On-line Error Detection in Systolic Polynomial Basis Multiplier over GF(2^m) Using Parity Prediction Method

（具即時錯誤偵測能力之心臟型有限場多項式基底乘法器設計）

Chi-Ting Ma(馬季廷)[1], Chia-Jen Wu(吳嘉仁)[2], Che Wun Chiou(邱綺文)[3]

[1]Department of Computer Science and Information Engineering
Ching Yun University, Chung-Li 320, Taiwan
Email: m9713007@cyu.edu.tw

[2]Institute of Computer, Communication, and System Engineering
Ching Yun University, Chung-Li 320, Taiwan
Email: m9652004@cyu.edu.tw

[3]Department of Computer Science and Information Engineering
Ching Yun University, Chung-Li 320, Taiwan
Email: cwchiou@cyu.edu.tw

Abstract

Finite field arithmetic has been widely used in many cryptosystems, especially Elliptic Curve Cryptosystem (ECC). Recently, the new developed fault based cryptanalysis would attack both symmetrical and asymmetrical cryptosystems effectively. Thus, eliminating cryptographic computation errors becomes critical in preventing such kind of attacks. A simple way to eliminating cryptographic computation errors is to output correct or corrected ciphers. Therefore, we present a novel systolic polynomial basis multiplier in GF(2^m) with concurrent error detection capability using parity prediction method.

Keywords: Finite Fields、Error Detection、Polynomial Basis multiplier、Cryptography

摘要

現今許多的密碼系統皆廣泛利用有限場數值運算來提升加解密運算速度，而有限場(Galois Field)

乘法器為橢圓曲線密碼系統的核心數值運算，因此有限場乘法器的設計變得非常重要。近年興起的植入錯誤式密碼攻擊法(Fault Based Cryptanalysis)，可以利用破壞硬體加解密電路來快速破解密碼系統，使得密碼系統的安全性及保密性受到極大的威脅。為了防止植入錯誤式密碼攻擊法的最簡單方法就是避免輸出錯誤的資料，換句話說，如何讓加解密電路具有錯誤偵測能力是非常重要的。本文在此對有限場多項式基底之心臟型乘法器提出一種同位元預測法(Parity prediction)的錯誤偵測架構電路，其具有較節省電路成本之錯誤偵測能力和較快速的運算速度。
關鍵詞：有限場、錯誤偵測、多項式基底乘法器、密碼學。

一、簡介

隨著科技的快速發展, 電腦已成為每個人日常生活中不可缺少的夥伴，資訊安全的問題越來越重要, 例如電子交易系統給現代文明人帶來極大的便捷，只要透過 ATM 提款卡坐在家裡，利用讀卡機將提款卡資料讀到網路上點點滑鼠即可達到交易的效果，也因為如此方便的效果，如果駭客在資料傳輸的過程將資料竊取，輕則影響隱私權，重責導致存款被盜領或是被冒用人頭戶等等，因此如何在這個傳輸過程有良好的保護是絕對重要，也因此我們需要一個完善的密碼系統(Cryptosystem)。

密碼學領域中常見的密碼系統主要分為兩種類， 一種為秘密金鑰密碼系統(Secret Key Cryptosystem)及公開金鑰密碼系統(Public Key Cryptosystem)兩大類。秘密金鑰系統中較著名的有 AES(Advanced Encryption Standard) 、DES(Data Encryption Standard) 、IDEA(International Data Encryption Algorithm)，主要的特色為加密金鑰及解密金鑰相同，因此又稱為對稱式密碼系統，也因為金鑰相同因此加解密速度快是秘密金鑰密碼系統最大的優點，而其最大的問題是要如何讓發送端與接收端擁有相同的金鑰。公開金鑰密碼系統較著名的有 RSA (Rivest、Shamir、Adleman)、橢圓曲線密碼系統(Elliptic Curve Cryptosystem，ECC)等加密系統，因為其加解密需擁有公鑰及私鑰兩把不同的金鑰，主要的特色為兩把金鑰需相互對應，因此又稱為非對稱式密碼系統，也就是說用公鑰加密後的密文必須要使用私鑰才能得到解密後的明文，公開金鑰密碼系統中不會有發送端與接收端金鑰傳送的問題。

