通信情報保護學會誌
第4卷 第1號, 1994. 3

유한체 $GF(2^m)$상에서의 승산회로

양 형 규*, 안 영 화**

1. 서 론

유한체(finite field) $GF(2^m)$은 2^m개의 원소를 갖는 체로서, 집합의 각 원소를 m비트 바이너리(binary)로 표현할 수 있기 때문에 회로응용에 적합하다. 실제로 $GF(2^m)$상에서의 연산은 스위칭 이론(switching theory)과 컴퓨터 연산 그리고 오류 정정 부호(error correcting codes)에 이용되어 왔으며, 최근 암호이론(cryptography)에도 활발히 응용되고 있다. 예를 들면, Reed-Solomon 부호의 부호기와 복호기, 그리고 BCH 부호의 복호기 등에서 사용되고 있고, 또한 비밀통신에서 디지탈 메세지(digital message)의 암호화(encryption) 및 복호화(decryption)회로에도 사용되고 있다. 따라서 유한체상에서의 연산 알고리즘은 처리속도 및 하드웨어량에 관계하는 기본적이고 중요한 문제로서, VLSI 구현을 위해 최적의 알고리즘이 요구된다.

유한체(finite field) $GF(2^m)$상에서 임의의 두 원소의 곱을 계산하기 위한 승산회로는 그 구성이 대부분 순차 논리 회로(sequential logic circuit)인 선형궤환 시프트 레지스터(linear feedback shift register)를 사용한 직렬형이다. 이러한 회로는 간단하고 상대적으로 경제적이나, 처리속도면에서는 오히려 늦다. 반면 최근 발표된 $GF(2^m)$상에서의 승산회로는 그 구성이 조합 논리 회로(combinational logic circuit)를 사용한 병렬형이다. 이러한 회로는 처리속도가 빠를 뿐만 아니라 규칙성을 갖기 때문에 VLSI화에 적합하다. 따라서 본고에서는 효율적으로 VLSI화할 수 있는 병렬형 승산회로에 관해서만 기술하고자 한다.

Yeh, Reed와 Truong등에 의해 제안된 Systolic 승산회로는 점화식을 이용하여 구성하였고, Laws와 Rushforth등에 의해 제안된 Cellular array 승산회로는 4개의 게이트를 단위 셀(unit cell)로 구성하여 규칙성을 갖고 있으며, 또한 변형된 Cellular array 승산회로도 2개의 게이트를 단위 셀로 구성하여 규칙성을 갖고 있다. 한편 Wang과 Omura 등에 의해 제안된 승산회로는 원소를 정규기저(normal basis)로 표현하여 구성하였다.

본고의 구성은 1장의 서론에 이어, 2장에서 유한체의 일반적 성질 및 원소표시 방법에 관해 기술하였다. 3장은 유한체 $GF(2^m)$상에서 승산 알고리즘 및 승산회로에 관해 기술하였으며, 4장에서는 결론으로서 본고의 끝맺음을 하였다.

2. 유한체(Galois Field)

2.1 유한체의 성질

유한체는 Galois(1811~1832)가 발견하였으

* 정회원, 성균관대학교 정보공학과 박사과정 재학중
** 종신회원, 강남대학교 전자계산학과 조교수

므로 통상 Galois Field라 하며, 기초체(ground field) $GF(P)$와 확대체(extension field)$GF(P^m)$으로 나눌 수 있다. 여기서 P와 m은 각각 소수와 양의 정수이고, P와 P^m는 유한체의 원소수로 보통 유한체의 크기(order)라 한다.

일반적으로 유한체는 실수의 성질중 사칙연산 성질만을 가지며, 2개 이상의 원소를 갖는 집합 S에서 다음과 같은 공리 A1~A7을 만족한다.

A1. 임의의 원소 $x, y \in S$에 대해 가산과 승산이 정의되고 그 결과는 집합 S에 포함된다.

A2. 교환법칙 : 임의의 원소 $x, y \in S$에대해 가산과 승산의 교환법칙이 성립한다.

$$x+y=y+x$$
$$x \cdot y=y \cdot x$$

A3. 결합법칙 : 임의의 원소 $x, y, z \in S$에 대해 가산과 승산의 결합법칙이 성립한다.

$$x+(y+z)=(x+y)+z$$
$$x \cdot (y \cdot z)=(x \cdot y) \cdot z$$

A4. 분배법칙 : 임의의 원소 $x, y, z \in S$에 대해 분배법칙이 성립한다.

$$x \cdot (y+z)=x \cdot y+x \cdot z$$

A5. 0원의 존재 : 임의의 원소 $x \in S$에 대해 $x+0=x$를 만족시키는 원소 $0 \in S$가 단 한개 존재한다.

A6. 단위원의 존재 : 임의의 원소 $x \in S$에 대해 $x \cdot 1=x$을 만족시키는 원소 $1 \in S$가 단 한 개 존재한다.

