Journal of The Institute of Electronics and Information Engineers Vol.53, NO.2, February 2016 http://dx.doi.org/10.5573/ieie.2016.53.2.070
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2016-53-2-9

다항식에 기초한 유한체상의 P=2인 경우의 곱셈기 설계

(Design of the Multiplier in case of P=2 over the Finite Fields based on the Polynomial)

박 춘 명*

(Chun-Myoung Park©)

요 약

본 논문에서는 다항식에 기초하여 유한체상의 P=2인 경우의 효율적인 곱셈기를 구성하는 방법을 제안하였다. 제안한 곱셈기 회로는 다항식의 연산부와 mod F(α) 연산부, 모듈러 연산부로 구성된다. 또한, 이들 각 연산부는 모듈 구조를 가지므로 m의 확장에 따른 회로 구성이 용이하며 회로 구성에 사용한 소자는 AND 게이트와 XOR 게이트만으로 구성하여 정규성, 확장성이 용이하며 이를 기반으로 VLSI화에 적합하다. 제안한 곱셈기는 기존의 곱셈기에 비해 좀 더 콤펙트, 규칙적, 정규성과 확장성이 용이하며 최근의 IoT 환경에서의 여러 분야에 적용 및 응용이 가능할 것이다.

Abstract

This paper proposes the constructing method of effective multiplier based on the finite fields in case of P=2. The proposed multiplier is constructed by polynomial arithmetic part, mod F(α) part and modular arithmetic part. Also, each arithmetic parts can extend according to m because of it have modular structure, and it is adopted VLSI because of use AND gate and XOR gate only. The proposed multiplier is more compact, regularity, normalization and extensibility compare with earlier multiplier. Also, it is able to apply several fields in recent hot issue IoT configuration.

Keywords : Polynomial, primitive irreducible polynomial, arithmetic operation, module, transformation etc

Ⅰ. 서 론

최근의 초고도화 정보융합 분야의 핵심인 ICT 분야에 있어 유한체상의 연산은 매우 중요한 분야[1~4]로 대두되고 있다. 특히 최근의 ICT 분야의 Hot Issue인 IoT 분야의 핵심 영역에 유한체상의 연산은 통신 채널 및 저장매체에서 발생하는 오류를 정정하기 위한 오류정정[5-7] 회로로 부터 진보된 컴퓨터 등의 분야에 활용된다. 또한 차세대의 성장 동력 산업용 메모리, 디지털 레이더 신호처리, 이동통신, 위성통신, 패킷 스위칭 시스템, CD, DAT로 손꼽히는 디지털 보안 및 서명, 디지털 워터마킹 가정용 보안시스템, RF용 스마트카드 등 유한체상의 연산에 대한 응용유한체 승산의 전개기법과 그 회로의 구성기법은 모두 정규화, 고속화, 간략화에 초점을 맞추어 VLSI에 적합한 하드웨어 구조의 개발을 그 목표로 하였다. 특히 소수 P=2인 유한체상의 곱셈은 신호처리와 화상처리 분야에서 특별한 계산을 요하거나 범용 컴퓨터 계산의 고속화를 보조하는 고성능 컴퓨터 설계에도 응용[8~10]되고 있다.

* 평생회원, 한국교통대학교 컴퓨터공학과
(Department of Computer Engineering, Korea National University of Transportation)
© Corresponding Author(E-mail: cmpark@ut.ac.kr)
※ 이 논문은 2014년도 한국교통대학교 교내학술연구비의 지원을 받아 수행한 연구임
Received ; December 16, 2015 Revised ; December 26, 2015
Accepted ; January 22, 2016

Ⅱ. 유한체

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, 환, 체 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 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))

Property 1) GF(P^m)상에서 임의의 원소 a에 대한 영원의 곱은 0이다. a • 0=0

Property 2) GF(P^m)상에서 임의의 원소 a의 P배는 0이다. P • a=0

Property 3) GF(P^m)상에서 a≠0인 경우에 대하여 임의의 원소 a의 P^m 승은 a이다.

