논문번호 03-01-07

KOA 기반의 유한체 승산기 설계

Design of Finite Field Multiplier based on KOA

변기영*, 나기수**, 김흥수**
GiYoung Byun*, GiSoo Na**, and HeungSoo Kim**

요 약

본 논문에서는 KOA를 적용하여 유한체 승산의 새로운 연산기법을 제시하였다. 먼저, 승산의 전개를 위해 주어진 다항식을 2분 또는 3분하여 각각 2항식과 3항식으로 재구성한 후 정의된 보조다항식을 사용하여 승산을 이루도록 하였다. 승산된 다항식에 모듈러 환원을 적용하기 위해 mod $F(\alpha)$ 연산식을 새롭게 전개하여 제시하였다. 제시된 연산기법들을 적용하여 GF(2^m)상의 승산회로를 구성하였고, Parr의 회로와 비교하였다. 비교논문의 경우 GF((2^4)^n)을 전제함으로써 그 적용이 매우 제한적이나, 본 논문에서는 m=2^n과 m=3^n인 경우를 보임으로써 그 적용이 Parr의 회로에 비해 보다 확장되었다.

Abstract

This paper proposes new multiplicative techniques over finite field, by using KOA. At first, we regenerate the given polynomial into a binomial or a trinomial to apply our polynomial multiplicative techniques. After this, the product polynomial is archived by defined auxiliary polynomials. To perform multiplication over GF(2^m) by product polynomial, a new mod $F(\alpha)$ method is induced. Using the proposed operation techniques, multiplicative circuits over GF(2^m) are constructed. We compare our circuit with the previous one as proposed by Parr. Since Parr's work is premised on GF((2^4)^n), it will not apply to general cases. On the other hand, the our work more expanded adaptive field in case m=3^n.

I. 서 론

유한체(Finite Fields)는 Galois체 또는 간단히 GF라 하며, 오류정정부호, 스위칭이론 및 암호화 등의 분야에 적용되는 연산체계이다[1,2]. 유한체 연산으로는 가산, 승산, 제산, 승산에 대한 역원, 멱승(exponentiation) 등의 연산이 있다. 유한체 연산은 표준, 정규, 쌍대기저 등에 의해 각 형식에 따른 다항식으로 표현된 원소들의 연산과 모듈러 환원의 두 단계 연산을 거쳐 이루어진다. 각 기저들은 그 특성에 따라 연산별 효율성과 그 회로구현의 용이성이 달라지므로, 효율적인 연산 기법의 개발을 위해 선택적으로 사용된다[3]. 예를 들어, 표준기저로 표현된 유한체 원소들의 가산은 자리올림을 고려하지 않으므로 각 비트별 XOR연산에 의해 쉽게 이루어지나, 승산은 다항식의 승산과 모듈러 환원이 함께 적용되므로 가산에 비해 복잡하게 연산된다. 유한체 승산은 가산을 제외한 여타 연산의 기반이 되는 연산이므로 효율적인 연산기법을 개발하기 위한 많은 연구가 진행되었다.

다양한 유한체 연산기법들에 대한 회로구현에 있어 고속과 대용량의 신호 처리능력, 회로의 최적화 및 소형화 등은 중요한 요소들이다. 특히, 현재 비약적으로 발전하고 있는 반도체 기술에 힘입어 VLSI로의 구현을 위해 회로의 정규화 및 모듈화 특성이 강조되고 있

* 가톨릭大學校 情報通信電子工學部
(School of Information, Communication & Electronics Eng., Catholic Univ.)
** 仁荷大學校 電子工學科
(Dept. of Electronic Eng., InHa Univ.)

接受日:2003年 3月 18日, 修正完了日:2004年 6月 18日

다. 유한체 연산 기법 및 구현 회로를 간략히 소개하면, 표준기저를 이용한 Laws[4]의 셀-배열 승산기와 Yeh[5]의 시스토릭[6] 승산기가 있다. 정규기저를 이용한 승산기로는 Massey- Omura[7] 승산기와 이를 VLSI로 설계한 Wang[8]의 회로가 있다. 쌍대기저를 이용한 승산기로는 Berlekamp[9]의 비트 직렬 승산기가 있으며 이들은 각 기저들의 특성을 활용한 대표적 승산기법 및 회로로 알려져 있다. 한편, Kara-tsuba와 Ofman[10]은 2진수 시스템에서 다항식으로 주어진 2진수열의 승산을 가산과 감산의 형식으로 바꾸어 표현함으로써 설계된 시스템의 복잡도를 개선할 수 있음을 보였고, 이를 Karatsuba-Ofman 알고리즘(KOA)라 한다. Parr[11, 12]는 KOA를 기반으로 한 다항식 승산연산과 Mas-trovito[13]의 모듈러 연산기법을 결합하여 복합체 GF($(2^4)^m$)상의 회로 복잡도를 개선한 새로운 승산회로를 제안하였다.

본 논문에서는 KOA를 기반으로 하여 표준기저를 적용한 새로운 유한체 승산 연산기법을 제안하고자 한다. Parr의 경우 GF(2^4)를 기반으로 하여 GF($(2^4)^m$)으로의 확장을 전개한 반면, 본 논문에서는 GF(2^2)과 GF(2^3)으로부터 각각의 단위 연산항을 정의한 후, m으로 확장하여 다항식의 승산을 전개하였다. 본 논문에서 제안한 승산회로는 다항식 승산 연산부와 모듈러 연산부가 독립적으로 구성되며, 빠른 연산동작을 위해 입출력 구조를 병렬로 구성하였다. m에 대한 수식전개를 사용하여 회로의 구성기법을 보였고, 회로 구성에 필요한 소자의 수를 제시하였다. 설계의 예로써 GF(2^4)와 GF(2^9)상의 승산회로를 보였고, Parr의 회로와 구성 및 적용 소자의 수와 지연시간에 대한 비교를 하여 그 결과를 표로 정리하였다. 비교 결과 본 논문에서 제안한 새로운 GF(2^m)상의 승산회로는 Parr의 회로에 비해 보다 확장된 적용범위를 가지며, 회로 복잡도, 동작속도, 그리고 확장성 면에서 비교 우위를 보였으며, 정규화된 구조는 VLSI에 적합하다.

본 논문의 구성을 간략히 소개하면 1장의 서론에 이어, 2장에서는 KOA를 기반으로 한 다항식의 승산과 모듈러 환원의 전개를 제시하였고, 이들로부터 GF(2^m)상의 승산을 전개 하였다. 2장의 논의를 바탕으로 3장에서는 GF(2^m)상의 병렬 승산기를 설계하였다. 4장에서는 본 논문과 타 논문의 승산기들의 구성을 각 항목별로 비교하였으며, 결론으로 본 논문의 끝맺음을 하였다.

II. GF(2^m)상의 승산 전개

2.1 유한체상의 원소 표현과 가산 연산

유한체[1,2] GF(2^m)은 양의 정수 m에 대하여 2^m개의 원소들로 구성된 수 체계이며, 그 원소들의 연산이 사칙연산에 대하여 닫혀있다. GF(2^m)은 0과 1을 원소로 갖는 기초체 GF(2)를 m차원으로 확장한 확장체이며, GF(2^m)상의 모든 연산은 모듈로(modulo) 2 연산을 기반으로 이루어 진다. 0을 제외한 모든 원소들은 원시원소 α에 의해 표현되며, α는 기약다항식 $F(x)=f_0+f_1x+\cdots+f_{m-2}x^{m-2}+f_{m-1}x^{m-1}+x^m$의 근이 된다. 따라서, $F(\alpha)=0$이 되며 식 (1)이 성립한다.