A7. 역원의 존재 : 임의의 원소 $x \in S$에 대해 $x+y=0$을 만족시키는 가산 역원(음원) $y \in S$가 단 한 개 존재하고, 0 이외의 임의의 원소 $x \in S$에 대해 $x \cdot y=1$을 만족시키는 승산역원(역원) $y \in S$가 단 한 개 존재한다.

또한 유한체 $GF(P)$ 및 $GF(P^m)$상의 원소는 다음과 같은 성질을 갖고 있다.

(1) $GF(P)$ 및 $GF(P^m)$상의 임의의 원소 x의 P배는 0이다.

$$P \cdot x=x+x+x+ \ \dots \ +x \equiv 0 \qquad (2.1)$$

(2) $GF(P)$ 및 $GF(P^m)$상의 임의의 원소 x에 대하여 다음 식이 성립한다.

$$x^{P-1} \equiv 1$$
$$x^{P^m-1} \equiv 1 \text{(Fermat 정리)} \qquad (2.2)$$

(3) $GF(P)$ 및 $GF(P^m)$상의 임의의 원소 x, y에 대하여 다음 식이 성립한다.

$$(x+y)^P \equiv x^P+y^P$$
$$(x+y)^{P^m} \equiv x^{P^m}+y^{P^m} \qquad (2.3)$$

(4) $GF(P)$ 및 $GF(P^m)$상의 임의의 원소 x에 대하여 다음 식이 성립한다.

$$x^i \cdot x^j \equiv x^{(i+j) \bmod (P-1)}$$
$$x^i \cdot x^j \equiv x^{(i+j) \bmod (P^m-1)} \qquad (2.4)$$

2.2 유한체 $GF(2^m)$상에서의 원소표시

유한체 $GF(P^m)$상에서의 원소수는 P^m개로 $GF(P)$상의 m차 원시다항식

$$P(x)=x^m+f_{m-1}x^{m-1}+ \ \dots \ +f_0$$
$$(\text{단 } f_i \in GF(P)) \qquad (2.5)$$

의 원시근으로 표현되며, 각각의 원소는 P개의 상태를 갖는 m디지트로 나타낼 수 있다. 이와 같은 표시방법을 기저에 의한 $GF(P^m)$상에서의 원소표시 방법이라 한다. 기저에 의한 원소표시 방법에는 관용기저(conventional basis)에 의한 방법과 정규기저(normal basis)에 의한 방법이 있다. 본고에서는 디지탈 회로화가 용이한 $P=2$인 $GF(2^m)$상에서의 기저표시 방법에 관해서만 기술하기로 한다.

2.2.1 관용기저에 의한 원소표시

원시다항식의 원시근을 α라고 하면 $GF(2^m)$상

의 원소는 α^0, α^1, α^2, ..., α^{m-1}의 선형결합으로 표시할 수 있다. 즉,

$$F(\alpha)=c_0+c_1\alpha+c_2\alpha^2+\ldots+c_{m-1}\alpha^{m-1}$$
$$=\sum_{i=1}^{m-1}c_i\alpha^i \quad (\text{단 } c_i\in GF(2)) \qquad (2.6)$$

으로 $GF(2^m)$상의 모든 원소를 표시할 수 있다. 이 식을 벡터로 표시하면 다음과 같다.

$$[c_0,\ c_1,\ c_2,\ \ldots,\ c_{m-1}]$$

이러한 표현방법을 관용기저에 의한 $GF(2^m)$상의 원소표시 방법이라 하며, 원시근 α의 멱승들은 모든 원시다항식에 대하여 선형독립이므로 모든 원시다항식은 관용기저를 갖는다.

예로써 $m=3$인 $GF(2^3)$상의 원소를 구해보자. 생성다항식(generating polynomial)인 $GF(2)$상의 원시다항식 $P(x)=x^3+x^2+1$을 선택하고 원시근을 α라고 하면, $P(\alpha)=0$이므로

$$\alpha^3+\alpha^2+1=0$$
$$\alpha^3=\alpha^2+1$$

이 성립한다. 따라서 유한체 $GF(2^3)$상의 모든 원소를 원시다항식의 근 α의 다항식으로 표현하면 표2.1과 같다.

표 2.1 관용기저에 의한 $GF(2^3)$상의 원소표시

원 소	α^2 α^1 α^0	벡 터
α^*	0	0 0 0
α^0	1	0 0 1
α^1	α	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha+1$	1 0 1
α^4	$\alpha^2+\alpha+1$	1 1 1
α^5	$\alpha+1$	0 1 1
α^6	$\alpha^2+\alpha$	1 1 0

2.2.2 정규기저에 의한 원소표시

원시다항식의 원시근을 α라고 할 때 α^{2^0}, α^{2^1}, α^{2^2}, ..., $\alpha^{2^{m-1}}$의 선형독립일 경우 이들의 선형결합으로 $GF(2^m)$상의 모든 원소를 표시할 수 있다. 즉,

$$F(\alpha)=n_0\alpha^{2^0}+n_1\alpha^{2^1}+n_2\alpha^{2^2}+\ldots+n_{m-1}\alpha^{2^{m-1}}$$
$$=\sum_{i=1}^{m-1}n_i\alpha^{2^i} \quad (\text{단 } n_i\in GF(2)) \qquad (2.7)$$

으로 $GF(2^m)$상의 모든 원소를 표시할 수 있다. 이 식을 벡터로 표시하면 다음과 같다.

$$[n_0,\ n_1,\ n_2,\ \ldots,\ n_{m-1}]$$

이러한 표현방법을 정규기저에 의한 $GF(2^m)$상의 원소표시 방법이라 한다. 그러나 $GF(2)$상의 m차 원시다항식은 모두 정규기저를 갖지 못한다.

