전류모드 CMOS를 이용한 GF(p^m)상의 셀 배열 승산기

Cell array multiplier in GF(p^m) using Current mode CMOS

최 재 석
Jai-Sock, Choi

요 약

본 논문에서는 GF(P^n)상에서의 새로운 승산 알고리듬과 승산기 구성법을 나타내었다. 유한체 상에서의 두 원소에 대한 승산공식을 유도하였고 유도된 수식에 의해 승산기를 구성하였다. 적용예로 GF(3) 승산 모듈과 덧셈 모듈을 전류모드 CMOS 기법을 적용하여 구현하였다. 이러한 모듈을 기본 모듈로 사용하여 GF(3^n)승산기를 설계하였고 SPICE를 통하여 검증하였다. 제시된 승산기는 규칙적인 셀 구조를 사용하였고 단순히 규칙적인 내부 결선으로 구성된다. 따라서, 유한체 상에서 차수가 m 차로 증가하는 승산에 대해서도 간단히 확장이 가능하다.

ABSTRACT

In this paper, a new multiplication algorithm which describes the methods of constructing a multiplierover GF(p^m) was presented. For the multiplication of two elements in the finite field, the multiplication formula was derived. Multiplier structures which can be constructed by this formula were considered as well. For example, both GF(3) multiplication module and GF(3) addition module were realized by current-mode CMOS technology. By using these operation modules the basic cell used in GF(3^m) multiplier was realized and verified by SPICE simulation tool. Proposed multipliers consisted of regular interconnection of simple cells use regular cellular arrays. So they are simply expansible for the multiplication of two elements in the finite field increasing the degree *m*.

Keywords : Multiple-Valued Logic(MVL), Galois Fields, Multiplier, Cell array, Current mode CMOS.

I. 서 론

VLSI 소자의 내부결선은 집적도가 높아짐에 따라 칩의 공간 점유율측면에서 더욱더 큰 문제점으로 작용하게 되었다. 따라서 그 동안 이를 해결하려는 노력이 다방면에서 진행되어왔다. 반도체의 경우, 70% 정도가 내부결선, 20% 정도가 Isolation,나머지 10% 정도만이 소자인 것을 보면 내부결선을 줄이는 것이 가장 큰 효과를 얻을 수 있다. 한편, 다치논리(Multi-Valued Logic:MVL)분야에서의 회로 실현은 전압의 LEVEL과 극성으로 데이터가 표현되는 전압모드방식과 전류의 세기와 방향으로 데이타를 표현하는 전류모드방식으로 나누어진다. 전압모드의 경우 radix의 증가에 따라 공급전원의 크기가 함께 증가하는 단점이 있으므로 스위칭 속도 감소와 전력소모의 문제점을 야기 시킨다.

전류모드의 경우 1977년 I^2L(Integrated Injection Logic)회로에 의한 4치 회로가 발표되면서 I^2L을 이용한 MVL회로 구현이 시작되었고[3] CCD(Charge Coupled Device)가 1970년 Boyle 과 Smith에 의해 시작된 이후 CCD를 이용한 MVL 회로 구현에 많은 연구가 이루어지고 있다.[9] 최근에는 I^2L과 동일한 동작속도와 전력소모, 칩 점유율 및 우수한 동작특성을 갖는 전류모드 CMOS 회로에 의한 다치논리회로 실현이 활발히 연구되고 있다[4-9] 한편 유한체(Finite Field)를 수학적 배경으로한 다치논리함수의 실현에 대한 연구가 활발히 진행되어 왔는데, 유한체(또는 Galois체)는 2진 논리를 수행하는 부울체의 확장이라는 점에서 다치논리이론의 주 관심 분야가 되었으며, 스위칭 이론, CODING 및 암호서기법(cryptographic)등과 같은 분야에서 널리 응용되고 있다.

$GF(2^m)$상의 연산 특히,$GF(2^m)$상의 연산은 BCH 부호, Reed-Solomon 부호 와 보안 통신에 요구되는 암호화(encryption)와 복호화(decrytion)등 에서 쓰이고 있어 $GF(2^m)$상의 승산에 대한 연구가 널리 이루어져 왔다.[10-13,16-20]

C.S.YEH 등은 $GF(2^m)$상에서 표준기저(standard basis)로 표현된 임의의 두 원소의 승산을 행하는 Messey-Omura승산 알고리듬을 VLSI화에 적합하도록 제안하였다.[10] $GF(2^m)$ 상의 연산에 비하여 단자당 높은 함수 능력및 고밀도 실현이 가능한 $GF(2^m)$상의 승산에 대한 연구가 T.H.KIM[12] 등에 의해 이루어졌다. 그들은 원시기약다항식(Primitive Irreducible Polynomial) F(X)를 사용하여 생성시킨 LSD 치환 다항식 T(α)를 사용하여 α의 내림차순으로 mod F(X)연산을 수행하는 알고리듬을 제안하고 전압모드 3치 회로로 실현하였다. 단점으로는 원시기약다항식을 사용하여 LSD 치환다항식을 생성한뒤, 데이터선별을 위한 별도의 제어신호를 필요로한다.[12] 이상과 같은 기존 알고리듬의 단점을 개선하여 차수 m이 증가하는 경우에도 확장이 용이한 셀 배열 승산기를 제안하였다. 또한 GF(3)상의 가산모듈과 승산모듈을 전류모드 CMOS회로에 의하여 설계하여 2차원 승산기의 기본 셀을 구성하고 이를 SPICE로 검증하였다.

