시스템 복잡도 개선을 위한 AOP 기반의 병렬 유한체 승산기

정회원 변 기 영*, 나 기 수**, 윤 병 희**, 최 영 희**, 한 성 일**, 김 흥 수**

Low System Complexity Parallel Multiplier for a Class of Finite Fields based on AOP

Gi-Young Byun*, Gi-Su Na**, Byung-Hee Yoon**, Young-Hee Choi**,

Sung-Il Han**, Heung-Soo Kim** *Regular Members*

요 약

본 논문에서는 보다 빠른 연산동작의 구현을 위해 시스템 복잡도를 개선한 새로운 GF(2^m) 승산기를 제안한다. m차 기약 AOP가 갖는 특성으로부터 승산 중 발생하는 모듈러 환원의 과정을 순환이동특성으로 간략화 하였고, 이후 AND와 XOR 게이트들의 배열구조를 사용하여 승산을 이루도록 하였다. 본 논문에서 제안한 승산기는 $m(m+1)$개의 2-입력 AND게이트와 $(m+1)^2$개의 2-입력 XOR게이트만으로 구성되며 연산에 소요되는 지연시간은 $T_A+\lceil \log_2 m \rceil T_X$이다. 제안된 승산기와 타 승산기를 비교하여 그 결과를 보였고, 비교 결과 회로구성 및 복잡도 개선에 우수한 특성을 가지며 VLSI 구현에 적합함을 확인하였다.

ABSTRACT

This study focuses on the hardware implementation of fast and low-system-complexity multiplier over GF(2^m). From the properties of an irreducible AOP of degree m, the modular reduction in GF(2^m) multiplicative operation can be simplified using cyclic shift operation. And then, GF(2^m) multiplicative operation can be established using the array structure of AND and XOR gates. The proposed multiplier is composed of $m(m+1)$ 2-input AND gates and $(m+1)^2$ 2-input XOR gates. And the minimum critical path delay is $T_A+\lceil \log_2 m \rceil T_X$. Proposed multiplier obtained have low circuit complexity and delay time, and the interconnections of the circuit are regular, well-suited for VLSI realization.

I. 서 론.

유한체(Finite Field)는 Galois체, 또는 간단히 GF라 하며, 오류정정부호, 스위칭이론, 컴퓨터 구조 및 암호화 등의 분야에 적용되고 있는 연산체계이다[1,2]. 유한체를 구성하는 원소들은 표준, 정규, 쌍대기저 등에 의해 각 형식에 따른 다항식 또는 벡터형식으로 표현되며, 각 기저의 특성에 따라 연산별 효율성과 그 회로구현의 용이성이 달라진다[3]. 일반적으로 표준기저의 경우 타 기저에 비하여 기약다항식의 선택이 자유롭고, 최적화된 하드웨어의 구현이 용이한 장점이 있다[3]. 표준기저를 적용한 유한체 연산 중 승산은 제산, 승산에 대한 역원, 멱승(exponentiation) 등 가산을 제외한 여타 연산의 기반이 되는 연산이다. 따라서, 고속 및 대용량의 연산시스템을 개발하기 위해 구성소자의 수에 따른 회로복잡도와 연산지연시간으로 일컬어지는 시스템 복잡도를 개선할 수 있는 효율적인 승산기법의 개발 및 최적화된 승산회로의 구현은 오랫동안 관심의 대상이 되어왔다.

* 가톨릭대학교 정보통신전자공학부(gybyun@catholic.ac.kr), ** 인하대학교 전자공학과 회로및시스템연구실(hskim@inha.ac.kr),
논문번호 : 030305-0722, 접수일자 : 2003년 7월 18일

본 논문에서는 표준기저를 적용한 유한체 승산기법 및 그 회로구현에 대하여 논의하고자 한다. 이에 관련한 연구동향을 간략히 살펴보면, 1971년 Law[4]가 셀-배열형 승산기를 제안한 이후, 1984년 Yeh[5]는 대용량의 신호 처리를 위한 시스토릭 승산기를 제안하였고, 이후 많은 승산기법 및 그 구현회로들이 제시되었다. 1989년 Itoh와 Tsujii[6]는 기약 AOP를 적용하여 시스템의 복잡도를 개선한 GF(2^m)상의 병렬 승산기를 제안하였다. 이 후 Hasan[7], Lee[8]등이 이 분야에 중요한 진전을 이루었다.

