論文 89-26-4-11

GF(2^m)상의 셀배열 승산기의 구성

(A Construction of Cellular Array Multiplier Over GF(2^m))

成 賢 慶*, 金 興 壽*

(Hyeon Kyeong Seong and Heung Soo Kim)

要 約

본 논문에서는 유한체 GF(2^m)상에서 두 원소들의 승산을 실현하는 셀배열승산기를 제시한다. 이 승산기는 승산연산부, mod연산부, 원시기약 다항식연산부로 구성한다. 승산연산부는 AND와 XOR 게이트로 설계한 기본셀의 배열을 이루며, mod연산부 역시 AND와 XOR게이트에 의한 기본셀을 배열하여 구성하였다. 원시 기약다항식 연산부는 XOR게이트들, D플립플롭 회로들과 한개의 NOT게이트를 사용하여 구성하였다.

본 논문에서 제시한 승산기는 회선경로선택의 규칙성, 간단성, 배열의 모듈성과 병발성의 특징을 가지며 특히 차수 m이 증가하는 유한체의 두 원소들의 승산에서 확장성을 가지므로 VLSI 실현에 적합하다.

Abstract

A cellular array multiplier for performing the multiplication of two elements in the finite field GF(2^m) is presented in this paper. This multiplier is consisted of three operation part; the multiplicative operation part, the modular operation part, and the primitive irreducible polynomial operation part. The multiplicative operation part and the modular operation part are composed by the basic cellular arrays designed AND gate and XOR gate. The primitive iirreducible operation part is constructed by XOR gates, D flip-flop circuits and a inverter. The multiplier presented here, is simple and regular for the wire routing and possesses the properties of concurrency and modularity. Also, it is expansible for the multiplication of two elements in the finite field increasing the degree m and suitable for VLSI implementation.

I. 서 론

유한체는 스위칭이론, 오진정정부호, 디지탈신호처리 및 화상처리, 디지탈통신의 암호화 및 해독화를 요하는 보안통신 등에서 많이 응용되고 있다. 특히 유한체 GF(2^m)는 신호처리와 화상처리 분야에서 특별한 계산을 요하거나 범용 컴퓨터계산의 고속화를 보조하는 고성능 전용 컴퓨터의 설계에 주목을 받고 있으며 Reed-Solomon부호기 및 복호기의 VLSI 설계에 사용되고 있다.[1~8]

유한체상에서 가산 및 승산은 관용2진 산술연산과는 현저하게 다르므로 실제적으로 유용성과 단순성에 기인하여 유한체 GF(2^m)에 관한 연구가 활발히

*正會員, 仁荷大學校 電子工學科
(Dept. of Elec. Eng., Inha Univ.)

接受日字 : 1988年 12月 9日

진행되고 있으며 GF(2^m)상에서 가산은 직접적이고 비트 독립적인 mod 2연산으로 관용2진 가산보다 쉬운 반면 승산은 관용2진 승산보다 어렵고 복잡한 계산을 요한다. 최근에는 이와 같이 GF(2^m)상에서 산술연산을 실행하기 위한 시스템들의 설계가 VLSI 실현에 적합한 구조를 가져야 한다.[9,10]

유한체 GF(2^m)상의 승산을 위한 여러 알고리듬이 지난 십수년간 제안되어 왔으나 불행하게도 이들 알고리듬은 불규칙한 회선경로선택(wire routing), 복잡한 제어문제, 비모듈화 구조 및 병발성의 부족때문에 VLSI구조의 설계에 부적합하였다. 그러나 최근 Yeh 등[5]은 유한체 GF(2^m)상에서 임의의 두 기저원소인 A와 B의 승산 P=A.B+C를 실행하는 1차원과 2차원의 시스토릭(systolic)구조를 개발하였으며 Wang 등[6]은 유한체상에서 각 원소들을 제곱하여 정규기저형(normal basis form)으로 한 후 순환이동하면 m개의 2진비트로 표현이 가능한 Massay-Omura 승산알고리듬을 이용하여 VLSI설계에 적합한 파이프라인 구조를 설계하였다.

또한 유한체에서 표조사방법(table look-up)이나 유클리드(Euclid's) 알고리듬을 사용하여 역원을 구하는 관용방법은 VLSI회로에서 쉽게 실현되지 않는다.[6] 그러나 이들은 Massay-Omura 승산기를 이용하여 역원회로를 설계하였다. 그리고, Scott 등[8]은 표준기저(standard basis)로 표현된 각 원소들의 유한체 승산을 실행하는 고속승산기를 제시하였다. 이 승산 알고리듬은 직렬입출력의 파이프라인 구조를 가지며 구조의 규칙성에 기인하여 차수 m이 큰 유한체의 승산에 적합하다.