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

기약다항식 $F(x)$에 의해 GF(2^m)상의 모든 원소들은 m보다 낮은 차수를 갖는 α의 다항식으로 구성되며, 다항식을 구성하는 각 기저들, $\{\alpha^{m-1}, \alpha^{m-2}, \cdots, \alpha, \alpha^0=1\}$을 표준기저라 한다. 표준기저를 적용한 GF(2^m)상의 임의의 원소 $A(\alpha)$는 식 (2)와 같이 표현되며, 이때 기저들의 각 계수들, $a_{m-1}, \cdots, a_1, a_0$은 모두 GF(2)상의 원소이다.

$$A(\alpha) = a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 \qquad (2)$$

식 (2)와 같이 표준기저로 표현된 GF(2^m)상의 두 원소를 $A(\alpha)$와 $B(\alpha)$에 대한 가산 $S(\alpha)$는 식 (3)과 같다.

$$S(\alpha) = s_{m-1}\alpha^{m-1} + \cdots + s_1\alpha + s_0 \qquad (3)$$

식 (3)에서 $S(\alpha)$의 각 계수 s_i는 $a_i \oplus b_i$이며, 여기서 아래첨자 i는 0부터 m-1이하의 정수이다. 또한, 연산기호 $\oplus$는 모듈로 2 가산이며, +는 선형결합을 나타낸다.

2.2 KOA 기반의 다항식 승산 전개 (1)

양의 정수 n에 대하여, $m=2^n$이며 식 (2)와 같이 표준기저를 적용하여 (m-1)차 이하의 다항식으로 표현된 GF(2^m)상의 원소 $A(\alpha)$를 $m/2$개의 항으로 이분하여 2항식으로 표현할 수 있다.

정의 1. $m=2^n$인 GF(2^m)상의 원소를 표준기저의 선형

결합으로 표현할 때, $m/2$개의 항을 갖는 다항식으로 분할하여 2항식으로 표현하면 식 (4)와 같다.

$$\begin{aligned} A(\alpha) &= a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \cdots + a_1\alpha + a_0 \\ &= (a_{m-1}\alpha^{m/2-1} + a_{m-2}\alpha^{m/2-2} + \cdots + a_{m/2+1}\alpha + a_{m/2})\alpha^{m/2} \\ &\quad + (a_{m/2-1}\alpha^{m/2-1} + a_{m/2-2}\alpha^{m/2-2} + \cdots + a_1\alpha + a_0) \\ &= A_h(\alpha)\alpha^{m/2} + A_l(\alpha) \end{aligned} \quad (4)$$

정의 1과 같이 2항식으로 표현된 $m=2^n$인 GF(2^m)상의 두 원소 $A(\alpha)=\alpha^{m/2}A_h(\alpha)+A_l(\alpha)$와 $B(\alpha)=\alpha^{m/2}B_h(\alpha)+B_l(\alpha)$ 승산을 전개하기 위해 필요한 보조다항식들을 정의 2에 나타내었다.

정의 2. 정의 1에 의해 2항식으로 표현된 $A(\alpha)$와 $B(\alpha)$의 각 계수다항식들 $A_h(\alpha)$, $A_l(\alpha)$, $B_h(\alpha)$, $B_l(\alpha)$로부터 보조다항식을 식 (5)와 같이 정의한다.

$$D_{hh[2]}(\alpha) = A_h(\alpha)B_h(\alpha) \quad (5\text{-}1)$$

$$D_{hl[2]}(\alpha) = [A_h(\alpha)+A_l(\alpha)][B_h(\alpha)+B_l(\alpha)] \quad (5\text{-}2)$$

$$D_{ll[2]}(\alpha) = A_l(\alpha)B_l(\alpha) \quad (5\text{-}3)$$

정의 1에 의해 2항식으로 표현된 $A(\alpha)$와 $B(\alpha)$승산은 정의 2의 보조다항식들의 가산으로 표현할 수 있으며 이를 정리 1에 보였다.

정리 1. $m=2^n$인 GF(2^m)상의 두 원소 $A(\alpha)$와 $B(\alpha)$각각 정의 1과 같이 2항식으로 표현한 후, 정의 2의 보조다항식들을 사용하여 승산 $C(\alpha)=A(\alpha)B(\alpha)$를 전개하면 식 (6)과 같다.

$$\begin{aligned} C(\alpha) &= D_{hh[2]}(\alpha)\alpha^m \\ &\quad + [D_{hh[2]}(\alpha)+D_{hl[2]}(\alpha)+D_{ll[2]}(\alpha)]\alpha^{m/2} + D_{ll[2]}(\alpha) \end{aligned} \quad (6)$$

증명. 정의 1에 의해 2항식으로 표현된 $A(\alpha)=\alpha^{m/2}A_h(\alpha)+A_l(\alpha)$와 $B(\alpha)=\alpha^{m/2}B_h(\alpha)+B_l(\alpha)$의 승산은 식 (7)과 같다.

$$\begin{aligned} C(\alpha) &= A_h(\alpha)B_h(\alpha)\alpha^m \\ &\quad + [A_h(\alpha)B_l(\alpha)+B_h(\alpha)A_l(\alpha)]\alpha^{m/2} \\ &\quad + A_l(\alpha)B_l(\alpha) \end{aligned} \quad (7)$$

α^m항과 상수항의 계수 $A_h(\alpha)B_h(\alpha)$와 $A_l(\alpha)B_l(\alpha)$를 정의 2에서 각각 $D_{hh[2]}(\alpha)$와 $D_{ll[2]}(\alpha)$로 정의하였다. 정의 2의 $D_{hl[2]}(\alpha)$을 전개하면 식 (8)과 같다.

$$\begin{aligned} D_{hl[2]}(\alpha) &= A_h(\alpha)B_h(\alpha) + A_h(\alpha)B_l(\alpha) \\ &\quad + B_h(\alpha)A_l(\alpha) + A_l(\alpha)B_l(\alpha) \end{aligned} \quad (8)$$

식 (8)에 $D_{hh[2]}(\alpha)$와 $D_{ll[2]}(\alpha)$의 정의를 적용하여 전개하면 식 (9)와 같다.

$$\begin{aligned} &A_h(\alpha)B_l(\alpha) + B_h(\alpha)A_l(\alpha) \\ &\quad = D_{hh[2]}(\alpha) + D_{hl[2]}(\alpha) + D_{ll[2]}(\alpha) \end{aligned} \quad (9)$$

식 (9)의 결과는 식 (6)의 $\alpha^{m/2}$항의 계수이다. 이상과 같이 2항식으로 표현된 $A(\alpha)$와 $B(\alpha)$의 승산 $C(\alpha)$는 정의 2의 보조다항식과 그 가산으로 표현된다.
증명 끝.

예제 1. $n=1$, 즉 $m=2$인 GF(2^2)상의 두 원소 $A(\alpha)$와 $B(\alpha)$는 정의 1에 의해 식 (10)와 같이 각각 2항식으로 표현된다.

$$A(\alpha) = A_h(\alpha)\alpha + A_l(\alpha) = a_1\alpha + a_0 \quad (10\text{-}1)$$

$$B(\alpha) = B_h(\alpha)\alpha + B_l(\alpha) = b_1\alpha + b_0 \quad (10\text{-}2)$$

식 (10)의 각 계수다항식을 식 (5)에 대입하여 보조다항식들을 연산하면 식 (11)과 같다.

$$D_{hh[2]}(\alpha) = A_h(\alpha)B_h(\alpha) = a_1b_1 \quad (11\text{-}1)$$

$$\begin{aligned} D_{hl[2]}(\alpha) &= [A_h(\alpha)+A_l(\alpha)][B_h(\alpha)+B_l(\alpha)] \\ &= [a_1 \oplus a_0][b_1 \oplus b_0] \end{aligned} \quad (11\text{-}2)$$

$$D_{ll[2]}(\alpha) = A_l(\alpha)B_l(\alpha) = a_0b_0 \quad (11\text{-}3)$$

식 (11)에서 유도한 세 보조다항식을 정리 1에 대입하여 승산 $C(\alpha)$를 전개하면 식 (12)와 같다.

$$\begin{aligned} C(\alpha) &= a_1b_1\alpha^2 + [a_1b_1 \oplus a_0b_0 \oplus (a_1 \oplus a_0)(b_1 \oplus b_0)]\alpha \\ &\quad + a_0b_0 \end{aligned} \quad (12)$$

