行政院國家科學委員會專題研究計畫　成果報告

里德．所羅門解碼器之解碼策略

計畫類別：個別型計畫
計畫編號：NSC92-2218-E-009-019-
執行期間：92 年 09 月 01 日至 93 年 07 月 31 日
執行單位：國立交通大學電子工程研究所

計畫主持人：張錫嘉

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 93 年 11 月 3 日

An Universal VLSI Architecture for Bit-Parallel Computation in GF(2^m)

應用在里德．所羅門解碼之萬用型 GF(2^m)乘法器

里德．所羅門解碼器之解碼策略　　計畫編號：NSC92-2218-E-009-019

執行期間：92 年 9 月 1 日 至 93 年 7 月 31 日

主持人：張錫嘉 交通大學電子工程系助理教授

一、中文摘要

錯誤更正碼（Error-Control Codes）主要是用來保護數位資料，使其不會因為人為破壞或是傳輸過程發生錯誤而喪失。與其它錯誤更正碼比較，里德．所羅門碼具有最小冗值[1]的特性，相當適合用來消除突發性錯誤（burst error），近年來已被廣泛應用於數位通訊、光碟儲存以及高畫質電視等資訊家電系統。

為了探討里德．所羅門碼的解碼策略，我們針對有限場（finite field，GF(2^m)）的計算，提出一種架構在蒙哥馬利乘法理論下的通用 VLSI 架構，能夠對應各種有限場的 irreducible polynomial（或者說可對應各種次方值 m）。在實作上，使用 0.18μm 1P6M 的製程技術，能夠達到 125Mhz 的工作頻率。對於實現一個 m 小於 8 的萬用型的 GF(2^m)乘法器，總共使用了 1.4K 個邏輯個數。至於倒數運算，也可以藉由增加些許（0.3K）的控制電路來實現。

根據這樣萬用型的 GF(2^m)乘法器，未來我們將提出特別定義的 DSP，可同時解錯誤更正系統中的里德．所羅門碼以及加解密系統中的 AES（Advanced Encryption System）、ECC（Elliptic Curve Cryptography）。

英文摘要

While digital data are transmitted over a channel or a storage medium, error control coding techniques are usually utilized to mitigate the errors introduced during manufacturing or by user damage. Among the most well-known error-control codes, the Reed-Solomon(RS) codes are undoubtedly the most widely used block codes in storage and communications systems due to its excellent short burst error correcting capability.

In order to discuss the decoding strategy of Reed-Solomon decoders, an universal VLSI architecture for GF(2^m) computation is presented. Based on Montgomery multiplication algorithm, the proposed architecture is suitable for multiple class of GF(2^m) with arbitrary field degree m. After implemented by 0.18μm 1P6M process, our universal architecture can work successfully at 125MHz clock rate. For the finite field multiplier, the total gate count is 1.4K for GF(2^m) with any field degree m≤8, whereas the inverse operation can be achieved by the control unit with little gate count of 0.3K.

According to the universal GF(2^m) multipliers, a special definition of DSP processor can be proposed for communication systems. Not only Reed-Solomon codes can be decoded, but also the AES（Advanced Encryption System） or ECC（Elliptic Curve Cryptography） defined for security can also be decoded in our approach.

[1] 最小冗值，the lowest redundancy，means with the same error correct capability, RS code needs fewest overhead parity bytes.

二、計畫的緣由與目的

有限場的計算存在於許多的應用當中，例如錯誤更正碼或是加解密系統。如表一所示，不同應用的有限場定義也不相同，這意味著針對每一種不同的定義，必須製作其專屬的有限場乘法器。然而，隨著數位信號處理的技術越來越成熟，越來越多的的系統都仰賴數位信號處理器來處理資料；因此，對於數位信號處理器，一個通用的有限場乘法器是必要的。