對稱式密碼系統跟非對稱式密碼系統中，對稱式密碼系統速度較快，相對的安全性就較低，在使用相同的加密位元數時，非對稱式密碼系統可以得到比較好的加密效果，能夠有力的防止密碼系統遭受破解，但因為非對稱密碼系統必需使用兩把金鑰加解密，速度也就較慢，也因為這樣的特點這兩大類密碼系統至今仍然是市場的主流。

在密碼系統核心運算的部份，已經不是單純的加法、乘法運算，近年來興起的有限場(Galois field,或Finite field)乘法器的乘法運算、除法運算與反元素運算已經漸漸成為密碼系統中重要的運用，特別是AES、RSA與ECC等密碼系統中也扮演相當重要的角色。因為在加密系統中的乘法器是最重要也最複雜的運算核心，且是最耗費時間的階段。在實現有限場乘法器中常用的基底有三種，分別為多項式基底(Polynomial Basis, PB) [2,4,10,11,13,15,17,19,21,26,31,33]、雙重基底(Dual Basis, DB) [7,12,14,16,20,23,24,28,29,30]、正規基底(Normal Basis, NB) [1,3,5,6,8,9,18,27]。

這三種基底分別代表著不同的特性及優點。多項式基底表示法的優點在於透過數學多項式的特性運用在硬體架構的低複雜度設計、規則化、簡單性、和模組化，因此多項式基底乘法器適合用在VLSI 乘法器設計。正規基底乘法的優點，是有限場中元素的平方運算可以利用循環的二進位位移達成，因此在執行平方運算、反元素運算和指數運算上有著非常高效率。而雙重基底

因使用兩種基底來做轉換，因此其電路成本相對較低，在本文中所採用的多項式基底乘法器依據其特性，設計出適用於FPGA上實現的乘法器架構。

隨著電腦科技的進步，駭客攻擊的手法層出不窮，在文獻探討中，植入錯誤式攻擊法(Fault Based Cryptanalysis)在破解秘密金鑰與公開金鑰密碼系統的技術上，利用非經由加密演算法破解而以外在因素的方式進行攻擊，利用不同的電力頻率或電壓導致加密晶片產生錯誤的運算結果，且已經被證明是相當有效的技術，藉由所得到的錯誤之運算結果推測出加密時所使用的金鑰，進而達到破解的目的，Kelsey 等人已經證明使用差分攻擊法只需要 50 至 200 個密文就能破解對稱式加密系統的DES(Data Encryption Standard)。為抵抗這種新型的植入錯誤式攻擊法，如何讓企圖破解密碼系統的駭客無法得到正確輸出，是目前有效的方法之一。

目前已經有許多學者提出防止植入錯誤式攻擊法的方法，主要可分為重覆運算法[25, 32]和同位元預測法[22, 26]，在 Reyhani-Masoleh 和 Hasan [10]針對有限場多項式位元並列和串列乘法器，利用同位元預測法提出非線上即時錯誤偵測方法，這個方法只能做到非線上即時錯誤偵測方法，本文針對此一缺點進行改良，乘法器架構改採用運算速度較快速的心臟收縮型乘法器配合同位元預測法的演算法，達到降低電路成本特性的錯誤偵測乘法器。

二、有限場之多項式基底乘法器

多項式在數學上，是以項次(Terms)結構總合表示，每一項包含一變數或多變數上升冪次與係數相乘表示之。若以多項式基底運算，係數是模以一個質數，稱之為有限場多項式基底(Polynomial basis)，以$GF(2^m)$表示。以下例子為一變數多項式：

$$A = a_{m-1}x^{m-1} + \cdots + a_2x^2 + a_1x^1 + a_0x^0$$
$$= \sum_{i=0}^{m-1} a_i x^i \qquad a_i, x^i \in \{0,1\}$$

此處a_i是係數，x是變數，下例為一多項式表示：

$$x^7 + x^5 + x^4 + x^3 + x + 1$$

若在有限場$GF(2^m)$中多項式與多項式數學運算，相同冪次方之變數與係數運算完成後再模(Modulo)一個質數可得運算結果，也就是在加法運算是用互斥或閘(XOR)，乘法運算用及閘(AND)，例如

$$(x^7 + x^5 + x^3 + x^2 + x + 1) + (x^6 + x^4 + x^3 + x + 1)$$
$$= x^7 + x^6 + x^5 + x^4 + x^2$$