예제 2. 예제 1의 논의를 확장하여 n=2, 즉 m=4인 GF(2^4)상의 두 원소 $A(\alpha)$와 $B(\alpha)$의 승산을 전개하면 다음과 같다. 먼저, 정의 1에 의해 $A(\alpha)$와 $B(\alpha)$를 식 (13)과 같이 각각 2항식으로 표현한다.

$$\begin{aligned} A(\alpha) &= A_h(\alpha)\alpha + A_l(\alpha) \\ &= [a_3\alpha + a_2]\alpha^2 + [a_1\alpha + a_0] \qquad (13\text{-}1) \\ B(\alpha) &= B_h(\alpha)\alpha + B_l(\alpha) \\ &= [b_3\alpha + b_2]\alpha^2 + [b_1\alpha + b_0] \qquad (13\text{-}2) \end{aligned}$$

식 (13)의 각 계수다항식을 식 (5)에 대입하여 보조다항식들을 연산하면 식 (14)와 같다.

$$D_{hh[2]}(\alpha) = A_h(\alpha)B_h(\alpha) = [a_3\alpha + a_2][b_3\alpha + b_2] \quad (14\text{-}1)$$

$$\begin{aligned} D_{hl[2]}(\alpha) &= [A_h(\alpha) + A_l(\alpha)][B_h(\alpha) + B_l(\alpha)] \\ &= [(a_3 \oplus a_1)\alpha + (a_2 \oplus a_0)][(b_3 \oplus b_1)\alpha + (b_2 \oplus b_0)] \end{aligned} \quad (14\text{-}2)$$

$$D_{ll[2]}(\alpha) = A_l(\alpha)B_l(\alpha) = [a_1\alpha + a_0][b_1\alpha + b_0] \quad (14\text{-}3)$$

식 (14-3)의 연산은 예제 1과 동일하며, 식 (14-1)의 다항식에서 그 계수들을 a_3, a_2, b_3, b_2로 치환하여 연산할 수 있다. 식 (14-2) 또한, $(a_3 \oplus a_1)$, $(a_2 \oplus a_0)$, $(b_3 \oplus b_1)$, $(b_2 \oplus b_0)$의 연산을 선행한 후 예제 1의 결과에 대입할 수 있다. 이렇게 동일한 연산 과정을 거쳐 유도한 보조다항식들을 식 (6)에 적용함으로써 GF(2^4)상의 $A(\alpha)$와 $B(\alpha)$의 승산을 유도할 수 있다. 예제 2에서 유도한 승산 결과는 n=3, 즉 m=8인 경우의 보조다항식이 되며, 이러한 재귀연산은 임의의 정수 n으로 확장 가능하다.

2.3 KOA 기반의 다항식 승산 전개 (2)

양의 정수 n에 대하여 $m=3^n$인 경우, 표준기저에 의해 $(m-1)$차 이하의 다항식으로 표현된 GF(2^m)상의 원소 $A(\alpha)$을 $m/3$개 항으로 삼분하여 3항식으로 표현가능하다.

정의 3. $m=3^n$인 GF(2^m)상의 원소를 표준기저의 선형결합으로 표현할 때, $m/3$개의 항을 갖는 다항식으로 분할하여 2항식으로 표현가능하며 식 (15)와 같다.

$$\begin{aligned} A(\alpha) &= a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \cdots + a_1\alpha + a_0 \\ &= (a_{m-1}\alpha^{m/3-1} + a_{m-2}\alpha^{m/3-2} + \cdots + a_{2m/3})\alpha^{2m/3} \\ &+ (a_{2m/3-1}\alpha^{m/3-1} + a_{2m/2-2}\alpha^{m/3-2} + \cdots + a_{m/3})\alpha^{m/3} \\ &+ (a_{m/3-1}\alpha^{m/3-1} + a_{m/3-2}\alpha^{m/3-2} + \cdots + a_0)\alpha^{m/3} \\ &= A_h(\alpha)\alpha^{2m/3} + A_m(\alpha)\alpha^{m/3} + A_l(\alpha) \qquad (15) \end{aligned}$$

정의 3과 같이 3항식으로 표현된 $m=3^n$인 GF(2^m)상의 두 원소 $A(\alpha)=A_h(\alpha)\alpha^{2m/3}+A_m(\alpha)\alpha^{m/3}+A_l(\alpha)$와 $B(\alpha)=B_h(\alpha)\alpha^{2m/3}+B_m(\alpha)\alpha^{m/3}+B_l(\alpha)$의 승산을 전개하기 위해 필요한 보조다항식들을 정의 4에 나타내었다.

정의 4. 정의 3에 의해 3항식으로 표현된 $A(\alpha)$와 $B(\alpha)$의 각 계수다항식들 $A_h(\alpha)$, $A_m(\alpha)$, $A_l(\alpha)$, $B_h(\alpha)$, $B_m(\alpha)$, $B_l(\alpha)$로부터 승산 전개에 필요한 보조다항식을 식 (16)와 같이 정의한다.

$$D_{ll[3]}(\alpha) = A_l(\alpha)B_l(\alpha) \qquad (16\text{-}1)$$

$$D_{mm[3]}(\alpha) = A_l(\alpha)B_l(\alpha) \qquad (16\text{-}2)$$

$$D_{hh[3]}(\alpha) = A_h(\alpha)B_h(\alpha) \qquad (16\text{-}3)$$

$$D_{hm[3]}(\alpha) = [A_h(\alpha) + A_m(\alpha)][B_h(\alpha) + B_m(\alpha)] \qquad (16\text{-}4)$$

$$D_{hl[3]}(\alpha) = [A_h(\alpha) + A_l(\alpha)][B_h(\alpha) + B_l(\alpha)] \qquad (16\text{-}5)$$

$$D_{ml[3]}(\alpha) = [A_m(\alpha) + A_l(\alpha)][B_m(\alpha) + B_l(\alpha)] \qquad (16\text{-}6)$$

정의 3에 의해 3항식으로 표현된 $A(\alpha)$와 $B(\alpha)$의 승산은 정의 4의 보조다항식들의 가산으로 표현할 수 있으며 이를 정리 2에 보였다.

정리 2. $m=3^n$인 GF(2^m)상의 두 원소 $A(\alpha)$와 $B(\alpha)$를 각각 정의 3과 같이 3항식으로 표현한 후, 정의 4의 보조다항식들을 사용하여 $A(\alpha)$와 $B(\alpha)$의 승산 $C(\alpha)$를 전개하면 식 (17)과 같다.

$$\begin{aligned} C(\alpha) &= D_{hh[3]}(\alpha)\alpha^{4m/3} \\ &+ [D_{hh[3]}(\alpha) + D_{hm[3]}(\alpha) + D_{mm[3]}(\alpha)]\alpha^{3m/3} \\ &+ [D_{hl[3]}(\alpha) + D_{hh[3]}(\alpha) + D_{mm[3]}(\alpha) + D_{ll[3]}(\alpha)]\alpha^{2m/3} \\ &+ [D_{ml[3]}(\alpha) + D_{mm[3]}(\alpha) + D_{ll[3]}(\alpha)]\alpha^{m/3} + D_{ll[3]}(\alpha) \end{aligned} \qquad (17)$$

증명. 3항식으로 표현된 $A(\alpha)$와 $B(\alpha)$의 승산을 전개한 후 식 (16)의 보조다항식을 적용하여 정리 1과 동

일한 방법으로 전개하여 증명할 수 있다.
증명 끝.