예로써 $m=3$인 $GF(2^3)$상의 원소를 구해보자. 정규기저를 갖는 $GF(2)$상의 원시다항식 $P(x)=x^3+x^2+1$을 선택하고 원시근을 α라고 하면, $P(\alpha)=0$이므로

$$\alpha^3+\alpha^2+1=0$$
$$\alpha^3=\alpha^2+1$$

이 성립한다. 따라서 유한체 $GF(2^3)$상의 모든 원소를 원시다항식의 근 α의 다항식으로 표현하면 표2.2와 같다.

표 2.2 정규기저에 의한 $GF(2^3)$상의 원소표시

원 소	α^{2^0} α^{2^1} α^{2^2}	벡 터
α^*소	0	0 0 0
α^0	$\alpha^{2^0}+\alpha^{2^1}+\alpha^{2^2}$	1 1 1
α^1	α^{2^0}	1 0 0
α^2	α^{2^1}	0 1 0
α^3	$\alpha^{2^0}+\alpha^{2^2}$	1 0 1
α^4	α^{2^2}	0 0 1
α^5	$\alpha^{2^1}+\alpha^{2^2}$	0 1 1
α^6	$\alpha^{2^0}+\alpha^{2^1}$	1 1 0

3. $GF(2^m)$상에서의 승산회로

본고에서는 효율적으로 VLSI화 할 수 있는 $P=2$인 $GF(2^m)$상에서의 승산 알고리즘 및 승산회로에 관해서만 논하기로 한다.

3.1 Systolic 승산 회로

관용기저로 표현된 $GF(2^m)$상의 피승산원소 $A(\alpha)$와 승산원소 $B(\alpha)$는 각각 식(3.1)과 식(3.2)로 표현할 수 있다.

$$A(\alpha)=\sum_{n=0}^{m-1}a_n\alpha^n \tag{3.1}$$

$$B(\alpha)=\sum_{k=0}^{m-1}b_k\alpha^k \tag{3.2}$$

또한 승산 후의 원소 $Y(\alpha)$는 다음 식으로 표현할 수 있다.

$$\begin{aligned}Y(\alpha)&=A(\alpha)\cdot B(\alpha)\\&=(\sum_{n=0}^{m-1}a_n\alpha^n)(\sum_{k=0}^{m-1}b_k\alpha^k)\\&=\sum_{k=0}^{m-1}(A(\alpha)\alpha^k)b_k\\&=\sum_{n=0}^{m-1}(\sum_{k=0}^{m-1}a_n^{(k)}b_k)\alpha^n\end{aligned} \tag{3.3}$$

식(3.3)을 정리하면

$$\begin{aligned}&\sum_{k=0}^{m-1}(A(\alpha)\alpha^k)b_k\\&=(a_0+a_1\alpha+a_2\alpha^2+\ldots+a_{m-1}\alpha^{m-1})\alpha^0b_0\\&\quad\cdots\cdots\cdots\cdots\cdots\cdots\\&\quad+(a_0+a_1\alpha+a_2\alpha^2+\ldots+a_{m-1}\alpha^{m-1})\\&\quad\alpha^{m-1}b_{m-1}\end{aligned} \tag{3.4}$$

이다. 여기서 괄호 밖의 α^k를 괄호 안에 넣고 식(2.5)의 원시다항식으로 $(m-1)$차 이하로 낮추면 다음 식(3.5)와 같이 표현된다.

$$\begin{aligned}Y(\alpha)=&(a_0^{(0)}+a_1^{(0)}\alpha+a_2^{(0)}\alpha^2+\\&\ldots+a_{m-1}^{(0)}\alpha^{m-1})b_0\\&+(a_0^{(1)}+a_1^{(1)}\alpha+a_2^{(1)}\alpha^2+\\&\ldots+a_{m-1}^{(m-1)}\alpha^{m-1})b_1\\&\cdots\cdots\cdots\cdots\cdots\cdots\\&+(a_0^{(m-1)}+a_1^{(m-1)}\alpha+a_2^{(m-1)}\alpha^2+\\&\ldots+a_{m-1}^{(m-1)}\alpha^{m-1})b_{m-1}\end{aligned} \tag{3.5}$$

따라서 식(3.5)로부터 다음 식을 얻을 수 있다.