II. 유한체의 기본성질 과 승산알고리즘

1. 유한체의 기본 성질[13,14,17]

유한체 $GF(p^m)$은 p를 소수로 하고 m을 양의정수로 한다. 여기서 P를 유한체 F의 m차 유한 확대체라 할 때 p^m개로 구성되는 유한체가 유일하게 존재함을 정의한다.

$$F(X) = \sum_{i=0}^{m} \{ f_i X^i : \forall f_i \in GF(p) \} \quad (1)$$

로 나타내고 원시기약다항식(Primitive Irreducible Polynomial) F(X)가 임의의 한 근 α 를 갖는다면

$$GF(p^m) = \{ 0, \alpha, \alpha^p, \ldots, \alpha^{p-2}, \alpha^{p-1} \} = 1 \quad (2)$$

또한, $F(\alpha) = 0$ 이므로

$$F(\alpha) = \{ \alpha^m + f_{m-1}\alpha^{m-1} + \ldots + f_1\alpha + f_0 \} = 0$$

$$\alpha^m = f_{m-1}\alpha^{m-1} + f_{m-2}\alpha^{m-2} + \ldots + f_1\alpha + f_0$$

$$= \sum_{i=0}^{m} \{ f_i\alpha^i : \forall f_i \in GF(p) \} \quad (3)$$

따라서 $GF(p^m)$ 상의 모든 원소들은 윗 식에 의해 m차 이하의 다항식으로 표현이 가능하다.

즉,

$$GF(p^m) = \{ \sum_{i=0}^{m-1} a_i\alpha^i : \forall a_i \in GF(p) \} \quad (4)$$

$GF(p^m)$ 상의 중요한 산술적 성질을 살펴보면 다음과 같다.

1) $GF(p^m)$상의 임의의 원소 α 에 대하여

$$\alpha^{p^m} = \alpha, \ \alpha^{p^m-1} = 1 : \forall \alpha \in GF(p^m) \quad (5)$$

2) $GF(p^m)$상의 임의의 두 원소 α , β에 대하여

$$(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m} : \forall(\alpha, \beta) \in GF(p^m) \quad (6)$$

3) $GF(p^m)$상의 임의의 원소 α 에 대하여

$$\alpha^i \cdot \alpha^j = \alpha^{(i+j) \bmod (P^m - 1)} \quad (7)$$

2. 승산 알고리듬

유한체의 기본 성질에 따라 차수가 m차인 임의의 두 원소 A(α), B(α)는 m-1차인 다항식의 곱으로 표현이 가능하므로 본 논문의 승산기를 구성하기 위한 승산 알고리즘을 다음과 같이 얻을 수 있다.

(정리 1)

$R^k(\alpha)$를 k번째 부분곱, R_i^k를 부분곱의 i차 항의 계수라 할 때, 부분곱의 각 계수는 다음 식에 의하여 구하여 진다. p는 기초체의 기수이며 f_i는 원시기약다항식의 계수이다.

$$R_i^0 = a_i \cdot b_{m-1} \quad ; i = 0, 1, \cdots, m-1, \ k = 0 \quad (8a)$$

$$R_0^k = a_0 \cdot b_{m-1-k} + R_{m-1}^{k-1} \cdot (p - f_0) \quad ; i = 0, \quad (8b)$$
$$k = 1, 2, \cdots, m-1$$

$$R_i^k = a_i \cdot b_{m-1-k} + R_{m-1}^{k-1} \cdot (p - f_i) + R_{i-1}^{k-1} \quad (8c)$$
$$; i = 1, 2, \cdots, m-1$$
$$k = 1, 2, \cdots, m-1$$

(증명)

$$\text{피승수 } A(\alpha) = \sum_{i=0}^{m-1} a_i \cdot \alpha^i \quad (9)$$

$$\text{승수 } B(\alpha) = \sum_{i=0}^{m-1} b_i \cdot \alpha^i \quad \text{라 할때} \quad (10)$$

승산치 $R(\alpha) = A(\alpha) \cdot B(\alpha) \bmod F(\alpha)$로 나타낼 수 있다.