예제 3. n=1, 즉 m=3인 GF(2^3)상의 $A(\alpha)$와 $B(\alpha)$는 정의 4에 의해 식 (18)과 같이 각각 3항식으로 표현된다.

$$A(\alpha) = A_h(\alpha)\alpha^2 + A_h(\alpha)\alpha + A_l(\alpha) = a_2\alpha^2 + a_1\alpha + a_0 \quad (18\text{-}1)$$

$$B(\alpha) = B_h(\alpha)\alpha^2 + B_h(\alpha)\alpha + B_l(\alpha) = b_2\alpha^2 + b_1\alpha + b_0 \quad (18\text{-}2)$$

식 (18)의 각 계수다항식로부터 보조다항식들을 연산하면 식 (19)와 같다.

$$D_{ll[3]}(\alpha) = A_l(\alpha)B_l(\alpha) = a_0b_0 \quad (19\text{-}1)$$

$$D_{mm[3]}(\alpha) = A_m(\alpha)B_m(\alpha) = a_1b_1 \quad (19\text{-}2)$$

$$D_{hh[3]}(\alpha) = A_h(\alpha)B_h(\alpha) = a_2b_2 \quad (19\text{-}3)$$

$$D_{hm[3]}(\alpha) = [A_h(\alpha)+A_m(\alpha)][B_h(\alpha)+B_m(\alpha)] = [a_2\oplus a_1][b_2\oplus b_1] \quad (19\text{-}4)$$

$$D_{hl[3]}(\alpha) = [A_h(\alpha)+A_l(\alpha)][B_h(\alpha)+B_l(\alpha)] = [a_2\oplus a_0][b_2\oplus b_0] \quad (19\text{-}5)$$

$$D_{ml[3]}(\alpha) = [A_m(\alpha)+A_l(\alpha)][B_m(\alpha)+B_l(\alpha)] = [a_1\oplus a_0][b_1\oplus b_0] \quad (19\text{-}6)$$

식 (19)에서 유도한 보조다항식들을 정리 2에 대입하여 승산 $C(\alpha)$를 전개하면 식 (20)과 같다.

$$C(\alpha) = a_2b_2\alpha^4 + [a_2b_2\oplus(a_2\oplus a_1)(b_2\oplus b_1)\oplus a_1b_1]\alpha^3 + [a_2b_2\oplus(a_2\oplus a_0)(b_2\oplus b_0)\oplus a_1b_1\oplus a_0b_0]\alpha^2 + [a_1b_1\oplus(a_1\oplus a_0)(b_1\oplus b_0)\oplus a_0b_0]\alpha + a_0b_0 \quad (20)$$

예제 4. 예제 3의 논의를 확장하여 n=2, 즉 m=9인 GF(2^9)상의 두 원소 $A(\alpha)$와 $B(\alpha)$의 승산을 전개하면 다음과 같다. 먼저, 정의 3에 의해 $A(\alpha)$와 $B(\alpha)$를 식 (21)과 같이 각각 3항식으로 표현한다.

$$A(\alpha) = A_h(\alpha)\alpha^2 + A_m(\alpha)\alpha + A_l(\alpha) \quad (21\text{-}1)$$

$$B(\alpha) = B_h(\alpha)\alpha^2 + B_m(\alpha)\alpha + B_l(\alpha) \quad (21\text{-}2)$$

식 (21-1)에서 $A(\alpha)$의 각 계수다항식들은 $A_h(\alpha)$=$a_8\alpha^2$ +$a_7\alpha$+a_6, $A_m(\alpha)$=$a_5\alpha^2$+$a_4\alpha$+a_3, $A_l(\alpha)$=$a_2\alpha^2$+$a_1\alpha$+a_0이며 $B(\alpha)$의 각 계수다항식들도 동일한 형태이다. 이 계수다항식을 식 (16)에 대입하여 보조다항식들을 연산하면 식 (22)와 같다.

$$D_{ll[3]}(\alpha) = [a_2\alpha^2 + a_1\alpha + a_0][b_2\alpha^2 + b_1\alpha + b_0] \quad (22\text{-}1)$$

$$D_{mm[3]}(\alpha) = [a_5\alpha^2 + a_4\alpha + a_3][b_5\alpha^2 + b_4\alpha + b_3] \quad (22\text{-}2)$$

$$D_{hh[3]}(\alpha) = [a_8\alpha^2 + a_7\alpha + a_6][b_8\alpha^2 + b_7\alpha + b_6] \quad (22\text{-}3)$$

$$D_{hm[3]}(\alpha) = [(a_8\oplus a_5)\alpha^2 + (a_7\oplus a_4)\alpha + (a_6\oplus a_3)][(b_8\oplus b_5)\alpha^2 +(b_7\oplus b_4)\alpha + (b_6\oplus b_3)] \quad (22\text{-}4)$$

$$D_{hl[3]}(\alpha) = [(a_8\oplus a_2)\alpha^2 + (a_7\oplus a_1)\alpha + (a_6\oplus a_0)][(b_8\oplus b_2)\alpha^2 + (b_7\oplus b_1)\alpha + (b_6\oplus b_0)] \quad (22\text{-}5)$$

$$D_{ml[3]}(\alpha) = [(a_5\oplus a_2)\alpha^2 + (a_4\oplus a_1)\alpha + (a_3\oplus a_0)][(b_5\oplus b_2)\alpha^2 + (b_4\oplus b_1)\alpha + (b_3\oplus b_0)] \quad (22\text{-}6)$$

식 (22-1), (22-2), (22-3)은 모두 이차다항식의 승산으로 예제 3과 그 연산형식이 동일하다. 식 (22-4), (22-5), (22-6)의 경우도 계수들의 가산이 선행되는 조건외에는 동일한 연산형식이다. 이렇게 동일한 연산 과정을 거쳐 유도한 보조다항식들을 식 (17)에 적용함으로써 GF(2^9)상의 $A(\alpha)$와 $B(\alpha)$의 승산을 유도할 수 있다. 예제 4의 승산 결과는 n=3, 즉 m=27인 경우의 보조다항식이 되며, 이러한 재귀연산은 임의의 정수 n에 대하여 m=3^n으로 확장 가능하다.

2.4 모듈러 환원의 일반식 유도

두 m-1차 다항식의 승산결과는 2(m-1)차의 다항식이 되므로 식 (6) 또는 (17)의 $C(\alpha)$=$A(\alpha)B(\alpha)$는 2(m-1)차의 다항식이 되며 이를 식 (23)에 보였다.

$$C(\alpha) = c_{2(m-1)}\alpha^{2(m-1)}+\cdots+c_m\alpha^m+c_{m-1}\alpha^{m-1}+\cdots \cdots+c_1\alpha+c_0 \quad (23)$$

$C(\alpha)$를 GF(2^m)상의 원소로 표현하기 위해 기약다항식 $F(\alpha)$에 의한 모듈러 환원을 거쳐야 하며, 그 결과 유도된 m-1차 다항식을 $P(\alpha)$라 하면 식 (24)와 같다.

$$P(\alpha) = A(\alpha)B(\alpha) \bmod F(\alpha) = C(\alpha) \bmod F(\alpha) = p_{m-1}\alpha^{m-1} + \cdots + p_1\alpha + p_0 \quad (24)$$

식 (24)의 $P(\alpha)$를 유도하기 위하여 식 (23)의 $C(\alpha)$의 m 이상의 차수를 갖는 α에 대한 모듈러 환원이 적용되어야 한다. 모듈러 환원의 일반식을 유도하기 위해 필요한 표기를 정의 5에 나타내었다.

정의 5. 0을 포함한 양의 정수 i에 대하여 GF(2^m)상의 원소 α^{m+i}에 mod $F(\alpha)$ 연산의 결과는 m-1차 이하의 다항식으로 표현가능하며 이를 식 (25)에 나타내었다.

$$\alpha^{m+i} = f_{m-1}{}^{[i]}\alpha^{m-1} + f_{m-2}{}^{[i]}\alpha^{m-2} + \cdots + f_1{}^{[i]}\alpha + f_0{}^{[i]} \quad (25)$$

식 (25)에서 우항의 각 계수들에 표기한 위 첨자 [i]는 좌항의 차수 m+i에서의 i를 나타낸다. 식 (25)에서 i=0를 대입하여 전개하면 식 (26)과 같다.

$$\alpha^{m+0} = f_{m-1}{}^{[0]}\alpha^{m-1} + f_{m-2}{}^{[0]}\alpha^{m-2} + \cdots + f_1{}^{[0]}\alpha + f_0{}^{[0]} \quad (26)$$

식 (1)과 (26)을 비교하여 $f_{m-1}{}^{[0]}=f_{m-1}$, …, $f_1{}^{[0]}=f_1$, $f_0{}^{[0]}=f_0$ 임을 알 수 있다. 이후, 식 (25)의 i에 1부터 시작하여 정수를 재귀적으로 대입하면 임의의 정수 i에 대한 α^{m+i}로부터 α^{m+i+1}에 대한 mod $F(\alpha)$ 연산을 유도할 수 있다.