$$\begin{aligned}Y(\alpha)\cdot\alpha^k&=a_0^{(k)}+a_1^{(k)}\alpha+a_2^{(k)}\alpha^2+\\&\quad\ldots+a_{m-1}^{(k)}\alpha^{m-1}\\&=\sum_{n=0}^{m-1}a_n^{(k)}\alpha^n\end{aligned} \tag{3.6}$$

그러므로 승산 후의 $Y(\alpha)$의 계수는 다음 식과 같다.

$$\begin{aligned}y_n&=a_n^{(0)}+a_n^{(1)}b_1+a_n^{(2)}b_2+\\&\quad\ldots+a_n^{(m-1)}b_{m-1}\end{aligned} \tag{3.7}$$

한편 식(3.6)의 $A(\alpha)\alpha^k$는 $k=0$일 때 $A(\alpha)\alpha^0=A(\alpha)$이기 때문에 $0\le n\le m-1$에서

$$a_n^{(0)}=a_n \tag{3.8}$$

이고, $1\le k\le m-1$일 때

$$\begin{aligned}A(\alpha)\alpha^k&=A(\alpha)\alpha^{k-1}\alpha\\&=\sum_{n=0}^{m-1}a_n^{(k-1)}\alpha^{n+1}\\&=\sum_{n=1}^{m-1}a_{n-1}^{(k-1)}\alpha^n+a_{m-1}^{(k-1)}\alpha^m\end{aligned} \tag{3.9}$$

이다. 식(3.9)에 식(2.5)의 원시다항식을 대입하여 정리하면 다음 관계식들을 구할 수 있다.

$$\begin{aligned}a_n^{(k)}&=f_na_{m-1}^{(k-1)}+a_{n-1}^{(k-1)}(1\le k\le m-1)\\a_0^{(k)}&=f_0a_{m-1}^{(k-1)}\end{aligned} \tag{3.10}$$

식(3.10)으로부터 $a_n^{(k)}$를 구하여 식(3.3)에 대입하면 승산후의 원소 $Y(a)$를 구할 수 있으며, 또한 식(3.7)의 계수를 얻는 회로를 구성하면 $GF(2^m)$상의 Systolic 승산회로가 된다.

예로써 $m=4$인 $GF(2^4)$상의 승산회로를 구성해 보자. 승산 후의 원소 $Y(a)$의 각 계수는 식(3.11) ~ (3.14)와 같이 구해지며, 승산회로는 그림 3.1과 같다.

$$\begin{aligned}y_0&=a_0b_0+f_0(f_3a_3+a_2)b_2+\\&\quad f_0(f_3(f_3a_3+a_2)+f_2a_3+a_1))b_3\end{aligned} \tag{3.11}$$

$$y_1=a_1b_0+(f_1a_3+a_0)b_1+(f_1(f_3a_3+a_2)$$

$$+f_0a_3))b_2+(f_1(f_3(f_3a_3+a_2)+$$
$$f_2a_3+a_1)+f_0(f_3a_3+a_2))b_3 \quad (3.12)$$
$$y_2=a_2b_0+(f_2a_3+a_1)b_1+(f_2(f_3a_3+a_2)$$
$$+f_1a_3+a_0))b_2+(f_2(f_3(f_3a_3+a_2)+$$
$$f_2a_3+a_1)+f_1(f_3a_3+a_2)+f_0a_3))b_3 \quad (3.13)$$
$$y_3=a_3b_0+(f_3a_3+a_2)b_1+(f_3(f_3a_3+a_2)+$$
$$f_2a_3+a_1))b_2+(f_3(f_3(f_3a_3+a_2)+f_2a_3+a_1)$$
$$+f_2(f_3a_3+a_2)+f_1a_3+a_0))b_3 \quad (3.14)$$

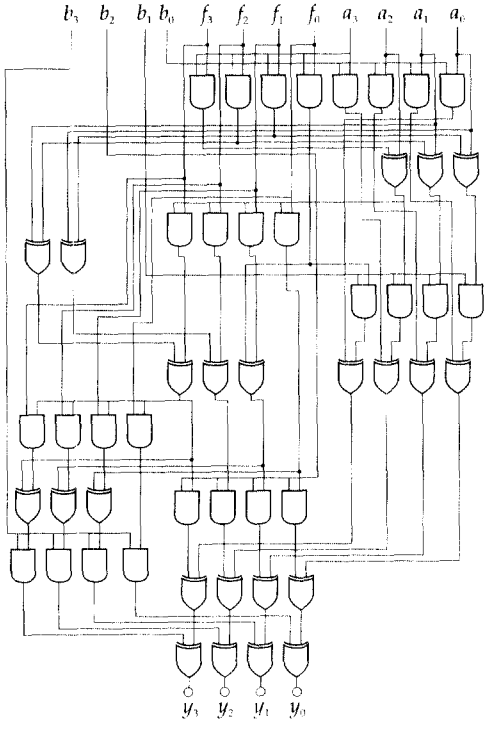


그림 3.1 $GF(2^4)$상의 Systolic 승산회로

이 승산회로는 점화식을 이용하기 때문에 회로구성이 불규칙하고 복잡하며, $GF(2^m)$상의 m값이 변할 경우 승산회로를 다시 구성해야 하는 단점이 있다.