$$R^{k}(\alpha) = A(\alpha) \cdot \sum_{i=0}^{m-1} b_i^{k-1} \alpha^{i} \bmod F(\alpha)$$

$$= A(\alpha) \cdot b_{m-1-k} + [\sum_{i=0}^{m-1} R_i^{k-1} \alpha^{i} \cdot \alpha] \bmod F(\alpha)$$

$$= A(\alpha) \cdot b_{m-1-k} + [R_{m-1}^{k-1} \alpha^{m}] \bmod F(\alpha) + \sum_{i=0}^{m-2} R_i^{k-1} \alpha^{i+1}$$

기약다항식 $F(x)$에 α 를 대입하면

$F(\alpha) = 0$

$$\alpha^{m} = -\sum_{i=0}^{m-1} f_i \cdot \alpha^{i} = \sum_{i=0}^{m-1} (p - f_i) \cdot \alpha^{i}$$ 이므로

$$= A(\alpha) \cdot b_{m-1-k} + [R_{m-1}^{k-1} \sum_{i=0}^{m-1} (p - f_i)\alpha^{i}] + \sum_{i=0}^{m-2} R_i^{k-1} \alpha^{i+1}$$

$$= A(\alpha) \cdot b_{m-1-k} + \sum_{i=0}^{m-1} R_{m-1}^{k-1} (p - f_i) \alpha^{i} + \sum_{i=1}^{m-1} R_{i-1}^{k-1} \alpha^{i}$$

$$= [a_0 \cdot b_{m-1-k} + R_{m-1}^{k-1} (p - f_0)] + \sum_{i=1}^{m-1} (a_i \cdot b_{m-1-k} + R_{m-1}^{k-1} (p - f_i) + R_{i-1}^{k-1}) \alpha^{i}$$

$$= \sum_{i=0}^{m-1} R_i^{k} \alpha^{i} \qquad (11)$$

계수 비교에 의하여

$$R_0^{k} = a_0 \cdot b_{m-1-k} + R_{m-1}^{k-1} (p - f_0) \qquad (12a)$$

; i = 0, k = 1, 2, ⋯, m-1

$$R_i^{k} = a_i \cdot b_{m-1-k} + R_{m-1}^{k-1} (p - f_i) + R_{i-1}^{k-1} \qquad (12b)$$

; i = 1, 2, ⋯, m-1,

k = 1, 2, ⋯, m-1

$R^{-1}(\alpha) = 0$ 으로 초기화하면

$$R_i^{0} = a_i \cdot b_{m-1} \; ; \; i = 0,1,2,\cdots, m-1, \; k=0 \qquad (13)$$

증명끝

3. 승산기 구조

이상의 승산 알고리즘에 근거하여 두 원소 $A(\alpha)$, $B(\alpha)$의 곱을 실행하는 셀 배열 승산기를 구성한다. 승산과정은 다음 6 단계로 나누어질 수 있다.

(승산 과정)

단계 1. 부분곱을 0, k를 0으로 초기화한다.

단계 2. GF(p^m)상의 피승산원소 $A(\alpha)$의 계수들과 기약 다항식 $F(\alpha)$의 계수의 보수를 취해 받아들인다.

단계 3. 승산원소 $B(\alpha)$의 m-1-k차 항의 계수를 받아들인다.

단계 4. 부분곱을 생성한다.

단계 5. k가 m-1인지 확인하고 m-1이면 부분곱의 계수들을 출력하고 승산과정을 종료한다.

단계 6. 생성된 부분곱에 α를 곱한후 k를 증분하고 단계 3으로 간다.

먼저 1 차원 배열 승산기를 구성하면 그림 1 과 같다. 1차원 배열 승산기의 기본셀은 승산 모듈과 가산모듈 및 디멀티플렉서로 구성되며 그림 2 와 같다.

1 차원 셀배열 승산기는 승산원소 $B(\alpha)$의 계수들이 직렬로 입력되어 매 클럭마다 부분곱을 생성하여 최종적으로 m번째 클럭에서 승산값인 $R^{m-1}(\alpha)$의 계수들이 병렬로 출력되도록 구성되었다.

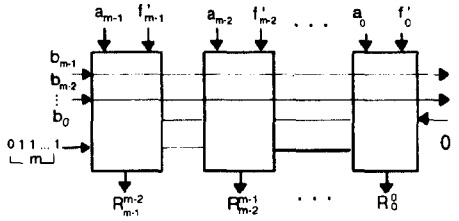


그림 1. 1 차원 배열 승산기

Fig. 1. Linear cellular array for miplication over GF(p^m)

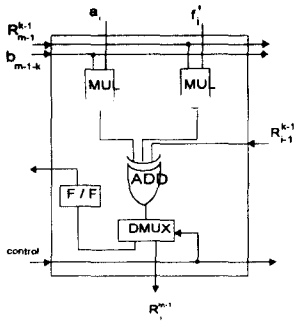


그림 2. 1 차원 배열 승산기 기본셀

Fig. 2. The basic cell for linear cellular array multiplier over GF(p^m)

