연산 모듈의 결합에 의한 $GF(2^m)$상의 병렬 승산 회로의 설계

변기영*, 김흥수*
인하대학교 전자공학과

Design of Parallel Multiplier Circuit synthesized operation module over GF(2^m)

Gi-Young Byun*, Heung-Soo Kim*
Dept. of Electronic Engineering, Inha University, Inchon 402-751, Korea
g1991196@inhavision.inha.ac.kr

Abstract

In this paper, a new parallel multiplier circuit over $GF(2^m)$ has been proposed. The new multiplier is composed of polynomial multiplicative operation part and modular arithmetic operation part, irreducible polynomial operation part. And each operation has modular circuit block. For design the new proposed circuit, it develop generalized equations using frame each operation idea and show a example for $GF(2^4)$.

I. 서 론

최근 급격히 발전하고 있는 디지털 통신 및 저장 매체의 개발에 있어 유한체 연산 시스템은 매우 중요한 분야로 주목받고 있다. Law[1]의 유한체 승산 연산 회로 이후 현재까지 다양한 형태의 회로들[2-5]이 제안되어 왔으며, 이들은 오류 정정 회로, 컴퓨터 메모리, 이동 통신, 패킷 스위칭 시스템 등의 분야와 함께, 최근에는 디지털 보안 및 서명, 디지털 워터 마킹 등 그 적용 영역이 날로 확장되고 있다[6]. VLSI로 대변되는 반도체 기술의 비약적인 발전에 힘입어 점차 고속의 동작 특성을 가지며, 대용량의 신호 처리가 가능한 연산 회로가 요구되고 있다. 또한, 정규(모듈)화 되고, 그 확장의 용이함과 일반성을 갖추며, 회로의 구현이 용이하여 VLSI의 구현에 유리한 연산 회로 개발의 필요성이 대두되고 있다.

본 논문에서는 Parr[7]의 유한체 승산 회로 구성 기법으로부터, 이를 변형하여 새로운 연산 기법과 회로 구조를 갖는 $GF(2^m)$상의 병렬 승산 회로를 제안하였다. 본 논문에서 제안한 승산 회로는 다항식 승산 연산 부와 기약 다항식 처리 부, 그리고 모듈러 연산 부로 구성되며, 설계의 예로써 $GF(2^4)$상의 병렬 승산 회로를 보였다. 제안된 승산 회로의 동작을 시뮬레이션 하여 보였고, 그 특징과 장점을 요약하여 결론을 맺었다.

II. 유한체의 수학적 성질

유한체[8-10]란 유한개의 원소들로 이루어진 집합으로 그 원소들간의 연산이 사칙 연산에 대하여 닫혀있는 집합체를 말한다. 유한체는 기초체 $GF(p)$와 이를 확장한 확장체 $GF(p^m)$으로 구분된다. 이때, p와 m은 각각 소수와 양의 정수이며 p 또는 p^m은 유한체 구성 원소의 수를 나타낸다. 예를 들어, $GF(2)$는 0과 1의 두 원소로 구성되며, 이러한 기초체를 확장한 확장체 $GF(2^m)$은 2^m개의 원소를 갖는다. 따라서, $GF(2^m)$은 양의 정수 m에 대하여 2^m개의 원소들로 구성된 수 체계라 할 수 있다. 현재의 실용 회로는 $GF(2^m)$이 주류를 이루며, 일부 분야에서 $GF(p^m)$에 대한 연구가 진행되고 있으나, 본 논문에서 언급되는 유한체는 $GF(2^m)$에 국한하기로 한다.

유한체 상의 연산은 모듈러 연산을 통해 이루어진다. $GF(2)$상의 연산은 모듈러 2 연산을 통해 0 또는 1의

결과를 갖는다. $GF(2^m)$의 경우 원시 기약 다항식 또는 간략히 기약 다항식이라 불리우는 다항식 $F(x)$를 사용한 모듈러 연산에 의해 이루어지며, 연산의 결과는 다시 유한체의 원소로 표현된다.