3.2 Cellular Array 승산회로

관용기저로 표현된 $GF(2^m)$상의 승산 후의 원소 $Y(\alpha)$는 다음 식으로 표현할 수 있다.

$$\begin{aligned} Y(\alpha)&=A(\alpha)B(\alpha)\\ &=(\sum_{n=0}^{m-1}a_n\alpha^n)(\sum_{k=0}^{m-1}b_k\alpha^k)\\ &=\sum_{k=0}^{m-1}(b_k(\sum_{n=0}^{m-1}a_n\alpha^n)\alpha^k)\\ &=\sum_{k=0}^{m-1}(b_k A(\alpha)\alpha^k\\ &=y_m^{(m-1)} \end{aligned} \quad (3.15)$$

여기서 $y_m^{(m-1)}$은 $(m-1)$번 좌측으로 시프트한 m번째 부분합을 의미하며, 그 내용은 다음과 같다.

$$y_1^{(0)}=b_{m-1}A(\alpha)$$
$$y_1^{(1)}=((b_{m-1}A(\alpha))\alpha) \bmod P(\alpha)$$
$$y_2^{(1)}=(y_1^{(1)}+b_{m-2}A(\alpha))$$
$$y_2^{(2)}=(y_2^{(1)}\alpha) \bmod P(\alpha)$$
$$=(y_1^{(1)}+b_{m-2}A(\alpha))\alpha) \bmod P(\alpha)$$
$$y_3^{(2)}=(y_2^{(2)}+b_{m-3}A(\alpha))$$
$$y_3^{(3)}=(y_3^{(2)}\alpha) \bmod P(\alpha)$$
$$=(y_2^{(2)}+b_{m-3}A(\alpha))\alpha) \bmod P(\alpha)$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$y_{m-1}^{(m-1)}=(y_{m-1}^{(m-2)}\alpha) \bmod P(\alpha)$$
$$=((y_{m-2}^{(m-2)}+b_1A(\alpha))\alpha) \bmod P(\alpha)$$
$$y_{m-1}^{(m-1)}=(y_{m-1}^{(m-1)}+b_0A(\alpha)) \quad (3.16)$$

따라서 식(3.16)은 순차적인 승산출력을 나타내며, 이를 회로화하면 $GF(2^m)$상의 Cellular Array 승산회로를 구성할 수 있다.

예로써 $m=4$인 $GF(2^m)$상의 승산회로를 구성해 보면 그림 3.2와 같다.

이 승산회로는 4개의 게이트를 셀 단위로 하여 구성되기 때문에 회로구성이 간단하고 규칙적이다. 또한 $m\geq r$인 $GF(2^r)$상에서도 승산이 가능하다.

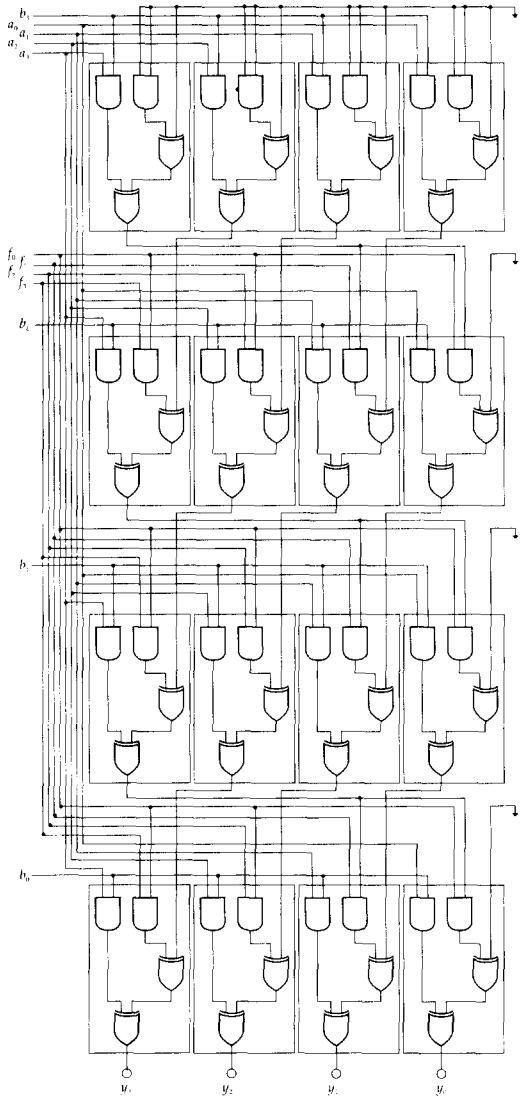


그림 3.2 $GF(2^4)$상의 Celluler Array 승산회로

3.3 변형된 Celluar Array 승산회로

관용기저로 표현된 $GF(2^m)$상의 승산 후의 원소 $Y(\alpha)$는 식(3.17)와 같이 표현할 수 있다.