즉 m-1 단위 시간동안은 매 클럭마다 생성되는 부분곱이 DMUX (demultiplexer)의 하단 플립플롭에 저장되어

다음연산을 대비하고 마지막 m번째 클럭에서 제어신호에 의하여 최종 승산값이 DMUX의 하단 플립플롭에 저장되지 아니하고 직접 출력되도록 설계되었다. 따라서 승산을 위하여 소요되는 시간은 m 이며, 연산을 수행하기 위해 필요한 최소한의 단위 시간은 승산모듈 지연시간, 가산 모듈 지연시간, 그리고 플립플롭에서의 지연시간을 합친 시간이다. 한편 2 차원 셀배열 승산기를 구성하면 그림 3과 같으며 기본셀은 그림 4와 같다.

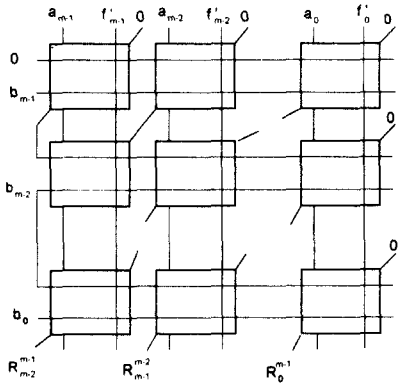


그림 3. GF(p^m)상의 승산을 위한 2차원 셀배열
Fig.3. 2-dimensional cellular array for multiplication over GF(p^m)

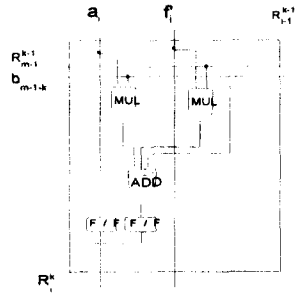


그림 4. 2 차원 배열 승산기 기본셀
Fig.4. The basic cell for 2-dimensional cellular array multiplier over GF(p^m)

2차원 셀배열 승산기는 2개의 유한체 승산 모듈과 1개의 유한체 가산 모듈 및 2 개의 플립 플롭으로 설계된 그림 4의 기본셀을 2 차원적 배열로 구성하여 설계된다. p가 2인 경우에는 유한체 승산 모듈은 AND게이트, 유한체 가산 모듈은 XOR게이트로 각각 대체될 수 있다.승산기의 동작은 상측부에는 피승산원소 A(α)의 계수들이 좌측으로부터 내림차순으로 입력되고, 좌측부에는 승산원소 B(α)의 계수들이 위로부터 내림차순으로 입력된다. 각 행에서 1단위 시간이 지연되어 m단위 시간후에 최종승산값이 최하단 행에서 출력된다.

연산을 수행하기 위하여 필요한 최소한의 단위 시간은 승산모듈 지연시간, 가산 모듈 지연시간, 그리고 플립플롭에서의 지연시간을 합친 시간이다. 본 승산기의 k번째 행은 k번째 부분곱인 $R^k(\alpha)$를 계산하고 여기서 생성된 부분곱은 k+1번째 행에만 전달된다.

Ⅲ. 회로설계 및 시뮬레이션 검토

1. 전류모드 CMOS회로의 기본 구성체 (basic building blocks)

전류모드 CMOS회로를 구성하는 기본이 되는 기본 구성 체를 보면 다음과 같다.

① CM(current mirror)

전류미러 회로는 전류모드회로를 구성하는 가장 기본적이고 중요한 회로이다. CM은 전류모드 회로에 있어서 복제, 기준전류의 실수배의 전류생성및 전류의 방향을 바꾸어 주는 역할을 한다.

② WS(wired sum)

입력전류들의 단순한 접속에 의하여 구성되며 KCL 법칙에 의하여 쉽게 해석이 된다.

③ PT(pass transistor)

Gate에 걸리는 등가 전위차에 의하여 ON / OFF 스위치 동작을 한다.

즉, 다음 동작을 수행한다.(x : 게이트 입력)

$$I_{out} = \begin{cases} I_{in} & ; \ x = \text{high} \\ 0 & ; \ x = \text{low} \end{cases}$$

2. GF(3)상의 연산모듈

기본 구성체를 사용하여 유한체 승산 모듈을 설계하였다.

① 승산 모듈 (multiplication module)

승산은 표 1. 과 같이 mod 3 연산을 수행한다. 또한, 두 입력의 산술 합은 표 2. 와 같다.

