2014년 6월 전자공학회 논문지 제 51권 제 6 호
Journal of The Institute of Electronics and Information Engineers Vol. 51, NO. 6, June 2014 http://dx.doi.org/10.5573/ieie.2014.51.6.117

논문 2014-51-6-14

듀얼기저에 기초한 효율적인 곱셈기 설계

(Design of the Efficient Multiplier based on Dual Basis)

박 춘 명*

(Chun-Myoung Park©)

요 약

본 논문에서는 기저변환을 사용하여 효율적인 곱셈기를 구성하는 방법을 제안하였다. 제안한 곱셈기는 두 입력부분 중 한 입력을 듀얼기저로 변환하는 표준-듀얼 기저 변환회로 모듈과 주어진 m차 기약다항식에 의해 b_m부터 b_{m+k}를 발생시키는 bm+k차 발생연산모듈, m^2개의 AND 게이트와 m(m-1)개의 EX-OR 게이트로 구성되는 다항식 승산모듈로 구성된다. 또한, 듀얼기저로 표현되는 출력부분을 표준기저로 변화시켜주는 듀얼-표준 기저 변환회로 모듈로 구성되며, 각 연산부의 구성에 필요한 기본 연산모듈을 정의하였다.

Abstract

This paper proposes the constructing method of effective multiplier using basis transformation. Th proposed multiplier is composed of the standard-dual basis transformation circuit module to change one input into dual basis the operation module to generate from bm to bm+k by the m degree irreducible polynomial, and the polynomial multiplicative module to consist of m^2 AND and m(m-1) EX-OR gates. Also, the dual-standard basis transformation circuit module to change the output part to be shown as a dual basis into standard basis is composed. The operation modules to need in each operational part are defined.

Keywords : Basis, multiplier, polynomial, primitive irreducible polynomial, transformation etc.

Ⅰ. 서 론

최근의 초고도화 정보융합 분야의 핵심인 ICT 분야에 있어 유한체상의 연산[1]은 매우 중요한 분야로 대두되고 있다. 유한체상의 연산은 통신[2] 채널 및 저장매체에서 발생하는 오류를 정정하기 위한 오류정정[3-4] 회로로 부터 진보된 컴퓨터 등의 분야에 활용된다. 또한 차세대의 성장 동력 산업용 메모리, 디지털 레이더 신호처리, 이동통신, 위성통신, 패킷 스위칭 시스템, CD (Compact Disk), DAT(Digital Audio Tape)로 손꼽히는 디지털 보안 및 서명, 디지털 워터마킹[5] 가정용 보안시스템, RF용 스마트 카드 등 유한체 상의 연산에 대한 응용유한체 승산의 전개기법과 그 회로의 구성기법은 모두 정규(모듈)화, 고속화, 간략화에 초점을 맞추어 VLSI에 적합한 하드웨어 구조의 개발을 그 목표로 하였다. 특히 소수 P=2인 유한체 GF(2^m)상의 연산[6]은 신호처리와 화상처리 분야에서 특별한 계산을 요하거나 범용 컴퓨터 계산의 고속화를 보조하는 고성능 컴퓨터 설계에도 응용되고 있다. 최근 빠른처리 속도와 복잡도를 고려한 VLSI 구현에 있어서는 규칙성과 모듈화가 매우 중요한 요소가 되며, 이에 적합한 승산기 설계에

* 평생회원, 한국교통대학교 컴퓨터공학과
(Department of Computer Engineering, Korea National University of Transportation)
© Corresponding Author(E-mail: cmpark@ut.ac.kr)
※ 이 논문은 2013년도 한국교통대학교 교내학술연구비의 지원을 받아 수행한 연구임
접수일자: 2014년04월29일, 수정일자: 2014년05월08일
수정완료: 2014년05월29일

관한 연구가 활발히 펼쳐지고 있으며 꾸준히 발전하고 있다.[7~9]

Ⅱ. 유한체

1. 유한체의 정의

집합을 구성하는 원소들에 대하여 이항 연산이 정의되며 이 연산들이 특정한 공리계를 만족시킬 때 이 집합과 연산을 함께 묶어 대수적 체계라고 한다. 대수학에서 정의하는 집합의 조건에 따라 군(Group), 환(Ring), 체(Field) 등의 집합들이 정의된다. 군은 대수학의 기본이 되는 집합으로, 원소들 간의 이항 연산이 정의되며 그 항등원과 역원이 정의되는 집합을 말한다. 군을 보다 구체화하여 정수 집합에 대한 덧셈과 곱셈이 정의되는 집합을 환이라 한다. 환의 조건을 만족하면서 아래 정의1의 조건을 추가적으로 만족하는 집합을 체라 한다.