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

Property 4) GF(P^m)상에서 양의 정수 m에 대하여 임의의 두 원소 a, b의 P^m 승은 선형특성이 성립한다.

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

Property 5) GF(P^m)상에서 임의의 원소 a에 대하여 다음이 성립한다.

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

Property 6) 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 관용기저라 한다. 이외의 유한체상의 성질은 증명없이 참고문헌을 참조하였다.

Ⅲ. 원시원소와 기약다항식

기초체 GF(2)상의 연산은 1 비트들의 연산으로 이루어진다. 기초체의 원소를 m 비트로 묶어 2^m개의 원소를 갖는 유한체로 확장할 수 있으며, 이를 확장체라 하고 GF(2^m)으로 표시한다. GF(2^m)상의 임의의 한 원소 α를 가정하여, GF(2^m)을 구성하는 2^m개의 원소를 표현하면 식(1)과 같다.

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

0과 1은 각각 기초체의 원소이므로 모든 확장체의 원소가 된다. 식(1)에서 보인 GF(2^m)의 모든 원소들은 α의 지수형식으로 표현하기 위해 0은 α^*으로, 1은 α^0으로 각각 표현하였다. 식(1)과 같이 GF(2^m) 상의 모든 원소들을 표현하기 위해 사용되는 α를 원시원소라 한다. 한편, GF(2^m)상의 임의의 변수 x를 가정하여 GF(2)상의 계수를 가지며 최고차 항의 계수가 1인 다항식 F(x)를 가정하여 식(2)에 나타내었다.

표 1. GF(2m)상의 가약다항식

Table 1. Irreducible Polynomials over GF(2m).

m	GF(2^m)상의 F(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

F(x) = xm+fm-1xm-1+ .... +f2x2+f1x+f0 (2)

0 보다 크고 m보다 작은 차수를 갖는 GF(2^m)상의 어떤 다항식으로도 식(2)의 다항식 F(x)를 나눌 수 없을 때, 다항식 F(x)를 원시기약다항식, 또는 간략히 기약다항식이라 한다. GF(2)상의 연산은 mod2 연산에 의해 유한체의 조건이 만족됨과 같이 GF(2^m)의 모든 원소와 그 연산의 결과는 modF(x) 연산에 의해 유한체의 조건을 만족시킬 수 있다. GF(2^m)상의 각 m에 대한 기약다항식은 유일하지는 않다. 그러나 연산항의 최소화를 통해 빠르고 간략한 연산을 이루기 위해 최소의 항을 갖는 기약다항식이 모듈러 연산에 주로 사용된다. GF(2^m)상의 각 m=1 부터 9까지 유한체 연산에 자주 인용되는 대표적 기약다항식들을 표1에 보였다.

Ⅳ. 표준기저를 적용한 유한체의 원소표현

모듈러 연산의 정의에 의해, 0≤i≤2^m-2인 i에 대하여 α^i에 대한 modF(α) 연산은 식(3)과 같이 표현된다.

$$\alpha^i = Q(\alpha)F(\alpha) + R(\alpha) \quad (3)$$

식(3)의 Q(α)는 α^i를 기약다항식 F(α)로 나누어 구한 몫이며, R(α)은 그 나머지이다. 모듈러 연산의 정의에 의해, 식(3)에서 α^i=R(α)이 되며, 이때 R(α)는 (m-1)차 이하의 다항식으로 표현된다. 따라서, GF(2^m)상의 모든 원소들에 대한 modF(α) 연산의 결과는 (m-1)이하의 차수를 갖는 다항식이 되며 식(4)와 같다.

