쉬프트 레지스터를 이용한 GF(2^m)상의 병렬 승산기 설계

신 부 식 박 동 영 박 춘 명 김 흥 수
인 하 대 학 교 전 자 공 학 과

Design of Parallel Multiplier in GF(2^m) using Shift Registers

Boo Sik Shin Dong Young Park Chun Myeong Park Heung Soo Kim
Dept. of Electronics Inha University

ABSTRACT

In this paper , a method for constructing parallel-in,parallel-out multipliers in GF(2^m) is presented.The proposed system is composed of two operational parts by using shift register.

One is a multiplicative arithmetical operation part capable of the multiplicative arithmetic and modulo 2 operation to all product terms with the same degree. And the other is an irreducible polynomial operation part to outputs from the multiplicative arithmetical operation part.

Since the total hardware is linearly m dependant to GF(2^m),this system has a reasonable merit when m increases. And also this system is suited for VLSI implementation due to simple,regular,and concurrent properties.

1 . 서 론

본 논문에서는 error-correcting code ,switching theory 및 digital signal processing 등에서 유한체 원소상의 산술연산시 사용되는 GF(2^m)승산기의 한가지 구성방법을 제시하였다.

GF(2^m)승산기는 이미 70년대 초에 C.K.Rushforth<1> 등에 의해 제안되었으며 최근에는 VLSI화에 적합한 구조를 갖는 승산기가 C.S.Yeh<2>, C.C.Wang<3>등에 의해 고안된 바 있다.

그러나 C.K.Rushforth<4> 승산기는 wire-routing 등이 VLSI에 문제로 지적되었으며<2,3> , m의 증가에 따라 H/W가 m^2에 비례하는 구조를 갖는 단점을 포함하였다. 또한 C.S.Yeh<2>는 VLSI가 가능하나 C.K.Rushforth<4>와 같이 m^2에 비례하는 방대한 H/W 구조를 가지며, C.C.Wang<3>은 계산과정이 수반되는 PLA의 재 프로그램에 의해서만 기약다항식의 변경이 가능한 제약사항을 내포하였다.

따라서, 본 논문에서는 위의 문제점을 고려하여,m의 증가시 H/W가 m에 선형적 증가 구조를 가지며 아울러 VLSI의 실현이 용이한 GF(2^m)승산기를 shift register를 이용하여 구성하였다.

제안된 승산기는 관용기저 다항식을 입력으로 사용하며 , 각 원소의 다항식 계수들 간의 승법 산술과 mod 2 연산을 행하는 "승법산술연산부"와 기약다항식에 의해 승법산술연산부의 출력을 modulo 연산하는 "modulo 연산부" 의 2개 연산부로 구성되었다.

본 논문은 2 장에서 Galois체 원소의 m 승법 성질을 기술하고,3 장에서 병렬입출력형 GF(2^m)승산기 구조의 설계방법을 제시하였다.

2 . 승산 알고리즘

Galois체란 P를 솟수, m을 양의 정수라할때 P^m개의 유한원소로 체를 형성한는 유한체를 의미하며 일반적으로 GF(P^m)으로 표시한다.

GF(p^m)의 체원소는 원시원소 α에 의해서 생성되며, 이때 α는 GF(p^m)상의 원시 기약다항식 $F(\alpha)=f_{m-1}\alpha^{m-1}+f_{m-2}\alpha^{m-2}+\ldots\ldots+f_2\alpha^2+f_1\alpha+f_0$의근이다. 따라서 GF($p^m$)의 원소집합 E는 식(1)과 같이 표현이 가능하다.

$$E = \{ 0, \alpha^1, \alpha^2, \alpha^3, \ldots, \alpha^{p^2}, \alpha^{p^m} = 1 \} \quad (1)$$

GF(2^m)의경우 α^i , $\alpha^j \in E$ 일때 각 체원소 α^i , α^j 는 식(2)와 같은 다항식형태로 표시된다.

$$\alpha^i = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \ldots + a_2\alpha^2 + a_1\alpha + a_0$$
$$\alpha^j = b_{m-1}\alpha^{m-1} + b_{m-2}\alpha^{m-2} + \ldots + b_2\alpha^2 + b_1\alpha + b_0$$
여기서 $a,b \in \{0,1\}$ (2)

식(2)의 두 체원소간 승산을 실행하기 위하여 α^i 와 α^j 의 각 항에 의한 계수연산을 다음과 같이 정의하자<4>.