[정의 1]

가산과 승산이 정의된 정수의 집합에서 다음의 조건들을 만족하는 집합을 체라 한다.

1) 교환 법칙
   a+b=b+a, a • b=b • a (∀a,b∈GF(P^m))
2) 결합 법칙
   a+(b+c)=(a+b)+c
   a • (b • c)=(a • b) • c (∀a,b,c∈GF(P^m))
3) 분배 법칙
   a • (b+c)=(a • b)+(a • c) (∀a,b,c∈GF(P^m))
4) 영원의 존재
   a+0=0+a=a 인 영원 0이 존재 (∀a∈GF(P^m))
5) 단위원의 존재
   a • 1 = 1 • a인 단위원 1 이 존재 (∀a∈GF(P^m))
6) 역원의 존재
   a+(−a)=0인 a의 가산에 관한 역원 −a가 존재
   (∀a∈GF(P^m))
   a • (−a)=1인 a의 승산에 관한 역원 −a가 존재
   (∀a≠0∈GF(P^m))

유한체상에서 정의된 산술연산은 체내의 값들에 대하여 수행하면 그 결과는 항상 그 체의 원소가 되며, P^m개의 서로 다른 값을 갖는다. 유한체상에서 원소들에 관하여 연산을 수행할 때 그 연산의 결과가 유한체에 닫혀있기 위해, 유한체상의 연산은 모듈러(Modular, mod) 연산을 기반으로 이루어진다. 모듈러 연산이란 나머지 연산으로도 알려져 있으며, GF(P)상의 연산 결과를 P로 나눈 후 그 나머지만을 취하는 연산 기법이다.

GF(P^m)상의 원소 사이에 정의된 가산과 승산에 대하여 GF(P^m)에서의 수학적 성질은 다음과 같다. (단, ∀a,b,c∈GF(P^m))

P1) GF(P^m)상에서 임의의 원소 a에 대한 영원의 곱은 0이다. a • 0=0

P2) GF(P^m)상에서 임의의 원소 a의 P배는 0이다.
   P • a=0

P3) GF(P^m)상에서 a≠0인 경우에 대하여 임의의 원소 a의 P^m 승은 a이다.

$$a^{p^m}=a,\ a^{p^m-1}-1=1$$

P4) GF(P^m)상에서 양의 정수 m에 대하여 임의의 두 원소 a, b의 P^m 승은 선형특성이 성립한다.

$$(a+b)^{p^m}=a^{p^m}+b^{p^m}$$

P5) GF(P^m)상에서 임의의 원소 a에 대하여 다음이 성립한다.

$$a^i \cdot a^j=a^{i+j(\mathrm{mod}\,p^m-1)}$$

P6) GF(P^m)상의 원소들은 $A(\alpha)=\sum_{i=1}^{m-1} A_i\alpha^i$로 표시되며, 각 A_i∈GF(P)의 원소이다.

이 때 GF(P^m)상에서의 m차 원시기약다항식의 임의의 한 원소 a를 가정하여 P^m개의 원소들 $\alpha_0,\alpha_1,\alpha_2,\ldots,\alpha_{m-1}$을 GF($P^m$)상의 벡터공간의 기저라고 한다. 이 기저를 표준기저라고 하며, 기저를 구성하는 모든 원소들은 선형독립이다. 단, α는 P를 변으로 하고 정수체 Z_P의 원소를 계수로 하는 m차 기약다항식의 근이며, P_i∈Z_P(i=0,1,2,…,m−1)이다. 표준기저는 유한체 및 디지털 연산 등에 폭넓게 이용되는 가장 일반적인 기저표현으로 관용기저(Conventional basis)라 한다.

2. 유한체 GF(P)의 연산

GF(P)상의 연산은 연산 결과를 P로 나눈 후 그 나머지만을 취하는 모듈러 연산을 말하며, 아래의 간단한

예를 통해 연산의 결과가 유한체에 닫혀있는지를 살펴본다.