GF(2m) = {0,1,α1,α2, ⋯ ,αq-2}

= {am-1αm-1+ ⋯ +a1α1+a0} (4)

식(4)에서 $\alpha^{m-1},\cdots,\alpha,1$들은 다항식을 이루는 기저가 되며, 각 기저들의 계수 a_{m-1}, ⋯, a_1, a_0들은 모두 GF(2)의 원소이다. 식(4)의 다항식에서 선형결합을 이루는 m개의 기저들을 표준기저라 한다. 표준기저는 유한체 및 디지털연산 등에 폭넓게 이용되는 가장 일반적인 기저표현으로 관용기저로도 알려져 있다. 식(4)와 같이 GF(2^m)상의 원소들을 표준기저들의 선형결합으로 표현하는 기법을 다항식표현기법이라 한다. 또한, 이를 보다 간략화하여 기저들의 계수만을 취해 이진수열로 표현하는 기법을 벡터표현기법이라 한다.

Ⅴ. 원시원소와 기약다항식

1. 1차 다항식 곱셈

GF(2)상의 원소들을 계수로 갖는 1차 다항식 $S_1(x)$과 $T_1(x)$을 식(5)에 보였다.

$$S_1(x) = s_1x + s_0 \quad (5)$$
$$T_1(x) = t_1x + t_0$$

$S_1(x)$과 $T_1(x)$는 모두 2개의 항으로 구성된 2항식의 구조를 갖는다. $S_1(x)$과 $T_1(x)$를 곱셈하여 전개하면 2차 다항식이 유도되며, 이를 P'(x)라 할 때 식(6)과 같다.

$$p'(x) = S_1(x)T_1(x) = p_2'x^2 + p_1'x + p_0' \quad (6)$$

2항식 S1(x)과 $T_1(x)$의 각 계수들로부터 P'(x)의 계수를 표현하기 위해 다음과 같은 정의1을 하였다.

[정의 1]

식(5)에서 보인 $S_1(x)$과 $T_1(x)$의 각 계수들로부터 보조항 $d_{ll[2]}$, $d_{hl[2]}$, $d_{hh[2]}$를 식(7)과 같이 정의한다.

$$d_{ll[2]} = s_0t_0 \quad (7)$$
$$d_{hl[2]} = (s_1 \oplus s_0)(t_1 \oplus t_0)$$
$$d_{hh[2]} = S_1t_1$$

2. 2차 다항식 곱셈

GF(2)상의 원소들을 계수로 갖는 2차 다항식 $S_2(x)$와 $T_2(x)$를 식(8)에 보였다.

$$S_2(x) = s_2x^2 + s_1x + s_0 \quad (8)$$
$$T_2(x) = t_2x^2 + t_1x + t_0$$

$S_2(x)$와 $T_2(x)$는 모두 3개의 항으로 구성된 3항식의 구조를 갖는다. $S_2(x)$와 $T_2(x)$를 곱셈하여 전개하면 4차 다항식이 유도되며, 이를 P'(x)라 할 때 식(9)와 같다.

$$P'(x) = S_2(x)\,T_2(x) = p_4'x^4 + p_3'x^3 + p_2'x^2 + p_1'x + p_0' \quad (9)$$

3항식 $S_2(x)$와 $T_2(x)$의 각 계수들로부터 P'(x)의 계수를 표현하기 위해 다음과 같은 정의3을 하였다.

[정의 3]

식(8)에서 보인 $S_2(x)$와 $T_2(x)$의 각 계수들로부터 보조항 $d_{ll[3]}$, $d_{mm[3]}$, $d_{hh[3]}$, $dh_{m[3]}$, $d_{hl[3]}$, $d_{ml[3]}$를 식(10)과 같이 정의한다.

$$\begin{aligned} d_{ll[3]} &= s_0 t_0 \\ d_{mm[3]} &= s_1 t_1 \\ d_{hh[3]} &= s_2 t_2 \\ d_{hm[3]} &= (s_2 \oplus s_1)(t_2 \oplus t_1) \\ d_{hl[3]} &= (s_2 \oplus s_0)(t_2 \oplus t_0) \\ d_{ml[3]} &= (s_1 \oplus s_0)(t_1 \oplus t_0) \end{aligned} \quad (10)$$

3. 2항식 곱셈 전개

양의 정수 m과 n을 가정하여 다항식을 구성하는 항의 수가 $m=2^n$개로 주어지는 (m-1)차 다항식은 2항식으로 구성되며 다음과 같이 확장하여 적용할 수 있다.