以二進位表示法

10101111 + 01011011 =11110100

多項式基底的加法運算式中，對於任何元素$A, B \in GF(2^m)$可以表示成：

$$A = \sum_{i=0}^{m-1} a_i x^i$$

$$B = \sum_{j=0}^{m-1} b_j x^j$$

此處$a_i, b_j \in GF(2)$

C是A加B計算結果表示成:

$$C = A + B$$

$$= \sum_{i=0}^{m-1} a_i x^i + \sum_{j=0}^{m-1} b_j x^j$$

$$= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} (a_i x^i + b_j x^j)$$

模數運算的運算過程在下列方程式中表示：

$$\begin{aligned} & C(x) \\ & = A(x)B(x) \bmod P(x) \\ & = \left(a_0 x^0 + a_1 x^1 + a_2 x^2 + ... + a_{m-1} x^{m-1}\right) B(x) \bmod P(x) \\ & = \begin{pmatrix} a_0 x^0 B(x) \bmod P(x) + a_1 x^1 B(x) \bmod P(x) + a_2 x^2 B(x) \bmod P(x) + ... \\ + a_{m-1} x^{m-1} B(x) \bmod P(x) \end{pmatrix} \\ & = c_0 x^0 + c_1 x^1 + c_2 x^2 + ... + c_{m-1} x^{m-1}, \quad c_i \in \{0,1\}, 0 \le i \le m\text{-}1. \end{aligned} \tag{1}$$

$$B(x) = b_0 + b_1 x + b_2 x^2 + ... + b_{m-2} x^{m-2} + b_{m-1} x^{m-1}$$

$$\begin{aligned} & xB(x) \\ & = b_0 x + b_1 x^2 + b_2 x^3 + ... + b_{m-2} x^{m-1} + b_{m-1} x^m \\ & = \begin{pmatrix} b_0 x + b_1 x^2 + b_2 x^3 + ... + b_{m-2} x^{m-1} + \\ b_{m-1}\left(p_0 + p_1 x + p_2 x^2 + ... + p_{m-1} x^{m-1}\right) \end{pmatrix} \\ & = \begin{pmatrix} b_{m-1} p_0 + \left(b_0 + b_{m-1} p_1\right) x + \left(b_1 + b_{m-1} p_2\right) x^2 + ... + \\ \left(b_{m-2} + b_{m-1} p_{m-1}\right) x^{m-1} \end{pmatrix} \end{aligned} \tag{2}$$

模數運算實例部份當 $C(x) = A(x) \times B(x) \bmod P(x)$，其中假設 m=4 的情況下，$A(x) = 0011$，$B(x) = 0010$，$P(x) = 10011$ 根據公式(1)與(2)可以求得 $C(x) = 0110$。

因此可以發現在使用硬體設計乘法器中，多項式基底因具有規則性、簡單性、模組化和低複雜度，相當適合在 VLSI 的設計，圖 1 即為利用公式(1)與(2)所實現出，由 $m \times m$ 個 U 細胞電路所組成的有限場多項式基底心臟型乘法器。