정리 3. 임의의 양의 정수 i에 대하여, α^{m+i}에 대한 다항식 표현이 식 (25)와 같을 때, α^{m+i+1} mod $F(\alpha)$ 연산 결과 유도한 다항식의 각 계수들은 식 (17)의 계수들로부터 유도할 수 있으며 식 (27)과 같다.

$$f_k{}^{[i+1]} = f_{k-1}{}^{[i]} \oplus f_{m-1}{}^{[i]} f_k \quad (1 \le k \le m-1)$$
$$= f_{m-1}{}^{[i]} f_0 \quad (k = 0) \quad (27)$$

식 (27)의 위 첨자 [i]에서 i=0인 [0]는 표현을 단순화하기 위해 생략하기로 한다.

증명. 정의 5에 의해 α^{m+i+1}에 대한 다항식 표현은 식 (28)과 같이 나타낼 수 있다.

$$\alpha^{m+i+1} = f_{m-1}{}^{[i+1]}\alpha^{m-1} + f_{m-2}{}^{[i+1]}\alpha^{m-2} + \cdots + f_1{}^{[i+1]}\alpha + f_0{}^{[i+1]} \quad (28)$$

한편, 식 (25)의 양변에 α를 승산하여 전개하면 식 (29)과 같다.

$$\begin{aligned}
&(\alpha^{m+i})\alpha \\
&= f_{m-1}{}^{[i]}\alpha^{m} + f_{m-2}{}^{[i]}\alpha^{m-1} + \cdots + f_1{}^{[i]}\alpha^2 + f_0{}^{[i]}\alpha \\
&= f_{m-1}{}^{[i]}(f_{m-1}{}^{[i]}\alpha^{m-1} + f_{m-2}{}^{[i]}\alpha^{m-2} + \cdots \\
&\quad \cdots + f_1{}^{[i]}\alpha + f_0{}^{[i]}) + f_{m-2}{}^{[i]}\alpha^{m-1} + f_{m-3}{}^{[i]}\alpha^{m-2} + \cdots \\
&\quad \cdots + f_1{}^{[i]}\alpha^2 + f_0{}^{[i]}\alpha \\
&= (f_{m-2}{}^{[i]} \oplus f_{m-1}{}^{[i]} f_{m-1}{}^{[i]})\alpha^{m-1} + \cdots \\
&\quad \cdots + (f_0{}^{[i]} \oplus f_{m-1}{}^{[i]} f_0{}^{[i]})\alpha + f_{m-1}{}^{[i]} f_0{}^{[i]}
\end{aligned} \quad (29)$$

식 (28)과 (29)은 모두 α^{m+i+1}에 대한 mod $F(\alpha)$연산의 결과로 동일한 식이다. 식 (29)에서 $0 \le k \le m-1$인 정수 k를 가정하여 k=0인 경우와 $1 \le k \le m-1$인 경우로 구분하여 요약하면 식 (27)과 같다.

증명 끝.

정리 4. 식 (23)의 $C(\alpha)$에 mod $F(\alpha)$ 연산 후 유도한 $P(\alpha)$의 각 계수들은 식 (30)과 같이 나타낼 수 있다.

$$p_i = c_i \oplus \sum_{k=0}^{m-2} c_{m+k} f_i^{[k]} \quad (30)$$

증명 정리 3으로 부터 m 이상의 차수를 갖는 모든 α에 대한 mod $F(\alpha)$ 연산 결과를 식 (23)에 대입하면 식 (31)과 같다.

$$\begin{aligned}
P(\alpha) &= C(\alpha) \bmod F(\alpha) \\
&= c_{2m-2}\alpha^{2m-2} + \cdots + c_m\alpha^m \\
&\quad + c_{m-1}\alpha^{m-1} + \cdots + c_1\alpha + c_0 \bmod F(\alpha)
\end{aligned}$$

$$
\begin{aligned}
&= c_{m-1}\alpha^{m-1} + \cdots + c_1\alpha + c_0 \\
&+ c_m[f_{m-1}\alpha^{m-1} + f_{m-2}\alpha^{m-2} + \cdots + f_1\alpha + f_0] \\
&+ c_{m+1}[f_{m-1}{}^{[1]}\alpha^{m-1} + f_{m-2}{}^{[1]}\alpha^{m-2} + \cdots + f_1{}^{[1]}\alpha + f_0{}^{[1]}] \\
&+ \cdots + c_{2m-2}[f_{m-1}{}^{[m-2]}\square^{m-1} + f_{m-2}{}^{[m-2]}\square^{m-2} \\
&+ \cdots + f_1{}^{[m-2]}\alpha + f_0{}^{[m-2]}] \\
= &[c_{m-1}\oplus c_m f_{m-1}\oplus c_{m+1}f_{m-1}{}^{[1]}\oplus\cdots\oplus c_{2m-2}f_{m-1}{}^{[m-2]}]\alpha^{m-1} \\
&+ [c_{m-2}\oplus c_m f_{m-2}\oplus c_{m+1}f_{m-2}{}^{[1]}\oplus\cdots\oplus c_{2m-2}f_{m-2}{}^{[m-2]}]\alpha^{m-2} \\
&+ \cdots + [c_1\oplus c_m f_1\oplus c_{m+1}f_1{}^{[1]}\oplus\cdots\oplus c_{2m-2}f_1{}^{[m-2]}]\alpha \\
&+ [c_0\oplus c_m f_0\oplus c_{m+1}f_0{}^{[1]}\oplus\cdots\oplus c_{2m-2}f_0{}^{[m-2]}] \qquad (31)
\end{aligned}
$$

식 (31)과 식 (24)을 비교하면 $P(\square)$의 각 계수들은 $C(\alpha)$의 계수들과 기약다항식 $F(\alpha)$로부터 식 (30)과 같이 표현된다.

증명 끝.

III. GF(2^m)상의 병렬 승산기 설계

3.1 GF(2^m)상의 병렬 승산기의 구성

본 장에서는 앞 장에서 논의한 다항식 분할 기법을 적용한 다항식의 승산 전개와 mod $F(\alpha)$ 연산을 기반으로 GF(2^m)의 두 원소 $A(\alpha)$와 $B(\alpha)$의 승산을 연산하는 승산기를 설계하였다. 먼저 본 논문에서 제안한 승산기의 구성을 그림 1에 보였다.

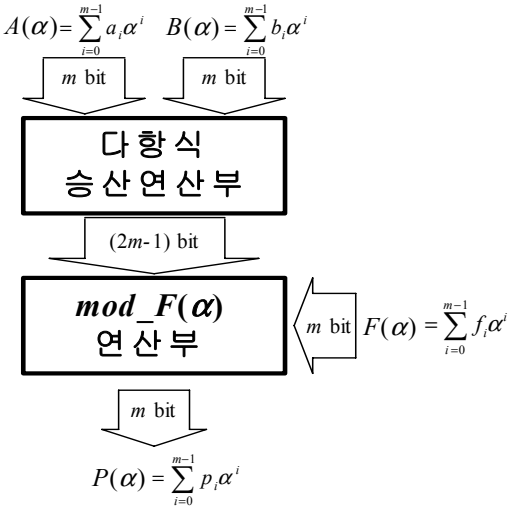


그림 1. GF(2^m)상의 병렬 승산기 구성도

Fig. 1. Block diagram of GF(2^m) parallel multiplier

그림 1에서 다항식 승산 연산부는 정의 2와 정리 1, 그리고 정의 4와 정리 2를 기반으로 설계할 수 있으며 두 m-1차 다항식의 승산을 위해 두 쌍의 m비트 입력과 승산 $C(\alpha)$의 결과로 $2m$-1비트의 출력을 갖는다. mod $F(\alpha)$ 연산부는 GF(2^m)상의 m에 의해 결정된 기약다항식 $F(\alpha)$의 계수들과 정리 4를 기반으로 다항식 승산 연산부의 출력을 입력으로 받아 $P(\alpha)$의 각 계수들을 연산한다. 각 연산부는 모두 모듈의 형식으로 설계됨으로써 m에 대한 확장과 VLSI에 유리하도록 하였다.