가. GF(2)의 연산

GF(2)은 {0, 1}의 원소로 유한체를 구성하며, 이에 대한 가산과 승산에 대한 연산을 나타내면 표1과 같이 mod2에 의하여 연산된다. 가산 및 승산의 항등원으로 구성된 최소화 집합 {0, 1}은 최소의 유한체이며 GF(2)로 표기하고 이를 2진체(Binary field), 또는 기초체(Ground field)라 한다. 표 1에서 mod2 승산의 결과는 일반적인 산술 연산에서의 승산 결과와 동일하다. 따라서, 모듈러 승산의 연산기호 ⊙는 일반 승산의 연산기호 ●로 대치되어 사용되거나 또는 생략되기도 한다. 이후 본 논문에서의 모듈러 승산의 연산기호 ⊙를 가급적 생략하기로 하며 필요한 경우에 ●로 대치한다.

표 1. GF(2)의 연산표 (a) 가산 (b) 승산
Table 1. Arithmetic table over GF(2)

(a) Addition

⊕	0	1
0	0	1
1	1	0

(b) Multiplication

⊙	0	1
0	0	0
1	0	1

나. 원시원소와 원시기약다항식

기초체 GF(2)상의 연산은 1비트들의 연산으로 이루어진다. 기초체의 원소를 m비트로 확장하여 2^m개의 원소를 갖는 새로운 유한체를 구성 할 수 있으며, 이를 확장체(Extension field)라 하고 GF(2^m)으로 표현한다. GF(2^m)상의 임의의 한 원소 a를 가정하여, GF(2^m)를 구성하는 원소 집합은 식(1)과 같다.

$$GF(2^m)=\{0,1,\alpha^1,\alpha^2,\cdots,\alpha^{2m-3},\alpha^{2m-2}\} \quad (1)$$

식(1)로부터 GF(2^m)의 경우, 0을 제외한 모든 원소들은 α의 지수표현으로 나타낼 수 있다. 이와 같이 GF(2^m)상의 원소들을 표현하기 위해 사용되는 α를 GF(2^m)의 원시원소(Primitive element)라고 한다. 한편, GF(2^m)상의 임의의 변수 x를 가정하여 GF(2)상의 계수를 가지며 최고차항의 계수가 1인 다항식 P(x)를 가정하여 식(2)에 나타내었다.

$$P(x)=x^m+p_{m-1}x^{m-1}+\cdots+p_1x+p_0 \quad (2)$$

여기서, 0보다 크고 m보다 작은 차수를 갖는 GF(2^m)상의 어떤 다항식으로도 식(2)의 다항식 P(x)를 나눌 수 없을 때, 이 다항식 P(x)를 원시기약다항식(Primitive irreducible polynomial), 또는 간략히 기약다항식이라고 한다. GF(2)의 연산은 mod2 연산에 의해 유한체의 조건이 만족됨과 같이 GF(2^m)상의 모든 원소와 그 원소들 사이의 연산 결과는 원시기약다항식 P(α)에 대하여 모듈러P(x) 연산을 행하여 유한체의 조건을 만족시킬 수 있다. GF(2^m)상의 각 m에 대한 기약다항식은 여러 가지가 있을 수 있다. 하지만, 연산항의 최소화를 통해 보다 빠르고 간략한 연산이 행해질 수 있도록 최소의 항을 갖는 기약 다항식의 형태가 모듈로 연산에 주로 사용된다.

예를 들어 각 m=1부터 11까지 유한체 연산에 주로 사용되는 GF(2^m)상에서의 기약 다항식들을 표 2에 보였다.

표 2. GF(2^m)상의 원시기약다항식
Table 2. Primitive irreducible polynomials over GF(2^m).

m	GF(2^m)상의 P(x)
1	$x+1$
2	x^2+x+1
3	x^3+x+1
4	x^4+x+1
5	x^5+x^2+1
6	x^6+x+1
7	x^7+x+1
8	$x^8+x^4+x^3+x^2+1$
9	x^9+x^4+1
10	$x^{10}+x^3+1$
11	$x^{11}+x^2+1$

다. 확장체 GF(2^2) 연산

GF(4)상에서의 승산의 경우, 원소 2에 대하여 승산에 대한 역원을 가지고 있지 않기 때문에 체를 형성할 수 없으므로 확장체의 형태가 필요하다. 따라서 GF(2^2)로 나타내면 이는 GF(2)에 대한 확장체를 의미한다. 기약

표 3. GF(4)의 원소
Table 3. Elements over GF(4).