표 1. 승 산 표
Table 1. Multiplication table

×	IA 0	1	2
IB 0	0	0	0
1	0	1	2
2	0	2	1

표 2. 진 리 치 표
Table 2. Truth table

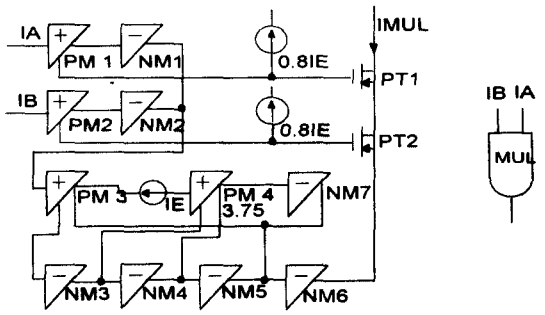
합	0	1	2	3	4
출력	0	0	1	2	1

IA*IB = IB*IA

표 2.에서 더 추가될 조건은 두 입력 중 0 인 입력이 존재할 때 출력이 0 이 되어야 한다는 조건이다. 즉,

$$IMUL = (IA * IB) \bmod 3 \qquad (14)$$

회로를 구성하면 그림 5 와 같다.



PM : Positive current Mirror PT : Pass Transistor
IE : Current source NM : Negative current Mirror

(a) 회 로 (b) 기 호

그림 5. GF(3)상의 승산 모듈
Fig. 5. Multiplication module for GF(3)

PM3으로 두 입력의 산술 합 연산된 신호가 입력되고, 출력전류와 PM4에 의하여 복제된 3.75IE값과 비교되어 NM4와 NM5를 ON/OFF시킨다. NM4가 ON되면 NM5는 OFF되고, NM4가 OFF되면 NM5는 ON된다. NM3의 출력이 4IE일 때 NM5가 ON되고, NM4는 OFF되어 PM3의 출력 값과 NM7의 출력 값의 차분 값이 NM6에 의하여 복제된다. 출력은 PT1과 PT2에 의하여 입력 값들이 IE이상일 때만 출력된다.

3. 시뮬레이션

시뮬레이션은 PSPICE에 의하여 수행하였으며, 5μ CMOS 공정기술에 의해 파라미터를 결정한다.[6] MOS의 회로 모델은 Level 3을 사용하고 단위전류 IE는 15μA로 한다. 그림 6은 승산모듈에 대한 시뮬레이션 결과이다.

그림에서 IA, IB는 피승수(또는 승수)이다. 그림 6(a)에서 IA를 0, 15uA, 30uA의 15uA간격으로 증분 시키고 IB역시 0, 15uA, 30uA로 각각 인가시의 출력을 보았을 때 mod 3연산을 함을 알 수 있다. 그림 6(b)는 과도 해석한 출력 파형으로 IA를 (2 2 1 1)로 입력하고 IB를 (2 1 1 0)로 입력하였을 때의 결과이다. 최대 지연 시간은 IA가 2로 남아 있고 IB가 2에서 1로 천이할 때로 32nsec로 측정되었다.

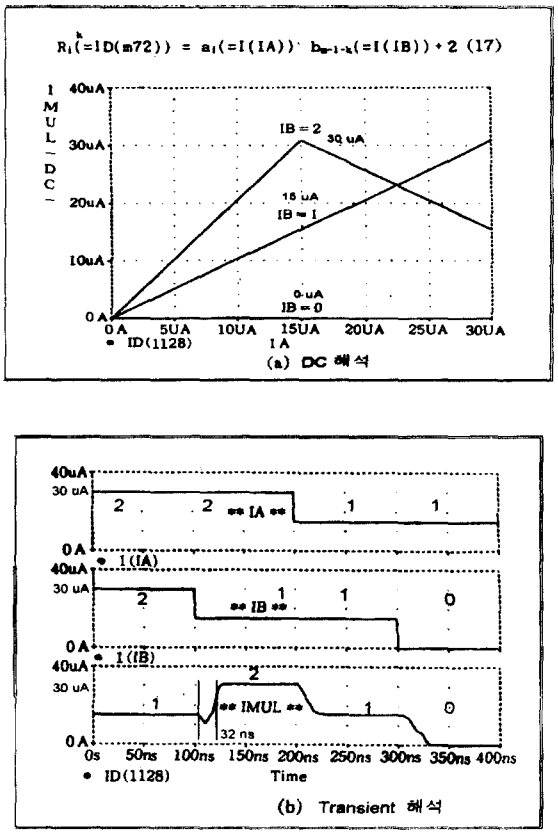


그림 6. 승산모듈에 대한 시뮬레이션 결과
Fig. 6. Simulation results of the multiplication module

그림 7은 2차원 배열 승산기의 기본 셀에 대한 시뮬레이션 결과이다. 기약다항식의 계수를 2로 하고 부분 곱의 계수를 1과 0으로 입력하고, 두 입력 IA1과 IB1의 값을 변화시킨다.

