$GF(P^{nm})$상의 다항식 분할에 의한 병렬 승산기 설계

오진영, 윤병희, 나기수, 김흥수
인하대학교 전자공학과
인천광역시 남구 용현동 253 인하대학교
e-mail : jinga@ee.inha.ac.kr

A Parallel Multiplier By Multidigit Numbers Over $GF(P^{nm})$

Jin Y. Oo, Byoung H. Yoon, G.S. Na, Heung S. Kim
Dept. Of Electronic Eng. Inha Univ,
253 Yong-hyundong Namgu Incheon 402-751 Korea
e-mail : jinga@ee.inha.ac.kr
FAX : 82-32-868-3654

ABSTRACT

In this paper proposes a new bit-parallel structure for a multiplier over $GF((P^n)^m)$, with k=nm. Mastrovito Multiplier, Karatsuba-ofman algorithm are applied to the multiplication of polynomials over $GF(2^n)$. This operation has a complexity of order $O(k^{\log_2 3})$ under certain constrains regarding k. A complete set of primitive field polynomials for composite fields is provided which perform modulo reduction with low complexity. As a result, multiplier for fields $GF(P^k)$ with low gate counts and low delays are constructed. The architectures are highly modular and thus well suited for VLSI implementation.

I. 서론

최근 집적회로 기술의 비약적인 발전으로 인해 단일 칩 상에 방대한 양의 회로가 집적 될 수 있게 되었지만 복잡하고 다양한 기능을 구현하기 위해 더 많은 소자들을 더 적은 면적의 칩 속에 집적해야 하는 것이 현재 집적회로 기술이 해결해야 할 과제로 떠오르고 있다. 이러한 문제들은 내부 결선도로 인한 구성의 한계로부터 기인하는 것이며 이를 해결하기 위한 많은 연구가 계속되고 있다. 그 중 최근 주목받고 있는 분야가 다치논리이론을 회로에 적용하는 것이다. 이는 하나의 신호선에 오직 두 개의 신호레벨만을 전송하는 것 보다 동일한 신호선에 더 많은 신호를 전송함으로써 내부결선의 복잡성을 감소시킬 수 있는 장점이 있다.

유한체는 컴퓨터 네트웍 및 통신 시스템등의 코딩, 암호화 등에 널리 쓰이고 있다. $GF(2^m)$상의 연산은 BCH 부호, Reed-Solomon부호, digital signal processing, error control coding과 보안 통신에 요구되는 암호화와 복호화등에서 상용되며, 이에 따라 승산과 역원계산에 관한 연구가 많이 이루어져 왔다. [1-3]

본 논문에서는 다치논리이론을 $GF(P^k)$에서의 표준기저로 표현된 승산기를 설계한다. $GF(P^n)$에서의 승산은 유한체에서의 연산을 하고, 결과는 $GF(P^m)$상의 원소들의 계수가 되고 Karatsuba-Ofman Algorithm(KOA)을 적용한 기약다항식 $G(x)$의 원소가 승산을 하면 $GF((P^n)^m)$에서의 승산과 같게 된다.[11] 여기서 k는 n×m을 의미하며 P개의 원소로 구성된 $GF(P)$의 k차 유한확대체 $GF(P^k)$으로 표시한다. 이때 P를 소수, P^k를 $GF(P^k)$의 크기라 한다. 여기서는 원소 사이에는 교환법칙, 결합법칙 및 분배법칙이 성립하고 영원, 단위원 및 가산과 승산에 대한 역원이 각각 유일하게 존재한다. 또한 $GF(P^k)$상에서의 모든 산술 연산은 mod P 연산으로 이루어진다[15].