GF(2)상의 원소들을 계수로 가지며, 그 항의 수가 $m=2^n$인 (m-1)차 다항식 A(x)와 B(x)를 식(11)에 보였다.

$$\begin{aligned} A(x) &= a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0 \\ B(x) &= b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_1x + b_0 \end{aligned} \quad (11)$$

식(11)에서 보인 A(x)와 B(x)는 그 항의 수를 $m=2^n$개로 가정하였으므로, 각각 m/2개의 항을 갖는 다항식들로 표현이 가능하며 식(12)와 같이 2항식으로 나타낼 수 있다.

$$\begin{aligned} A(X) &= a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0 \\ &= x^{m/2}(a_{m-1}x^{m/2-1} + a_{m-2}x^{m/2-2} + \cdots + a_{m/2+1}x + a_{m/2}) \\ &\quad + (a_{m/2}x^{m/2-1} + a_{m/2-2}x^{m/2-2} + \cdots + a_1x + a_0) \\ &= x^{m/2}A_h(x) + A_1(x) \end{aligned}$$

$$\begin{aligned} B(X) &= b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_1x + b_0 \\ &= x^{m/2}(b_{m-1}x^{m/2-1} + b_{m-2}x^{m/2-2} + \cdots + b_{m/2+1}x + b_{m/2}) \\ &\quad + (b_{m/2}x^{m/2-1} + b_{m/2-2}x^{m/2-2} + \cdots + b_1x + b_0) \\ &= x^{m/2}B_h(x) + B_1(x) \end{aligned} \quad (12)$$

식(12)에서 보인 2항식의 각 계수 다항식들 $A_h(x)$, $A_l(x)$, $B_h(x)$, $B_l(x)$로부터 A(x)와 B(x)의 곱셈을 전개하기 위해 다음 정의2를 하였다.

[정의 2]

식(12)에서 보인 A(x)와 B(x)의 각 계수다항식들 $A_h(x)$, $A_l(x)$, $B_h(x)$, $B_l(x)$로 부터 다음 식(13)과 같이 정의하였다.

$$\begin{aligned} D_{ll[2]}(x) &= A_l(x)B_l(x) \\ D_{hh[2]}(x) &= A_h(x)B_h(x) \\ D_{hl[2]}(x) &= [A_h(x) + A_l(x)][B_h(x) + B_l(x)] \end{aligned} \quad (13)$$

4. 3항식 곱셈 전개

양의 정수 m과 n을 가정하여 다항식을 구성하는 항의 수가 $m=3^n$개로 주어지는 $(m-1)$차 다항식은 삼분에 의해 3항식으로 구성되며 다음과 같이 확장하여 적용할 수 있다.

다항식들의 각 계수들이 모두 $GF(2)$상의 원소임을 가정한 $m=3^n$인 $(m-1)$차 다항식 $A(x)$와 $B(x)$를 각각 $m/3$개의 항을 갖는 다항식들로 식(14)에 보였다.

