VCGM를 사용한 고속병렬 승산기 설계에 관한 연구

정회원 변 기 영*, 성 현 경**, 김 흥 수*

A Study on the Design of Highly Parallel Multiplier using VCGM

Gi-Young Byun*, Hyeon-Kyeong Seong**, Heung-Soo Kim* ***Regular Members***

요 약

본 논문에서는 GF(2^m)상의 표준기저를 사용한 새로운 형태의 고속병렬 승산회로를 제안하였다. 승산회로의 구성에 앞서, 연산에 필요한 벡터코드들을 생성하는 벡터코드생성모듈(VCGM)을 제안하였다. 이를 통해 연산에 필요한 모든 벡터코드들을 찾을 수 있으며 이들로부터 기저들간의 독립된 모듈러 가산을 취해 승산이 이루어지도록 하였다. 이러한 과정을 수식을 통해 보임으로써, m에 대한 일반화된 회로의 설계가 가능하도록 하였으며, 간단한 형태의 승산회로구성의 예를 GF(2^4)를 통해 보였다. 본 논문에서 제안된 승산회로는 그 구성이 VCGM, AND 블럭, EX-OR 블럭을 통해 이루어짐으로 m에 대한 확장이 용이하며 VLSI에 유리하다. 또한, 회로내부에 메모리 소자를 사용하지 않고, 연산과정 중 소자에 의해 발생하는 지연시간이 적으므로 고속의 연산을 수행할 수 있다. 제안된 회로의 연산동작을 시뮬레이션을 통해 검증하였으며, 참고문헌의 승산기와 그 구성을 비교하였다.

ABSTRACT

In this paper, a new designed circuit of highly parallel multiplier using standard basis over GF(2^m) is presented. Prior to construct the multiplier circuit, we provide the Vector Code Generate Module(VCGM) that generate each vector codes for multiplication. Using these VCGMs, we can get all vector codes necessary for operation and modular sum up each independent corresponding basis, respectively. Following the equations in this paper, we can design generalized multiplier to m. For the proposed circuit in this paper, we show the example in GF(2^4) using VCGMs. In this paper, we build a multiplier with VCGMs, AND blocks, and EX-OR blocks. Therefore the proposed circuit is easy to generalize for m and advantageous for VLSI. Also, it need no memory element and the latency not less fewer then other circuit. We verify the proposed circuit by functional simulation and show its result. Finally, we compare the circuit composition with other works and show its result with a table.

I. 서 론

유한체는 오류정정부호, 스위칭이론 및 암호이론 등의 분야에 널리 적용되고 있는 연산체계이다. 유한체에서 중요하게 다루어지는 연산으로는 가산, 승산, 제산, 승산에 대한 역원등이 있으며, 회로 복잡도(complexity)와 처리속도(speed)를 고려한 최적의 연산 알고리즘을 찾기 위한 연구가 오랜 기간 지속되고 있다.

대표적인 유한체 연산 알고리즘 및 그 구현회로를 간략히 소개하면 1971년, Laws등이 표준기저를 이용한 Cellular-Array 승산기[1]를 보였다. 이후, Yeh 등이 제안한 Systolic 승산기[2], 정규기저를 이용한 Massey-Omura승산기[3]와 이를 VLSI화시킨 C.C.Wang등[4]의 회로가 대표적으로 잘 알려져 있다. 이들의 연구이외에도 많은 연구결과들이 도출되어 왔으며[5-10] 최근, kiamal의 MUX를 적용한 승산기[11]와 Lee의 AOP, ESP조건에서 구현한 Bit-parallel

* 인하대학교 전자공학과 (g1991196@inhavision.inha.ac.kr), ** 상지대학교 컴퓨터 정보공학부 (hkseong@mail.sangji.ac.kr)
논문번호 : 020038-0124, 접수일자 : 2002년 1월 24일

systolic multipliers[12]에 이르고 있다. 이들은 각각 저마다의 독특한 회로설계 알고리즘과 회로구성으로 그 효용성을 입증 받았으며, 보다 개선된 회로구현을 위한 연구는 계속될 것으로 전망된다.