본 논문에서는 유한체 GF(2^m)상에서 두 원소들의 승산을 실현하는 셀배열승산기를 제시하였다. 이 승산기는 승산연산부, mod연산부, 원시기약 다항식연산부로 구성된다. 승산연산부는 AND와 XOR게이트로 설계한 기본셀의 배열을 이루며 mod연산부는 AND와 XOR게이트의 기본셀을 배열하여 구성한다. 또한 원시기약 다항식연산부는 XOR게이트들, D플립플롭 회로들과 한개의 NOT게이트를 사용하여 구성한다.

본 논문에서 제시한 승산기는 회선경로선택의 규칙성, 간단성, 배열의 모듈성, 병발성의 특징을 가지며 특히 차수 m이 증가하는 유한체의 두 원소들간의 승산에서 확장성을 가지므로 VLSI 실현에 적합하다.

본 논문의 서술과정은 제Ⅱ장에서 유한체 GF(2^m)의 수학적 성질과 승산알고리듬을 논의하고 제Ⅲ장에서는 셀배열승산기의 구성으로써 승산연산부, mod연산부, 원시기약 다항식연산부를 논의하고 제Ⅳ장에서는 본 논문에서 제시한 승산기와 타 논문의 승산기들과 비교검토를 하였고 제Ⅴ장에서 결론을 논하였다.

Ⅱ. 유한체의 기본성질과 승산알고리듬

1. 유한체의 기본성질[11,12]

유한체 GF(p^m)은 p가 솟수이고 m이 양의 정수인 p^m개의 원소들을 갖는다. 유한체 GF(2^m)은 2^m개의 원소들을 가지며 GF(2^m)은 2개의 원소들을 갖는 기초체(ground field) GF(2)의 확대체이다. 즉, 유한체 GF(2)는 {0, 1}의 원소들로 구성된다.

GF(2^m)에서 모든 산술연산은 그 결과를 mod2 연산하므로 이루워진다. GF(2^m)의 0이 아닌 모든 원소들은 원시원소 α에 의해 생성되며 α는 GF(2^m)의 원시기약 다항식 F(x)=0의 근이다.

$$F(x)=\sum_{i=0}^{m} f_i . x^i \qquad (1)$$

여기서 F(x)는 최고차수 m의 계수인 $f_m=1$인 모닉 다항식(monic polynomial)이다. 또한, GF(2^m)의 0이 아닌 원소들은 α의 멱(power)으로서 표현이 가능하며 다음과 같다.

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

이다.

원시기약 다항식 $F(\alpha)=0$이므로 $F(\alpha)=\alpha^m+f_{m-1}.\alpha^{m-1}+\cdots+f_1.\alpha+f_0$에서

$$\alpha^m=\sum_{i=0}^{m-1} f_i . \alpha^i \qquad (3)$$

이다.

그러므로 GF(2^m)상의 원소들은 m보다 더 낮은 차수를 갖는 α의 다항식으로 다음과 같이 표현할 수 있다.

$$GF(2^m)=\{\sum_{i=0}^{m-1} a_i . \alpha^i \mid a_i \in GF(2)\} \qquad (4)$$

이다.

유한체 GF(2^m)의 유용한 성질들을 증명없이 설명하면 다음과 같다.

1) GF(2^m)에서 임의의 한 원소 α에 대하여

$$\alpha^{2^m}=\alpha,\ \alpha^{2^m-1}=1;\ \forall \alpha \in GF(2^m) \qquad (5)$$

2) GF(2^m)에서 임의의 두 원소들 α와 β에 대하여

$$(\alpha+\beta)^2=\alpha^2+\beta^2;\forall \alpha, \beta \in GF(2^m) \qquad (6)$$

3) GF(2^m)에서

$$\alpha^i \cdot \alpha^j = \alpha^{i+j(\mathrm{mod}2^m-1)} = \alpha^{r(\mathrm{mod}2^m-1)} ; \forall \alpha^i, \alpha^j, \alpha^r \in GF(2^m) \quad (7)$$

단, $i+j(\mathrm{mod}2^m-1)$은 $i+j=r(\mathrm{mod}2^m-1)$이다.