$GF(2^m)$상의 0이 아닌 (2^m-1)개의 원소들은 원시 원소 α를 통하여 식 (1)과 같이 나타낼 수 있다.

$$GF(2^m) = \{0, \alpha^0, \alpha^1, \cdots, \alpha^{q-2} \mid q=2^m\} \quad (1)$$

$$F(x) = x^m + f_{m-1}x^{m-1} + \cdots + f_1x + f_0 \quad (2)$$

한편, $GF(2^m)$상의 기약다항식 $F(x)$를 식 (2)와 같이 나타낼 때, α는 $F(x)$의 한 근이 되므로 $F(\alpha)=\alpha^m+f_{m-1}\alpha^{m-1}+\cdots+f_1\alpha+f_0=0$이 성립한다. 따라서, α^m은 식 (3)과 같이 $(m-1)$차 이하의 다항식으로 나타낼 수 있다.

$$\alpha^m = f_{m-1}\alpha^{m-1} + \cdots + f_1\alpha + f_0 \quad (3)$$

식 (3)으로부터 식 (1)의 모든 원소들을 식 (4)와 같이 $(m-1)$이하의 차수를 갖는 α의 다항식으로 표현할 수 있으며 이때, 기저를 이루는 α^{m-1}, $\cdots$, α, $\alpha^0=1$들을 표준 기저(standard basis)라 한다.

$$GF(2^m) = \{0, \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{q-2}\}_{\mathrm{mod}\_F(\alpha)} = \{x_{m-1}\alpha^{m-1}+\cdots+x_1\alpha+x_0 \mid x_i \in GF(2), 0 \le i \le m-1\} \quad (4)$$

III. 이항식의 승산 연산 기법 및 모듈러 연산 기법

3.1 이항식의 승산 연산 기법

두 개의 항으로 구성된 다항식을 이항식이라 하며, 임의의 양의 정수 n에 대하여 $m=2^n$의 항을 갖는 다항식 $A(x)$와 $B(x)$는 식 (5)과 같이 이항식으로 나타낼 수 있다.

$$\begin{aligned} A(x) &= a_{m-1}x^{m-1} + \cdots + a_1x + a_0 \\ &= x^{m/2}(a_{m-1}x^{m/2-1} + a_{m-2}x^{m/2-2} + \cdots + a_{m/2+1}x + a_{m/2}) \\ &\quad + (a_{m/2-1}x^{m/2-1} + a_{m/2-2}x^{m/2-2} + \cdots + a_1x + a_0) \\ &= x^{m/2}A_h(x) + A_l(x) \\ B(x) &= b_{m-1}x^{m-1} + \cdots + b_1x + b_0 \\ &= x^{m/2}(b_{m-1}x^{m/2-1} + b_{m-2}x^{m/2-2} + \cdots + b_{m/2+1}x + b_{m/2}) \\ &\quad + (b_{m/2-1}x^{m/2-1} + b_{m/2-2}x^{m/2-2} + \cdots + b_1x + b_0) \\ &= x^{m/2}B_h(x) + B_l(x) \end{aligned} \quad (5)$$

식 (5)의 $A(x)$와 $B(x)$는 각각 $A_h(x)$와 $A_l(x)$, $B_h(x)$와 $B_l(x)$의 두 계수 다항식을 갖는 이항식으로 표현되었다. 이 계수 다항식들을 사용하여 승산에 필요한 보조 다항식들을 식 (6)와 같이 정의하였다.

$$\begin{aligned} &D_{ll}(x) = A_l(x)B_l(x),\ D_{hh}(x) = A_h(x)B_h(x), \\ &D_{hl}(x) = [A_h(x)\oplus A_l(x)][(B_h(x)\oplus B_l(x)] \end{aligned} \quad (6)$$

식 (6)의 보조 다항식들을 사용하여 $A(x)$와 $B(x)$의 승산 $P'(x)$를 나타낼 수 있으며 식 (7)과 같다.

$$\begin{aligned} P'(x) &= A(x)B(x) \\ &= D_{hh}(x)x^m + [D_{hh}(x)+D_{hl}(x)+D_{ll}(x)]x^{m/2} + D_{ll}(x) \end{aligned} \quad (7)$$

식 (5)에서 $A_h(x)$, $A_l(x)$, $B_h(x)$, $B_l(x)$는 모두 $x^{m/2-1}$차 이하의 다항식이며 항의 개수가 $x^{m/2}$개이다.