정 의 1 >

$$\alpha^i\alpha^j = (\alpha^i\cdot\alpha^j, \alpha^{i+1}\cdot\alpha^{j+1}, \ldots, \alpha^{j+i}\cdot\alpha^{i-i}, \alpha^{j-i}\cdot\alpha^i)$$

단,1) i→j;i,j는 $i\geq 0$, $j\geq 0$ 및 $i\geq j$ 인 정수
i→j;i,j는 $i\geq 0$, $j\geq 0$ 및 $i\geq j$ 인 정수
2) $\alpha^i, \alpha^j \in E$ (3)

정 의 2 >

$a^{(i)}$와 $b^{(j)}$가 a,b∈{ 0,1 }이며 각각 α^i 와 α^j 의 계수일 때

$$a^{(i)}\alpha^i \; b^{(j)}\alpha^j = (a^{(i)}b^{(j)})\cdot\alpha^{i+j} \qquad (4)$$

정 의 3 >

$$\alpha^i \alpha^j = \alpha^{i+j} = \alpha^f \qquad (5)$$

f=i+j , $0\le i,j\le m-1$, $0\le f\le 2(m-1)$

위의 정의들을 이용하면 식(6)이 성립한다.

$$a^{(i)}\alpha^i b^{(j)}\alpha^j = (a^{(i)}b^{(j)})\;\alpha^{i+j} \qquad (6)$$

이때, 임의 두 기저원소 A,B를

$$A = \sum a_i \alpha^i \;,\; B = \sum b_j \alpha^j \qquad (7)$$

라고 하면 A와 B의 승산은 식(8)과 같다.

$$\begin{aligned} A\cdot B &= \Big[\sum^{m-1} a^{(i)}\alpha^i\Big]\;\Big[\sum^{m-1} b^{(j)}\alpha^j\Big] \\ &= \sum^{m-1}_{i=0}\Big(\sum^{m-1}_{j=0} a^{(i)}\alpha^i\Big)\,b^{(j)}\alpha^j \\ &= \sum^{m-1}_{i=0}\sum^{m-1}_{j=0} a^{(i)}b^{(j)}\alpha^{i+j} \\ &= a^{(0)}b^{(0)} + (a^{(0)}b^{(1)} + a^{(1)}b^{(0)})\,\alpha + (a^{(0)}b^{(2)} + a^{(1)}b^{(1)} + a^{(2)}b^{(0)})\,\alpha^2 + \cdots\cdots \\ &\quad + (a^{(0)}b^{(m-1)} + a^{(1)}b^{(m-2)} + \cdots\cdots + a^{(m-2)}b^{(1)} + a^{(m-1)}b^{(0)})\,\alpha^{m-1} + \\ &\quad \cdots\cdots + (a^{(m-2)}b^{(m-1)} + a^{(m-1)}b^{(m-2)})\,\alpha^{2m-3} + (a^{(m-1)}b^{(m-1)})\,\alpha^{2m-2} \end{aligned} \qquad (8)$$

또한 식(8)은 정의1-3에 의해 식(9)와 같이 표시가 가능하다.

$$\begin{aligned} A\cdot B &= a^{(0)}\cdot b^{(0)} + (a^{(0)}\cdot b^{(1)} + a^{(1)}\cdot b^{(0)})\,\alpha + (a^{(0)}\cdot b^{(2)} + \cdots\cdots \\ &\quad + (a^{(m-2)}\cdot b^{(m-1)} + a^{(m-1)}\cdot b^{(m-2)})\,\alpha^{m-1} + \cdots\cdots + (a^{(m-1)}\cdot b^{(m-1)})\,\alpha^{2m-3} + \\ &\quad (a^{(0)}\cdot b^{(1)})\,\alpha^{2(m-1)} \\ &= a^{(0)}\cdot b^{(0)} + (a^{(0)}\cdot b^{(1)} + a^{(1)}\cdot b^{(0)})\,\alpha^i + (a^{(m-1)}\cdot b^{(i+1)})\,\alpha^{2m-2+i} \end{aligned}$$

; $1\le i\le m-1$ (9)

이제 식(9) 좌변항의 모든 동일차수 i에 대해 mod 2 연산을 적용하면 , 각 적산항이 단일이며 차수가 0,1,2,...,2(m-1)인 식(10)과 같이 된다.

A·B mod 2 = [식(9) 좌변항] mod 2 (10)