II. $GF((P^n)^m)$에서의 승산

유한체에서의 승산은 다음과 같이 두 단계로 이루어진다.[12-14]

1) 일반적인 다항식 승산
2) 다항식의 모듈러 연산

여기서 사용되는 모든 연산은 $GF(P^n)$내에서 수행되고, $GF((P^n)^m)$는 $GF(P^n)$에서 $GF((P^n)^m)$로 확장된 유한체이고 최대 m-1차의 다항식을 갖는 $A(x)$, $B(x)$, $C(x)$로

이루어진다.

$$A(x)=a_{m-1}x^{m-1}+\ldots+a_0,\ a_i\in GF(G^n) \quad (1)$$

$$B(x)=b_{m-1}x^{m-1}+\ldots+b_0,\ b_i\in GF(G^n) \quad (2)$$

$$C(x)=c_{m-1}x^{m-1}+\ldots+c_0,\ c_i\in GF(G^n) \quad (3)$$

A=A(x)modP(x), B=B(x)modP(x), C=C(x)modP(x) $\in$GF((P^n)^m). 확장체의 기약다항식은 GF(P^n)에서의 원소를 계수로 갖는 m차의 기약 다항식 G(x)이다. 유한장에서의 원소A와 B의 승산은 다음과 같다.

$$C(x)=C'(x)\bmod G(x)=A(x)\times B(x)\bmod G(x) \quad (4)$$

여기서 사용되는 계수들의 모든 연산은 GF(P^n)내에서 수행되고 GF(P^n)에서의 기약 다항식은 다음과 같다.

$$Q(y)=y^n+q_{n-1}y^{n-1}+\ldots+q_0,\ q_i\in GF(P) \quad (5)$$

본 논문에서는 Mastrovito가 제안한 승산기를 이용하여 GF(P^n)에서의 승산기을 구성하였다.[12-13]

GF(P^n)상에서 원소를 A(y), B(y), C(y)라 하면 승산은 C(y)={A(y)B(y)} mod Q(y)가 되고 원소는 n보다 작은 차수의 다항식을 가지게된다.

$$c_{n-1}y^{n-1}+\ldots+c_0=(a_{n-1}y_{n-1}+\ldots+a_0)\times(b_{n-1}y^{n-1}+\ldots+b_0)\bmod Q(y) \quad (6)$$

여기서 A(y)는 피승수이고, B(y)는 승수이다. 따라서 A(y)와 Q(y)로 생성행렬 Z를 만들어 낼 수 있다.

생성행렬 Z= f(A(y),Q(y))는 다음과 같은 행렬식으로 나타낼 수 있다.

$$C=\begin{pmatrix}c_0\\c_1\\\vdots\\c_{n-1}\end{pmatrix}=ZB=\begin{pmatrix}f_{0,0}&\cdots&f_{0,n-1}\\\vdots&\vdots&\vdots\\f_{n-1,0}&\cdots&f_{n-1,n-1}\end{pmatrix}\begin{pmatrix}b_0\\b_1\\\vdots\\b_{n-1}\end{pmatrix} \quad (7)$$

계수 $f_{ij}\in$GF(P)는 a_i와 q_i에 의해서 표현 될수 있다. j=0 ; i=0, ... ,n-1이면 a_i이고, j=1, ... ,n-1 ; i=0, ... ,n-1이면 $u(i-j)\,a_{i-j}+\sum_{t=0}^{i}q_{j-1-t}\,a_{n-1-t}$이 된다.

$u(t)=1(t\geq 0)$

일반적인 곱셈을 수행한 후 다항식이 n차 이상이 되는 경우 다음 행렬과 같이 나타낼 수 있다.

$$\begin{pmatrix}y_n\\y_{n+1}\\\vdots\\y_{2n-2}\end{pmatrix}\equiv\begin{pmatrix}q_{0,0}&\cdots&q_{0,n-1}\\\vdots&\vdots&\vdots\\q_{n-1,0}&\cdots&q_{n-1,n-1}\end{pmatrix}\begin{pmatrix}1\\y\\\vdots\\y_{n-1}\end{pmatrix}\bmod Q(y) \quad (8)$$

Q행렬은 Z행렬을 만드는데 필요하다. n차의 기약다항식 Q(y)을 이용하여 y^n, y^{n+1}, ... , y^{2n-2}를 mod Q(y)에서의 다항식으로 바꾸어 주는 Q행렬은 Q(y) = $y^n+q_{n-1}y^{n-1}+\ldots+q_0$, $q_i\in GF(P)$의 계수들을 이용하여 구한다.