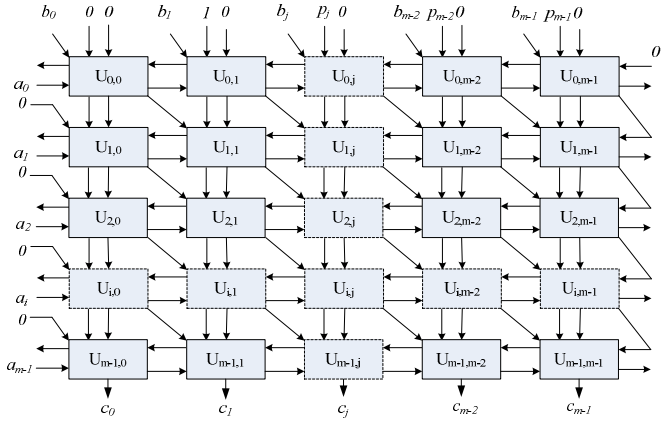

圖 1 有限場多項式基底之心臟型乘法器

其中每個U細胞電路的內部電路如圖 2 所示。

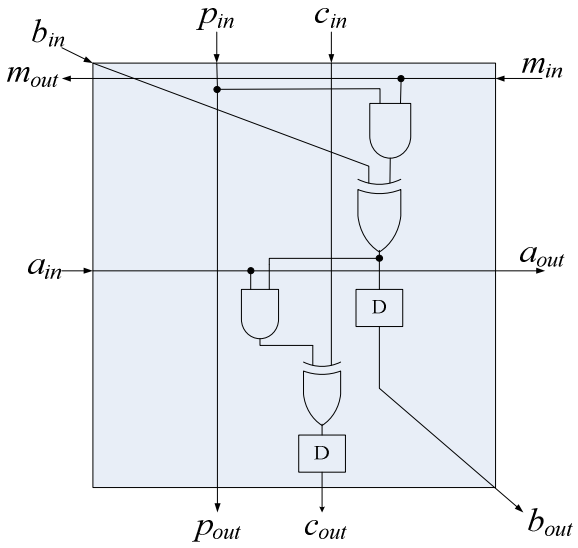

圖 2 U 細胞

三、錯誤偵測能力設計

在錯誤偵測階段所使用的是同位元預測方法(Parity prediction)，同位元預測法，是一個已經有明確概念的方法，能夠預測出運算結果的相同位元以用來和實際運算出來的結果做比對，由於要預測出運算結果必須使用另一個演算法，若是在設計時，將兩種演算法分離將會造成電路成本提高，所以最好的同位元預測法應該是依據原始演算法加以改良，使得只需增加少許的電路，

就能將其合併成一個具有乘法功能且有同位元預測法的演算法。

文獻探討中，同位元預測法常設計於一般平行架構與串列式架構的多項式基底之有限場乘法器之中，在 Bayat Sarmadi 和 Hasan [26]中所討論的錯誤偵測架構，即為採用此種方法。主要的設計理念是將乘法器的運算過程中為成多個部份，針對多個部份各別做錯誤偵測，在乘法器運算結束之後將所得到的所有預測位元經過 XOR Tree，若結果為 0 即代表所得到運算結果並未遭受植入錯誤；而相反地，得到結果為 1 將得知此運算結果是遭受植入錯誤，是一錯誤的運算結果。圖 3 為此一架構的示意圖。

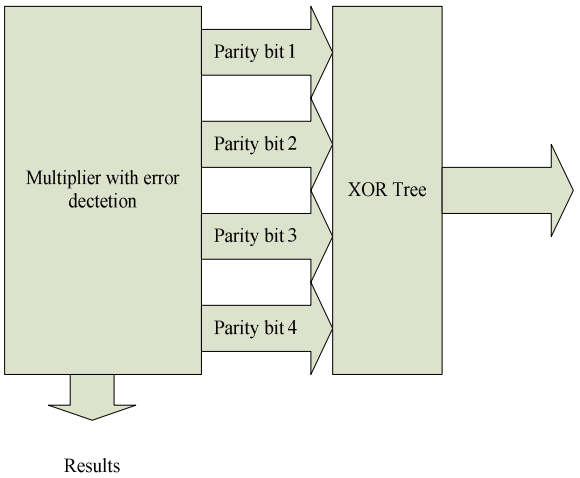

圖 3 同位元預測法示意圖

對論文中所使用的同位元預測法做進一步說明，選用此方法的原因是參考了文獻中 Lee et al. [12]在 2005 年提出的論文，利用雙重基底(Dual basis)之有限場乘法器的特性做出具有預測同位元的功能並達到偵錯能力和 Bayat Sarmadi 和 Hasan [26]在 2007 所提出的平行計算有限場乘法器同位元預測法，並將這兩篇論文的想法做一結合應用在心臟型多項式基底乘法器。

有限場的乘法運算依據前面章節所介紹的有限場乘法器之公式 1 與公式 2 可以達成，為了實現同位元預測法，必須設計另一個運算法來追蹤原本的乘法運算，由於乘法器是使用心臟型具有規律性的硬體架構，因此可以將同位元預測法設計成每計算出一列結果做比對一次，以達到快速偵測錯誤之目的。