[예제 1] n=1, 즉 m=2이며 $GF(2)$상의 계수를 갖는 가장 간단한 이항식을 구성하는 두 일차 다항식 $S_1(x)$와 $T_1(x)$를 식 (8)에 보였다.

$$S_1(x) = s_1x + s_0, \quad T_1(x) = t_1x + t_0 \quad (8)$$

두 일차 다항식의 승산 전개에 앞서, 승산에 필요한 보조항들을 식 (6)에 따라 식 (9)와 같이 나타낼 수 있다.

$$D_{ll}(x)=s_0t_0,\ D_{hl}(x)=(s_1\oplus s_0)(t_1\oplus t_0),\ D_{hh}(x)=s_1t_1 \quad (9)$$

$S_1(x)$와 $T_1(x)$의 모든 계수들, s_1, s_0, t_1, t_0를 $GF(2)$상의 원소들이라 가정하면, $D_{ll}(x)$, $D_{hl}(x)$, $D_{hh}(x)$도 $GF(2)$상의 원소가 된다. 식 (9)의 보조 다항식들을 사용하여 식 (8)에 보인 두 일차 다항식의 승산을 식 (10)과 같이 나타낼 수 있다.

$$\begin{aligned} P'(x) &= S_1(x)T_1(x) = p'_2x^2+p'_1x+p'_0 \\ &= D_{hh}(x)x^2+[D_{hh}(x)+D_{hl}(x)+D_{ll}(x)]x+D_{ll}(x) \\ &= s_1t_1x^2 + \{s_1t_1\oplus(s_1\oplus s_0)(t_1\oplus t_0)\oplus s_0t_0\}x + s_0t_0 \end{aligned} \quad (10)$$

유도된 이차 다항식 $P'(x)$의 각 계수들, $p'_2=s_1t_1$, $p'_1=\{s_1t_1\oplus(s_1\oplus s_0)(t_1\oplus t_0)\oplus s_0t_0\}$, $p'_0=s_0t_0$는 모두 $GF(2)$상의 원소가 된다. 예제 1의 과정을 토대로 하여 n=2, 즉 m=4인 경우로 논의를 확장하면 예제 2와 같다.

[예제 1] $GF(2)$상의 계수를 가지며 n=2, 즉 m=4를 가정하여 네 개의 항으로 구성된 두 삼차 다항식을 $A(x)$

와 $B(x)$라 하고 식 (11)에 나타내었다.

$$A(x) = a_3x^3 + a_2x^2 + a_1x + a_0$$
$$B(x) = b_3x^3 + b_2x^2 + b_1x + b_0 \qquad (11)$$

두 삼차 다항식을 이항식으로 나타내면 식 (12)과 같다.

$$A(x) = x^2A_h(x) + A_l(x)$$
$$A_h(x) = a_3x + a_2,\ A_l(x) = a_1x + a_0$$
$$B(x) = b_3x^3 + b_2x^2 + b_1x + b_0$$
$$B_h(x) = b_3x + b_2,\ B_l(x) = b_1x + b_0 \qquad (12)$$

식 (12)로 부터 식 (6)에서 정의한 보조 다항식들을 유도하면 식 (13)와 같다.

$$D_{ll}(x) = A_l(x)B_l(x) = (a_1x + a_0)(b_1x + b_0),$$
$$D_{hl}(x) = [A_h(x)+A_l(x)][B_h(x)+B_l(x)]$$
$$= [(a_3\oplus a_1)x+(a_2\oplus a_0)][(b_3\oplus b_1)x+(b_2\oplus b_0)],$$
$$D_{hh}(x) = A_h(x)B_h(x) = (a_3x + a_2)(b_3x + b_2) \qquad (13)$$

식 (13)에서 보인 보조 다항식들은 모두 일차 다항식의 승산 구조를 가지므로 그 연산 과정은 식 (10)의 경우와 같다. 연산된 보조 다항식들을 식 (7)에 대입하여 전개하면 식 (14)과 같다.