계수 $q_{i,j}$는 j=0, i=1,...,n-2인 경우 $q_{i-1,n-1}$이고, i=1, ... , n-2, j=1, ... ,n-2인 경우, $q_{i-1,n-1}\,q_{i-1,n-1}\,q_{0,j}$ 가 된다.원소 A(y)는 고정되어 있고 원소B(y)를 곱한다.

[예.1] GF(3^2)상의 원시 다항식 $Q(y)=y^2+y+2$로 놓고 원시근을 α로 정의하면 $Q(\alpha)$=0이다.

고정된 생성행렬(Z)을 만들기 위한 A(y)= $\alpha^6=\alpha+2$로 놓으면 생성행렬Z는 다음과 같은 형태로 나타난다.

$$C=\begin{bmatrix}c_0\\c_1\end{bmatrix}=\alpha^6B=ZB=\begin{bmatrix}2b_0+b_1\\2b_1+(b_0+2b_1)\end{bmatrix} \quad (8)$$

1. Karatsuba-Ofman 알고리즘 (KOA)에 의한 승산

GF(P^m)상에서의 기약다항식 G(x)의 원소의 승산은 GF((P^n)^m)에서의 원소를 원소에 포함하게 되기 때문에 좀더 효과적인 방법으로 KOA를 적용하였다.[11],[14]

이 알고리즘은 짝수개의 항을 가진 다항식을 절반으로 나누어고 나누어진 다항식을 하나의 계수로 놓는다.

다항식 A(x)와 B(x)를 연산할 경우 각 다항식은 최대 m-1차이고, 계수는 m개를 가지고 있다. C'(x)=A(x)B(x)에서 C'(x)의 최대 차수는 2m-2이다.

두 다항식을 차수가 높은 쪽과 낮은 쪽으로 절반씩 나누게 되면 다음과 같이 표시된다.

$$A=x^{\frac{m}{2}}(x^{\frac{m}{2}-1}a_{m-1}+\ldots+a_{\frac{m}{2}})+(x^{\frac{m}{2}-1}a_{\frac{m}{2}-1}+\ldots+a_0)=x^{\frac{m}{2}}A_h+A_l \quad (9)$$

$$B=x^{\frac{m}{2}}(x^{\frac{m}{2}-1}b_{m-1}+\ldots+b_{\frac{m}{2}})+(x^{\frac{m}{2}-1}b_{\frac{m}{2}-1}+\ldots+b_0)=x^{\frac{m}{2}}B_h+B_l \quad (10)$$

위 식들을 임의의 다항식D(x)로 정의하면 다음과 같다.

$$\begin{aligned}D_0(x)&=A_l(x)B_l(x)\\D_1(x)&=[A_l(x)+A_h(x)][B_l(x)+B_h(x)]\\D_2(x)&=A_h(x)B_h(x)\end{aligned} \quad (11)$$

따라서 다항식 C'(x)=A(x)B(x)는 다음과 같이 나타난다.

$$C'(x)=D_0(x)+x^{m/2}[D_1(x)-D_0(x)-D_2(x)]+x^mD_2(x) \quad (12)$$

여기서 구해진 A_l,A_h는 다시 반복해서 각각의 절반으로 반복해서 나누었다.

2. 유한체GF((P^n)^m)에서의 승산

다항식 A(x),B(x)는 유한체 GF((P^n)^m)의 원소이지만 C'(x)는 유한체로 바꾸어 주어야 하는데, 기약다항식 G(x)를 사용하여 축약을 하였다. 이 단계에서 '-'가 발생하게 된다. 2진의 경우는 '-'에 무관하지만 다치의 경우는 가산의 역원 (P-p)을 사용하였다.

다항식의 연산 $A(x)\times B(x)$에서 생성된 다항식은 2m-2차의 $C'(x)$이고, 이 다항식을 mod $G(x)$안에서의 모듈러 연산 결과로 다항식 $C(x)$를 얻었다.