본 논문에서는 유한체 연산에 관한 기존의 연구결과를 토대로, GF(2^m)상의 표준기저를 이용하여 VCGM(Vector Code Generate Module)를 제안하였고, 이를 승산회로에 적용하여 보다 간략화 되고 고속의 연산이 가능한 새로운 승산기를 제안하였다. 본 논문에서 제안한 VCGM는 벡터의 각 비트들의 병렬연산에 의해 동작되며, 회로모듈 내에 별도의 메모리소자를 필요로 하지 않으므로, 시간지연이 적게 발생하여 고속의 동작특성을 갖는다. 또한, 회로구성을 모듈화, 블록화 함으로써 m에 대한 확장과 VLSI(Very Large Scale Integrate)에 유리하도록 하였다. 제안된 회로의 구성방법에 대하여 m에 대한 일반화된 수식과 이를 통한 회로의 구현을 보였다. 설계의 예로써 GF(2^4)상의 승산회로를 설계하였으며, 설계된 회로의 동작을 시뮬레이션을 통해 확인하였고, 그 결과를 첨부하였다. 그리고, 참고문헌과 함께 게이트 수 및 연산처리시간을 비교하였으며 그 결과를 표에 정리하였다. 본 논문에서 제안한 회로구성의 특징중 하나인 회로구성의 모듈화 및 블럭화에 따라, 현재 통신분야에 널리 적용되고 있는 GF(2^8)상의 승산회로를 포함하여 m에 대한 일반화된 회로설계가 용이하다.

본 논문의 구성을 간략히 소개하면 1장의 서론에 이어, 2장에서는 본 논문에서 제안한 승산회로 구성을 위해 필요한 승산의 전개방식과 VCGM설계에 필요한 행렬방정식을 수식을 통해 정립하였다. 3장에서는 2장의 수식을 바탕으로 GF(2^m)상의 m에 대하여 일반화된 승산회로와 m=4의 적용 예를 보였다. 4장에서는 본 논문과 비교문헌의 승산기 구성을 비교하였으며, 결론으로 본 논문의 끝맺음을 하였다.

Ⅱ. GF(2^m)상의 승산과 벡터코드의 생성

2.1 유한체 상의 승산

유한체는 Golois에 의해 발견된 수학의 한 분야로 Galois체, 또는 간단히 GF라 한다. 유한체를 개략적으로 정의하면 유한개의 원소로 이루어진 집합에 대하여 그 원소들간의 연산이 사칙연산에 대하여 닫혀있는 집합체를 말한다.

유한체는 기초체(ground field) GF(p)와 이를 확장한 확대체(extension field) GF(p^m)로 구분된다. 여기서 p와 m은 각각 소수와 양의 정수이며, p 또는 p^m은 유한체 구성원소의 수를 나타낸다. 예를 들어, 유한체 GF(2)는 0과 1의 두 원소로 구성되며, 이러한 기초체를 확장한 확장체 GF(2^m)은 2^m개의 원소를 갖는다. 현재의 실용회로는 GF(2^m)이 주류를 이루며, 일부 분야에서 GF(p^m)에 대한 연구가 진행되고 있으나[13-15], 본 논문에서 언급되는 유한체는 GF(2^m)에 국한하기로 한다.

GF(2^m)상의 0(zero element)이 아닌 (2^m-1)개의 원소들은 원시원(primitive element) α 를 통하여 식 (1)과 같이 나타낼 수 있다. GF(2^m)상의 원시다항식 (primitive polynomial) $F(x)$를 식(2)와 같이 나타낼 때, α 는 $F(x)$의 근이므로 $F(\alpha)=0$이 성립한다.

따라서, $F(x)$에 의해 GF(2^m)의 각 원소들은 식(3)과 같이 차수가 (m-1)이하의 α 의 다항식으로 표현된다.