$$\begin{aligned}P'(x) &= D_{hh}(x)\boldsymbol{x}^4+[D_{hh}(x)+D_{hl}(x)+D_{ll}(x)]\boldsymbol{x}^2+D_{ll}(x)\\ &= a_3b_3\boldsymbol{x}^6 + [a_3b_3\oplus(a_3\oplus a_2)(b_3\oplus b_2)\oplus a_2b_2]\boldsymbol{x}^5\\ &+ [a_2b_2\oplus a_3b_3\oplus(a_3\oplus a_1)(b_3\oplus b_1)\oplus a_1b_1]\boldsymbol{x}^4\\ &+ [a_3b_3\oplus(a_3\oplus a_2)(b_3\oplus b_2)\oplus a_2b_2\oplus(a_3\oplus a_1)(b_3\oplus b_1)\\ &\quad\oplus(a_3\oplus a_2\oplus a_1\oplus a_0)(b_3\oplus b_2\oplus b_1\oplus b_0)\oplus a_1b_1\\ &\quad\oplus(a_2\oplus a_0)(b_2\oplus b_0)\oplus(a_1\oplus a_0)(b_1\oplus b_0)\oplus a_0b_0]\boldsymbol{x}^3\\ &+ [a_1b_1\oplus(a_2\oplus a_0)(b_2\oplus b_0)\oplus a_0b_0\oplus a_1b_1]\boldsymbol{x}^2\\ &+ [a_1b_1\oplus(a_1\oplus a_0)(b_1\oplus b_0)\oplus a_0b_0]\boldsymbol{x} + a_0b_0 \qquad (14)\end{aligned}$$

예제 1에서와 동일하게 식 (14)의 결과는 n=3, 즉 m=8인 경우의 보조 다항식 연산에 적용될 수 있다.

3.2 모듈러 연산 기법

$GF(2^m)$상의 모든 원소들은 기약 다항식 $F(x)$에 의한 모듈러 연산에 의해 m-1차 이하의 다항식으로 표현될 수 있음을 2 장에서 논의하였다. 3.1절에서 논의한 두 이항식의 승산 $P'(x)$를 $GF(2^m)$상의 원소로 표현하기 위해 기약 다항식에 의한 모듈러 연산이 적용되어야 한다. 이를 위해 식 (7)으로부터 임의의 양의 정수 i에 대하여 α^{m+i}에 모듈러 연산을 적용한 다항식 표현을 식 (15)와 같이 정의하였다.

$$\alpha^{m+i} = f_{m-1}^{[i]}\alpha^{m-1} + f_{m-2}^{[i]}\alpha^{m-1} + \cdots + f_1^{[i]}\alpha + f_0^{[i]} \qquad (15)$$

식 (15)로부터 α^{m+i+1}에 대한 다항식 표현은 식 (16)과 같이 나타낼 수 있다.

$$\alpha^{m+i+1} = f_{m-1}^{[i+1]}\alpha^{m-1} + f_{m-2}^{[i+1]}\alpha^{m-1} + \cdots + f_1^{[i+1]}\alpha + f_0^{[i+1]} \qquad (16)$$

식 (15)과 (16)으로부터 α^{m+i}의 계수로부터 α^{m+i+1}의 계수를 유도하는 일반식을 유도할 수 있으며 식 (17)과 같다.

$$f_k^{[i+1]} = f_{k-1}^{[i]} \oplus f_{m-1}^{[i]} f_k \qquad (1\le k\le m-1)$$
$$= f_{m-1}^{[i]} f_k \qquad (k = 0) \qquad (17)$$

[예제 3] 기약 다항식 $F(x)=x^4+x+1$을 적용하여 $GF(2^4)$상의 모듈러 연산을 적용하기 위해 식 (7)으로부터 식 (18)를 유도할 수 있다.

$$\alpha^4 = f_3\alpha^3 + f_2\alpha^2 + f_1\alpha + f_0 \qquad (18)$$

식 (18)에서 f_3=0, f_2=0, f_1=1, f_0=1이다. 식 (18)로부터 식 (16)과 (17)을 적용하여 α^5에 대한 다항식 표현을 유도할 수 있으며 식 (19)와 같다.