이러한 연구동향을 배경으로 본 논문에서는 기약 AOP의 성질을 이용하여 순환이동(Cyclic Shift, CS)에 의한 모듈러 환원의 구현 및 AND와 XOR의 배열구조를 갖는 병렬 유한체 승산회로를 새롭게 제안하였다. 본 논문에서 제안한 회로는 $(m+1)^2$개의 2-입력 AND 게이트, $m(m+1)$개의 2-입력 XOR 게이트로 구성되며, 메모리나 스위치 같은 별도의 소자를 필요로 하지 않는다. 또한 입력된 신호로부터 최종출력에 이르기까지 소요되는 연산지연시간은 $T_A+\lceil \log_2 m \rceil T_X$이다. 4장에서 기존의 연구들과의 비교를 논의하겠지만, 본 논문에서 제안한 회로는 회로의 정규성을 가지면서 기존의 연구에 비해 시스템의 복잡도를 보다 개선하였다. 또한, 모듈화된 AND와 XOR 게이트의 배열구조를 가지면서 각 게이트들의 배선구조가 동일성과 규칙성을 유지하므로 VLSI에 매우 유리하다.

본 논문의 구성을 간략히 소개하면 1장의 서론에 이어, 2장에서는 간략한 유한체의 성질에 대한 논의와 함께 본 논문에서 새롭게 제안한 GF(2^m)상의 승산전개 기법을 보였다. 2장의 논의를 바탕으로 3장에서는 기약 AOP를 기반으로 새로운 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 승산전개

2.1 유한체상의 원소표현[1,2]과 기약 AOP[6-8]

유한체 GF(2^m)은 양의 정수 m에 대하여 2^m개의 원소들로 구성된 수 체계이며, 그 원소들간의 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 이루어진다. 0을 제외한 GF(2^m)상의 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 근이다. 따라서, $F(\alpha)=0$이 되며, $\alpha^m=f_{m-1}\alpha^{m-1}+f_{m-2}\alpha^{m-2}+\cdots+f_1\alpha+f_0$이 성립한다. 이에 따라 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 (1)과 같이 표현된다. 식 (1)에서 각 기저들의 계수들, $a_0, a_1, \cdots, a_{m-1}$은 모두 GF(2)상의 원소이다.

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

식 (1)에서 보인 $A(\alpha)$의 각 계수들에 대하여 $A_i=a_i \oplus 1$, $0 \le i \le m-1$,를 정의하면 $A(\alpha)$는 식 (2)와 같이 표현될 수 있다.

$$A(\alpha) = A_0 + A_1\alpha + \cdots + A_{m-1}\alpha^{m-1} + A_m\alpha^m \quad (2)$$

식 (2)에서 사용된 기저들, $\{\alpha^m, \alpha^{m-1}, \cdots, \alpha, 1\}$을 식 (1)에서 사용된 표준기저의 확장기저라 하며, $A_m=1$이다. 확장기저로부터 GF(2^m)상의 승산에 필요한 유용한 특성을 도출할 수 있으며, 이를 정의 1에 나타내었다.

정의 1[8]. GF(2^m)상의 임의의 원소 $A(\alpha)$를 확장기저를 적용하여 식 (2)와 같이 표현할 때, 각 기저의 계수들에 대한 순환이동을 식 (3)와 같이 정의한다.

$$A^{(1)}(\alpha) = A_m + A_0\alpha + \cdots + A_{m-2}\alpha^{m-1} + A_{m-1}\alpha^m \quad (3)$$

이러한 순환이동을 $i(i=0, 1, 2, \cdots, m)$번, 실행하면 식 (2)의 각 계수들은 우측 방향으로 i번 순환이동되며, 이를 $A^{(i)}(\alpha)$로 표현하기로 한다.