2) 승산알고리듬

유한체 GF(2^m)에서 임의의 두 원소들 A와 B를 각각 다음과 같이 표현할 수 있다.

$$A=\sum_{i=0}^{m-1} a_i \cdot \alpha^i \quad (8)$$

이고

$$B=\sum_{j=0}^{m-1} b_j \cdot \alpha^j \quad (9)$$

이다. 이 때 이 두 원소들의 합 S는

$$S=A+B=\sum_{k=0}^{m-1} s_k \cdot \alpha^k \quad (10)$$

여기서 $s_k=a_i+b_j(\mathrm{mod}2)$이고 $0\le k\le m-1$이다. 그러므로 GF(2^m)에서의 가산은 직접적이고 m개의 비트 독립적인 XOR게이트들에 의하여 관용 2진 가산보다 쉽게 실현된다.

또한, GF(2^m)에서 임의의 두 원소들 A와 B의 승산에서 다음과 같이 승산계수 원소들을 정의한다.

〔정의 1〕 GF(2^m)에서 임의의 두 원소들 A와 B의 승산 P=A.B에서 A의 계수원소를 a_i, B의 계수원소를 b_j라 하면 P의 계수원소 P_n은

$$P_n=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i \cdot b_j \quad (11)$$

이다. 여기서 $n=i+j$, $0\le n\le 2_m-2$로서 계수원소의 밑수 i와 j의 합이 P의 계수원소의 밑수 n와 같으며 n와 같은 계수원소항들만 mod2 연산항을 나타낸다.

예로서 GF(2^4)상의 두 원소들 A와 B의 승산에서 식 (11)에 의하여 $n=i+j=4$인 승산계수원소 P_4는

$$P_4=\sum_{i=0}^{3}\sum_{j=0}^{3} a_i \cdot b_j = a_1 \cdot b_3 + a_2 \cdot b_2 + a_3 \cdot b_1$$

이 된다.

정의 1을 이용하여 임의의 두 원소들의 승산 R는

$$\begin{aligned} R=A.B(\mathrm{modF}) &= \sum_{j=0}^{m-1} A \cdot b_j \cdot \alpha^j (\mathrm{modF}(\alpha)) \\ &= \sum_{i=0}^{m-1}(\sum_{j=0}^{m-1} a_i \cdot b_j)\,\alpha^{i+j} (\mathrm{modF}(\alpha)) \\ &= \sum_{n=0}^{2m-2} p_n \cdot \alpha^n (\mathrm{modF}(\alpha)) \\ &= (P_i+P_j)\ (\mathrm{modF}(\alpha)) \\ &= (\sum_{i=0}^{m-1} p_i \cdot \alpha^i + \sum_{j=m}^{2m-2} p_j \cdot \alpha^j)\ (\mathrm{modF}(\alpha)) \\ &= \sum_{i=0}^{m-1} p_i \cdot \alpha^i + (\sum_{j=0}^{2m-2} p_j \cdot \alpha^j)\ (\mathrm{modF}(\alpha)) \\ &= \sum_{k=0}^{m-1} R_k \cdot \alpha^k \end{aligned} \quad (12)$$

이다. 여기서 R_k는 원시기약 다항식 $F(\alpha)$에 의해 생성된 계수원소이다.

Ⅲ. 셀배열승산기의 구성

이 장에서는 GF(2^m)상의 승산 R=A.B(modF)를 실행하는 병렬입출력형 셀배열승산기의 구성을 논하였다. 그림 1은 GF(2^m)상의 두 원소들의 승산을 실행하는 셀배열승산기의 구성도이다.

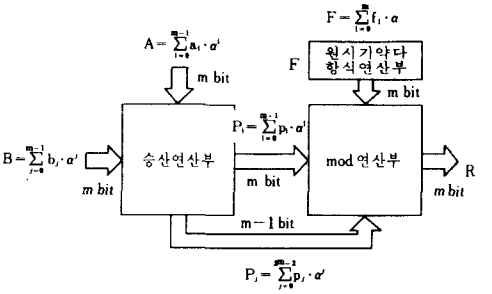


그림 1. GF(2^m)상의 셀배열승산기
Fig. 1. A cellular array multiplier in GF(2^m).

이 승산기는 GF(2^m)상의 두 원소들의 승산을 실행하는 승산연산부와 승산연산부의 출력을 입력으로 하여 원시기약 다항식에 의한 mod연산을 행하는 mod연산부와 원시기약 다항식을 산술연산 처리하는 기약 다항식 연산부로 구성되며 이들의 구성은 다음과 같다.