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

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

$$GF(2^m) = \{0, \alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{q-2}\}_{\mathrm{mod}F(x)} = \{x_{m-1}\alpha^{m-1} + \cdots + x_1\alpha^1 + x_0\} \quad (3)$$

식 (3)의 다항식의 각 계수들, $x_i \in$GF(2)이며, GF(2^m)의 모든 원소들에 대하여 α^{m-1}이하의 다항식으로 표현하는 방법을 다항식표현이라 한다. 그리고, α^{m-1}, α^{m-2}, ···, α^0=1의 기저들을 표준기저(standard basis)라 한다. 또한, 식 (3)의 다항식의 계수만을 표현하는 방법을 벡터표현(vector representation)이라 한다. GF(2^m)상의 임의의 두 원소를 A, B에 대한 표준기저에 의한 다항식 표현을 각각 식 (4), (5)와 같이 나타낼 때, 두 원소의 가산 S는 식 (6)과 같이 나타낼 수 있다.

$$A = a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} = \sum_{i=0}^{m-1} a_i \alpha^i \quad (4)$$

$$B = b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1} = \sum_{i=0}^{m-1} b_i \alpha^i \quad (5)$$

$$S = S_0 + S_1\alpha + \cdots + S_{m-1}\alpha^{m-1} \quad (6)$$

모듈러-2 가산을 $\oplus$기호로 나타낼 때, 식 (6)의 각 계수 $S_i = a_i \oplus b_i$ $(0 \le i \le m-1)$와 같이 간단히 구

할 수 있다. 따라서, 가산회로는 m개의 EX-OR게이트를 통해 쉽게 구현할 수 있다. 가산에 비해 승산은 매우 복잡하게 구현되며, 승산의 전개방식에 따라 다양한 회로구현이 가능하다[1-17]. 본 논문에서는 두 원소 A와 B의 승산을 P라 하고 그 전개방식을 식(7)에 나타내었다.

$$\begin{aligned} P &= AB = P_0 + P_1\alpha + \cdots + P_{m-1}\alpha^{m-1} \\ &= A\left(\sum_{i=0}^{m-1} b_i\,\alpha^i\right) = \sum_{i=0}^{m-1} b_i(A\,\alpha^i) \\ &= \sum_{i=0}^{m-1} b_i\left(\sum_{k=0}^{m-1} a_k^{(i)}\,\alpha^k\right) \end{aligned} \tag{7}$$

식 (2)의 $F(x)$에 의하여 α^k의 계수 $a_k^{(i)}$는 식 (8)과 같이 나타낼 수 있다.

$$\begin{aligned} a_k^{(i+1)} &= a_{k-1}^{(i)} \oplus f_{m-1}a_{m-1}^{(i)} \quad (1\le k\le m-1) \\ &= f_k\,a_{m-1}^{(i)} \quad (k=0) \end{aligned} \tag{8}$$

식(8)을 적용한 $A\alpha^i$의 연산은 i를 0에서 m-1까지 순차적으로 대입하여 반복적으로 구할 수 있다.

2. 행렬방정식[18-20]

GF(2^m)상의 원소들은 $F(x)$를 통해 m개 기저들의 선형결합에 의해 벡터로 표현됨을 전술하였다. GF(2^m)상의 임의의 두 원소들의 벡터표현 $\boldsymbol{x}$, $\boldsymbol{y}$에 대하여, 이들이 일정한 규칙 $\boldsymbol{T}$에 의해 각각 입출력의 관계를 가질 때 이를 $\boldsymbol{y} = \boldsymbol{Tx}$와 같이 표현할 수 있다. 여기서 $\boldsymbol{x}$, $\boldsymbol{y}$를 각각 $m\times1$구조를 갖는 m-튜플(tuple)벡터로 가정할 때, $\boldsymbol{T}$는 $m\times m$구조가지며, 전달행렬이라 할 수 있다.