한편, 다항식의 모든 계수가 1인 다항식을 AOP(All One Polynomial)라 하며, 그 중 $m+1$이 소수가 되는 GF(2^m)상의 기약다항식들을 기약 AOP라 한다. 이에 해당하는 m은 2, 4, 10, 12, 18, 28, 36, 52, 58, 60, 66, 82, 100, …등이다[8]. 기약 AOP의 성질로부터 GF(2^m)상의 모듈러 환원에 필요한 유용한 성질을 유도할 수 있으며, 식 (4)와 같다.

$$\alpha^m = \alpha^{m-1} + \alpha^{m-2} + \cdots + \alpha + 1 \quad (4\text{-a})$$

$$\alpha^{m+i} = \alpha^{i-1} \quad (4\text{-b})$$

식 (4)로부터 확장기저로 표현된 $A(\alpha)$에 α의 멱승에 대한 일반식을 유도할 수 있으며, 이를 정리 1에 정리하였다.

정리 1. 확장기저로 표현된 $A(\alpha)$에 α의 멱승을 승산한 결과를 일반식으로 표현하면 식 (5)와 같다.

$$\begin{aligned}(\alpha^i)A(\alpha) &= A_{<m-i+1>} + A_{<m-i+2>}\alpha + \cdots + A_{<m-i>}\alpha^m \\ &= \sum_{j=0}^{m} A_{<j-i>}\alpha^j \ , \ i=0, 1, \cdots, m \\ &= A^{(i)}(\alpha) \end{aligned} \quad (5)$$

식 (5)에서 $A_{<\theta>}$의 아래첨자 $<\theta>$는 $m+1$에 대한 모듈러 연산의 결과로 $0\le<\theta>\le m$인 양의 정수이다. 또한, 기호의 표현에 있어 $A^{(0)}(\alpha)=A(\alpha)$이다.

(증명) 정리 1의 증명을 위해 식 (2)와 같이 확장기저로 표현된 $GF(2^m)$상의 원소 $A(\alpha)$에 α를 승산한 결과는 식 (6)과 같다.

$$\begin{aligned}\alpha A(\alpha) &= A_0\alpha + A_1\alpha^2 + \cdots + A_{m-1}\alpha^m + A_m\alpha^{m+1} \\ &= A_m + A_0\alpha + A_1\alpha^2 + \cdots + A_{m-1}\alpha^m \end{aligned} \quad (6)$$

기약 AOP에 의한 모듈러 환원을 적용하면, 식 (4-b)에서 보인 바와 같이 $\alpha^{m+1}=\alpha^0=1$이 되며, $\alpha A(\alpha)=A^{(1)}(\alpha)$이 된다. 이와 동일하게 $A(\alpha)에 \alpha^i$을 승산한 후 이를 정리하면, 결국 $A(\alpha)$의 각 계수들이 순환이동되며 그 결과를 정리하면 식 (5)와 같다. 증명 끝.

2.2 AOP 기반의 $GF(2^m)$ 상의 승산 전개

표준기저로 표현된 유한체 원소들의 승산은 다항식의 승산과 그 결과에 기약다항식을 적용한 모듈러 환원의 두 연산 과정을 거치게 된다. 본 논문에서는 $GF(2^m)$상의 원소들을 식 (2)와 같이 확장기저로 표현한 후, 기약 AOP를 적용하여 새롭고 효율적인 승산 전개 기법을 논의하고자 한다.

본 논문에서 확장기저와 기약 AOP를 적용하여 새롭게 제안한 $GF(2^m)$상의 승산전개기법은 식 (7)과 같다.

$$\begin{aligned}P(\alpha) &= A(\alpha)B(\alpha) \\ &= \left(\sum_{l=0}^{m} A_l\alpha^l\right)\left(\sum_{k=0}^{m} B_k\alpha^k\right) \\ &= \sum_{k=0}^{m} B_k\left(\sum_{l=0}^{m} A_l\alpha^l\right)\alpha^k \\ &= \sum_{k=0}^{m} B_k\left(\sum_{j=0}^{m} A_{<j-k>}\alpha^j\right) \end{aligned} \quad (7)$$

식 (7)을 전개하여 유도한 $P(\alpha)$의 각 계수들, P_0, P_1, …, P_m의 일반식을 정리하면 식 (8)과 같다.

$$P_k = \sum_{n=0}^{m} B_n A_{<k-n>} \quad (8)$$

식 (9)에서 k는 $0\le k\le m$의 범위를 갖는 정수이다.