$$\alpha^5 = \alpha^{4+1} = f_3^{[1]}\alpha^3 + f_2^{[1]}\alpha^{m-1} + f_1^{[1]}\alpha + f_0^{[1]}$$
$$f_3^{[1]} = f_2 \oplus f_3\cdot f_3 = 0 \oplus 0\cdot 0 = 0$$
$$f_2^{[1]} = f_1 \oplus f_3\cdot f_2 = 1 \oplus 0\cdot 0 = 1$$
$$f_1^{[1]} = f_0 \oplus f_3\cdot f_1 = 1 \oplus 0\cdot 1 = 1$$
$$f_0^{[1]} = f_3\cdot f_0 = 0\cdot 1 = 0 \qquad (19)$$

동일한 방법을 반복 적용하여 모든 4차 이상의 α에 대한 다항식 표현을 유도할 수 있으며, 이를 표 1에 정리하였다.

3.3 승산 식 $P'(x)$에 대한 모듈러 연산 적용

본 절에서는 3.1절과 논의한 두 다항식 $A(x)$와 $B(x)$의 승산 전개의 결과 $P'(x)$에 대하여 3.2절에서 논의한 모듈러 연산 기법을 적용한 $P(x)=P'(x)_{mod_F(x)}$의 연산 기법에 대하여 논의하였다.

표 1. $GF(2^4)$상의 원소들에 대한 다항식 및 벡터 표현

원소	다항식 표현	벡터 표현
	$f_3\alpha^3+f_2\alpha^2+f_1\alpha+f_0$	$f_3\ f_2\ f_1\ f_0$
0	0	0 0 0 0
1	1	0 0 0 1
α	α	0 0 1 0
α^2	α^2	0 1 0 0
α^3	α^3	1 0 0 0
α^4	$\alpha+1$	0 0 1 1
α^5	$\alpha^2+\alpha$	0 1 1 0
α^6	$\alpha^3+\alpha^2$	1 1 0 0
α^7	$\alpha^3+\alpha+1$	1 0 1 1
α^8	α^2+1	0 1 0 1
α^9	$\alpha^3+\alpha$	1 0 1 0
α^{10}	$\alpha^2+\alpha+1$	0 1 1 1
α^{11}	$\alpha^3+\alpha^2+\alpha$	1 1 1 0
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1 1 1 1
α^{13}	$\alpha^3+\alpha^2+1$	1 1 0 1
α^{14}	α^3+1	1 0 0 1

두 $(m-1)$차의 다항식을 승산하여 $2(m-1)$차의 다항식 $P'(x)$를 유도할 수 있으며 이를 식 (20)에 나타내었다.

$$P'(x) = p'_{2m-2}x^{2m-2} + \cdots + p'_m x^m + p'_{m-1}x^{m-1} + \cdots + p'_1 x + p'_0 \qquad (20)$$

식 (20)에서 m차 이상의 α에 대하여 식 (16)과 (17)을 적용하여 $P(x)=P'(x)_{mod_F(x)}$의 연산 식을 나타내면 식 (21)과 같다.

$$\begin{aligned}
P(x) &= p'_{2m-2}x^{2m-2} + \cdots + p'_m x^m + p'_{m-1}x^{m-1} + \cdots + p'_1 x + p'_0 \\
&= [p'_{m-1}x^{m-1} + p'_{m-2}x^{m-2} + \cdots + p'_1 x + p'_0] \\
&+ p'_m[f_{m-1}x^{m-1} + f_{m-2}x^{m-2} + \cdots + f_1 x + f_0] \\
&+ p'_{m+1}[f_{m-1}{}^{[1]}x^{m-1} + f_{m-2}{}^{[1]}x^{m-2} + \cdots + f_1{}^{[1]}x + f_0{}^{[1]}] \\
&+ \cdots \\
&+ p'_{2m-2}[f_{m-1}{}^{[m-2]}x^{m-1} + f_{m-2}{}^{[m-2]}x^{m-2} + \cdots + f_1{}^{[m-2]}x + f_0{}^{[m-2]}] \\
&= [p'_{m-1}\oplus p'_m f_{m-1}\oplus p'_{m+1}f_{m-1}{}^{[1]}\oplus\cdots\oplus p'_{2m-2}f_{m-1}{}^{[m-2]}]x^{m-1} \\
&+ [p'_{m-2}\oplus p'_m f_{m-2}\oplus p'_{m+1}f_{m-2}{}^{[1]}\oplus\cdots\oplus p'_{2m-2}f_{m-2}{}^{[m-2]}]x^{m-2} \\
&+ \cdots \\
&+ [p'_1\oplus p'_m f_1\oplus p'_{m+1}f_1{}^{[1]}\oplus\cdots\oplus p'_{2m-2}f_1{}^{[m-2]}]x \\
&+ [p'_0\oplus p'_m f_0\oplus p'_{m+1}f_0{}^{[1]}\oplus\cdots\oplus p'_{2m-2}f_0{}^{[m-2]}] \qquad (21)
\end{aligned}$$