원소	a	1
0	0	0
1	0	1
a	1	0
a^2	1	1

표 4. GF(4)의 연산표 (a)승산 (b) 가산
Table 4. Arithmetic table over GF(4).

(a) Addition

⊕	0	1	A	B
0	0	0	0	0
1	0	1	A	B
A	0	A	B	1
B	0	B	1	A

(b) Multiplication

⊙	0	1	A	B
0	0	1	A	B
1	1	0	B	A
A	A	B	0	1
B	B	A	1	0

다항식 P(x)=x^2+x+1에 대한 근을 α라 할 때, GF(2^2)는 4개의 원소 {0, 1, α^1, α^2}로 유한체를 구성하며 {0, 1, A, B} 라고 표현한다. 기약다항식 P(x)=x^2+x+1의 근을 α라 하였으므로 근을 다항식에 적용하면 α^2+α+1=0이며, GF(2)에서 α^2=α+1이다. GF(4)에 대한 원소를 다항식의 형태로 표현하면 표 3과 같으며, 이 기약다항식의 원소들에 대하여, 승산 및 가산에 대한 모듈러연산을 행하면 표 4와 같이 표현된다.

Ⅲ. 듀얼기저 곱셈기

본 장에서는 표준 입/출력을 갖는 듀얼 기저 곱셈기를 설계하기 위하여 두 개의 입력부분을 받아들여 그 중 한 입력을 쌍대기저로 바꿔주는 표준-듀얼 기저변환회로모듈, 주어진 m차 기약 다항식에 의해 b_{m+k}를 발생시키는 b_{m+k}차 발생 연산 모듈, m^2개의 AND 게이트와 $m(m-1)$개의 EX-OR로 구성되는 다항식 승산 모듈, 듀얼기저로 표현되는 출력부분을 표준기저로 변화시켜주는 듀얼-표준 기저 변환 회로로 모듈을 제안하였다.

가. GF(2^m)상의 듀얼기저 병렬승산기의 구성

RS 부호의 인코더와 디코더에 사용되는 승산의 형태와 유사한 구조를 갖는 듀얼 기저 곱셈기는 두개의 입력부분 중 반드시 한쪽의 입력이 듀얼기저이며 승산의 결과도 듀얼기저로 표현된다.

$$\begin{bmatrix} f(a\beta) \\ f(a\beta\alpha) \\ \vdots \\ f(a\beta\alpha^{m-1}) \end{bmatrix}$$

$$= \begin{bmatrix} f(b\beta) & f(b\beta\alpha) & \cdots & f(b\beta\alpha^{m-1}) \\ f(b\beta\alpha) & f(b\beta\alpha^2) & \cdots & f(b\beta\alpha^m) \\ \vdots & \vdots & & \vdots \\ f(b\beta\alpha^{m-1}) & f(b\beta\alpha^m) & \cdots & f(b\beta\alpha^{2m-2}) \end{bmatrix} \cdot \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{bmatrix}$$

이 때 듀얼기저로 입력되는 부분을 표준-듀얼 기저 변환 회로를 사용하여 표준기저 입력부분으로 대치하고 또한, 승산의 결과를 표현되는 출력부분 역시 듀얼-표준 기저 변환 회로를 사용하여 표준기저 출력으로 바꿔준다면 두 개의 입력부분과 출력부분 모두 표준기저 의 형태를 유지하게 되어 승산기 전후에 붙게 되는 다른 모듈형태들과 상호 입출력 관계가 매끄럽게 이어지게 된다. 예를 들어 RS 부호의 복호과정 중에서 패리티 체크 행렬은 t중 오류정정일 경우 생성다항식이 $G(x)=(x+\alpha)(x+\alpha^2)\cdots(x+\alpha^{2t})$ 이고 부호 다항식 $C(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}$일 때 식(3)과 같다.

$$S = H \cdot C^T$$

$$\begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & \alpha & \cdots & \alpha^{n-1}) \\ 1 & \alpha^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{2t} & \cdots & (\alpha^{2t})^{n-1} \end{bmatrix} \cdot \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} \quad (3)$$