예제 1. $GF(2^4)$상의 두 원소 $A(\alpha)$와 $B(\alpha)$를 정의 1의 확장기저로 표현하여 $A(\alpha)=A_0+A_1\alpha+A_2\alpha^2+A_3\alpha^3+A_4\alpha^4$와 $B(\alpha)=B_0+B_1\alpha+B_2\alpha^2+B_3\alpha^3+B_4\alpha^4$로 나타내었다. 이 때, $A(\alpha)$와 $B(\alpha)$의 승산결과 $P(\alpha)$, $P(\alpha)=P_0+P_1\alpha+P_2\alpha^2+P_3\alpha^3+P_4\alpha^4$를 식 (7)에 적용하여 전개하면 식 (9)와 같다.

$$\begin{aligned}P(\alpha) &= \sum_{k=0}^{4} B_k\left(\sum_{j=0}^{4} A_{<j-k>}\alpha^j\right) \\ &= B_0(A_{<0-0>}+A_{<1-0>}\alpha+A_{<2-0>}\alpha^2+A_{<3-0>}\alpha^3+A_{<4-0>}\alpha^4) \\ &+ B_1(A_{<0-1>}+A_{<1-1>}\alpha+A_{<2-1>}\alpha^2+A_{<3-1>}\alpha^3+A_{<4-1>}\alpha^4) \\ &+ B_2(A_{<0-2>}+A_{<1-2>}\alpha+A_{<2-2>}\alpha^2+A_{<3-2>}\alpha^3+A_{<4-2>}\alpha^4) \\ &+ B_3(A_{<0-3>}+A_{<1-3>}\alpha+A_{<2-3>}\alpha^2+A_{<3-3>}\alpha^3+A_{<4-3>}\alpha^4) \\ &+ B_4(A_{<0-4>}+A_{<1-4>}\alpha+A_{<2-4>}\alpha^2+A_{<3-4>}\alpha^3+A_{<4-4>}\alpha^4) \\ &= B_0(A_0 + A_1\alpha + A_2\alpha^2 + A_3\alpha^3 + A_4\alpha^4) \\ &+ B_1(A_4 + A_0\alpha + A_1\alpha^2 + A_2\alpha^3 + A_3\alpha^4) \\ &+ B_2(A_3 + A_4\alpha + A_0\alpha^2 + A_1\alpha^3 + A_2\alpha^4) \\ &+ B_3(A_2 + A_3\alpha + A_4\alpha^2 + A_0\alpha^3 + A_1\alpha^4) \\ &+ B_4(A_1 + A_2\alpha + A_3\alpha^2 + A_4\alpha^3 + A_0\alpha^4) \end{aligned} \quad (9)$$

식 (9)의 결과에 대하여 식 (8)을 적용하여 $P(\alpha)$의 각 기저들에 대하여 표현하면 식 (10)과 같다.

$$\begin{aligned}P_0 &= B_0A_0 + B_1A_4 + B_2A_3 + B_3A_2 + B_4A_1 \\ P_1 &= B_0A_1 + B_1A_0 + B_2A_4 + B_3A_3 + B_4A_2 \\ P_2 &= B_0A_2 + B_1A_1 + B_2A_0 + B_3A_4 + B_4A_3 \\ P_3 &= B_0A_3 + B_1A_2 + B_2A_1 + B_3A_0 + B_4A_4 \\ P_4 &= B_0A_4 + B_1A_3 + B_2A_2 + B_3A_1 + B_4A_0 \end{aligned} \quad (10)$$

Ⅲ. AOP 기반의 GF(2^m) 병렬 승산기

2장에서 논의한 바와 같이, 본 논문에서는 AOP를 기반으로 하여 확장기저로 표현된 GF(2^m)상의 두 원소 $A(\alpha)$와 $B(\alpha)$의 승산을 피 승산항의 순환이동과 승산항 의 각 계수를 순차적이고 반복적으로 승산한 후 동일 차수의 계수들을 모듈러 가산함으로써 이루었다. 이러한 승산전개의 회로구현을 위해 피 승산항의 계수들에 대한 순환이동(Cyslic Shift, CS) 연산모듈과 그 결과에 승산항의 각 계수들을 승산하는 부분곱(Partial Product, PP) 연산모듈, 그리고 동일한 차수의 계수들을 모듈러 가산하는 모듈러 가산(Modular Summation, MS) 연산모듈들이 각각 필요하며, 이를 그림 1에 도시하였다.