$$\begin{aligned} A(x) &= a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0 \\ &\quad + (a_{(2m/3)-1}x^{(m/3)-1} + a_{(2m/3)-2}x^{(m/3)-2} + \cdots + a_{m/3})x^{m/3} \\ &\quad + (a_{(m/3)-1}x^{(m/3)-1} + a_{(m/3)-2}x^{(m/3)-2} + \cdots + a_0) \\ &= A_h(x)x^{2m/3} + A_m(x)x^{m/3} + A_l(x) \\ B(x) &= b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_1x + b_0 \\ &= (b_{m-1}x^{(m/3)-1} + b_{m-2}x^{(m/3)-2} + \cdots + b_{2m/3})x^{(2m)/3} \end{aligned}$$

$$+ (b_{(2m/3)-1}x^{(m/3)-1} + b_{(2m/3)-2}x^{(m/3)-2} + \cdots + b_{m/3})x^{m/3}$$
$$+ (b_{(m/3)-1}x^{(m/3)-1} + b_{(m/3)-2}x^{(m/3)-2} + \cdots + b_0)$$
$$= B_h(x)x^{2m/3} + B_m(x)x^{m/3} + B_1(x) \quad (14)$$

[정의 3]

식(14))에서 보인 3항식의 각 계수다항식들 $A_h(x)$, $A_m(x), A_l(x), B_h(x), B_m(x), B_l(x)$로부터 $A(x)$와 $B(x)$의 각 계수다항식들로부터 곱셈전개에 필요한 식(15)와 같이 정의하였다.

$$D_{ll[3]}(x) = A_l(x)B_l(x)$$
$$D_{mm[3]}(x) = A_m(x)B_m(x)$$
$$D_{hh[3]}(x) = A_h(x)B_h(x)$$
$$D_{hm[3]}(x) = [A_h(x) + A_m(x)][B_h(x) + B_m(x)]$$
$$D_{hl[3]}(x) = [A_h(x) + A_l(x)][B_h(x) + B_l(x)]$$
$$D_{ml[3]}(x) = [A_m(x) + A_l(x)][B_m(x) + B_l(x)] \quad (15)$$

5. modF(α) 연산

$GF(2^m)$상의 모든 원소들은 mod$F(a)$연산에 의해 $m-1$차 이하의 다항식으로 표현된다. 즉, $GF(2^m)$상의 원소 a^m은 기약다항식 $F(\alpha)=\alpha^m+f_{m-1}\alpha^{m-1}+ \ldots + f_0$를 적용한 mod$F(a)$ 연산에 의해 식(16)과 같이 $(m-1)$ 이하의 차수를 갖는 다항식으로 표현된다.

$$a^m{}_{\mathrm{mod}F(a)} = f_{m-1}a^{m-1} + f_{m-2}a^{m-2} + \cdots + f_0 \quad (16)$$

기약다항식에 의한 모듈러 연산식을 유도하기 위해 임의의 양의 정수 i를 가정하여 a^{m+i}에 mod$F(a)$ 연산한 결과로 표현된 $m-1$차 다항식의 각 계수들에 대한 표기를 정의4에 정의하였다.

[정의 4]

양의 정수 i에 대하여 $GF(2^m)$상의 원소 a^{m+i}에 mod$F(a)$ 연산한 결과를 $m-1$차 이하의 다항식으로 표현할 수 있으며, 이를 식(17)에 나타내었다.

$$a^{m+i} = f_{m-1}{}^{[i]}a^{m-1} + f_{m-2}{}^{[i]}a^{m-2} + \cdots + f_1{}^{[i]}a + f_0{}^{[i]} \quad (17)$$

식(17)에서 우항의 각 계수들에 표기한 위 첨자 $[i]$는 좌항 a의 차수 $m+i$에서의 i를 나타낸다.

식(17)의 첨자 i에 0을 대입하면 다음 식(18)과 같다.

$$a^{m+0} = f_{m-1}{}^{[0]}a^{m-1} + f_{m-2}{}^{[0]}a^{m-2} + \cdots + f_1{}^{[0]}a + f_0{}^{[0]} \quad (18)$$

식(18)에서 우항의 각 계수들에 표기한 위 첨자 [0]은 좌항 a의 차수 $m+i$에서 $i=0$임을 나타낸다. 식(16)과 식(18)은 모두 a^m에 mod$F(a)$ 연산하여 유도한 동일식이므로 두 식의 각 계수들을 비교하여 $f_{m-1}{}^{[0]} = f_{m-1}, f_{m-2}{}^{[0]} = f_{m-2}, \cdots, f_0{}^{[0]} = f_0$임을 확인할 수 있다.