$$\begin{aligned} Y(\alpha) &= A(\alpha)B(\alpha) \\ &= (\sum_{n=0}^{m-1} a_n \alpha^n)(\sum_{k=0}^{m-1} b_k \alpha^k) \\ &= \sum_{n=0}^{m-1} a_n (B(\alpha)\alpha^n) \\ &= \sum_{n=0}^{m-1} a_n B_n(\alpha) \\ &= y_m^{(m-1)} \end{aligned} \tag{3.17}$$

여기서 $y_m^{(m-1)}$은 $(m-1)$번 좌측으로 시프트한 m번째 부분합을 의미하며, 이 연산과정은 mod부와 승산부로 나눌 수 있다.

mod부의 연산과정은 $B_i(\alpha)$의 연산과정으로 다음 식들과 같다.

$$B_0(\alpha) = B(\alpha)$$

$$\begin{aligned} B_1(\alpha) &= \alpha\, B_0(\alpha) \bmod P(\alpha) \\ &= \alpha\, B(\alpha) \bmod P(\alpha) \end{aligned}$$

$$\begin{aligned} B_2(\alpha) &= \alpha\, B_1(\alpha) \bmod P(\alpha) \\ &= \alpha(\alpha\, B(\alpha) \bmod P(\alpha)) \bmod P(\alpha) \end{aligned}$$

. . . . . .

$$\begin{aligned} B_{m-1}(\alpha) &= \alpha\, B_{m-2}(\alpha) \bmod P(\alpha) \\ &= \alpha\,(\alpha\,(\ldots \alpha B(\alpha) \bmod P(\alpha))\ldots) \\ &\quad \bmod P(\alpha) \end{aligned} \tag{3.18}$$

한편 승산부의 연산과정은 피승산원소 $A(\alpha)$와 식(3.18)로 표현되는 mod부의 연산결과와의 합과 곱으로 표현할 수 있다.

$$\begin{aligned} y_1^{(1)} &= a_0 B_0(\alpha) \\ &= a_0 B(\alpha) \end{aligned}$$

$$\begin{aligned} y_2^{(1)} &= y_1^{(0)} + a_1 B_1(\alpha) \\ &= a_0 B(\alpha) + a_1(\alpha B(\alpha) \bmod P(\alpha)) \end{aligned}$$

$$\begin{aligned} y_3^{(2)} &= y_2^{(1)} + a_2 B_2(\alpha) \\ &= a_0 B(\alpha) + a_1(\alpha B(\alpha) \bmod P(\alpha)) + \\ &\quad a_2(\alpha(\alpha B(\alpha) \bmod P(\alpha)) \bmod P(\alpha)) \end{aligned}$$

. . . . . .

$$y_{m-1}^{(m-1)}=y_{m-1}^{(m-2)}+m_{m-1}B_{m-1}(\alpha)$$

$$=a_0B(\alpha)+a_1(\alpha)B(\alpha^n) \bmod P(\alpha)$$

$$+ \cdots\cdots\cdots\cdots\cdots$$

$$+a_{m-1}(\alpha(\alpha(\ldots(\alpha B(\alpha) \bmod P(\alpha))$$

$$\ldots.) \bmod P(\alpha)) \qquad (3.19)$$

따라서 식(3.19)는 순차적인 승산 출력을 나타내며, 이를 회로화하면 $GF(2^n)$상의 변형된 Cellular Array 승산회로를 구성할 수 있다.

예로써 $m=4$인 $GF(2^4)$상의 승산회로를 구성해 보면 그림 3.3과 같다.

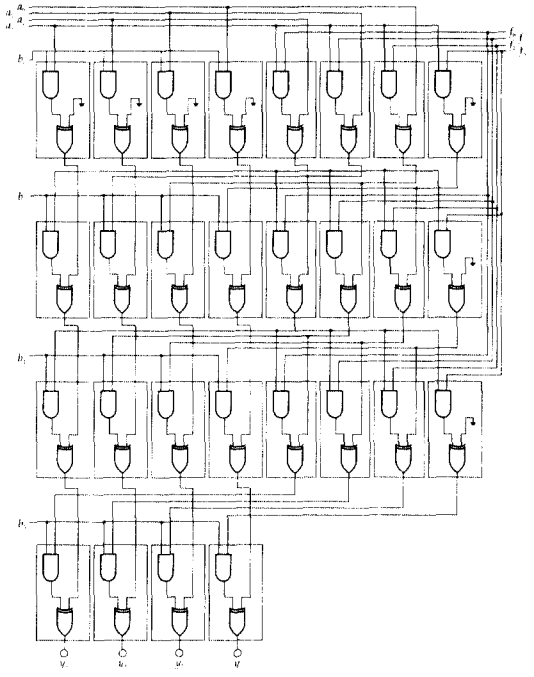


그림 3.3 $GF(2^4)$상의 변형된 Cellular Array 승산회로

이 승산회로는 Cellular Array 승산회로와 유사하게 2개의 게이트를 셀 단위로 하여 구성되기 때문에 회로구성이 간단하고 규칙적이다. 또한 $m \geq r$인 $GF(2^r)$상에서도 승산이 가능하다.