식(10)은 승법산술연산부의 구조식이다. 또한 식(10)에서 차수가 m,m+1,m+2,...,2(m-1)인 항들을 차수가 m-1차수 이하의 항으로 낮추기 위해 기약다항식P(α)에 의한 modulo 연산은 식(11)과 같이 실행한다.(5)

$$\alpha^{2m-1+i} = \alpha^{2m-1+i} \bmod (\alpha^{m-1}P(\alpha)) \qquad (11)$$

; $0\le i\le (m-1)$

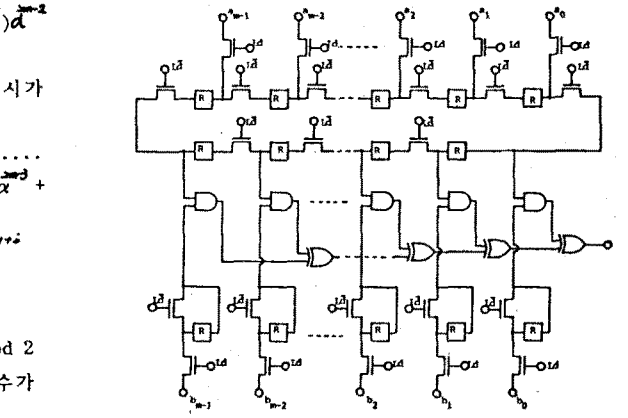
식 (11)은 α 의 차수를 하나 낮추는 것을 의미하며 식(11)의 결과를 다음 단으로 궤환시키는 과정을 m-1회 반복실행하며 이를 수식으로 나타내면 식(12)와 같다.

$$\alpha = (\ldots((\alpha^{2m-1+i} \bmod (\alpha^{m-1}P(\alpha))) \bmod (\alpha^{m-2}P(\alpha)))\ldots) \bmod P(\alpha) \qquad (12)$$

3 . 승산기의 구조

제안된 승산기의 구조는 병렬입출력의 형태로서 승산부와 mod부로 나누어 연산을 행한다.

승산부의 구조를 다항식 계수만의 형태로 표현하면 식(9)에 의하여 다음과 같이 표현이 가능하다.



위에서 횡축은 같은차수 항들간의 mod 2연산을 의미하며 종축은 두 다항식 계수간의 승산을 의미한다. 즉 최고차수의 항부터 mod 2 연산에의한 출력값을 얻으며 회로는 다음과 같다.

R: CYCLIC SHIFT REGISTER

Ld SIGNAL:

그림 1. 승법산술 연산부

Fig.1. Multiplicative arithetical operation part

mod부의 연산은 식 (11)에 의하여 다음과 같이 구성된다.

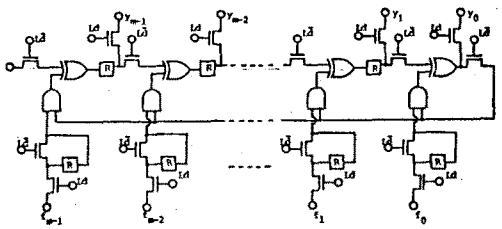


그림 2. Modulo 연산부

Fig.2. Modulo operation part

제안된 승산기는 5m-1 개의 shift register가 필요하며 2m-1의 clock이 요구된다.

예) GF(2^4) 승산기 설계

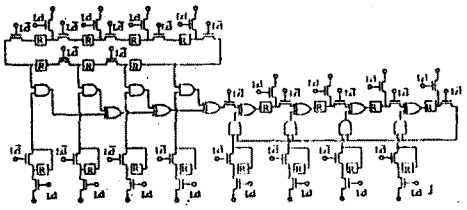


그림 3. GF(2^4) 승산기 구성

Fig.3. Construction of GF(2) multiplier

4. 결 론

본 논문에서는 GF(2^m)승산기 구성방법 한가지를 제안하였다. 제안된 승산기는 승산부와 mod부로 구분하여 연산을 실행하며 쉬프트 레지스터를 사용하여 승산기의 구조가 m에 선형적으로 비례하도록 설계되었다. 또한 회로변경 없이 GF(2^m)상 모든 기약다항식의 사용이 가능하다. 따라서, 본 논문에서 제안한 방식은 m이 증가할 때 하드웨어적으로 유리한 이점을 제공하는 반면에 쉬프트레지스터 사용에 따른 지연의 단점도 수반된다. 그러므로 승법산술연산부와 modulo연산부의 병렬처리가 요구된다.

참 고 문 헌

1. B.A.Laws and C.K.Rushforth,"A Cellular-Array multiplier for GF(2^m)," IEEE Trans. Comput. Vol. C-20, PP.1573-1578,Dec. 1971.

2. C.S.Yeh , I.S.Reed and T.K.Trung," Systolic-multipliers for finite field GF(2^m)," IEEE Trans.comput.,vol.c33,pp.357-360, apr.1984.

3. C.C. Wang, T.K. Trung 외,"VLSI architectures for computing multiplications and inverses in GF(2^m),"IEEE Trans. Comput.,vol.c-34, pp.709-717,aug.1985.

4. 박동영, 강성수, 김흥수, " GF(2^m)상의 승법과 승법역 계산을 위한 가변형 산술시스템의 설계," 전자공학회 논문지 88년 5월호 게재예정.

5. 원동호, 김병찬, "GF(2^m)상의 승산기 구성에 관한 연구," 전기전자공학 학술대회 논문집, PP.845-849, 1987.