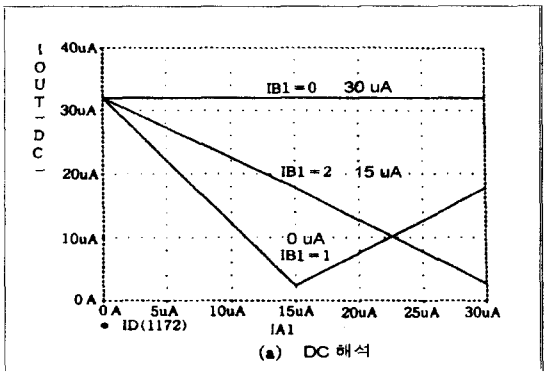
$$R_i^k = a_i \cdot b_{m-1-k} + R_{m-1}^{k-1} \cdot f'_1 + R_{i-1}^{k-1} \quad \text{에서}$$

$$R_{m-1}^{k-1} = 1,\ f'_i = 2 \text{ 및 } R_{i-1}^{k-1} = 0 \text{ 이므로}$$

$$R_i^k(=ID(m72)) = a_i(=I(IA)) \cdot b_{m-1-k}(=I(IB)) + 2 \qquad (17)$$

그림 7(a)는 IA1를 0에서 15uA간격으로 30uA까지 증분 시키고 IB1의 값을 0, 15uA, 30uA로 각각 입력할 때의 출력파형으로 (3)식을 만족함을 알 수 있다. 그림 7(b)는 IA1은 (1 2 2)로 입력하고 IB1은 (2 2 0)로 입력할

때의 출력 파형으로 최대 지연 시간은 IB1이 2로 유지되고 IA1이 1에서 2로 천이할 때로 64nsec로 측정되었다.



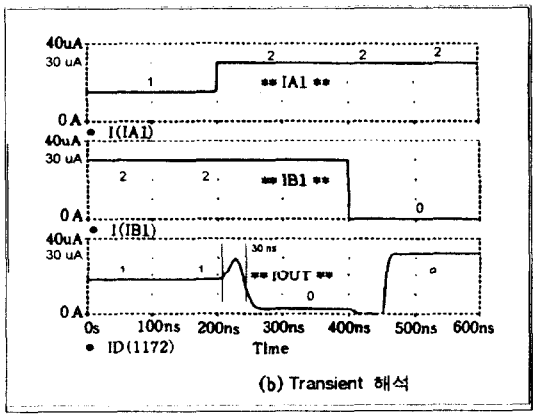


그림 7. 기본셀의 시뮬레이션 결과
Fig.7. Simulation results of the basic cell

로 인수분해 된다.

예로써 GF(3^2)상의 2 차원 배열 승산기를 구성하면 그림 8과 같다. 그림에서 f'_i는 f_i의 가산에 대한 역원이다. GF(3^2)상의 원소를 구하려면, P=3,m=2 이므로 2장의 수학적 성질로 부터 $X^3 - X$ 의 기약인자를 찾아 그 중 2차 다항식을 선택하면 된다.

$$X^{3^2} - X = X^9 - X$$
$$= X(X^4 + 1)(X^4 - 1)$$
$$= X(X^2 + 2X + 2)(X^2 + X + 2)(X^4 - 1)$$

여기서 GF(3) 상의 2 차 기약다항식 $F(X) = X^2 + X + 2$ 로 하고 임의의 한 근을 α 라 하면

$$F(\alpha) = \alpha^2 + \alpha + 2 = 0$$
$$\alpha^2 = -(\alpha + 2) = 2\alpha + 1$$

GF(3^2)상의 원소는 기약다항식에 의하여 표 3.과 같이 표시된다.

표 3. GF(3^2) 상의 원소
Table 3. Elements over GF(3^2)

멱승표현	벡터표현
0	0 0
α	1 0
α^2	2 1
α^3	2 2
α^4	0 2
α^5	2 0
α^6	1 2
α^7	1 1
α^8	0 1

예를 들면, 피승수 $A(\alpha)$ 와 승수 $B(\alpha)$를 다음과 같이 택하였을 때 승산출력 $R(\alpha)$를 구해보면 다음과 같다.

$A(\alpha) = \alpha^5 = (2\ 0)$, $B(\alpha) = \alpha^6 = (1\ 2)$ 로 택하면

$$R(\alpha) = A(\alpha) \cdot B(\alpha)$$
$$= \alpha^{11} = \alpha^3 = (2\ 2) \qquad (18)$$

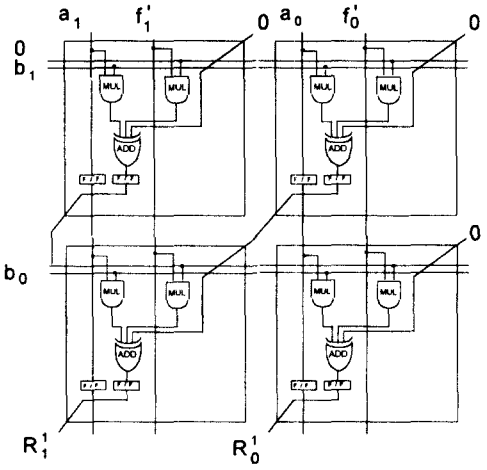


그림 8. GF(3^2)상의 승산기
Fig.8. Multiplier over GF(3^2)

Ⅳ. 비교 및 검토

기존 논문의 결과와 비교하기 위하여 제안한 승산 알고리듬을 p=2인 GF(2^m)에 적용하면 가산 모듈은 XOR 게이트로 승산 모듈은 AND 게이트로 대체된다. 이는 p=2 인 경우에 대하여 적용한 다음의 가산표와 승산표를

통하여 확인할 수 있다.