1. 승산연산부

GF(2^m)상의 두 원소들의 승산을 실행하는 승산연산부는 AND와 XOR게이트로 설계된 기본셀의 배열에 의해 구성된다. 그림 2는 기본셀의 회로도이다.

이 기본셀은 a_i비트와 b_i비트의 AND연산과 전단의 출력 I와 mod연산을 행하며 이 기본셀의 출력 Y_i는

$$Y_i=(a_i \cdot b_i) \oplus I \quad (13)$$

이다. 여기서 i는 i번째 셀을 나타낸다.

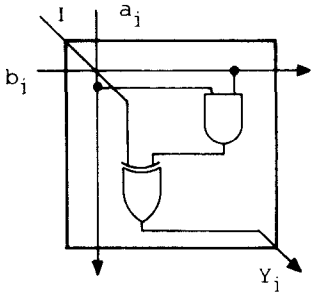


그림 2. 승산연산부의 기본셀
Fig. 2. The basic cell of multiplicative operation part.

이 기본셀의 배열에 의한 GF(2^m)상의 두 원소들의 승산을 실행하는 승산연산부는 그림 3과 같다. 여기서 상측에는 $A=\sum_{i=0}^{m-1} a_i \cdot \alpha^i$ 의 계수원소들이 입력으로 가해지고 좌측에는 $B=\sum_{j=0}^{m-1} b_j \cdot \alpha^j$의 계수원소들이 입력으로 가해진다. $P=A \cdot B$의 계수원소들은 $P_n=\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i \cdot b_j$이 출력으로 나타난다. 이 때 승산연산부의 동작시간은 1단위 시간이 소비된다.

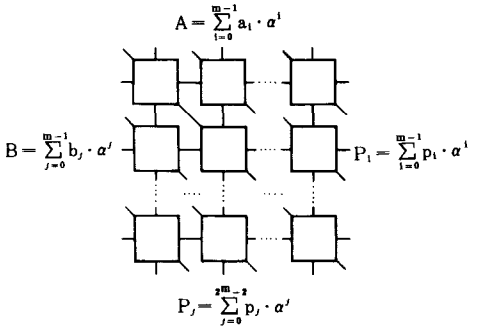


그림 3. GF(2^m)상의 승산연산부
Fig. 3. The multiplicative operation part in GF(2^m).

2. mod연산부

승산연산부의 출력을 입력으로 하는 mod연산부는 AND와 XOR게이트로 설계된 기본셀의 배열에 의해 구성된다. 그림 4는 기본셀의 회로도이며 이 셀의 출력 R_i는

$$R_i=(P_j \cdot F) \oplus P_i \qquad (14)$$

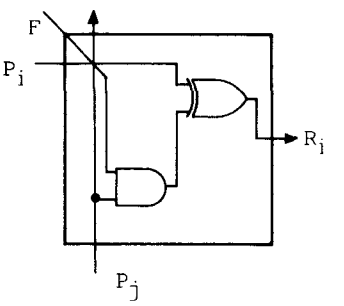


그림 4. mod연산부의 기본셀
Fig. 4. The basic cell of modular operation part.

이다. 여기서 P_i, P_j는 승산연산부의 출력이고 F는 원시기약다항식 연산부의 출력이다. 또한 i는 {0, 1, ⋯, m−1}이고 j는 {m, m+1, ⋯, 2^m-2}이다.

이 기본셀의 배열에 의한 GF(2^m)상의 승산연산부와 원시기약다항식 연산부의 출력을 입력으로 하는 mod연산부는 그림 5와 같다. 여기서 상측은 원시기약다항식 연산부의 출력이, 좌측은 승산연산부의 출력 $P_i=\sum_{i=0}^{m-1} p_i \cdot \alpha^i$의 계수원소들이, 하측은 $P_j=\sum_{j=0}^{2^m-2} p_j \cdot \alpha^j$의 계수원소들이 각각 가해지고, 우측은 $R=\sum_{k=0}^{m-1} R_k \cdot \alpha^k$의 계수원소들이 출력된다. 이 때 mod연산부의 동작은 원시기약다항식 연산부에서 한 비트씩 우회 이동할 때마다 mod연산을 실행하도록 동기화되어 있다면 mod연산부의 동작시간은 m−1단위 시간이 소비된다.