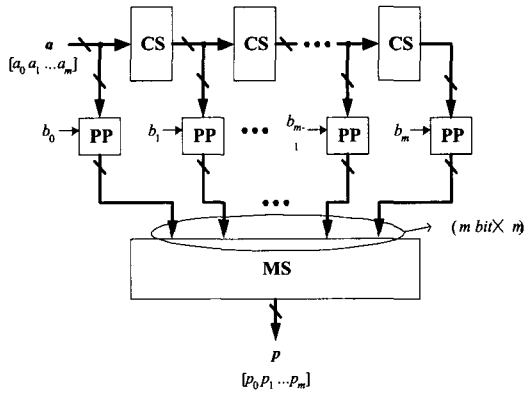


그림 1. 제안된 GF(2^m) 병렬 승산기의 구성도
Fig. 1. Architecture of proposed GF(2^m) parallel multiplier

그림 1에서 굵은선 화살표는 m비트 병렬 신호흐름을 나타낸다. 예제 1에서 논의한 GF(2^4)상의 두 원소들에 대한 승산회로를 구현하기 위해 필요한 CS, PP, MS 연산모듈을 각각 그림 2에 보였다. 그림 2 (a) CS 연산모듈은 게이트를 사용하지 않고 결선에 의해서만 이루어지므로 연산에 필요한 게이트 및 지연시간은 없다. (b) PP 연산모듈은 승산항의 계수 B_k와 피 승산항들의 계수들, A_0, $\cdots A_m$,이 부분곱을 이루는 연산모듈로 2-입력 AND 게이트를 m개 배열함으로써 구현될 수 있다. 본 논문에서는 AND 게이트를 ⊙로 기호화하였다.

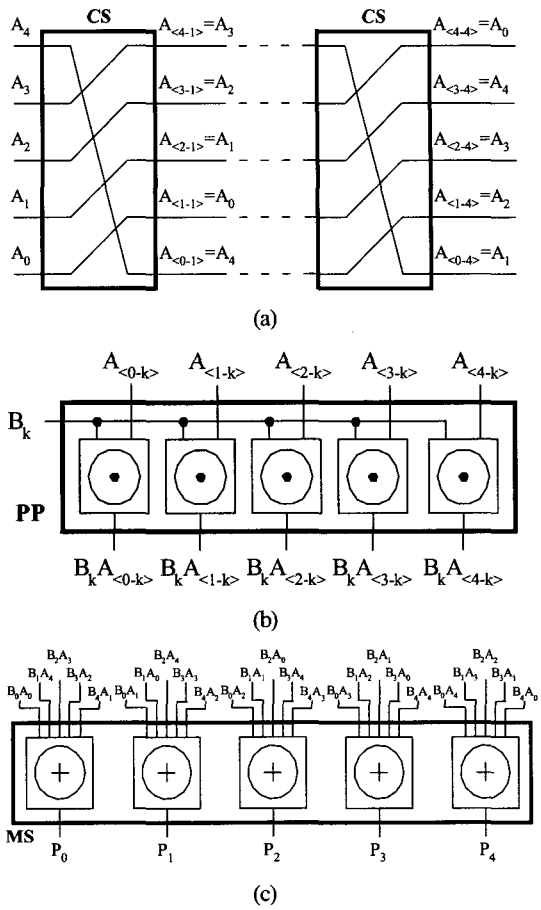


그림 2. 각 연산 모듈, (a) CS, (b) PP, (c) MS
Fig. 2. Each operational module, (a) CS, (b) PP, (c) MS

