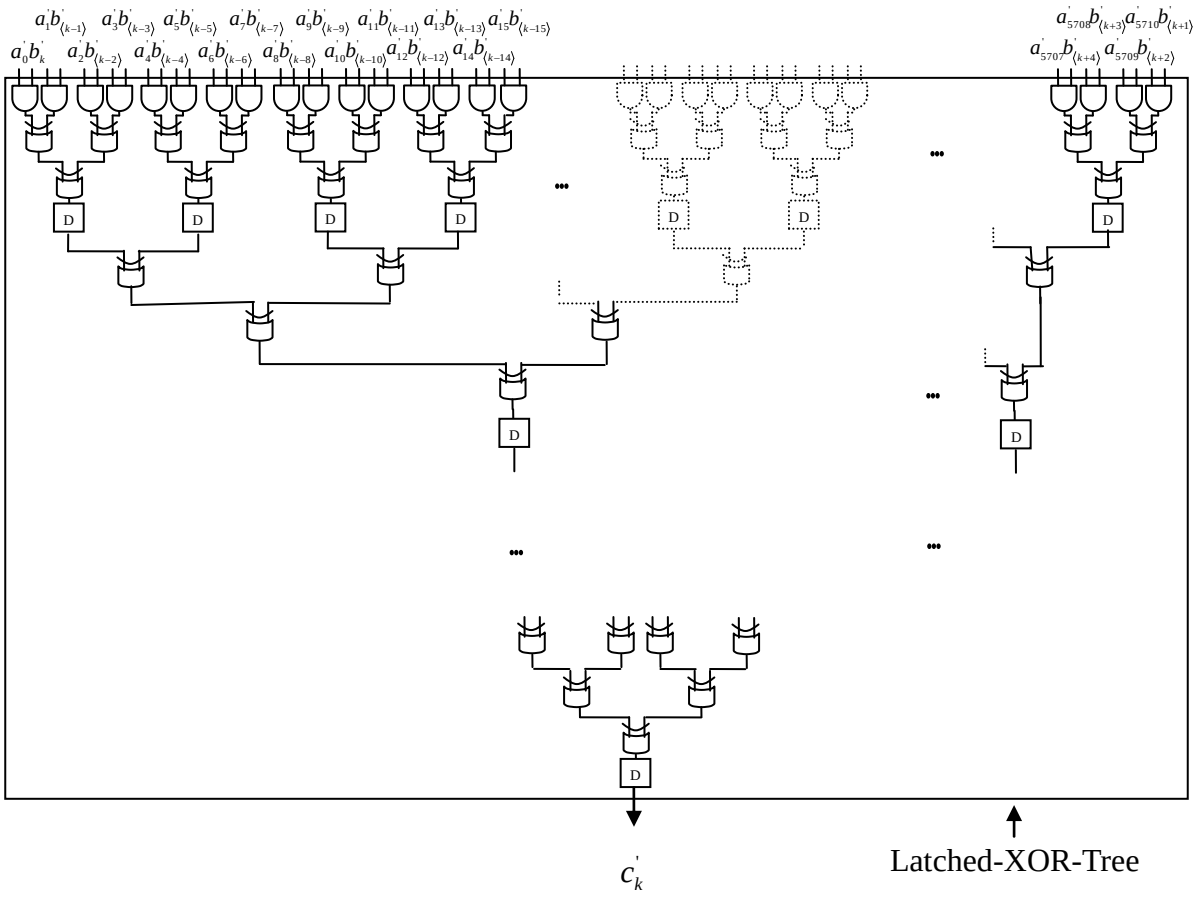
圖一：產生結果位元c_k'之傳統高斯正規基底乘法器電路



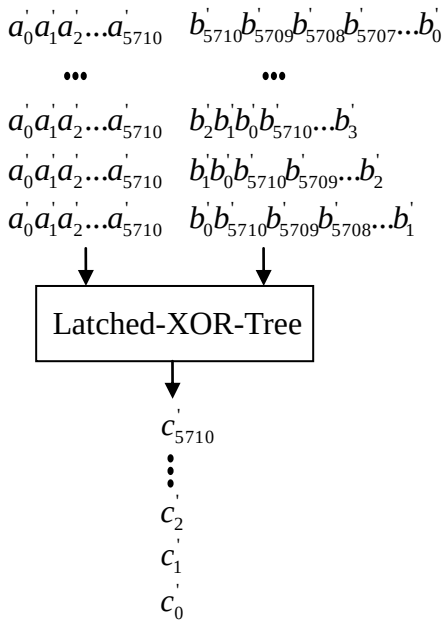
圖二：傳統位元-並列高斯正規基底乘法器

肆、新型管線化位元_並列高斯正規基底乘法器

在 2013 年，Chiou et al. [47]提出利用一個管線化結果位元電路重覆使用 *mt*+1 次，以順序產生 *mt*+1 之結果位元，以節省硬體成本，並可適合智慧型行動裝置之使用。Chiou et al. [47]每一互斥或閘即加一正反器，但是依照 NanGate's Library Creator and the 45-nm FreePDK Based Kit from North Carolina State University (NCSU) [49]，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，所以 Chiou et al. [47]提出的乘法器並不是最佳的結構。有鑑於此，經過模擬計算的結果，我們發現如果每三層互斥或閘再加一個 D 型正反器，可以有效的改善此問題。圖三為我們以 m=571 為例，畫出我們的管線化位元-並列高斯正規基底乘法器。圖四則為利用圖三執行乘法的情況。新型管線化位元-並列高斯正規基底乘法器和其他乘法器比較如表一及表二所示。表一及表二是以美國國家標準技術局(National Institute of Standards and Technology, NIST)建議之 5 個 *m* 值來比較。和 Chiou et al. [47]相比，我們的新型管線化位元-並列高斯正規基底乘法器平均可節省 66% chip area。



圖三：管線化位元-並列高斯正規基底乘法器(以 GF(2^{571})為例)



圖四：利用管線化位元-並列高斯正規基底乘法器執行乘法 (以 GF(2^{571})為例)

表一：成本比較-邏輯閘數

乘法器			傳統高斯正規基底乘法器 (圖二)	Chiou et al.[47] 乘法器	新型管線化高斯正規基底乘法器
m	t	邏輯閘			
163	4	AND	425756	652	652
		XOR	425756	651	651
		D	0	1309	187
233	2	AND	217622	466	466
		XOR	217155	465	465
		D	0	935	134
283	6	AND	2886601	1698	1698
		XOR	2881504	1697	1697
		D	0	3401	485
409	4	AND	2678132	1636	1636
		XOR	2676495	1635	1635
		D	0	3276	467
571	10	AND	32609810	5710	5710
		XOR	32604099	5709	5709
		D	0	11425	1631

表二：成本比較-Chip area

乘法器		傳統高斯正規基底乘法器 (圖二) (a)	Chiou et al.[47] 乘法器 (b)	新型管線化高斯正規基底乘法器 (圖三) (c)	節省硬體成本	
m	*t*	Area (μm^2)			1-(c)/(a)	1-(c)/(b)
163	4	1132511	7652	2578	99.77%	66.30%
233	2	578129	5466	1843	99.68%	66.26%
283	6	7670224	19894	6708	99.91%	66.28%
409	4	7121218	19164	6461	99.90%	66.28%
571	10	8672980	66850	22562	99.97%	66.24%
平均					99.84%	66.27%

伍、結論