주어진 조건에 대한 전달행렬에 대하여 이를 상사변환(similar transformation)에 의해 식(9)와 같이 표현될 수 있다.

$$T' = P^{-1}TP = \begin{pmatrix} C_1 & & & 0 \\ & C_2 & & \\ & & \ddots & \\ 0 & & & C_s \end{pmatrix} \tag{9}$$

식 (9)의 $\boldsymbol{P}$는 상사변환행렬이라 하며 $m\times m$구조를 갖는다. 한편, $\boldsymbol{T}$가 $m\times m$구조를 갖는 행렬이므로 $\boldsymbol{T}$의 특성다항식(characteristic equation)의 차수는 m이 되고 특성다항식의 최고차항 λ^m의 계수는 1이 된다. 이 성질을 갖는 다항식을 모닉(monic)다항식이라 하며, 모든 모닉다항식은 어떤 행렬의 특성다항식임을 보여준다. 특성다항식 $c(\lambda)=c_0+c_1\lambda+\cdots+c_{m-1}\lambda^{m-1}+\lambda^m$는 식 (10)의 행렬로 나타낼 수 있으며, 이때의 행렬 $\boldsymbol{C}$를 특성다항식 $c(\lambda)$의 동반행렬(companion matrix)라 한다.

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & -c_0 \\ 1 & 0 & 0 & \cdots & -c_1 \\ 0 & 1 & 0 & \cdots & -c_2 \\ & \vdots & & & \vdots \\ 0 & 0 & 0 & \cdots & -c_{n-1} \end{pmatrix} \tag{10}$$

GF(2^m)상의 원시다항식 $F(x)$를 통해 표준기저의 다항식표현으로 나타내어진 임의의 원소 α^i $(0\le i\le m-2)$로 부터 α^{i+1}의 다항식표현을 구하면 식 (11)과 같다.

$$\begin{aligned} \alpha^{i+1} &= \alpha^i\alpha \\ &= (x_{m-1}\alpha^{m-1} + \cdots + x_1\alpha^1 + x_0)\alpha \\ &= x_{m-1}\alpha^m + \cdots + x_1\alpha^2 + x_0\alpha \\ &= x_{m-1}(f_{m-1}\alpha^{m-1} + \cdots + f_1\alpha^1 + f_0) \\ &\quad + x_{m-2}\alpha^{m-1} + \cdots + x_1\alpha^2 + x_0\alpha \\ &= (x_{m-2}\oplus x_{m-1}f_{m-1})\alpha^{m-1} + \cdots + (x_1\oplus x_{m-1}f_2)\alpha^2 \\ &\quad + (x_0\oplus x_{m-1}f_1)\alpha + x_{m-1}f_0 \end{aligned} \tag{11}$$

원시다항식 $F(x)$는 모닉 다항식의 조건을 만족한다. 또한, 유한체의 성질에 의해 식 (12)와 같이 동반행렬로 표현되며, 이에 따라 식 (11)을 행렬표현 형식으로 나타내면 식 (13)와 같다.

$$T = \begin{pmatrix} 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & \cdots & 0 & -f_1 \\ 0 & 1 & \cdots & 0 & -f_2 \\ & \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 & -f_{m-1} \end{pmatrix} \tag{12}$$

$$\alpha^{i+1} = T\,\alpha^i$$

$$\begin{pmatrix} x_0^{(i+1)} \\ x_1^{(i+1)} \\ \vdots \\ x_{m-2}^{(i+1)} \\ x_{m-1}^{(i+1)} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & \cdots & 0 & -f_1 \\ 0 & 1 & \cdots & 0 & -f_2 \\ & \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 & -f_{m-1} \end{pmatrix} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \\ \vdots \\ x_{m-2}^{(i)} \\ x_{m-1}^{(i)} \end{pmatrix} \tag{13}$$

식 (13)의 열 벡터 표현에서 x는 아래첨자 0, 1, …, m-1로 표현된 기저들의 가중치 비트를 의미하며, 위첨자 (i), $(i+1)$은 원소 α의 지수를 의미한다.

Ⅲ. VCGM에 의한 고속병렬 승산회로의 설계

식 (13)을 통해 GF(2^m)상의 임의의 원소 α^i로부터 α^{i+m}까지, 연산에 필요한 원소들의 벡터표현을

구할 수 있다. 이를 회로로 구현하면 그림 1과 같으며 본 논문에서는 이를 벡터코드 생성모듈 (VCGM)이라 하였다. 그리고, 그림 2는 식(8)과 같이 VCGM를 구성하는 1비트 단위셀의 회로를 보였다. GF(2^m)상의 승산연산을 위해 소요되는 단위셀은 $m(m-1)$개이다.