$C(x)= c_{m-1}\,x^{m-1}+\ldots+c_0 \equiv C'(x) \bmod G(x)$

mod $G(x)$에 의한 축약을 행렬로 나타내면 2m-1개의 $C'(x)$의 계수를 이용하여 m개의 $C(x)$계수로 다음 행렬과 같이 나타냈다.

$$\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & r_{0,0} & \cdots & r_{0,m-2} \\ 0 & 1 & \cdots & 0 & r_{0,0} & \cdots & r_{1,m-2} \\ \vdots & \vdots & \vdots & 0 & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & r_{0,0} & \cdots & r_{m-1,m-2} \end{pmatrix} \begin{pmatrix} c'_0 \\ \vdots \\ c'_{m-1} \\ c'_m \\ \vdots \\ c'_{2m-2} \end{pmatrix} \quad (12)$$

위 행렬에서 $r_{i,j}$로 표시된 축약행렬 R은 하나의 $G(x) = x^m+ g_{m-1}\,x^{m-1}+\ldots+g_0$에 의해서 항상 일정하게 할당된다. 즉 R은 $G(x)$에 의해서 다음과 같이 결정된다. $r_{i,j}$는 j=0, i=0, ... ,m-1 일 경우 g_i가 되고 i =0, ... , m-1 , j=0 , ... , m-1 일 경우 $r_{i-1,j-1}+ r_{m-1,j-1}\,r_{i,0}$된다. 만일 j=0일 경우, $r_{i-1,j-1}$=0이 되고 $g_i \in GF(G^n)$이기 때문에 $r_{i,j} \in GF(G^n)$이다.

3. GF($(3^2)^4$) 상에서의 승산기

GF(3^4)에서의 기약다항식$G(x)$의 원소$A(x)$, $B(x)$, $C(x)$는 다음과 같이 나타낸다.

$A(x)= a_3\,x^3+ a_2\,x^2+ a_1x+ a_0$

$B(x)= b_3\,x^3+ b_2\,x^2+ b_1x+ b_0$

$C(x)= c_3\,x^3+ c_2\,x^2+ c_1x+ c_0$

; $a_i,\ b_i,\ c_i \in GF(3^4); A, B, C \in GF((3^2)^4)$ (13)

유한체에서의 승산은 $C(x)=A(x)\times B(x) \bmod G(x)$와 같이 연산되는데 이 연산에서 먼저 일반적인 다항식 승산이 이루어지고 유한체 다항식으로 모듈러 축약이 이루어진다. 이 두 연산은 GF(3^2)에서의 다항식 계수에서의 산술연산에 의해서 이루어진다.

위의 연산을 KOA에 적용시켜서 연산기의 설계하고. 주어진 다항식 $A(x)$, $B(x)$를 KOA에 의해서 두 번 반복해서 나누고 중간 변수를 d_i라 하였다. (i=0, ... ,8)

$d_0= a_0\,b_0$

$d_1=(a_0+ a_1)(b_0+ b_1)$

$d_2= a_1\,b_1$

$d_3=(a_0+ a_2)(b_0+ b_2)$

$d_4=(a_0+ a_1+ a_2+ a_3)(b_0+ b_1+ b_2+ b_3)$

$d_5=(a_1+ a_3)(b_1+ b_3)$

$d_6= a_2\,b_2$

$d_7=(a_2+ a_3)(b_2+ b_3)$

$d_8= a_3\,b_3$ (14)

이렇게 해서 만들어진 중간변수 d_i를 이용하여 승산결과의 다항식 $C'(x)$를 얻게 되고 계수들은 다음과 같이 나타냈다.

$c'_0= d_0$

$c'_1= d_1- d_0- d_2= d_1+2\,d_0+2\,d_2$

$c'_2= d_3- d_0- d_6+ d_2= d_2+ d_3+2\,d_0+2\,d_2$

$c'_3= d_4- d_5- d_3- d_7- d_1+ d_6+ d_8+ d_2$

$\quad = d_4+2\,d_5+2\,d_3+2\,d_7+2\,d_1+ d_6+ d_8+ d_2$

$c'_4= d_5- d_2- d_8+ d_6= d_5+ d_2+2\,d_8+2\,d_6$

$c'_5= d_7- d_6- d_8= d_7+2\,d_6+2\,d_8$

$c'_6= d_8$ (15)

위와 같이 $C'(x)$의 계수들을 구했고 다음은 모듈 연산에 의한 다항식 $C(x)$를 구했다.