表一：Irreducible Polynomial p(x)在不同應用下的定義

Cryptosystem		**AES system for GF(2^8), p(x) = $x^8+x^4+x^3+x+1$**
Flash		**(520,512) RS code for GF(2^{10}), p(x)= $x^{10}+x^3+x^2+x^1+1$**
ITU J.83	**Annex B**	**(128,122) RS code for GF(2^7), p(x) = x^7+x^3+1**
	Annex A,C	**(204,188) RS code for GF(2^8), p(x) = $x^8+x^4+x^3+x^2+1$**
	Annex D	**(207,187) RS code for GF(2^8), p(x) = $x^8+x^4+x^3+x^2+1$**
Blu-ray Disc	**LDC**	**(248,216) RS code for GF(2^8), p(x) = $x^8+x^4+x^3+x^2+1$**
	BIS	**(62,30) RS code for GF(2^8), p(x) = $x^8+x^4+x^3+x^2+1$**
	ADIP	**(15,9) RS code for GF(2^4), p(x) = x^4+x+1**

實際上，在有限場的運算中，加減法只是互斥的運算，我們感興趣是他的乘法運算和除法運算，而有限場的乘法運算主要在於 mod（modular）運算。因此，我們運用蒙哥馬利的理論來簡化 mod 運算，這個理論可以適用於各種的 irreducible polynomial 以及對應各種有限場的 m 值。

三、研究方法及成果

■ 蒙哥馬利乘法理論

當有限場元素在有限場次方值為 m，可以用多項式表示如下：:

$$A(x)=\sum_{i=0}^{m-1} a_i x^i = a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\ldots+a_1x+a_0$$

其中 $a_i \in GF(q)$。由於在多項式表示法中，有限場乘法即是多項式相乘再根據 irreducible polynomial 來作 mod 運算。假設有 A 和 B 兩個有限場元素, 而 *u(x)*為該有限場的 irreducible polynomial。則有限場的乘法可表示如下:

$$C(x)=A(x)B(x) \mod \mu(x) \qquad (2)$$

其中 *C(x)*也仍為該有限場的元素。

根據上述的 mod 運算特性，我們可以運用蒙哥馬利的乘法理論來計算 *C(x)*，如：

$$\hat{C}(x)=A(x)B(x)R^*(x) \mod \mu(x) \qquad (3)$$

$R^*(x)$ 為一固定的有限場元素，並且滿足 $R(x)R^*(x)=1 \ mod \ u(x)$，其中 $R(x)=x^m$。因此，*R(x)*和 *u(x)*總是維持互值的關係。式(3)也已經被證出可用接下來的兩多項式來取代:

$$Q(x)=A(x)B(x)\mu^*(x) \mod R(x) \qquad (4)$$

$$\hat{C}(x)=[A(x)B(x)+Q(x)\mu(x)]/R(x) \qquad (5)$$

其中 $u^*(x)$具有 $u(x)u^*(x)=1 \ mod \ R(x)$的特性。和式 3 比較,蒙哥馬利乘法理論將 mod 運算由 irreducible polynomial *u(x)*改成對 *R(x)*作 mod 和除法運算。因為 $R(x)=x^m$ ，所以在硬體實作上式(4)和式(5)的方法會較容易。此外，當 A 為多項式形式表現時,它可以被改寫成如下:

$$\hat{C}(x)=[a_{m-1}B(x)+[..[a_1B(x)+[a_0B(x)x^{-1} \bmod \mu(x)]]x^{-1} \bmod \mu(x)]...]x^{-1} \bmod \mu(x)$$

基於這個多項式和蒙哥馬利的乘法理論,我們可以推出有限場的蒙哥馬利乘法:

Montgomery multiplication algorithm (MM)

$S_0(x)=0;$

$for(i=0;i<m;i++)\{$

$\rho_i(x)=[(S_i(x)+a_iB(x))\mu^*(x)] \bmod x;$

$S_{i+1}(x)=[S_i(x)+a_iB(x)+\rho_i(x)\mu(x)]/x;$

$\}$

$\hat{C}(x)=S_m(x);$

其中 $u^x(x)$項為 irreducible polynomial *u(x)*的乘法反元素。

■ 萬用型 GF(2^m)有限場乘法器

由於在有限場中，各元素以位元的方法來表示，也就是說可以用二進位的表示法來簡化蒙哥馬利的乘法理論。因為 $u(x)$為 irreducible polynomial，$u(x)$和 $u^*(x)$除以 x 都會餘 1，意味著蒙哥馬利乘法理論中 $u^*(x)$項可以被省略。這使得 ρ(x)等於 $S_i(x)$和 $a_iB(x)$相加的最小位元值。