IV. $GF(2^m)$상의 승산 회로 설계

3 장에서 논의한 이항식 승산 및 모듈러 연산 기법을 토대로 $GF(2^m)$상의 승산 회로를 구성하기 위한 블록도를 그림 1에 보였다.

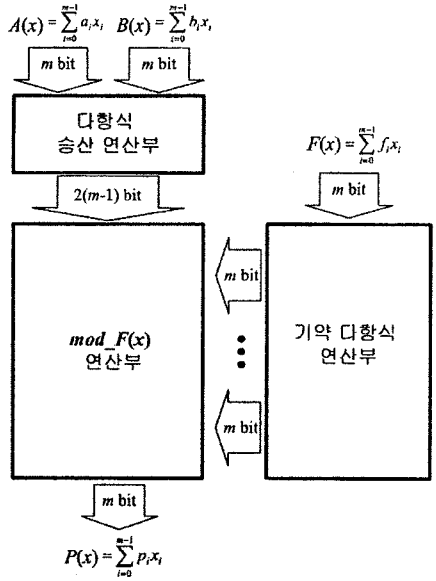
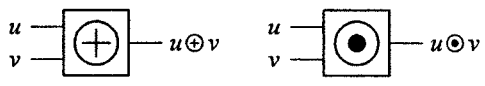


그림 1. $GF(2^m)$상의 승산회로를 구성하기 위한 블록도

4.1 다항식 승산 연산 부의 설계

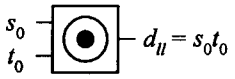
앞 3 장에서 두 일차 다항식의 승산 전개와 이를 확장하여 $m(=2^n)$개의 항을 갖는 다항식들의 승산 전개를 논의하였다. 본 절에서는 이항식의 승산을 회로로 구현하는 기법에 대하여 논의하였다. 회로의 구현을 위해 먼저, $GF(2)$상의 기본 연산 게이트를 그림 2에 정의하였다. 유한체 연산은 모듈러 연산을 토대로 이루어지며, $GF(2)$상의 가산과 승산을 만족하는 디지털 소자는 AND와 XOR이다. 일반적인 디지털 회로에 적용되는 이들 소자의 기호와는 별도로 유한체 연산에서는 모듈러 가산 및 승산의 연산자로 각각 $\oplus$와 $\odot$를 사용하며 이를 기호화하여 그림 2의 게이트를 사용하고 있다.



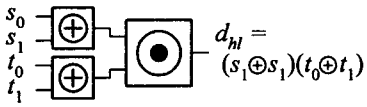
(a) $GF(2)$ 가산게이트 (b) $GF(2)$ 승산 게이트

그림 2. $GF(2)$ 기본 연산 게이트

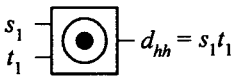
본 논문에서도 연산자와 연산 게이트의 일치를 위해 이에 따랐다. 그림 2의 $GF(2)$ 기본 연산 게이트를 사용하여 식 (6)에서 보인 보조항들의 회로를 설계하면 그림 3과 같다.



(a) $d_{ll}=s_0t_0$에 대한 회로



(b) $d_{hl}=(s_1\oplus s_0)(t_1\oplus t_0)$에 대한 회로



(c) $d_{hh}=s_1t_1$에 대한 회로

그림 3. 식 (6)의 보조항들에 대한 회로 설계

그림 3에서 보인 보조항들에 대한 회로를 사용하여 식 (7)에서 보인 $P'(x)$의 연산 회로를 구성할 수 있으며 그림 4와 같다.