同位元預測法中所使用的各個乘法運算元，其同位元表示如下：

$$A_p = (a_0 + a_1 + a_2 + ... + a_{m-1}),$$

$$B_p = (b_0 + b_1 + b_2 + ... + b_{m-1}),$$

$$C_p = (c_{p,0} + c_{p,1} + c_{p,2} + ... + c_{p,m-1}), \text{和}$$

$$P_p = p_0 + p_1 + p_2 + ... + p_{m-1} + p_m = p_0 + p_1 + p_2 + ... + p_{m-1}$$

並將 B_p^i 設成 B^i 的同位元之係數，即 $B_p^i = \sum_{j=0}^{m-1} b_j^i$ ，推導過程如下：

$$\begin{aligned} & B_p^0 = B_p \\ & B_p^{i+1} \\ & = (b_0^{i+1} + b_1^{i+1} + ... + b_{m-1}^{i+1}) \\ & = (b_0^i + b_1^i + ... + b_{m-1}^i) + b_{m-1}^i (p_1 + p_2 + ... + p_{m-1}) \\ & = B_p^i + b_{m-1}^i P_p \end{aligned} \quad (3)$$

依據公式 4.1，即可求得 C_p 表示如下：

$$\begin{aligned} & C_p \\ & = c_0 + c_1 + ... c_{m-1} \\ & = \sum_{i=0}^{m-1} a_i b_0^i + \sum_{i=0}^{m-1} a_i b_1^i + ... + \sum_{i=0}^{m-1} a_i b_{m-1}^i \\ & = \sum_{i=-0}^{m-1} a_i (b_0^i + b_1^i + ... + b_{m-1}^i) \\ & = \sum_{i=0}^{m-1} a_i B_p^i \end{aligned} \quad (4)$$

心臟型乘法器運算過程中配合公式 3 與公式 4，即能在心臟型乘法器每一列運算結束後立即求出與該列運算結果相對應的預測位元，如果心臟型乘法器最終計算出的結果 C 值與同位元預測法求得的 C_p 值，經過 XOR Tree 產生的位元做比對，若兩者的數值不一致時，即代表乘法器遭受破壞。

圖 4 為此一方法的電路架構圖，圖中右半部為心臟型乘法器為了清楚表示此方法，因此將電路由每一列的方塊來表示，將乘法器運算的結果和同位元預測方法的結果，在運算完成後經由 XOR Tree 的電路求得該方法所欲比對的數值，由於其錯誤比對是於運算結束後才比對。

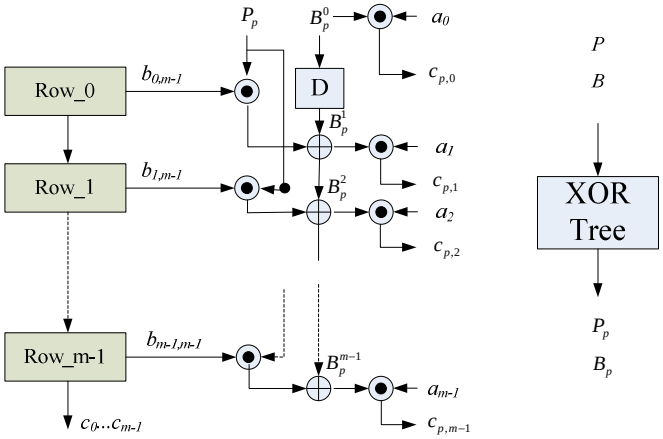

圖 4 同位元錯誤偵測法之有限場乘法器

四、同位元預測法乘法器比較

在文獻探討中將圖 4 與 Bayat Sarmadi 和 Hasan [26]在 2007 年所提出的方法做一比較，在相同的同位元錯誤偵測法之平行處理乘法器架構下，Bayat Sarmadi 和 Hasan [26]與圖 4 所使用的概念相當雷同，皆為利用有限場乘法器將每一列 c 值求出後，送進 XOR Tree 再與先前提出之方法得到預測的同位元做比對，然而圖 4 在偵錯方法所使用的電路成本較其來得低，而且在時間的延遲上也比較少，其中 Bayat Sarmadi 和 Hasan [26]中提到其預測同位元的所使用的位元數，設計時分別有 4、8、12、16、20 等五種情形，而這邊所選擇用來做比較的位元長度為 8 位元。表 1 為圖 4 與 Bayat Sarmadi 和 Hasan [26]中的錯誤偵測方法所需電路與耗費的時間做一比較，本文所提出的方法可以節省的時間約為 55%，電路成本節省約 50%。