식(3)에서 패리티 체크 행렬(H)과 부호 행렬 모두 표준기저상의 입력이며 결과식인 신드롬 행렬(S) 또한 표준기저상의 출력으로 표현된다. 따라서 본 논문에서 제안한 승산기는 유한체상의 승산기에서 승산기의 호환성과 연계성을 고려해 표준 입출력을 갖고, RS 부호의 인코더와 디코더의 승산구조와 유사한 구조를 갖는 듀얼기저 승산기의 특성을 결합하고, 회로지연시간을 효과적으로 줄일 수 있고 VLSI 구현에 적합한 형태의 병렬구조를 갖는 표준 입/출력을 갖는 듀얼기저 병렬 승산기이다. 표준 입/출력을 갖는 GF(2^m)상의 상대기저 병렬 승산기를 설계하기 위해서 두 개의 입력부분 B, C를

받아들여 그 중 B입력을 듀얼기저로 바꿔주는 표준-듀얼 기저 변환회로 모듈과 주어진 m차 기약 다항식에 의해 b_{m+k}를 발생시키는 b_{m+k}차 발생 연산 모듈, m^2개의 AND 게이트와 $m(m-1)$의 EX-OR로 구성되는 다항식 승산 모듈, 듀얼기저로 표현되는 출력부분 A를 표준기저로 변화시켜주는 듀얼-표준 기저 변환회로 모듈이 필요하다. 표준기저 형태인 m비트 $B(\alpha)$와 $C(\alpha)$가 다항식 승산 모듈의 입력으로 들어갈 때 입력 $B(\alpha)$를 표준-듀얼 기저 변환 모듈을 거쳐서 듀얼기저 형태로 변환하여 다항식 연산 모듈의 입력으로 넣고, 주어진 기약다항식 $P(\alpha)$과 듀얼기저로 변환되어진 입력 $B(\alpha)$부터 b_{m+k}차의 계수를 발생시켜서 다항식 연산 모듈에 입력으로 들어가게 된다. 다항식 연산 모듈에서는 병렬 구조로 표준기저의 입력 $C(\alpha)$와 듀얼기저의 입력 $B(\alpha)$, b_{m+k}차 발생 모듈에서 발생된 b_m부터 b_{m+k}차의 계수들을 입력으로 받아들여 승산을 행하게 되고 듀얼기저의 형태인 $A(\alpha)$로 출력하게 된다. 이때 출력 $A(\alpha)$를 듀얼-표준 기저변환모듈을 거쳐서 표준기저의 형태인 $A(\alpha)$로 최종 출력하는 구조를 나타낸다.

나. 표준기저에서 듀얼기저로의 기저변환

본 절에서는 트레이스 함수를 이용한 기저변환 즉, 표준기저와 듀얼기저의 변환과정의 구현 가능함을 증명하고 $GF(2^4)$와 $GF(2^5)$상에서 상호 기저변환을 가능하게 하는 기저변환을 제안한다. 표준기저에서 듀얼기저로의 변환을 구현하는 회로를 설계하기 위하여 $GF(2^4)$상에서 이미 알고 있는 기저변환행렬 G와 표준기저로 표현되는 다항식 $A(x)$, $\{a_0, a_1, a_2, a_3\}$를 승산하여 듀얼기저로 표현되는 다항식 $B(x)$, $\{b_0, b_1, b_2, b_3\}$를 얻어내는 구조의 행렬식을 표현하면 식(4)와 같다.

$$B = G \cdot A$$

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} g_{00}\ g_{01}\ g_{02}\ g_{03} \\ g_{10}\ g_{11}\ g_{12}\ g_{13} \\ g_{20}\ g_{21}\ g_{22}\ g_{23} \\ g_{30}\ g_{31}\ g_{32}\ g_{33} \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \quad (4)$$

식(4)에서 변환행렬 G는 고전적인 선형 블록 부호에서 생성행렬과 같이 간주되며 듀얼기저의 부호 중에서 선형독립인 행들로 구성한다. 변환 행렬 G를 구성하는 과정은 다음과 같다. 표준기저 A의 임의의 원소 α^0는 {1 0 0 0}으로 표현되고 이는 듀얼기저 B의 {0 0 0 1}로 변환됨을 알 수 있다. 이에 변환을 다음과 같은 행렬식으로 표현될 수 있다.