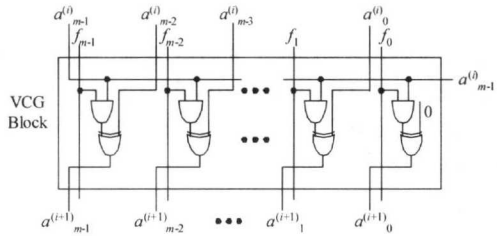


그림 1. GF(2^m)의 VCGM 회로

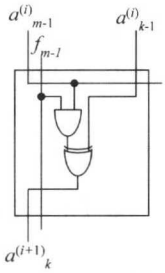


그림 2. VCGM의 단위 셀 회로

그림 1의 VCGM를 탑재한 GF(2^m)상의 임의의 두 원소에 대한 승산기 회로를 그림 3에 나타내었다.

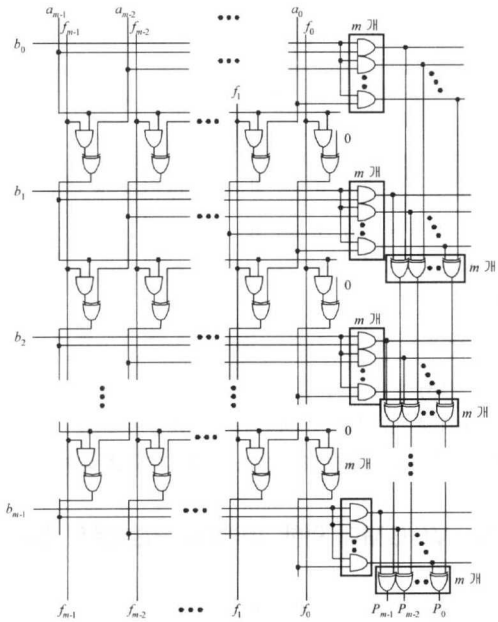


그림 3. 본 논문에서 제안한 GF(2^m)의 승산회로

본 논문에서 제안한 GF(2^m)의 승산회로로 부터 m=4에 대한 회로를 설계하기 위해 원시다항식을 다음과 같이 정의한다. $F(x) = x^4 + x + 1$.

이를 통해 GF(2^4)의 모든 원소들은 $\alpha^3, \alpha^2, \alpha^1, \alpha^0$의 기저들로 표현될 수 있으며 이를 표 1에 정리하였다.

표 1. 표준기저에 의한 GF(2^4)상의 원소표시

$F(x) = x^4 + x + 1$

원소	다항식표현	벡터표현
		$\alpha^3\ \alpha^2\ \alpha^1\ \alpha^0$
$\alpha^{-\infty}$	0	0 0 0 0
α^0	$\alpha^0 = 1$	0 0 0 1
α^1	α^1	0 0 1 0
α^2	α^2	0 1 0 0
α^3	α^3	1 0 0 0
α^4	$\alpha^1+\alpha^0$	0 0 1 1
α^5	$\alpha^2+\alpha^1$	0 1 1 0
α^6	$\alpha^3+\alpha^2$	1 1 0 0
α^7	$\alpha^3+\alpha^1+\alpha^0$	1 0 1 1
α^8	$\alpha^2+\alpha^0$	0 1 0 1
α^9	$\alpha^3+\alpha^1$	1 0 1 0
α^{10}	$\alpha^2+\alpha^1+\alpha^0$	0 1 1 1
α^{11}	$\alpha^3+\alpha^2+\alpha^1$	1 1 1 0
α^{12}	$\alpha^3+\alpha^2+\alpha^1+\alpha^0$	1 1 1 1
α^{13}	$\alpha^3+\alpha^2+\alpha^0$	1 1 0 1
α^{14}	$\alpha^3+\alpha^0$	1 0 0 1

GF(2^4)에 대하여 표 1을 만족하는 VCGM회로와 이를 탑재한 승산회로를 그림 4에 나타내었다. 또한, 회로의 동작을 확인하기 위한 시뮬레이션결과를 그림 5에 나타내었다.