五、結論與未來發展

以 FPGA 開發板來實現密碼系統中的錯誤偵測乘法器，可以模擬貼近真實硬體上面臨的問題並加以改善，以論文中所提出的方法和現有的方法具有更節省電路成本與更快的運算速度，其中具平行處理之心臟型有限場多項式基底乘法器，在錯誤偵測架構部份，同位元預測法可達到錯誤偵測的功能，且與同樣使用同位元預測法 Bayat Sarmadi 和 Hasan [26]的架構相比之下，在面對單一植入錯誤攻擊法時具有 100%的錯誤偵測能力，且能夠節省電路成本約 50%並且節省 55%時間。

表 1 同位元預測法乘法器比較

	Bayat Sarmadi 和 Hasan [26]	圖 4
Time Complexity		
Total delay (unit: ns)	124m	56m
Space Complexity		
2-input AND gates	m^2+8m	$2m^2 + 3m$
2-input XOR gates	$9m^2+7m$	$2m^2+85m$
Total transistor counts	$60m^2+31m$	$24m^2+528m$

參考文獻

[1] A. Reyhani Masoleh and M. A. Hasan, “A New Construction of Massey-Omura Parallel Multiplier over GF(2^m)”, IEEE Transactions Computers, vol. 51, no. 5, pp. 511-520, May. 2002.

[2] A. Reyhani Masoleh and M. A. Hasan, “Error Detection in Polynomial Basis Multipliers Over Binary Extension Fields”, Proc. of Cryptographic Hardware and Embedded Systems-CHES, vol. LNCS 2523, vol. 2523, pp. 515-528, 2002.

[3] A. Reyhani Masoleh and M. A. Hasan, “Fast Normal Basis Multiplication Using General Purpose Processors”, IEEE Transactions Computers, vol. 52, no. 11, pp. 1379-1390, November. 2003.

[4] A. Reyhani Masoleh and M. A. Hasan, “Fault Detection Architectures for Field Multiplication Using Polynomial Bases”, IEEE Transactions Computers, vol. 55, no. 9, pp. 1089-1103, September 2006.

[5] A. Reyhani Masoleh, “Efficient Algorithms and Architectures for Field Multiplication Using Gaussian Normal Bases”, IEEE Transactions Computers, vol. 55, no. 1, pp. 34-47, January 2006.

[6] B. Sunar and C. K. Koc, “An efficient optimal normal basis type II multiplier” , IEEE Trans. Computers, Vol. 50, No.1, pp.83-87, January 2001.

[7] C. C. Wang, “An algorithm to design finite field multipliers using a self-dual normal basis”, IEEE Trans. Computers, Vol.38, No.10, pp.1547-1459, October 1989.

[8] C. C. Wang, T. K. Truong, H. M. Shao, “VLSI architectures for computing multiplications and inverses in GF(2^m)” , IEEE Transactions Computers, Vol,C-34, No.8, pp.709-717, August 1985.

[9] C. W. Chiou, C. Y. Lee, J. M. Lin, “Concurrent error detection and correction in dual basis multiplier over GF(2^m)”, IET Circuits, Devices & Systems, vol. 3, no. 3, pp. 22-40, February. 2009.

[10] C. W. Chiou, L. C. Lin, F. H. Chou, “Low complexity finite field multiplier using irreducible trinomials”, Electronics Letters, vol. 39, no. 24, pp. 1709-1711, November 2003.

[11] C. Y. Lee, “Low-complexity bit-parallel systolic multipliers over GF(2^m)”, Integration, the VLSI Journal, vol. 41, no. 1, pp. 106-112, January 2008.

[12] C. Y. Lee, C. W. Chiou and J. M. Lin, “ Concurrent Error Detection in a Bit-Parallel Systolic Multiplier for Dual Basis of GF(2^m)”, Journal of Electronic Testing: Theory and Application , vol. 21, No. 5, pp. 539-549, October 2005.