3.2 연산부별 회로구성

예제 1에서 m=2인 GF(2^2)상의 두 원소 $A(\alpha)$와 $B(\alpha)$의 승산을 식 (11)의 보조다항식들을 사용하여 식 (12)와 같이 전개하였다. 식 (11)의 $D_{ll[2]}(\alpha)$과 $D_{hh[2]}(\alpha)$는 각각 1개의 AND 게이트로 구현 가능하며, $D_{hl[2]}(\alpha)$은 2개의 XOR 게이트와 1개의 AND 게이트로 구현 가능하다. 식 (12)의 $C(\alpha)$에 대한 회로는 그림 2와 같다.

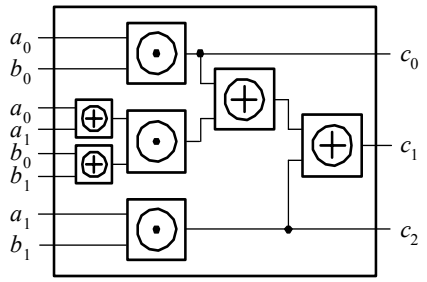


그림 2. 식 (12)의 $C(\alpha)$에 대한 회로 설계

Fig. 2. Circuit design of $C(\alpha)$ in Eq. (12)

또한, 예제 3의 식 (20)에서 전개한 GF(2^3)상의 $A(\alpha)$와 $B(\alpha)$의 승산 $C(\alpha)$에 대한 회로는 그림 3과 같다.

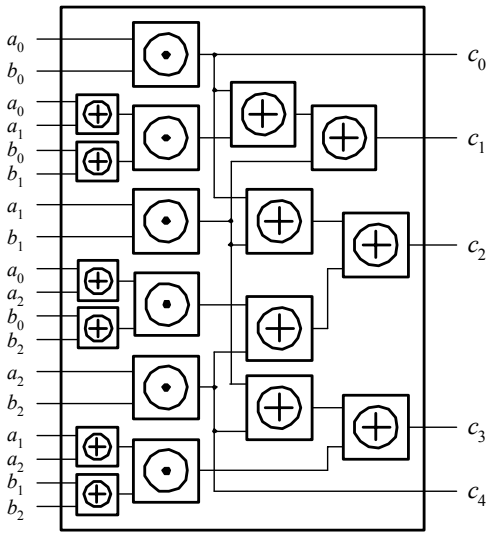


그림 3. 식 (20)의 $C(\alpha)$에 대한 회로 설계

Fig. 3. Circuit design of $C(\alpha)$ in Eq. (20)

본 논문에서는 AND와 XOR 게이트를 각각 ⊙와 ⊕로 기호화하였고, 2-입력 단자 게이트를 전제하였다. 예제 2와 예제 4에서 논의한 바와 같이 그림 2와 그림 3의 회로는 이후 확장된 회로의 기본 모듈로 사용된다.

정리 3을 기반으로 설계한 mod $F(\alpha)$ 연산부의 기본 모듈을 그림 4에 보였다.

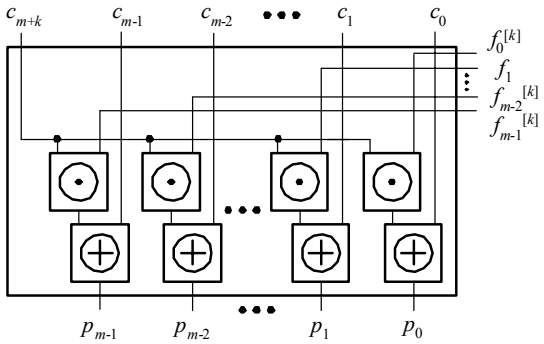


그림 4. mod $F(\alpha)$ 연산부의 기본 모듈

Fig. 4. Basic module of mod $F(\alpha)$ operation

3.3 GF(2^4)에 대한 승산기의 설계

그림 2와 4에서 보인 각 연산부의 모듈을 결합하여 $GF(2^m)$상의 병렬 승산회로를 구성할 수 있으며, GF(2^4)를 예로 보였다. GF(2^4)상의 $A(\alpha)=a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0$와 $B(\alpha)=b_3\alpha^3+b_2\alpha^2+b_1\alpha+b_0$의 승산 $C(\alpha)=A(\alpha)B(\alpha)$는 정리 1에 의해 식 (32)와 같이 유도된다.

$$C(\alpha) = D_{hh[2]}(\alpha)\alpha^4 + [D_{hh[2]}(\alpha) + D_{hl[2]}(\alpha) + D_{ll[2]}(\alpha)]\alpha^2 + D_{ll[2]}(\alpha) \quad (32)$$

식 (24)의 보조다항식 $D_{hh[2]}(\alpha)$, $D_{hl[2]}(\alpha)$, $D_{ll[2]}(\alpha)$의 연산은 예제 2에서 논의하였다. 식 (14)를 식 (32)에 대입하여 전개하면 식 (33)과 같이 6차의 다항식이 전개된다.

$$C(\alpha) = c_6\alpha^6 + c_5\alpha^5 + c_4\alpha^4 + c_3\alpha^3 + c_2\alpha^2 + c_1\alpha + c_0 \quad (33)$$

또한, GF(2^4)상의 기약다항식 $F(\alpha)=\alpha^4+\alpha+1$을 정리 3를 적용하여 α^4, α^5, α^6에 대한 mod $F(\alpha)$ 연산을 수행하면 식 (34)와 같다.

$$\begin{aligned}
\alpha^4 &= f_3^{[0]}\alpha^3 + f_2^{[0]}\alpha^2 + f_1^{[0]}\alpha + f_0^{[0]} \\
&\quad f_3^{[0]} = 0,\ f_2^{[0]} = 0,\ f_1^{[0]} = 1,\ f_0^{[0]} = 1. \\
\alpha^5 &= f_3^{[1]}\alpha^3 + f_2^{[1]}\alpha^2 + f_1^{[1]}\alpha + f_0^{[1]} \\
&\quad f_3^{[1]} = (f_2^{[0]} \oplus f_3^{[0]} f_3) = 0, \\
&\quad f_2^{[1]} = (f_1^{[0]} \oplus f_3^{[0]} f_2) = 1,\ f_1^{[1]} = (f_0^{[0]} \oplus f_3^{[0]} f_1) = 1, \\
&\quad f_0^{[1]} = f_3^{[0]} f_0 = 0. \\
\alpha^6 &= f_3^{[2]}\alpha^3 + f_2^{[2]}\alpha^2 + f_1^{[2]}\alpha + f_0^{[2]} \\
&\quad f_3^{[2]} = (f_2^{[1]} \oplus f_3^{[1]} f_3^{[1]}) = 1,\ f_2^{[2]} = (f_1^{[1]} \oplus f_3^{[1]} f_2^{[1]}) = 1, \\
&\quad f_1^{[2]} = (f_0^{[1]} \oplus f_3^{[1]} f_1^{[1]}) = 0,\ f_0^{[2]} = f_3^{[1]} f_0^{[1]} = 0.
\end{aligned} \quad (34)$$

식 (34)의 각 연산 결과들을 정리 4에 적용하여 $P(\alpha)$의 각 계수들을 구하면 식 (35)와 같다.

$$\begin{aligned}
p_3 &= c_3 \oplus c_4 f_3^{[0]} \oplus c_5 f_3^{[1]} \oplus c_6 f_3^{[2]} = c_3 \oplus c_6 \\
p_2 &= c_2 \oplus c_4 f_2^{[0]} \oplus c_5 f_2^{[1]} \oplus c_6 f_2^{[2]} = c_2 \oplus c_5 \oplus c_6 \\
p_1 &= c_1 \oplus c_4 f_1^{[0]} \oplus c_5 f_1^{[1]} \oplus c_6 f_1^{[2]} = c_1 \oplus c_4 \oplus c_5 \\
p_0 &= c_0 \oplus c_4 f_0^{[0]} \oplus c_5 f_0^{[1]} \oplus c_6 f_0^{[2]} = c_0 \oplus c_4
\end{aligned} \quad (35)$$

논의된 내용으로부터 GF(2^4)상의 승산기를 설계하면 그림 5와 같다.