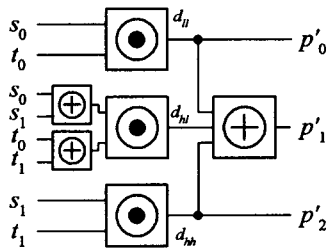


그림 4. 일차 다항식의 승산 $P'(x)$의 회로

식 (14)에서 보조 다항식 $D_{ll}(x)$, $D_{hl}(x)$, $D_{hh}(x)$은 모두 두 일차 다항식의 승산 구조를 갖는다. 따라서, 이들에 대한 회로의 구현에 그림 4의 회로를 적용할 수 있다.

4.2 기약 다항식 연산 부의 설계

임의의 양의 정수 i에 대하여 α^{m+i}에 대한 다항식 표현을 식 (16)과 같이 정의할 때, α^{m+i+1}에 대한 다항식 표현을 식 (17)에 나타내었다. 또한, α^{m+i}와 α^{m+i+1}의 각 계수들의 관계를 나타내는 일반식을 식 (18)에 나타내었다. 이로부터 $GF(2^m)$상의 m에 대한 기약 다항식의 각 계수 연산 회로를 설계할 수 있으며, 이를 그림 5에 나타내었다.

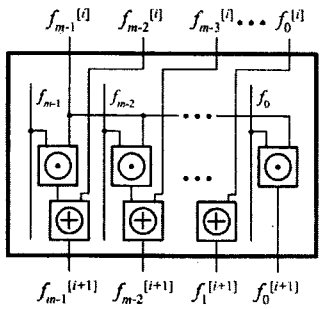


그림 5. 기약 다항식 연산 부

4.3 모듈러 연산 부의 설계

두 다항식 $A(x)$와 $B(x)$의 승산에 의해 유도된 $P'(x)$에 대하여 m차 이상의 x에 대한 모듈러 연산 과정을 식 (22)에 보였다. 이로부터 모듈러 연산을 수행하는 연산 회로를 설계할 수 있으며 이를 그림 6에 나타내었다.

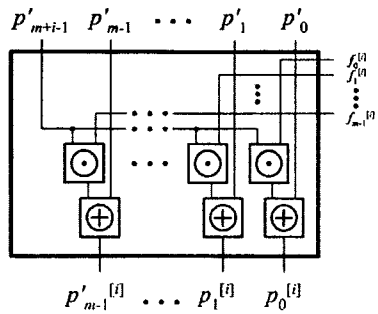


그림 6. 모듈러 연산 부

[예제 4] 지금까지의 논의를 토대로 $GF(2^4)$상의 승산 회로를 설계할 수 있다. 예제 1을 통해 $GF(2^4)$상의 두 원소 $A(x)$와 $B(x)$의 승산을 전개할 수 있으며, 이때 필요한 보조 다항식 $D_{ll}(x)$, $D_{hl}(x)$, $D_{hh}(x)$은 모두 일차 다항식의 승산 구조를 가지므로 그림 4의 회로를 적용할 수 있다. $GF(2^4)$상의 다항식 승산 연산 부의 회로는 그림 7과 같다. 그림 7에서 보인 $GF(2^4)$상의 다항식 승산 연산 부 회로와 그림 5와 6에서 보인 기약다항식 연산 부와 모듈러 연산 부를 배열하여 $GF(2^4)$상의 승산 회로를 구성하면 그림 8과 같다.