표 4. GF(2)상의 가산표
Table 4. Addition table over GF(2)

+	0	1
0	0	1
1	1	0

C.S.YEH 등이 제안한 systolic array 승산기는 기본 셀의 수에 있어서 1 차원 승산기의 경우 2 차원 승산기에 비하여 줄어드는 반면 데이터의 입.출력 방식의 차이로 연산 시간에 있어서는 동일하다. 그러나 본 논문의 방법에 비하여 기본 셀의 구성에 있어서는 게이트수가 증가하였고 2 차원 승산기의 경우 복잡도 및 연산 시간에서 단점이 있다.

표 5. GF(2)상의 승산표
Table 5. Multiplication table over GF(2)

×	0	1
0	0	0
1	0	1

따라서 제안한 승산기를 GF(2^m)상에 적용하여 기존 논문의 승산기와 승산속도 및 소자수면에서 비교하면 표 6과 같다.* 비교표에서 AND 게이트와 XOR 게이트의 수는 레지스터에 쓰인 게이트를 제외하고 계산한 것이며, 스위치의 수는 DMUX의 수이다.

표 6. 비 교 표
Table 6. The compared table

비교 내용	Yeh[10]		Wang[11]	Kim[12]	THIS PAPER	
	1-D	2-D			1-D	2-D
AND	3 m	$2m^2$	2m+1	3m	2m	$2m^2$
XOR	2 m	$2m^2$	$\sum[m/2i]$	4m-2	m (3INPUT)	m^2 (3INPUT)
REGIST -ER	10m+2	$7m^2+16$	4m-2	4m-2	m	$2m^2$
INVERT -ER	.	.	2	.	.	.
SWITCH	m	.	.	.	m	.
PASS -TR.	.	.	6m-2	4(m-1)	.	.
연산 시간	2m	2m	2m-1	m	m	m

C.C.Wang등이 제안한 승산기는 순회치환에 의해 간단히 자승회로를 구성할 수 있어 매우 간단한 역원회로를 구성할 수 있는 반면 기약다항식 변경시 회로설계를 다시해야 하며, 기약다항식에 따라 회로의 복잡도가 좌우되고 차수 m 이 증가함에 따라 회로의 복잡성이 매우 증가하게 된다. 동작시간은 2m-1단위 시간이다.

T.H.Kim등이 제안한 승산기는 입력부분을 수정하여 승산과 제산이 역원생성기상에서 실현될 수 있는 장점이 있으나, 먼저 승산부에서 승수와 피승수의 개별 곱 연산과 LSD 치환다항식 T(α)를 생성한 뒤 승산 처리부를 통하여 내림차순 mod F(x)승산을 수행하므로 본 논문의 방법과 비교하여 전체 연산시간이 늦어지고, 데이타 선별을 위한 별도의 제어 신호를 필요로 하는 단점이 있다.

본 논문에서 제안한 1 차원 셀 배열 승산기는 직렬입력 병렬출력형태를 갖고 있으며 출력을 얻기까지 m 단위 시간이 소요된다. 또한 간단한 기본셀의 규칙적 배열로 승산기를 구성하므로 설계 부담을 덜 수 있고, 규칙성, 모듈화, 병렬처리 등의 장점이 있으므로 고속연산 및 VLSI 실현에 적합하다.

제안한 2 차원 셀배열 승산기는 2 개의 AND게이트, 1 개의 3 입력 XOR게이트 및 2 개의 플립플롭으로 구성된 m^2개의 기본셀로 구성되며, 병렬 입.출력형이므로 1차원 승산기에 비하여 크기가 커지는 반면 파이프라인 구조로 변형할 수 있는 장점을 갖는다. 또한 C.S.YEH 등이 제안한 승산기와 비교하여 레지스터를 현저히 감소시켜 승산속도가 향상(m단위시간) 된다. 또한 본 논문에서 제안한 1, 2차원 승산기는 기약다항식의 제약을 받지 않으므로 확장이 용이하다.

V. 결 론

본 논문에서는 유한체 GF(p^m)상에서의 새로운 승산알고리듬을 제안하고, 제안한 승산 알고리듬을 바탕으로 1, 2 차원 승산기를 제안하였다. 또한 GF(3) 승산 모듈과 가산모듈을 전류모드 CMOS회로에 의하여 설계하였고, 시뮬레이션을 통하여 검증하였다. 이를 p=3인 GF(3^2)상에 적용예를 보였다.