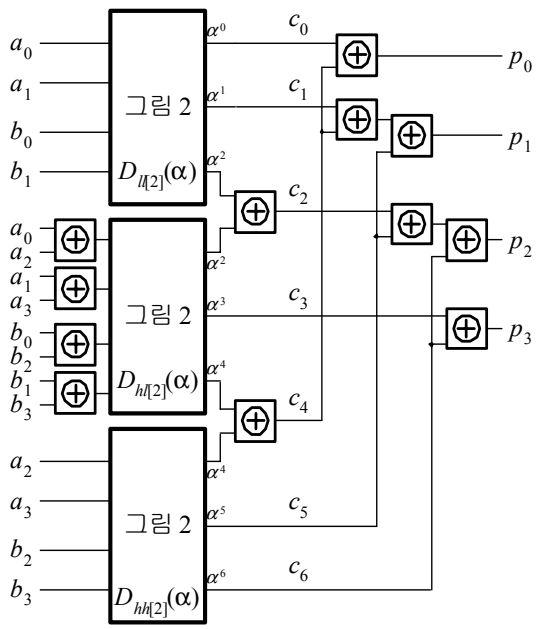


그림 5. KOA 기반의 GF(2^4) 승산기
Fig. 5. GF(2^4) multiplier based on KOA

그림 5에서 보조다항식 $D_{hh[2]}(\alpha)$, $D_{hl[2]}(\alpha)$, $D_{ll[2]}(\alpha)$의 연산회로는 모두 그림 2의 회로를 단위 연산블럭으로 하여 동일하게 적용된다.

3.4 GF(2^9)에 대한 승산기의 설계

그림 3와 4의 각 연산 모듈들로부터 $m=3^n$인 $GF(2^m)$상의 병렬 승산회로를 구성할 수 있으며, GF(2^9)를 설계의 예로 보였다. GF(2^9)상의 $A(\alpha)=a_8\alpha^8+\cdots+a_1\alpha+a_0$와 $B(\alpha)= b_8\alpha^8+\cdots+b_1\alpha+b_0$의 승산 $C(\alpha)=A(\alpha)B(\alpha)$는 정리 2에 의해 식 (36)과 같이 유도된다.

$$\begin{aligned} C(\alpha)=&D_{hh[3]}(\alpha)\alpha^{12}+[D_{hh[3]}(\alpha)+D_{hm[3]}(\alpha)+D_{mm[3]}(\alpha)]\alpha^9 \\ &+ [D_{hl[3]}(\alpha)+D_{hh[3]}(\alpha)+D_{mm[3]}(\alpha)+D_{ll[3]}(\alpha)]\alpha^6 \\ &+ [D_{ml[3]}(\alpha)+D_{mm[3]}(\alpha)+D_{ll[3]}(\alpha)]\alpha^3+D_{ll[3]}(\alpha) \end{aligned} \quad (36)$$

식 (36)의 보조다항식들은 예제 3의 식 (20)과 동일한 연산구조를 가지며 이를 전개하면 16차의 다항식이 전개되며, 식 (37)과 같다.

$$\begin{aligned} C(\alpha) = {} & c_{16}\alpha^{16} + \cdots + c_9\alpha^9 + c_8\alpha^8 + \cdots \\ & \cdots + c_1\alpha + c_0 \end{aligned} \quad (37)$$

유도된 식 (37)의 $C(\alpha)$에 GF(2^9)상의 기약다항식 $F(\alpha)= \alpha^9+\alpha+1$을 정리 3를 적용하여 α^9, …, α^{16}에 mod $F(\alpha)$ 연산을 수행한 후, 그 결과들을 정리 4에 적용하여 구한 $P(\alpha)$의 각 계수들은 식 (38)과 같다.

$$\begin{aligned} p_8 &= c_8\oplus c_{16}f_8^{[7]} = c_8\oplus c_{16} \\ p_7 &= c_7\oplus c_{15}f_7^{[6]}\oplus c_{16}f_7^{[7]} = c_7\oplus c_{15}\oplus c_{16} \\ p_6 &= c_6\oplus c_{14}f_6^{[5]}\oplus c_{15}f_6^{[6]} = c_6\oplus c_{14}\oplus c_{15} \\ p_5 &= c_5\oplus c_{13}f_5^{[4]}\oplus c_{14}f_5^{[5]} = c_5\oplus c_{13}\oplus c_{14} \\ p_4 &= c_4\oplus c_{12}f_4^{[3]}\oplus c_{13}f_4^{[4]} = c_4\oplus c_{12}\oplus c_{13} \\ p_3 &= c_3\oplus c_{11}f_3^{[2]}\oplus c_{12}f_3^{[3]} = c_3\oplus c_{11}\oplus c_{12} \\ p_2 &= c_2\oplus c_{10}f_3^{[1]}\oplus c_{11}f_3^{[2]} = c_2\oplus c_{10}\oplus c_{11} \\ p_1 &= c_1\oplus c_9f_2^{[0]}\oplus c_{10}f_3^{[1]} = c_1\oplus c_9\oplus c_{10} \\ p_0 &= c_0\oplus c_8f_0^{[0]} = c_0\oplus c_8 \end{aligned} \quad (38)$$

논의된 내용으로부터 GF(2^9)상의 승산기를 설계하면 그림 6과 같다.

그림 6에서 각 보조다항식 $D_{hh[3]}(\alpha)$, $D_{mm[3]}(\alpha)$, $D_{ll[3]}(\alpha)$, $D_{hm[3]}(\alpha)$, $D_{hl[3]}(\alpha)$, $D_{ml[3]}(\alpha)$들의 연산 회로는 모두 그림 3의 회로가 동일하게 적용된다.

IV. 비교 및 검토

본 논문에서 제시한 다항식 승산기법 및 Parr의 기법은 모두 KOA를 기반으로 전개됨으로 보조다항식의 정의와 승산식 $C(\alpha)$의 전개가 유사하다. 그러나, Parr는 유한체의 범위를 GF($(2)^4)^n$)으로 하였고, GF(2^4)를 기본 연산모듈로 정의하여 n의 증가에 따라 n^2개의 기본 연산모듈을 확장하도록 하였다. 그리고, 모듈러 연산을 위해 Masrtovito[13]가 제안한 연산기법을 적용하였다. 이에 비하여 본 논문에서는 주어진 GF(2^m)상의 m의 조건을 2^n, 또는 3^n으로 구분하여 각각 2항식과 3항식으로 구성하였고, 그 보조다항식을 통해 승산 전개를 제시하였다. 또한, 모듈러 연산을 위해 α^m mod $F(\alpha)$로부터 임의의 양 수 i에 대한 α^{m+i} mod $F(\alpha)$의