$C(x)\equiv C'(x) \bmod G(x)= c_3\,x^3+ c_2\,x^2+ c_1x+ c_0$ (16)

모듈러 축약은 위의 7개의 계수 c'_k의 선형 사상에 의해서 c_i를 구했다.

$c_i= c'_i+ \sum_{j=0}^{2} r_{i,j}\,c'_{j+4}; i=0,\ldots,3;\ r_{i,j} \in GF(3^2)$ (17)

축약 계수 $r_{i,j}$는 원시 다항식 $G(x)$에 의해서 결정된다. $G(x)= x^4+ \sum_{i=0}^{3} g_i\,x^i,\ g_i \in GF(3^2)$ (18)

원시 다항식 $G(x)$의 계수에 의해서 $r_{i,j}$는 i = 0, 1, 2, 3 ; j = 0일 때 g_i의 값을 갖고 i= 0, 1, 2, 3 ; j =1, 2일 때 $r_{i-1,j-1}+ r_{3,j-1}\,r_{i,0}$ 의 값을 갖게 된다. 이 장에서의 함수들을 이용해서 c_i를 구하면

$c_0= c'_0+ c'_4$

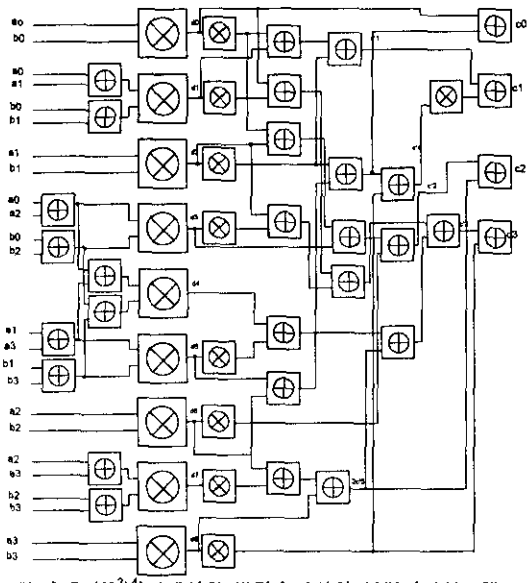
$c_1= c'_1+2\,c'_4$

$c_2= c'_2+2\,c'_5$

$c_3= c'_3+2\,c'_6$ (19)

GF(3^2)상에서의 원시 다항식 $Q(y)= y^2+y+2$와 GF(3^4) 상에서의 원시 다항식 $G(x)= x^4+x+2$를 적용하여 실제로 GF($(3^2)^4$)상에서의 승산을 블록 다이아그램으로 표현하였다. [그림1.]에서 표시된 입력 변수 a_0, a_1, a_2, a_3 와 b_0, b_1, b_2, b_3 출력 변수 c_0, c_1, c_2, c_3 들은 GF($(3^2)^4$)상에서의 원소를 나타내며, 각각의 변수들은 유한체에서의 원소를 나타내고 실

제로 2비트의 버스를 나타내고 있다.
그림1.에서 보면 모듈에 사용된 연산기들의 개수는72 mod3 승산기와 89 mod3 가산기를 사용하였다.