또한 기존의 방법과 비교를 위해 GF(2^m)상에 적용한 경우 승산속도 및 소자수면에서 다소 우수함을 보였다. 제안한 승산기는 회로 구성이 간단하며 규칙적인 셀 배열구조로 이루어져 차수 m이 증가함에 따른 확장이 용이하며, 유한체 승산을 필요로 하는 CD(Compact Disk)나 DAT(Digital Audio Tape) 등과 보안 통신에서 암호화나 복호 부분등의 응용 분야에서 매우 유용하다. 그러나, 2 차원 배열 승산기의 경우 승산기의 크기가 m^2 에 비례하므로 병렬 입출력 구조를 갖는 동시에 승산기의 크기가 차수 m에 선형적으로 비례하는 승산알고리듬이 요구되며 이에 대한 지속적인 연구가 필요하다.

접수일자 : 2001. 7. 1 수정완료 : 2001. 7. 17

참고 문헌

[1] M. KAMEYAMA and T. HIGUCHI,"Multiple-valued logic and special-purpose processors : Overview and Future," The 12th INT'L SYMP. on M.V.L, pp. 289~292, May 1982

[2] K. C. SMITH, "Multiple-valued logic : A Tutorial and Application," COMP. mag., pp. 17~27, April 1988.

[3] E. J. McCLUSKEY, "Logic design of multivalued I^2L logic circuits," Trans. on comp. , vol. c-28, pp. 546~559, Aug. 1979.

[4] Y. H. CHANG and J. T. BUTLER, "The design of current mode CMOS multiple valued circuits," The 21th INT'L SYMP. on M. V. L, pp.130~138, May 1991.

[5] T. YAMAKAWA, "CMOS multivalued circuits in hybrid mode," The 15th INT'L SYMP. on M. V. L, pp. 144~151, May 1985.

[6] S. P. ONNEWEER and H. G. KERKHOFF, "Current-mode CMOS high-radix circuits," The 16th INT'L SYMP. on M. V. L, pp. 60~69, May 1986.

[7] S. P. ONNEWEER and H. G. KERKHOFF, "High-radix current-mode CMOS circuits based on the truncated-difference operator," The 17th INT'L SYMP. on M. V. L, pp.188~195, May 1987.

[8] L. ZHIJIAN, and J. HONG, "CMOS fuzzy logic circuits in current mode toward Large Scale Integration," PROC. of the INT'L CONF. on fuzzy logic and neural networks, pp. 155~158, July 1990.

[9] H. G. Kerkhoff, and M. L. Tervoert, "Multiple-valued Logic Charge Coupled Devices," IEEE Trans. Computer, vol. c-30, pp. 644~652, Sept. 1981

[10] C.S.YEH, I.S.REED and T.K.TRUONG, "Systolic multipliers for finite field $GF(2^m)$", IEEE Trans. Computer, vol.C-33, pp.357~360, Apr. 1984

[11] C.C.WANG, T.K.TRUONG, H.M.SHAO,L.J.DEUTCH,J.K.OMURA and I.S.REED, "VLSI architecture for computing multiplications and inverses in $GF(2^m)$",IEEE Trans. Computer, vol. C-34, pp.709~717, Aug. 1985

[12] 김태한, "$GF(3^m)$상의 승산기 및 역원생성기 구성에 관한 연구",인하대학교 석사학위 청구 논문, Feb. 1990

[13] R.J.McELIECE, "Finite fields for computer scientists and engineers", KLUWER ACADEMIC, 1987

[14] 김응태, 박승안, "현대대수학", 경문사, 2000

[15] L.A. GLASSER and D.W.DOBBERPUHL,"The design and analysis of VLSI circuits", ADDISON WESLEY,1985

[16] S.BERKOVITS, J.KOWALCHUK, and B.S.CHANNING, "Implementing public key scheme", IEEE Commum. Mag., pp.2~3, May 1979

[17] H.S.KIM, "A construction of multiple-valued switching functions by Galois field", Ph.D. dissertation, Inha Univ., Incheon, Korea, Feb.1979.

[18] DAVID GREEN, "Modern logic design", ADDISON-WESLEY, 1986

[19] B.BENJAUTHRIT, and I.S.REED, "Galois Switching functions and their applications", IEEE Trans. Computer, vol.C-25, pp. 78~86, Jan. 1976

[20] O.ISHIZUKA, H. TAKARABE, Z. TANG, and H. MATSUMOTO, "Synhtesis of current-mode pass transister networks," The 21th INT'L SYMP. on M. V. L., pp. 139~146, May 1991.

최재석(Jai Sock Choi)
正會員
1988 인하대학교 전자공학과
1990 인하대학교 전자공학과(공학석사)
1997 인하대학교 전자공학과(공학박사)
1990-1995 (주)유니온 시스템 연구소
1999-현재 인덕대학 메카트로닉스과 전임강사

관심분야 : 논리회로설계, 스위칭이론, 시스템프로그래밍