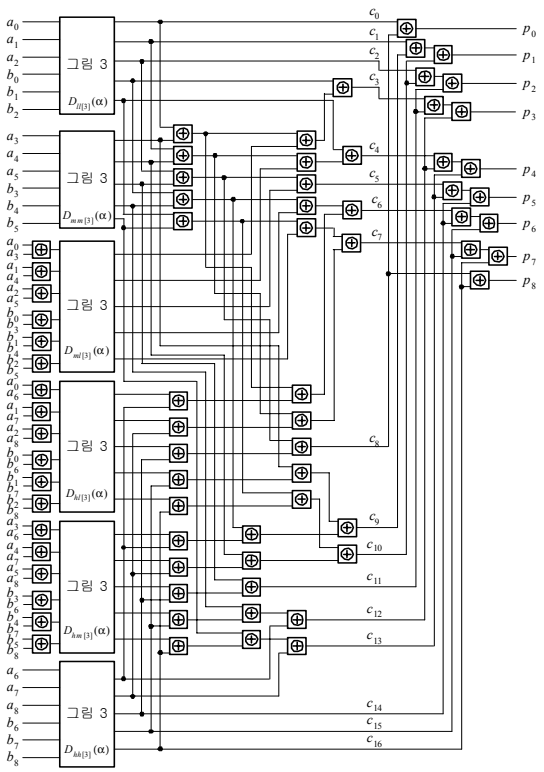


그림 6. KOA 기반의 GF(2^9) 승산기
Fig. 6. GF(2^9) multiplier based on KOA

연산식을 제시하였다. Parr의 GF($(2)^4)^n$)와 본 논문에서 제시한 GF(2^m)상의 승산회로의 구성을 비교하여 표 1에 보였다.

표 1. 승산 회로 구성의 비교
Table 1. Comparisons of the related parallel multiplier over GF(2^4)

적용체	Parr[11] GF($(2)^4)^n$)				본 논문 GF(2^m), $m=2^n$			
	AND	XOR	D_{AND}	D_{XOR}	AND	XOR	D_{AND}	D_{XOR}
GF(2^2)	·	·	·	·	3	6	1	4
GF(2^3)	·	·	·	·	6	18	1	5
GF(2^4)	12	18	1	4	9	24	1	7
GF(2^8)	48	62	1	5	27	91	1	10
GF(2^9)	·	·	·	·	36	150	1	9

비교 결과 GF(2^m)상의 $m=2^n$의 경우 본 논문과 Parr의 회로에서 적용한 AND와 XOR의 총 게이트 수는 근사한 결과를 가지나, Parr는 $m=3^n$에 대한 회로구성 기법을 제시하지 못하였다.

VI. 결론

본 논문에서는 KOA를 적용하여 $m=2^n$과 $m=3^n$일 때의 GF(2^m)상의 승산 연산기법과 그 구현회로를 제안하였다.

$m=2^n$과 $m=3^n$인 경우에 대하여 각각의 보조다항식을 정의한 후 각각의 승산식을 전개하였다. 또한 승산의 결과를 GF(2^m)상의 원소로 표현하기 위해 mod $F(\alpha)$ 연산을 새롭게 전개하였다. 제시된 연산기법을 적용하여 다항식 승산연산부와 mod $F(\alpha)$ 연산부를 각각 설계한 후 이들을 결합하여 전체 회로를 구성하였다.

설계된 회로의 구성을 Parr의 회로와 비교하였고, 그 결과를 표에 정리하였다. 비교결과 $m=2^n$의 경우 본 논문과 Parr의 회로는 비슷한 수의 소자를 가지나, $m=3^n$의 경우 Parr는 연산기법 및 구현회로를 제시하지 못하였다. 따라서, 본 논문에서 제시된 회로는 Parr에 비해 보다 연산영역을 확장하였다 할 수 있다. 또한, 모듈러 환원을 위한 연산식을 일반식으로 제시함에 따라 다양한 유한체 연산으로의 적용이 기대된다.

참고문헌

[1] S. Lin, *Error Control Coding*, Prentice-Hall, Inc. New Jersey, 1983.
[2] 이만영, *BCH부호와 Reed-Solomon부호,* 민음사, 1990.
[3] I.S. Hsu, T.K. Troung, L.J. Deutsch, and I.S. Reed, "A Comparison of VLSI Architecture of Field Multipliers Using Dual, Normal, or Standard Bases," *IEEE Trans. Computers*, vol. 37, no. 6, pp. 735-739, June 1988.
[4] B.A. Laws and C.K. Rushford, "A Cellular-Array Multiplier for GF(2^m)" *IEEE Trans. Computers*, vol. C-20, no. 12, pp. 1573-1578, Dec. 1971.
[5] C.S. Yeh, I.S. Reed, and T.K. Trung, "Systolic Multipliers for Finite Field GF(2^m)," *IEEE Trans. Computers*, vol. C-33, pp. 357-360, April 1984.

[6] H.T. Kung, "Why ssystolic architecture?" *IEEE Computer*, vol. 15, pp. 37-46, Jan. 1982.

[7] J.Omura and J.Massey, "Computational Method and Apparatus for Finite Fields," *U.S. Patent* no. 4,587,627, May 1986.

[8] C.C.Wang, T.K.Trung, H.M.Shao, L.J.Deutsch, J.K. Omura, and I.S.Reed, "VLSI Architecture for Computing Multiplications and Inverses in GF(2^m)," *IEEE Trans. Computers*, vol. C-34, pp. 709-717, Aug. 1985.

[9] E.R. Berlekamp, "Bit-Serial Reed-Solomon Encoders," *IEEE Trans. on Information Theory,* vol. IT-28, no. 6, pp. 869-874, Nov. 1982.

[10] A. Karatsuba and Y. Ofman, "Multiplication of Multidigit Numbers on Automata," *Sov. Phys.-Dokl. (Engl. transl.)*, vol. 7, no. 7, pp. 595-596, 1963.

[11] C. Parr, "A New Architecture for a Parallel Finite Field Multiplier with Low Complexity Based on Composite Fields," *IEEE Trans. Computers*, vol. 45, no. 7, pp. 856-861, July 1996.

[12] C. Parr, P. Fleischmann, and P. Roelse, "Efficient Multiplier Architectures for Galois Fields GF(2^{4n})," *IEEE Trans. Computers*, vol. 47, no. 2, pp. 162-170, Feb. 1998.

[13] E.D. Mastrovito, "VLSI Architectures for Multiplication in Galois Fields," Ph.D. thesis, Linkoping Univ., Dept. of Electrical Eng., Linkoping, Sweden, 1991.

[14] B. Sunar, C.K. Koc, "Mastrovito Multiplier for all trinomials," *IEEE Trans. Computers*, vol. 48, no. 5, pp. 522-527, May 1999.

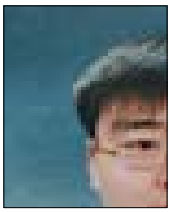
저 자 소 개

卞 基 寧 (正會員)

1994년 2월 : 인하대학교 전자공학과 졸업(공학사)
1996년 8월 : 동 대학원 전자공학과 졸업 (공학석사)
2003년 2월 : 동 대학원 전자공학과 졸업 (공학박사)
1994년 1월 ~ 1996년 8월 : (주) LG 전자 VCR사업부 회로설계연구원
2003년 ~ 현재 : 가톨릭대학교 정보통신전자공학부 강의전담교수.

<주관심분야> 정보 및 부호이론, 논리 시스템 설계, 유한체 이론의 응용 및 VLSI 구현, SoC(VHDL) 및 Embedded H/W 구현 등.

羅 基 秀 (正會員)



1997년 2월 : 건양대학교 컴퓨터공학과 졸업 (공학사)
1999년 2월 : 인하대학교 대학원 전자공학과 졸업 (공학석사)
1999년 3월 ~ 현재 : 동 대학원 전자공학과 박사과정

<주관심 분야> 디지털 로직, 오류정정부호 설계, 퍼지회로 설계

金 興 壽 (正會員)

한국전기전자학회 논문지 제7권 제2호 참조
현재 : 인하대학교 전자공학과 교수
<주관심분야> 회로 및 시스템, 스위칭이론, 논리회로설계, 퍼지논리, 다치논리 등