3.4 Massey-Omura 승산회로

$GF(2^m)$ 두 원소와 승산 후의 원소를 정규기저로 표시한 벡터 값은 다음과 같다.

$$A(\alpha) \Rightarrow [a_0, a_1, a_2, \ldots, a_{m-1}]$$

$$B(\alpha) \Rightarrow [b_0, b_1, b_2, \ldots, b_{m-1}]$$

$$Y(\alpha)=A(\alpha)\cdot B(\alpha) \Rightarrow [y_0, y_1, y_2, \ldots, y_{m-1}]$$

$$=[a_0, a_1, a_2, \ldots, a_{m-1}]$$

$$=[b_0, b_1, b_2, \ldots, b_{m-1}] \qquad (3.20)$$

여기서, 승산 후의 원소 $Y(\alpha)$의 계수 $y_i(0 \leq i \leq m-1)$는 피승산원소 $A(\alpha)$, 승산원소 $B(\alpha)$의 계수함수 f로 표시할 수 있으며 이를 승산함수라고 한다. $i=m-1$일 때 승산함수를

$$y_{m-1}=f(a_0, a_1, a_2, \ldots, a_{m-1};$$

$$b_0, b_1, b_2, \ldots, b_{m-1}) \qquad (3.21)$$

라고 하면 정규기저로 표시된 원소는 자승 성질로부터 다음 관계식을 얻을 수 있다.

$$Y^2(\alpha)=A^2(\alpha).B^2(\alpha)$$

$$[y_{m-1}, y_0, y_1, y_2, \ldots, y_{m-2}]$$

$$=[a_{m-1}, a_0, \ldots, a_{m-2}]$$

$$=[b_{m-1}, b_0, \ldots, b_{m-2}] \qquad (3.22)$$

식(3.22)로부터 $y_{m-2}, y_{m-3}, \ldots, y_0$에 승산함수를 적용하면 다음과 같이 표시된다.

$$y_{m-2}=f(a_{m-1}, a_0, \ldots, a_{m-2};$$

$$b_{m-1}, b_0, \ldots, b_{m-2})$$

$$y_{m-3}=f(a_{m-2}, a_{m-1}, \ldots, a_{m-3};$$

$$b_{m-2}, b_{m-1}, \ldots, b_{m-3})$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$y_0=f(a_1, a_2, \ldots, a_0;$$

$$b_1, b_2, \ldots, b_0) \qquad (3.23)$$

따라서 승산함수 f를 실현한 회로 m개를 사용, 각 승산함수 회로의 입력에 피승산원소와 승산원소의 계수를 바꾸어 접속하므로써 $GF(2^m)$상의 Massey-Omura 승산회로를 구성할 수 있다.

예로써 $m=4$인 $GF(2^4)$상의 승산회로를 구성해 보자. 정규기저를 갖는 원시다항식 $P(x)=x^4+x^1+1$을 선택하면, 승산 후 $Y(\alpha)$의 계수 y_i는 식 (3.24) ~ (3.27)과 같이 구해진다. 이에 대한 승산함수 회로 및 승산회로는 그림 3.4와 그림 3.5와 같다.

$$y_3=a_2b_2+a_3b_2+a_2b_3+a_3b_1+a_1b_3+a_3b_0+a_0b_3+a_1b_0+a_0b_1 \qquad (3.24)$$

$$y_2=a_1b_1+a_2b_1+a_1b_2+a_2b_0+a_0b_2+a_2b_3+a_3b_2+a_0b_3+a_3b_0 \qquad (3.25)$$

$$y_1=a_0b_0+a_1b_0+a_0b_1+a_1b_3+a_3b_1+a_1b_2+a_2b_1+a_3b_2+a_2b_3 \qquad (3.26)$$

$$y_0=a_3b_3+a_0b_3+a_3b_0+a_0b_2+a_2b_0+a_0b_1+a_1b_0+a_2b_1+a_1b_2 \qquad (3.27)$$

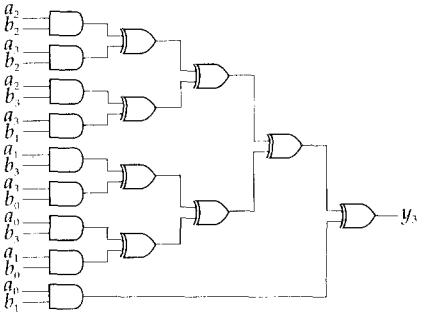


그림 3.4 $GF(2^4)$상의 승산함수 회로

이 승산회로는 $GF(2^m)$상의 m값과 원시다항식의 변경에 따라 승산함수가 달라지기 때문에 회로구성이 불규칙하고 복잡하며 다시 구성해야 되는 단점이 있다. 또한 정규기저의 선택에 어려움이 있다.