PP 연산모듈의 시스템 복잡도는 $(m+1)$개의 2-입력 AND 게이트와 2-입력 AND 게이트를 통과하면서 발생하는 지연시간을 T_A라 할 때, T_A이다. (c) MS 연산모듈은 각 PP 연산모듈로부터 연산된 부분 곱의 결과들로부터 동일 차수의 계수들에 대한 모듈러 가산을 이루는 블록으로 XOR 게이트들을 배열함으로써 구현될 수 있다. 본 논문에서는 XOR 게이트 ⊕로 기호화하였고, 간략화된 그림을 위해 GF(2^4)의 경우 5-입력 XOR로 표현하였다. 타 승산기와의 비교를 위해 2-입력 XOR로 구현하면, $m(m+1)$개의 게이트가 필요하며 이 게이트들로부터 발생하는 최소 지연시간은 $\lceil \log_2 m \rceil T_X$이다. 이를 종합하여 본 논문에서 제안한 GF(2^m)상의 병렬 승산 회로는 $(m+1)^2$개의 2-입력 AND 게이트와 $m(m+1)$개의 2-입력 XOR가 사용되며, 입력된 신호로부터 연산과정을 거쳐 최종 연산된 신호가 출력되기까지의 지연시간은 $T_A+\lceil \log_2 m \rceil T_X$ 이다.

Ⅳ. 비교 및 검토

본 논문과 동일하게 AOP를 기반으로 한 타 승산기와 회로소자의 수와 지연시간을 비교하여 표 1에 정리하였다.

표 1. AOP 기반의 병렬 GF(2^m) 승산기의 구성 비교
Table 1. Comparison of AOP-Based Parallel GF(2^m) Multipliers

multiplier	No. of XOR gates	No. of AND gates	Delay time
Itoh-Tsujii[6]	m^2+2m	m^2+2m+1	$T_A+\lceil \log_2 m+\log_2(m+2)\rceil T_X$
Hasan[7]	m^2+2m-2	m^2	$T_A+\lceil m+\log_2(m-1)\rceil T_X$
Lee I[8]	m^2+2m+1	m^2+2m+1	$T_A+T_X+T_L$
Lee II[8]	m^2+3m+2	m^2+2m-2	T_X+T_L
This paper	m^2+m	m^2+2m+1	$T_A+\lceil \log_2 m \rceil T_X$

표 1에서 보인바와 같이 본 논문에서 제안한 승산기는 XOR의 경우 가장 적은 소자를 가지며, AND의 경우 Hasan의 회로를 제외하면 타 승산기와 동일하다. 또한, Lee의 경우 회로구성에 있어 별도의 메모리소자(래치)가 필요함을 고려하면 본 논문에서 제안한 승산회로가 보다 비교우위에 있다 할 수 있다. 또한 지연시간의 경우 Itoh-Tsujii 및 Hasan의 회로에 비해 우월하며, 메모리 소자를 제어하기 위한 별도의 콘트롤 신호를 필요로 하지 않는 장점을 갖는다. 실용 GF(2^m) 연산회로에서 매우 큰 m이 적용됨을 고려할 때, 본 논문에서 개선한 시스템의 복잡도는 더욱 우수한 특성을 갖는다.

Ⅴ. 결 론

본 논문에서는 규칙적인 모듈 구조를 갖는 새로운 GF(2^m) 병렬 승산기를 제안하였다. AOP를 기반으로 유한체의 원소를 확장기저로 표현하였고, 순환이동 특성을 이용한 새로운 다항식 승산전개 기법을 보였다. 제안된 승산전개 기법으로부터 CS, PP, MS 연산모듈들을 정의하였고, 이들로부터 GF(2^m) 병렬 승산기를 설계할 수 있음을 GF(2^4)의 예로 보였다. 본 논문에서 제안한 승산기를 회로의 구성소자 수와 지연시간 등으로 타 승산기와 비교하였고, 그 결과 보다 유용함을 확인하였다. 또한, AND 또는 XOR로만 구성된 배열구조와 각 게이트들을 연결하는 동일한 배선구조, 그리고 m의 증가에 따른 각 연산모듈의 규칙적인 증가가 갖는 정규성은 VLSI 회로구현에 매우 유리하다 할 수 있다.