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} g_{00}\ g_{01}\ g_{02}\ g_{03} \\ g_{10}\ g_{11}\ g_{12}\ g_{13} \\ g_{20}\ g_{21}\ g_{22}\ g_{23} \\ g_{30}\ g_{31}\ g_{32}\ g_{33} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

여기서, 변환행렬의 첫 번째 열 g_{00}=0, g_{10}=0, g_{20}=0, g_{30}=1을 구할 수 있다.

표준기저 A의 임의의 원소 α^1는 {0 1 0 0}으로 표현되고 이는 듀얼기저 B의 {0 0 1 0}로 변환됨을 알 수 있다.

$$\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0\ g_{01}\ g_{02}\ g_{03} \\ 0\ g_{11}\ g_{12}\ g_{13} \\ 0\ g_{21}\ g_{22}\ g_{23} \\ 1\ g_{31}\ g_{32}\ g_{33} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

여기서, 변환행렬의 두 번째 열 g_{01}=0, g_{11}=0, g_{21}=1, g_{31}=0을 구할 수 있다.

표준기저 A의 임의의 원소 α^2는 {0 0 1 0}으로 표현되고 이는 듀얼기저 B의 {0 1 0 0}로 변환됨을 알 수 있다.

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0\,0\ g_{02}\ g_{03} \\ 0\,0\ g_{12}\ g_{13} \\ 0\,1\ g_{22}\ g_{23} \\ 1\,0\ g_{32}\ g_{33} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

여기서, 변환 행렬의 세 번째 열 g_{02}=0, g_{12}=2, g_{22}=0, g_{32}=0을 구할 수 있다.

마지막으로, 표준기저 A의 임의의 원소 α^3는 {0 0 0 1}으로 표현 되고 이는 듀얼기저 B의 {1 0 0 1}로 변환됨을 알 수 있다.

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0\,0\,0\ g_{03} \\ 0\,0\,1\ g_{13} \\ 0\,1\,0\ g_{23} \\ 1\,0\,0\ g_{33} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

여기서 변환행렬의 4번째 열 g_{03}=1, g_{13}=0, g_{23}=0, g_{33}=1을 얻을 수 있다.

따라서 위의 과정에서 순차적으로 얻은 열들로 변환 행렬을 구성하면 식(5)와 같다.

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 0\,0\,0\,1 \\ 0\,0\,1\,0 \\ 0\,1\,0\,0 \\ 1\,0\,0\,1 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} \tag{5}$$

식(5)에서 정리한 표준-듀얼 기저변환행렬을 검증하기 위하여 $GF(2^4)$상에서 표준기저상의 원소 α^5와 α^8에 대한 듀얼기저상의 원소를 구하면 다음과 같다.

표준기저상의 원소 $\alpha^5$$\{0\ 1\ 1\ 0\}$는 변환행렬 G에 적용하여 다음 행렬식에 의해 듀얼기저상의 $\{0\ 1\ 1\ 0\}$로 변환된다.

$$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0\,0\,0\,1 \\ 0\,0\,1\,0 \\ 0\,1\,0\,0 \\ 1\,0\,0\,1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

표준기저상의 원소 $\alpha^8$$\{1\ 0\ 1\ 0\}$는 변환 행렬 G에 적용하여 다음 행렬식에 의해 듀얼기저상의 $\{0\ 1\ 0\ 1\}$로 변환된다.

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0\,0\,0\,1 \\ 0\,0\,1\,0 \\ 0\,1\,0\,0 \\ 1\,0\,0\,1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

표준기저에서 듀얼기저로 변화된 결과 값은 모두 정의한 표준-듀얼 기저변환과 동일하게 변환되었음을 알 수 있다. 식 (5)는 다시 식(6)의 형태로 변환할 수 있고, $GF(2^4)$상에서 기약다항식 $P(x)=x^4+x+1$라 할 때 다음과 같은 선형 결합 형태의 변환 회로가 가능해진다.

$$\begin{bmatrix} 0\,0\,0\,1 \\ 0\,0\,1\,0 \\ 0\,1\,0\,0 \\ 1\,0\,0\,1 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} a_3 \\ a_2 \\ a_1 \\ a_0 + a_3 \end{bmatrix} \tag{6}$$

각각의 표준기저상의 다항식 $A(x)$, $\{a_0, a_1, a_2, a_3\}$는 식(6)에서 보인 전달 행렬 G에 의해 듀얼기저로 표현되는 다항식 $B(x)$, $\{b_0, b_1, b_2, b_3\}$로 표준-듀얼 기저변환 할 때, 전달 행렬 G의 4번째 행을 제외한 나머지 행들은 추가적인 소자의 연결 없이 서로 교차 연결 하고 4번째 행만이 단지 하나의 EX-OR 게이트만을 사용하여 표준기저의 $\{b_0, b_1, b_2, b_3\}$으로 기저 변환됨을 알 수 있다.