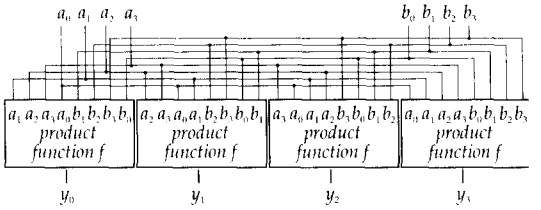


그림 3.5 $GF(2^4)$상의 Massey-Omura 승산회로

4. 결 론

유한체 $GF(2^m)$은 집합의 각 원소를 m비트 바이너리(binary)로 표현할 수 있기 때문에 디지탈 회로응용에 적합하다. 특히 암호이론 분야에 활발히 연구되고 있으며, 디지탈 메세지의 암호화 및 복호화 회로에 응용되고 있다. 그러므로 유한체상에서의 연산 알고리즘은 VLSI 구현 측면에서 최적의 알고리즘이 요구되고 있다.

본고에서는 유한체 $GF(2^m)$상에서 임의의 두 원소의 곱을 계산하는 병렬형 승산회로에 관해서만 논하였다. 이들 회로들은 일반적으로 원소의 표시방법에 따라 그리고 원시다항식의 선택에 따라 승산회로 구성의 복잡도 정도가 다르다. 관용기저상에서의 승산은 회로구성이 간단하고 규칙적인 반면, 정규기저상에서의 승산은 회로구성이 복잡하고 불규칙하다. 따라서 유한체 $GF(2^m)$상에서의 승산회로는 응용분야에 따라 적절히 선택해야 할 것이다.

향후 유한체 $GF(2^m)$상에서의 승산회로는 암호학 분야 뿐만 아니라 타분야에 응용될 전망이 크다. 따라서 효율적으로 VLSI화 할 수 있고 보다 고속으로 연산할 수 있는 알고리즘의 개발이 필요하다고 생각된다.

참 고 문 헌

[1] B. Benjauthrit, I.S. Reed, "Galois Switching Functions and Their Applications." IEEE Trans. on

Comput., Vol.C-25, pp.78~86, Jan., 1976.

[2] W.W. Peterson, Error-Correcting Codes, New York,Wiley,1981.

[3] 金彰圭, 李晩榮, "有限體 $GF(2^m)$上의 乘算器 設計에 關한 硏究", 通信學會 論文誌, 第14卷, 第3號, pp.235~239, 1989.

[4] 원동호, "유한체 $GF(2^m)$의 성질과 연산", 통신정보보호학회지, 제1권, 제2호, pp. 48~59 1991.

[5] 안영화, "유한체 $GF(2^m)$상의 승산회로 구성에 관한 연구", 강남대 논문집, 제21집, pp. 187~201, 1991.

[6] 안영화, 원동호, "유한체상에서 적암호의 구현에 관한 연구", 데이타 보호 기술 WORKSHOP 논문집, pp. 215~227, 1991.

[7] C.S. Yeh, I.S. Reed, T.K. Truong, "Systolic Multipliers for Finite Fields $GF(2^m)$, "IEEE Trans. on Comput, Vol. C-33, No.4, pp.357~1578, Apr., 1984.

[8] B.A. Laws, C.K. Rushforth, "A Cellular-Array Multiplizer for $GF(2^m)$," IEEE Trans. on Comput., Vol.C-20, pp.1573~1578, Dec. 1971.

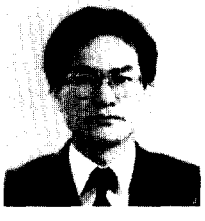
[9] D.Y. Pei, C.C Wang, J. Omura, "Normal Basis of Finite Field $GF(2^m)$," IEEE Trans. on Inform. Theory, Vol. Ⅱ-32, No.2, pp.285~287, Mar. 1986.

[10] 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 Inverse in $GF(2^m)$," IEEE Trans. on Comput., Vol.C-34, No.8, pp.709~716, Aug., 1985.

□ 著者紹介

양 형 규(정회원)

1983년 성균관대학교 전자공학과 졸업(공학사)
1985년 성균관대학교 대학원 전자공학과 졸업(공학석사)
1991년 ~ 현재 성균관대학교 정보공학과 박사과정 재학중
1985년 ~ 1991년 삼성전자 컴퓨터부문 선임 연구원



안 영 화(종신회원)

1975년 성균관대학교 전자공학과 졸업(공학사)
1977년 성균관대학교 대학원 전자공학과 졸업(공학석사)
1990년 성균관대학교 대학원 전자공학과 졸업(공학박사)
1983년 5월 ~ 1990년 2월 해군사관학교 전자공학과 조교수
1990년 3월 ~ 현재 강남대학교 전자계산학과 조교수