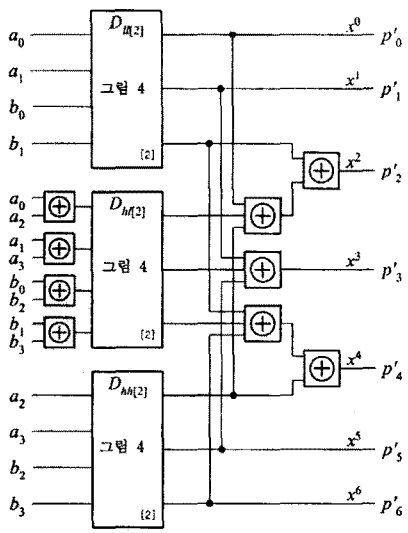


그림 7. $GF(2^4)$상의 다항식 승산 연산 부

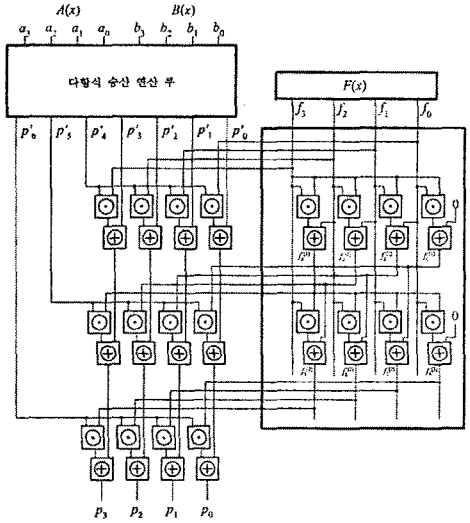


그림 8. $GF(2^4)$상의 승산 회로

V. 결 론

본 논문에서는 이항식의 승산 연산과 모듈러 연산 기법을 적용한 $GF(2^m)$상의 새로운 병렬 승산 연산 회로를 제안하였다. 본 논문의 승산 회로는 다항식 승산 연산 부와 기약 다항식 연산 부, 그리고 모듈러 연산 부로 구성되며 각 연산 부들은 모두 모듈 구조를 가지므로 m에 대한 확장과 회로의 구현이 용이하도록 하였다. 또한, 회로 구현에 필요한 소자를 AND와 XOR로 한정하였고, 병렬 연산 형식을 취하면서도 신호 입력의 시간차를 위한 시간 지연 회로 및 메모리 소자를 필요로 하지 않는다. 따라서, 본 논문에서 제안한 승산 회로는 VLSI에 매우 유리한 구조를 갖는다 할 수 있다.

본 논문에서 제시한 회로 설계의 일반성을 위해 각 연산 부별로 필요한 이론을 수식으로 전개하였고, 회로 설계에 적용될 각 단위 연산 모듈들을 정의, 설계하였다. 본 논문에서 제시한 $GF(2^m)$상의 승산회로 구성기법은 유한체 연산 회로의 개발에 유용한 연구라 사료되며 다양한 연산 회로 개발에 적용될 수 있으리라 사료된다.

참 고 문 헌

[1] B.A. Laws and C.K. Rushford, "A Cellular-Array Multiplier for GF(2^m)," *IEEE Trans. Comp.*, vol. C-20, no. 12, pp. 1573-1578, Dec. 1971.

[2] E.R. Berlekamp, "Bit-Serial Reed-Solomon Encoders," *IEEE Trans. Inf. Theory*, vol. 28, pp. 869-874, Nov. 1982.

[3] C.S. Yeh, I.S. Reed, and T.K. Trung, "Systolic multipliers for finite field GF(2^m)," *IEEE Trans. Com.*, vol. C-33, pp. 357-360, Apr. 1984.

[4] S.T.J. Fenn, M. Benaissa, and D. Taylor, "Bit-serial dual basis systolic multipliers for GF(2^m)," *IEEE ISCAS '95.*, vol. 3, pp. 2000-2003, 1995.

[5] K.Z. Pekmestzi, "Multiplexer-Based Array Multipliers," *IEEE Trans. Comp.*, vol. 48, no. 1, pp. 15-23. Jan. 1999.

[6] M.Y. Lee, *Error Correcting Coding Theory*, Mc Graw-Hill, New York, 1989.

[7] C. Paar, P. Felishmann, and P. Roelse, "Efficient Multiplier Architectures for Galois Fields GF((2^4)^n)," *IEEE Trans. Comp.*, vol. C-47, no. 2, pp. 162-170, Feb. 1998.

[8] A. Gill, *Linear Sequential Circuits*, McGraw-Hill Inc., 1966.

[9] Z. Kohavi, *Switching and Finite Automata Theory(2nd Ed.)*, McGraw-Hill Inc., 1978.

[10] S. Lin, D.J. Costello, *Error Control Coding (Fundamentals and Applications)*, Prentice-Hall, Inc,. 1983.