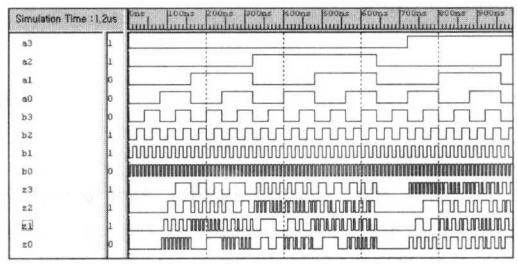


그림 5. 그림 4의 회로에 대한 시뮬레이션동작의 결과

Ⅳ. 비교 및 검토

본 논문에서 제안한 승산회로를 포함하여 참고문헌의 승산회로들은 저마다의 독특한 성질과 장점을

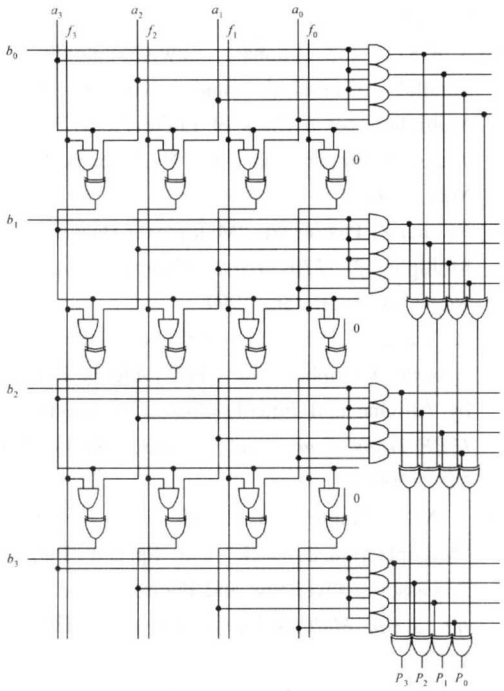


그림 4. 본 논문에서 제안한 GF(2^4)의 승산회로

갖는다. 일반적으로 사용되는 회로비교의 척도들은 간략화된 회로구성(minimization), 빠른 동작속도(speed), 저전력(low power)등을 들 수 있다. 회로의 간략화를 평가하기 위해서는 구성소자의 개수 및 소자간 결선의 수, 입출력단자의 수, 기타 부속회로 및 게이트의 존재여부, VLSI구현시 필요한 면적 등을 고려해야 한다. 또한, 동작속도는 입력이 인가되면서 회로의 동작출력이 나타나기까지의 소자에 의한 지연시간(latency)과 clock time등이 중요한 고려요소이다. 이외에도, 주변회로 블럭과의 호환 및 신호전달의 적합성, 예를 들어 엔코더, 디코더의 필요여부 등 다양한 항목을 통해 종합적으로 평가될 수 있으며, 적용하고자 하는 목적에 따라 일부항목에 대한 trade-off 조건을 고려할 수도 있다. 따라서, 일부 항목만의 단편적 비교를 통해 구성회로의 우열을 논하기는 쉽지 않은 문제이다. 그러나, 대략적이나마 회로의 비교를 위해 여타 참고문헌들은 그 구성회로의 소자 수와 시간지연에 대한 비교를 행하고 있으며 본 논문에서도 이에 따랐다.

참고문헌과 본 논문에서 제안한 승산회로의 구성을 표 2에 정리하였다. Law 등은 순차승산회로와 셀배열승산기의 두가지 형태를 제시하였고, Yeh 등 또한 직렬형(1D)와 병렬형(2D)의 두 가지 형태를 제시하였으나, 표 2에서는 병렬형을 갖는 승산회로의 비교를 위해 병렬형만을 취하였다.