참 고 문 헌

[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.Troun, L.J.Deutsch, and I.S.Reed, "A Comparison of VLSI Architecture of Multipliers using Dual, Normal, or Standard Bases," *IEEE Trans. Computers*, vol. C-37, pp. 735-739, 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] T.Itoh, and S.Tsujii, "Structure of Parallel Multipliers for a Class of Fields GF(2^m)," *Information and Computation*, vol. 83, pp. 21-40, 1989.

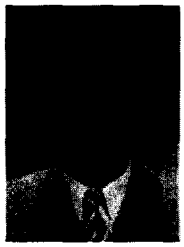
[7] M.A. Hasan, M.Z. Wang, and V.K. Bhargava, "Modular Construction of Low Complexity Parallel Multipliers for a Class of Finite Fileds GF(2^m)," *IEEE Trans. Computers*, vol. 41, no. 8, pp. 962-971, Aug. 1992.

[8] C.Y.Lee, E.H.Lu, and J.Y.Lee, "Bit-Parallel Systolic Multipliers for GF(2^m) Fields Defined by All-One and Equally Spaced Polynomials," *IEEE Trans. Computers*, vol. 50, No.5, pp.385-393, May 2001.

변 기 영(Gi-Young Byun) 정회원

1994년 2월 : 인하대학교 전자공학과 (공학사)
1998년 8월 : 인하대학교 대학원 전자공학과 (공학석사)
2003년 2월 : 인하대학교 대학원 전자공학과 (공학박사)
1994년 1월 ~ 1996년 8월 : (주)LG전자 VCR사업부 회로설계연구원
2003년 3월 ~ 현재 : 가톨릭대학교 정보통신 전자공학부 강의전담교수.
현재 IEEK, KICS 정회원, IEICE 해외회원
<주관심분야> 정보 및 부호이론, 논리시스템설계, 컴퓨터 구조, 유한체 이론의 응용 및 VLSI 회로구현 등

나 기 수 (Gi-Su Na) 정회원



1997년 2월 : 건양대학교 컴퓨터공학과 (공학사)
1999년 2월 : 인하대학교 대학원 전자공학과 (공학석사)
1999년 3월 - 현재 : 인하대학교 대학원 전자공학과 박사과정
<주관심 분야> 디지털 로직, 오류정정부호 설계, 퍼지회로 설계

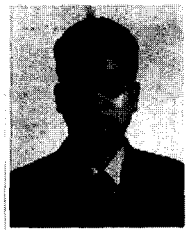
윤 병 희 (Byoung-Hee Yoon) 정회원

1997년 2월 : 원광대학교 전자공학과 (공학사)
1999년 2월 인하대학교 대학원 전자공학과 (공학석사)
1999년 3월 ~ 현재 : 인하대학교 대학원 전자공학과 박사과정
<주관심분야> 다치 프로세서, 다치 저장 소자 설계, VLSI 설계

한 성일 (Sung-Il Han) 정회원

1996년 2월 : 인하대학교 전자공학과 (공학사)
1998년 2월 인하대학교 대학원 전자공학과 (공학석사)
2000년 3월 - 현재 인하대학교 대학원 전자공학과 박사과정
1998년 3월 - 2000년 2월 : 대우통신 광통신 연구실 재직
2003년 3월 - 현재 : 인덕대학 정보통신과 전임강사
<주관심분야>: 다치논리, 회로설계, 디지털 로직, 마이크로 프로세서

최 영 희 (Young-Hee Choi) 정회원



1980년 2월 : 단국대학교 전자공학과 (공학사)
1982년 8월 : 인하대학교 대학원 전자공학과 (공학석사)
2000년 3월 ~ 현재 : 인하대학교 대학원 전자공학과 박사과정
1985년 3월 ~ 현재 : 재능대학 IT학부 정보전자계열 교수
<주관심분야> 유한체 연산회로설계, 다치논리 회로설계, SMPS 등

김 홍 수 (Heung-Soo Kim) 정회원

한국통신학회 논문지 제28권 제2A호 참조
현재 : 인하대학교 전자공학과 교수
<주관심분야> 회로 및 시스템, 스위칭이론, 논리회로설계, 퍼지논리, 다치논리 등