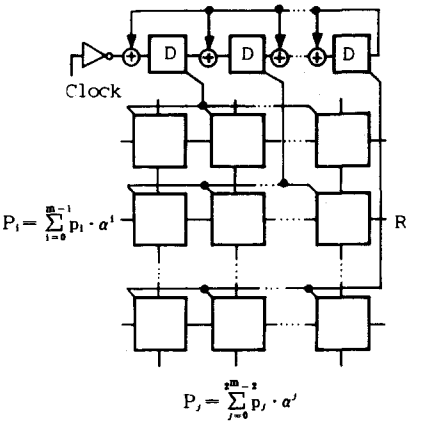


그림 5. GF(2^m)상의 mod연산부
Fig. 5. The modularity operation part in GF(2^m).

3. 원시기약다항식 연산부

GF(2^m)상의 원시기약다항식 $F(\alpha)=0$이고 모닉다항식이므로 $\alpha^m=\sum_{i=0}^{m-1} f_i \cdot \alpha^i$이다. 이 다항식에 의해 두 원소들의 승산에서 m이상의 차수를 m−1이하로 감소시킨다. GF(2^m)상의 원시기약다항식 연산부는 그림 6과 같다. 이 연산부는 XOR게이트들, D플립플롭회로들과 한개의 NOT게이트에 의해 구성되며 이 연산부의 동작은 원시기약다항식에 의한 D플립플롭회로의 출력이 한 비트씩 우회 이동하면서 각 셀내의 AND게이트들을 동작시킨다. 이 때 동작시간은 원시기약다항식의 계수원소들이 이미 원시기약다항식 연산부의 각 D플립플롭회로에 입력되었다고 가정하면 m−1단위 시간이 소요된다.

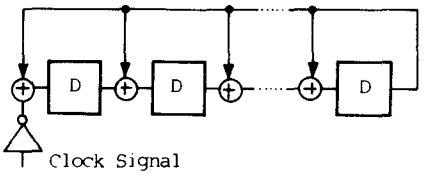


그림 6. GF(2^m)상의 원시 기약다항식 연산부
Fig. 6. The primitive irreducible operation part in GF(2^m).

위에서 설명한 GF(2^m)상의 승산기 구성에 의하여 GF(2^m)의 두 원소들 A와 B의 승산을 실행하는 셀배열 승산기는 그림 7과 같다. 여기서 GF(2^m)의 원시기약 다항식 중 $F(\alpha)=\alpha^4+\alpha+1$을 사용하였다.

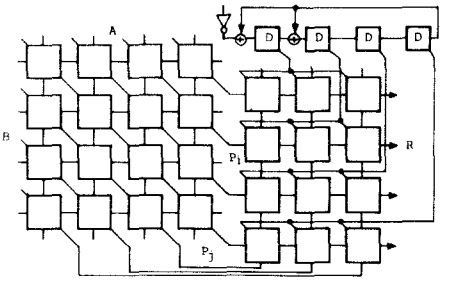


그림 7. GF(2^4)의 셀배열승산기
Fig. 7. The cellular array multiplier in GF(2^4).

Ⅳ. 비교 및 검토

본 장에서는 제시한 셀배열승산기를 타 논문의 승산기들과 비교하였으며 비교표가 표 1과 같다.

Yeh 등[5]이 제시한 시스토릭 승산기는 1차원 시스토릭 경우는 m이 증가할수록 게이트 수가 줄어드는 반면 2차원 시스토릭승산기는 게이트 수가 다소 증가하며 이 회로의 동작시간은 2m단위 시간이 소요된다. Wang 등[6]이 제시한 승산기는 게이트 수가 상당히 감소되며 동작시간이 2m−1단위시간이 소요된다. Scott등[8]은 AND게이트를 사용하지 않는 반면 스위치수가 많이 사용되는 것이 단점이며 이 회로의 동작시간은 2m단위시간을 갖는다.

본 논문에서 제시한 셀배열승산기는 AND게이트와 XOR게이트수가 다소 증가하는 반면 레지스터수가 상당히 감소됨을 보였으며 회로동작시간이 m단위시간이 소요되므로 타 논문의 승산기들에 비하여 다소 우수함을 보였다. 제시한 승산기는 회선경로선택의

표 1. 비교표
Table 1. The compared table.

	Yeh[5]		Wang[6]	Scott[8]	This paper
	1-D Systolic	2-D Systolic			
AND	3m	$2m^2$	2m+1	·	2m(m−1)
XOR	2m	$2m^2$	$\sum[m/2i]$	2m	$2m^2$
REGISTER	10m+2	$7m^2+16$	2m−1	4m+1	m
INVERTER	·	·	·	2	1
SWITCH	m	·	·	8m	·
CK TIME	2m	2m	2m−1	2m	m

단, [X]는 X보다 더 큰 가장 적은 정수
i 는 XOR 레벨수

규칙성, 간단성, 배열의 모듈성, 병발성의 이점을 가지며 특히 차수 m이 증가하는 유한체의 두 원소들간의 승산에서 확장성을 가지므로 VLSI실현에 적합하다.