V. 결 론

본 논문에서는 GF(2^m)상의 병렬승산을 구현하기 위한 새로운 승산의 전개방식을 수식을 통해 제시하였고, 그 설계의 예를 보였다. 피승수 A의 각 비트들이 승수 B와의 승산시의 변화를 VCGM를 통

표 2. GF(2^4)상의 승산회로 구성의 비교

Multiplier Item	Law[11]	Yeh[12] (2D)	M-O[13]	Mastrovito[8]	Fenn[6]	Koc[10]	Lee[12] type 1	Lee[12] type 2	This paper Fig. 4
1. Function	AB	AB+C	AB	AB	AB	AB	AB+C		AB
2. $F(x)$=	x^4+x+1	x^4+x+1	x^4+x^3+1	x^4+x+1	x^4+x+1	AOP	AOP		x^4+x+1
3. I/O format	parallel	parallel	parallel	parallel	parallel	parallel	parallel		parallel
4. Register	-	1-bit latch 112 ($7m^2$)	14 ($2m$)	8 ($2m$)	8 ($2m$)	-	1-bit latch 100 $4(m^2+1)$	1-bit latch 125 $5(m^2+1)$	-
5. EOR	32 ($2m^2$)	32 ($2m^2$)	24 ($2m^2-2m$)	15 $\fallingdotseq(m^2-1)$	15 (m^2-1)	15 (m^2-1)	25 (m^2+1)	30 $(m+1)\cdot(m^2+2)$	24 (m^2+2m)
6. AND	32 ($2m^2$)	32 ($2m^2$)	16 (m^2)	16 (m^2)	16 (m^2)	16 (m^2)	25 (m^2+1)	25 (m^2+1)	28 (m^2+3m)
7. Minimum possible clock period	D_A+2D_X	$D_A+D_X+2D_L$	D_A+3D_X	D_A+3D_X	D_A+3D_X	D_A+4D_X	$D_A+D_X+D_L$	D_X+D_L	D_A+D_X
comment	D_A = the propagation delay of one 2-input AND gate. D_X = the propagation delay of one 2-input XOR gate. D_L = the propagation delay of one latch. ( ) = the total gates number of generalization for m AOP means All One Polynomial of degree m								

해 보였고, 이를 통해 승산을 이루었다. 보다 높은 차수 m에 대한 확장된 회로의 구성에 대한 예를 보였으며, 표 2를 통해 참고문헌의 회로구성과의 비교를 보였다. 본 논문에서 제안한 승산회로는 VCGM 모듈과 AND, EX-OR 배열의 구조를 가짐으로써 m의 증가에 대하여 비교적 회로구성이 쉽고, 타 승산회로에 비해 그 연산속도가 비교적 빠른 특성을 갖는다. 유한체 연산의 핵심회로 중 하나인 승산회로에 대하여 본 논문에서 제안된 승산회로는 유효성과 적합성을 갖는다 할 수 있으며, 다양한 유한체 연산회로에 적용될 수 있으리라 전망된다.

참 고 문 헌

[1] B.A.Laws and C.K.Rushford, "A Cellular-Array Multiplier for GF(2^m)" *IEEE Trans. Computer*, vol. C-20, No.12, 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. Computer*, vol. C-33, pp. 357-360, Apr. 1984.

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

[4] 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. Comp.*, vol.C-34, pp. 709-717, Aug. 1985.

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

[6] S.T.J.Fenn, M.Benaissa, and D.Taylor, "GF(2^m) Multiplication and Division Over the Dual Basis," *IEEE Trans. Comp.*, vol.45, No.3, pp.37-46, Jan. 1982.

[7] I.S.Hsu, T.K.Troung, L.J.Deutsch, and I.S.Reed, "A Comparision of VLSI Architecture of Multipliers using Dual, Normal, or Standard Bases," *IEEE Trans. Computer*, vol. C-37, pp. 735-739, 1988.

[8] E.D.Mastrovito, "VLSI Design for Multiplication over Finite Fields," *LNCS-357, Proc. AAECC-6*, pp.297-309, Rome, July 1988, Spring-Verlag.