蒙哥馬利乘法中，遞迴的次數和有限場的次方值相關。當我們將式(4)和式(5)中的 $R(x)$更改成 x^d，其中 d 是大於等於 m 的常數。因為 $R^*_d(x) \bmod u(x)$是有限場的元素，所以他的乘法反元素 $R^*_d(x)$也同樣是有限場的元素，並且滿足 $R^*_d(x)R_d(x) = 1 \bmod u(x)$。這表示修改後的蒙哥馬利乘法理論，只要 m 小於等於 d 都可以適用。

Modified MM algorithm

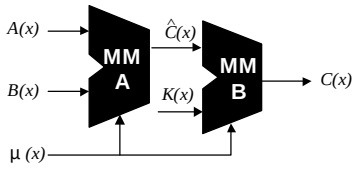
$$
\begin{aligned}
&MM(A(x),B(x),\mu(x))\{\\
&\ S_0(x)=0;\\
&\ for(i=0;i<d;i++)\{\\
&\qquad if(i\ge m)\qquad a_i=0;\\
&\qquad T(x)=S_i(x)+a_iB(x);\\
&\qquad S_{i+1}(x)=[T(x)+t_0\mu(x)]/x;\\
&\ \}\\
&\ \hat{C}(x)=S_d(x);\\
&\}
\end{aligned}
$$

其中 t_0 為暫存項 $T(x)$的最小位元值。

如果當有限場的次方值 m 小於等於 d 時，元素 A 的超過範圍 m 的位元值就為 0。由於蒙哥馬利的乘法在輸出值都伴隨一個 $R^*_d(x)$的常數項，必須藉著額外的蒙哥馬利乘法器乘上修正的常數項 K(x)使得結果正確。因此，整個有限場乘法 C(x)=A(x)B(x)可以被完成如下：

$$K(x) = x^{2d} \bmod \mu(x)$$
$$\hat{C}(x) = MM(A(x),B(x),\mu(x))$$
$$C(x) = MM(\hat{C}(x),K(x),\mu(x))$$

其中 $K(x)$為修正的常數項而 MM 指的是蒙哥馬利乘法器。換句話說，一個標準有限場乘法器，需要兩個蒙哥馬利乘法器作串聯，如圖一所示。值得一提的是，某些情況（如倒數運算或是乘加運算）下並不需要乘上常數項 K(x)，此時可以省略第二個蒙哥馬利乘法器。



圖一：兩階段式有限場乘法器。

■ 萬用型 GF(2^m)有限場反向器

許多應用中都必須使用有限場的倒數運算。一般是利用查表的方式上在電路上實現倒數運算。在此，我們可以藉由增加些許控制電路，在萬用型有現場乘法器上實現倒數運算。首先，先介紹 Fermat 的倒數理論如下：

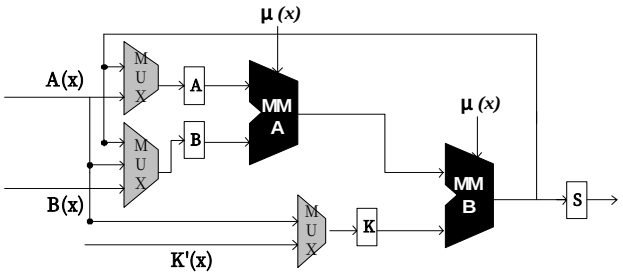
Fermat algorithm

$$
\begin{aligned}
&\beta^{-1} = \beta^{2^m-2}\\
&= \beta^{2+2^2+\ldots+2^{m-1}}\\
&= \beta^{2(1+2(1+\ldots))}\\
&= (\beta\ldots(\beta(\beta*\beta^2)^2)^2\ldots)^2
\end{aligned}
$$