已發表之位元-並列高斯正規乘法器架構，可分為心臟型陣列(systolic array)及非心臟型陣列(non-systolic array)架構。在 2013 年，Chiou et al. [47]第一個嘗試將非心臟型陣列的乘法器加上管線化設計，因此原本需要 mt+1 個 XOR-tree 單元的乘法器，減少到一個 XOR-tree 單元，重複在此 XOR-tree 單元執行 mt+1 次即可完成乘法動作。本論文秉持 Chiou et al. [47]精神，但是更進一步節省硬體成本。我們新型位元-並列高斯正規乘法器，是每三層互斥或(XOR)閘才加上正反器，代替 Chiou et al. [47]每一層互斥或(XOR)閘即加上正反器的架構。和 Chiou et al. [47]乘法器相比，此新型位元-並列高斯正規乘法器可節省約 66% chip area。

[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] N. Koblitz, "Elliptic curve cryptosystems," *Math. Computal.*, vol. 48, pp.203-209, 1987.

[2] V. S. Miller, "Use of elliptic curves in cryptography," *Advances in Cryptology Crypto'85*, LNCS 218, Springer-Verlag, pp.417-426, 1986.

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

[4] 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.

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

[6] 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.

[7] IEEE Standard 1363-2000, "IEEE standard specifications for public-key cryptography," Jan. 2000.

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

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

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

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

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

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

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

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

[47] 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.

[48] T.-P. Chuang, C. W. Chiou, S.-S. Lin, C.-Y. Lee, "Fault-tolerant Gaussian normal basis multiplier over GF(2^m)," IET Information Security, Vol.6, Iss.3, pp.157-170, Sep. 2012. NanGate Standard Cell Library [Online]. Available: http://www.si2.org/openeda.si2.org/projects/nangatelib.

[作者簡介]

沈崑賢、唐仲儀、洪士軒、劉兆平、和陳郭祐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)。