Ⅳ. 결 론

본 논문에서는 유한체상에서 표준 입/출력을 갖는 $GF(2^m)$상의 듀얼기저 곱셈기를 제안하였다. 본 논문의 곱셈기로는 표준-듀얼 기저변환부, 듀얼-표준 기저 변화부, b_{m+k}차 발생 연산부, 다항식 승산 연산부로 구성되며 각 연산부들은 모두 모듈구조를 가지므로 m에 대한 확장과 회로의 구현이 용이하다. 제안된 회로들은 회로구현에 필요한 소자를 AND 게이트와 EX-OR 게이트로 한정하였고, 병렬 연산형식을 취하면서도 신호 입력의 시간차를 위한 시간지연회로 및 메모리소자를 필요로 하지 않는다. 따라서, 본 논문에서 제안한 승산 회로는 그 구조의 정규성, 다른연산 모듈과의 호환성, 소자종류의 단순화 등에 의해 VLSI에 매우 유리한 구조를 갖는다.

REFERENCES

[1] A. Menezes, I. Blake, S. Gao, R. Mullin, S. Vanstone and T. yaghoobian, Applications of Finite Fields. Kluwer Academic Publisher, 1993.

[2] C.E. Shannon, “A Mathematical Theory of Communication,” Bell Syst. Thch. J., 27, pp. 379-423(part I), pp. 623-656 (part II), 2009.

[3] M.T. Lee, Error Correcting Coding Theory, McGraw-Hill, New York, 2010.

[4] R.W. Hamming, “Error Detecting and Error Correcting Codes,” Bell Syst. Thch. J., 29, pp. 147-160, 2011.

[5] J. Zhou and O. C. Au,“On the Security of Chaotic Convolutional Coder,” *IEEE Transaction of Circuit and Systems*, Vol.58, No.3, pp.595-606, Mar. 2011.

[6] P. A. Scott, S. E. Tarvares and L. E. Peppard, “A Fast Multiplier for GF(2^m),” *IEEE J. Select. Areas Commum.*, vol. SAC-4, Jan. 2010.

[7] E.D. Mastrovito, “VLSI Design for Multiplication over Finite Fields,” *LNCS-357, Proc. AAECC-6*, pp. 297-309, Rome, July 2012.

[8] J. L. Imaña,“Low Latency Polynomial Basis Multiplier,‘ *IEEE Transaction on Circuit and Systems*, Vol.58 No.5, pp935-946, May 2011.

[9] J. Adikari, A. Barsoum, M.A. Hasan, A.H.

Namin, C. Negre,"Improved Area-Time Tradeoffs for Field Multiplication Using Optimal Normal Bases," *IEEE Transactions on Computers*, Vol.62, No.1, pp.193 - 199, Jan. 2013.

저 자 소 개

박 춘 명(평생회원)

1983년 인하대학교 공과대학 전자공학과 공학사.
1886년 인하대학교 대학원 전자공학과(정보공학전공) 공학석사.
1994년 인하대학교 대학원 전자공학과(정보공학전공) 공학박사.
1995년～현재 한국교통대학교 컴퓨터공학과 교수
1984년～현재 대한전자공학회 평생회원 / IEEE Computer Society Member
2002년～2003년 UCI(University of California, Irvine) 교환교수
2009년 대한전자공학회 컴퓨터소사이어티 회장 / 본회 부회장
2010년～현재 대한전자공학회 컴퓨터소사이어티 명예회장
2014년 현재 한국정보통신학회 부회장
2014년 현재 대한임베디드공학회 상임이사
<주관심분야 : 차세대 디지털논리시스템 및 컴퓨터구조, 차세대 회로 및 시스템, 임베디드컴퓨터시스템, e-Learning 시스템 등>