[그림1.] GF((3²)⁴)상에서의 병렬승산기의 블럭다이어그램

III. 결론

본 논문에서는 종전의 유한체 승산기 보다 효과적인 연산을 위해 Karatsuba-Ofman 알고리즘을 적용하고, 이를 유한체GF((Pⁿ)ᵐ)상으로 확장하여 실제로 GF((3²)⁴) 승산기를 설계하였다. 이전 연산기를 사용할 경우 48 mod2 승산기와 62 mod 가산기를 사용하고 2^8개의 정보를 한꺼번에 보내는 반면 3치연산기의 경우 더 많은 게이트가 필요로 하지만 3^8개의 정보를 한꺼번에 보낼 수 있다는 장점이 있다. 또한 본 논문에서 사용한 알고리즘은 본 논문에서 볼 수 있는 것과 같이 원시 다항식, 피승수의 선택에 따라서 게이트의 개수에 큰 영향을 미치게 된다. 위 예제에서 선택한 원시 다항식으로 설계할 경우 많은 게이트를 줄일 수 있는 것을 알 수 있다. 따라서 차후 과제는 다치, 즉 GF(Pᵏ)상에서 가장 간단하게 승산기를 설계할 수 있는 원시다항식을 찾아 적용하고 더 적은 복잡도를 갖는 다치회로를 구현하는 것이다.

[참고 문헌]

[1] V.B Afanasyev, "Complexity of VLSI Imple mentat -ion of Finite Field Arethmetic," Proc.II.Int'l Workshop Algebraic and Combinatorial Coding Theory, pp.6-7,leningrad, Sept. 1990

[2] V.B Afanasyev, "On the Complexity of Finite Field Arithmetic,"Proc.Fifth Joint Soviet-Swedish Int'l Workshop Information Theory, pp.9-12,Moscow,Jan.1991

[3] R.E Blahut, Fast Algorithms for Digital signal Processing. Reading, Mass.:addison-Wesley, 1985

[4] A.Menezes,I.Blake, X. Gao,R.Mullin,S.Vanstone,and T.Yaghgoobil. applications of Finite Fields.Kluwer Academic Publisher,

[5]S.T.J.Fenn,M.Benaissa,andD.Taylor,"GF(2ᵐ)Multiplica tion and Divison over the DualBase, "IEEETrans .Computers,vol.45,no.3 ,pp.319-327 ,Mar.1996

[6]W.Geiselmann,"Algebraische algorithmenentwicklung am Beispiel derarithmetik in Endlichen Korpern,"PhD thesis, Universitat Karlsruhe, Fakultat Fur Informatik, Institut fur algorithmen und Kognitive Systems, Karlsruhe, Germany,1993.

[7] D.H.Green and I.S.Taylor,"Irreducible Polynomials over ComPosite Galois Fields and Their Appplications in Coding TechniQues," Proc.IEE,vol.121, no.,pp.935-39, Sept.1974.

[8]M.A.Hasan,M.Wang, and V.K.Bhargava, "Division and Bit-Serial Multiplication overGF(qᵐ),"IEEE Trans. Computers,vol.41,no.8pp962-971,Aug.1992

[9] T.Itohand S.Tsujii,"Structure of Parallel Multipliers for a Class of fields GF(2ᵏ),"Informaotion and Computers,vol,83,pp.21-40.1989

[10] Y.Jeong,"VLSI Algorithms and Architectures for Real-Time Computation over Finite Fields,"PhD thesis, Dept,of Electrical and Computer Eng., Univ.of Massachusetts at Amherst,Feb. 1995

[11] A.Karatsuba and Y.Ofman, "multiplication of multidigit numbers on Automata,"Sov. Phys.-Dokl. (English translation),vol.7,no.7,pp.595-596

[12] E.D. Mastrovito, "VLSI Design for Mutiplication over Finite Fields GF(2ᵐ),"Lecture Notes in Computer Science 357,pp.297-309 Berlin:Springer-verlag,mar.1989

[13] E.D.Masrovito,"VLSI Architectures for Computati -on in Galois Fields,"PhD thesis, Dept.of Electrical Eng.,Linkoping Univ.,Linkoping,Swesen,1991

[14] C.Paar, Efficient Multiplier Architectures For Galois Fields GF(2⁴ⁿ), IEEE Trans. Computer, vol.47,No.2,Feb 1998

[15] M.A.Hasan and V.K.Bhargava,"Division and bit-serial multiplication over GF(qᵐ),"IEE Proc.,part E, vol. 139, no.3,pp.230-236, May 1992