[13] C. Y. Lee, C. W. Chiou and J. M. Lin, “Concurrent Error Detection in a Polynomial Basis Multiplier over GF(2^m)”, Journal of Electronic Testing: Theory and Applications, vol. 22, no. 2, pp. 143-150,June. 2006.

[14] 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.

[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] E. R. Berlekamp, "Bit-serial Reed-Solomon encoder", IEEE Transactions Information Theory, Vol. IT-28, no. 6, pp.869-874, November 1982.

[17] G. Seroussi, "Table of Low-Weight Binary Irreducible Polynomials", Visual Computing Dept., Hewlett Packard Laboratories, August 1998.

[18] H. Fan and Y. Dai, "Key function of normal basis multipliers in GF(2^m)" , Electronics Letters, Vol,38, No. 23, pp.1431-1432, 7th November 2002.

[19] H. Wu, "Bit-Parallel Polynomial Basis Multiplier for New Classes of Finite Fields", IEEE Transactions Computers, vol. 57, no. 8, pp. 1023-1031, August 2008.

[20] H. Wu, M. A. Hasan and I. F. Blake, "New low-complexity bit-parallel finite field multipliers using weakly dual bases", IEEE Transactions on Computers, vol. 47, no. 11, pp. 1223-1234, November 1998.

[21] J. L. Massey and J. K. Omura, "Computational method and apparatus for finite field arithmetic", U.S. Patent no. 4587627, May. 1986.

[22] J.-S. Horng, C.-Y. Lee, I.-C. Jou, "Fault-based triangular basis multiplication over GF(2^m) using bit-level parity prediction scheme" , Tencon 2007.Proceedings of the IEEE Region 10 Conference, pp. 1-4, October 2007.

[23] M. Morii, M. Kasahara, and D. L. Whiting, "Efficient bit-serial multiplication and the discrete-time Wiener-Hopf equation over finite fields", IEEE Transactions Information Theory, Vol.35, No.6, pp.1177-1183, November 1989.

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

[25] R. Hughey, "Concurrent Error Detection on Programmable Systolic Arrays", IEEE Transactions Computers, vol. 42, no. 6, pp752-756, June 1993.

[26] S. Bayat Sarmadi and M. A. Hasan, "On concurrent detection of errors in polynomial basis multiplication", IEEE Transactions on Very Large Scale Integration Systems, vol. 15, no. 4, pp. 413-426, April, 2007.

[27] S. Oh, C. H. Kim, J. Lim, "Efficient normal basis multipliers in composite fields" , IEEE Trans. Computers, Vol.49, No.10, pp.1133-1138, October 2000.

[28] S. T. J. Fenn, D. Taylor and M. Benaissa, "A dual basis bit-serial systolic multiplier for GF(2^m)", Integration, the VLSI Journal, vol. 18, no. 2, pp. 139, June. 1995.

[29] S. T. J. Fenn, M. Benaissa and D. Taylor, " GF(2^m) Multiplication and Division Over the Dual Basis", IEEE Transactions on Computer, vol. 45, no. 3, pp. 319-327, March. 1996.

[30] S. T. J. Fenn, M. Benaissa, and D. Taylor, "Dual basis systolic multipliers for GF(2^m)", IEE Proc. Comput. Digit. Tech., vol.144, no.1, pp.43-46, January. 1997.

[31] S. T. J. Fenn, M. G. Parker, M. Benaissa, “Bit-serial multiplication in GF(2^m) using irreducible all-one polynomials”, IEE Proceedings: Computers and Digital Techniques, vol. 144, no. 6, pp. 391-393, November. 1998.

[32] S. Y. Kuo, S. C. Liang, “Concurrent Error Detection and Correction in Real-Time Systolic Sorting Arrays”, IEEE Transactions Computers, Vol. 41, No. 12, December 1992.

[33] S.T.J. Fenn, M. Gossel, M. Benaissa, “On-Line Error Detection for Bit-Serial Multipliers in GF(2^m)”, Journal of Electronic Testing: Theory and Application, vol. 13, no. 1, pp. 29-40, August 1998.