因此，有限場的倒數運算可以當成一連串的平方運算和乘法運算；當 m=4 時，總共需要 m-1=3 個週期來完成運算。電路實作上，只要將本的兩階段式有限場乘法器加上些許控制電路，讓 MMA 當作平方器使用，就可以實作出有限場反向器，如圖二所示。表二列出整個倒數運算的控制流程：一開始先輸入需要被倒數的有限場元素到 MMA 和 MMB，之後乘 MMB 所算出來的結果再當作 MMA 和 MMB 的輸入。在 m-2 的週期時，我們需要乘以一個常數項，也就是：

$$K'(x) = x^{-d} \bmod \mu(x),$$

其中此常數項 $K'(x)$只會跟 irreducible polynomial 有關。



圖三：通用式有限場反向器

表二：倒數運算時暫存器狀態

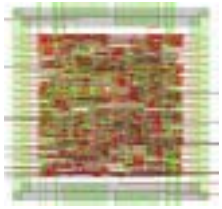
Register	ClockCycle		
	0	1~m-3	m-2
Reg A	A(x)	Out of MMB	Out of MMB
Reg B	A(x)	Out of MMB	Out of MMB
Reg K	A(x)	A(x)	K(x)
Reg S	0	0	Out of MMB

除此之外，在里德‧所羅門（Reed-Solomon）碼解碼程序中，不論是採用 Euclidean 或者 Berlekamp-Massey 理論，都用到了大量的乘加運算以及倒數運算。換言之，蒙哥馬利乘法理論所衍生之萬用型乘法器以及倒反器，在作相關解碼運算時將有相當大的好處。

■ 電路實現結果

我們利用 0.18um 1P6M 的製程技術來實現這個有限場乘法器以及反向器；邏輯閘個數約為 1700，面積為 0.16*0.16mm^2，運算頻率可以達到 125MHz。藉由插入一個管線暫存器，更可達到 250MHz 的運算速度。

Technology:	.18um 1P6M
Core size:	163*163um^2
Gate count:	1.7K
Speed:	125MHz



應用在 DSP 處理器時，與[1]相較，我們的架構不需額外的移位器。表三列出當有限場 m=8 時，兩者乘法器所需的週期數目（包含移位、乘法和加法）和最大延遲路徑。

表三：通用式乘法器的比較

	Critical path	Instruction cycle		
		C=AB	C=A/B	$C=\sum_{i=0}^{n-1} A_i B_i$
L. Song [1]	$8T_{AND}$ $+11T_{XOR}$	3	4*m*-4	3n-2
Proposed	$9T_{AND}$ $+15T_{XOR}$	2	2*m*-1	2*n*

四、結論與討論

基於蒙哥馬利的乘法理論，我們提出一個通用有限場乘法器。當我們設計有限場次方值為 d 的乘法器時，有限場次方值小於等於的 d 的都可以執行。由於所提出架構可以適用於各種不同的有限場次方值，應用在 DSP 處理器上，不論是通訊系統所需的錯誤更正碼（如 BCH、RS code），或者加解密系統（如 AES、RC4、ECC）等，都相當具有實用上的發展潛力。

本計畫屬一年期的國科會新進人員計畫，相關研究結果累計已發表 IEEE 會議論文 2 篇[2][3]以及專利申請[4]。

五、參考文獻暨相關著作

[1] L. Song, K.K. Parhi, I. Kuroda, and T. Nishitani, “Hardware/Software Codesign of Finite Field Datapath for Low Energy Reed-Solomon codecs”, IEEE Transactions on Very Large Scale Integration Systems, Vol. 8, No. 2, pp. 160-172, Apr. 2000.

[2] Chien-Ching Lin, Fuh-Ke Chang, Hsie-Chia Chang, and Chen-Yi Lee, “An Universal VLSI Architecture for Bit-Parallel Computation in GF(2^m),” has been accepted by IEEE APCCAS, Dec. 2004.

[3] Hsie-Chia Chang, Chien-Ching Lin, Tien-Yuan Hsiao, and et al., “Multi-level memory systems using error control codes,” in IEEE Int. Symposium on Circuits and Systems (ISCAS), vol. 2, pp. 393~396, Canada, May 2004.

[4] 吳介琮、汪大暉、張錫嘉, “組合多準位記憶單元並使其具備錯誤更正機制的方法,” 中華民國專利申請案號 93121302, 93 年 7 月 16 日。