V. 결 론

본 논문에서는 유한체 GF(2^m)상에서 두 원소들의 승산을 실현하는 셀배열승산기를 제시하였다. 이 승산기는 승산연산부, mod연산부, 원시기약다항식 연산부로 구성된다. 승산연산부는 AND와 XOR 게이트로 설계한 기본셀을 배열을 이루며, mod연산부는 AND와 XOR게이트의 기본셀의 배열하여 구성하였다. 또한 원시기약다항식 연산부는 XOR게이트들, D 플립플롭회로들과 한개의 NOT게이트를 사용하여 구성하였다. 이 승산기의 동작시간은승산연산부는 1단위시간이 소비되며 mod연산부와 원시기약다항식 연산부의 동작시간은 원시기약다항식의 계수원소들이 이미 원시기약다항식 연산부에 입력되었다고 가정하면 m−1단위시간이 소비된다. 그러므로 셀배열승산기의 동작시간은 m단위시간이 소요된다.

본 논문에서 제시한 승산기는 회선경로선택의 규칙성, 간단성, 배열의 모듈성, 병발성의 이점을 가지며 특히 차수 m이 증가하는 유한체의 두 원소들의 승산에서 확장성을 가지므로 VLSI실현에 적합하다.

參 考 文 獻

[1] H.T. Kung, "Why systolic architectures?," *IEEE Computer*, vol. 15, pp. 37-46, Jan. 1982.

[2] H.M. Shao, T.K. Truong, L.J. Deutsch, J.H. Yaeh and I.S. Reed, "A VLSI design of a pipeling reed-solomon decoder," *IEEE Trans. Comput.*, vol. C-34, pp. 393-403, May 1985.

[3] T.K. Truong, L.J. Deutsch, I.S. Reed, J.S. Hsu, K. Wang and C.S. Yeh, "The VLSI design of a reed-solomon encoder using Berlekamp's bit serial alogirithm," *IEEE Trans. Comput.*, vol. C-33, pp. 906-911, Oct. 1984.

[4] B.A. Laws and C.K. Rushforth, "A cellular-array multiplier for GF(2m)," *IEEE Trans. Comput.*, vol. C-20, pp. 1573-1578, Dec. 1971.

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

[6] C.C. Wang, T.K. Truong, H.M. Shao, L.J. Deutsch, J.K. Omura and I.S. Reed, "VLSI architecture for computing multiplications and inverses in GF(2m)," *IEEE Trans. Comput.*, vol. C-34, pp. 709-717, Aug. 1985.

[7] C.A. Mead and L.A. Conway, "Introduction to VLSI systems," Reading, MA, Addison-Wesley, 1980.

[8] P.A. Scott, S.E. Tarvares and L.E. Peppard, "A fast multiplier for GF(2m)," *IEEE J. Select. Areas Commun.*, vol. SAC-4, Jan. 1986.

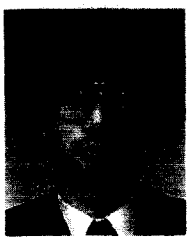
[9] I.S. Hsu, T.K. Truong, L.J. Deutsch and I.S. Reed, "A comparison of VLSI architecture of finite field multipliers using dual, normal, or standard bases," *IEEE Trans. Comput.*, vol. C-37, pp. 735-739, June 1988.

[10] B.B. Zhou, "A new bit-serial systolic multiplier over GF(2m)," *IEEE Trans. Comput.*, vol. C-37, pp. 749-751, June 1988.

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

[12] R. Lidl, H. Niederreiter and P.M. Cohn, "Finite fields," Reading, MA, Addison-Wesley, 1983. *

著 者 紹 介



成 賢 慶(正會員)

1955年 12月 21日生. 1982年 인하대학교 전자공학과 졸업. 1984年 인하대학교 대학원 전자공학과 공학석사학위 취득. 1985年 인하대학교 대학원 박사과정 입학. 주관심분야는 다치논리함수 구성이론 및 회로설계, VLSI설계 컴퓨터 구조설계, 정보 및 코딩이론, 디지탈신호처리 등임.

金 興 壽 (正會員) 第25卷 第10號 參照

현재 인하대학교 전자공학과 교수