[9] G.L.Feng, "A VLSI Architecture for Fast Inversion in GF(2^m)," *IEEE Trans. Computer*, vol. 38, No. 10, Oct. 1989.

[10] C.K.Koc, and B.Sunar, "Low-Complexity Bit Parallel Canonical and Normal Basis Multipliers for a Class of Finite Fields," *IEEE Trans. Computer*, vol. 47, No.3, pp.353-356. Mar. 1998.

[11] Kiamal Z. Pekmestzi, "Multiplexer-Based Array Multipliers," *IEEE Trans. Computer*, vol. 48, No.1, pp.15-23. Jan. 1999.

[12] 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. Comp.*, vol. 50, No.5, pp.385-393, May. 2001.

[13] M. Kameyama and T. Higuchi, "Multiple-valued Logic and Special Purpose Processors : Overview and Future," *Proc. IEEE Int. Symp. Multiple-Valued Logic*, pp.289-292, 1982.

[14] M. Nakajima and M. Kameyama, "Design of Highly Parallel Linear Digital System for ULSI Processors", *IEICE Trans*, Vol.E76-C, No.7, pp.1119-1125, Jul. 1993.

[15] Y.Hata, N.Kamiura, and K.Yamato, "Design of Multiple-Valued Programmable Logic Array with Unary Function Generators", *IEICE Trans*, Vol. E82-D No.9, pp.1154-1160, Sep. 1999.

[16] S.B.Wicker and V.K.Bhargava, *Error Correcting Coding Theory*, McGraw-Hill, New York, 1989.

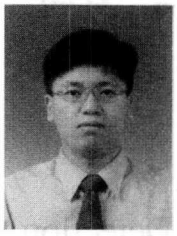
[17] S.Lin, *Error Control Coding*, Prentice-Hall, Inc. New Jersey, 1983.

[18] A.Gill, *Linear Sequential Circuits*, McGraw-Hill Book Co., Newyork. 1966.

[19] H.Anton, *Elementary Linear Algebra*, John Wiley & Sons, Inc., N.Y.1994.

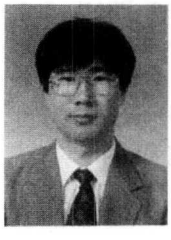
[20] E.Kreyszig, *Advanced Engineering Mathematics 8/e*, John Wiley & Sons, Inc., Newyork. 1999.

변 기 영(Gi-Young Byun) 정회원



1994년 2월 : 인하대학교 전자공학과 (공학사)
1998년 8월 : 인하대학교 전자공학과 (공학석사)
1999년 3월 ~ 현재 : 인하대학교 전자공학과 박사과정 수료
1994년 1월~1996년 8월 : (주)LG전자 VCR 사업부 회로설계 연구원
<주관심 분야> 정보이론, 부호이론, 다치논리시스템, VLSI설계, VHDL, 컴퓨터구조, 유한체 이론의 응용 및 회로구현 등

성 현 경(Hyeon-Kyeong Seong) 정회원



1982년 2월 : 인하대학교 전자공학과 (공학사)
1984년 2월 : 인하대학교 전자공학과 (공학석사)
1991년 2월 : 인하대학교 전자공학과 (공학박사)
1989년 3월~1991년 8월 : 부천전문대학 전자계산과 조교수
1991년 9월~현재 : 상지대학교 컴퓨터 · 정보공학부 부교수
<주관심 분야> Multiple-Valued Logic Design, Computer Architecture & VLSI 설계, Information & Cryptography theory, Digital Signal Processing 등

김 흥 수(Heung-Soo Kim) 정회원

1962년 12월 : 인하대학교 전기공학과 (공학사)
1965년 10월 : 연세대학교 전자공학과 (공학석사)
1979년 2월 : 인하대학교 전자공학과 (공학박사)
1968년 6월~1979년 2월 : 국립항공대학교 교수
1993년 9월~1994년 9월 : 일본 KEI-YO Univ. 교환교수
<주관심 분야> 회로 및 시스템, 논리회로설계, 퍼지논리, 다치논리 등