한편, 식(17)에 $i=1$을 적용하면 식(19)와 같다.

$$a^{m+1} = f_{m-1}{}^{[1]}a^{m-1} + f_{m-2}{}^{[1]}a^{m-2} + \cdots + f_1{}^{[1]}a + f_0{}^{[1]} \quad (19)$$

Ⅵ. 결 론

본 논문에서는 다항식에 기초하여 유한체상의 P=2인 경우의 효율적인 곱셈기를 구성하는 방법을 제안하였다. 제안한 곱셈기 회로는 다항식의 연산부와 mod F(α) 연산부, 모듈러 연산부로 구성된다. 또한, 이들 각 연산부는 모듈 구조를 가지므로 m의 확장에 따른 회로 구성이 용이하며 회로 구성에 사용한 소자는 AND 게이트와 XOR 게이트 만으로 구성하여 정규성, 확정성이 용이하며 이를 기반으로 VLSI화에 적합하다. 제안한 곱셈기는 기존의 곱셈기에 비해 좀 더 컴펙트, 규칙적이고, 정규성과 확장성이 용이하며 최근의 IoT 환경에서의 여러 분야에 적용 및 응용이 가능하다. 향 후 연구과제로서는 제안한 곱셈기를 최근의 체세대 ICT 분야에 분야에 적용하는 것으로 현재 연구 진행 중이다.

REFERENCES

[1] Jabir, A.M, Pradhan D.K. and Mathew J.,'GfXpress: A Technique for Synthesis and Optimization of Polynomials', IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, pp.698-711, Vol.27, Issue 4, 2008.
[2] Tummeltshammer P., Hoe J.C. and Puschel M.,'Time-Multiplexed Multiple-Constant Multiplication', IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, pp.1551-1563, vol.26, Issue 9, 2007.
[3] Fenn S.T.J., Benaissa. M. and Taylor, D.,'Finite field inversion over the dual basis,' IEEE Transactions on Very Large Scale Integration (VLSI) Systems, pp.134-137, Vol. 4, Issue 1, 1996.
[4] Imaña. J.L.,'Low Latency Polynomial Basis Multiplier,' IEEE Transactions on Circuits and Systems I, pp.935-946, Vol. 58, Issue 5, 2011.
[5] Psarakis, M., Gizopoulos, D. and Paschalis, A.'Built-in sequential fault self-testing of array multipliers,' IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, pp.449-460, Vol. 24, Issue 3, 2005.
[6] Paar C., Fleischmann P. and Soria-Rodriguez P.,'Fast arithmetic for public-key algorithms in Galois fields with composite exponents', IEEE Transactions on Computers, pp.1025-1034, Vol.48, Issue 10, 1999.
[7] Poolakkaparambil M., Mathew J., Jabir. A.M. and Pradhan, D.K.,'A Low-Complexity Multiple Error Correcting Architecture Using Novel Cross Parity Codes Over GF,' IEEE Transactions on Very Large Scale Integration (VLSI) Systems, pp.1448-1458, Vol.23, Issue 8, 2015.
[8] Dimitrakopoulos G. and Paliouras V.,'A novel architecture and a systematic graph-based optimization methodology for modulo multiplication,' IEEE Transactions on Circuits and Systems I, pp.354-370, Vol. 51, Issue 2, 2004.
[9] Jain S.K., Leilei Song and Parhi K.K.,'Efficient semisystolic architectures for finite-field arithmetic,' IEEE Transactions on Very Large Scale Integration (VLSI) Systems, pp.101-113, Vol. 6, Issue 1, 1998.
[10] Elleithy K.M. and Bayoumi M.A.,'A systolic architecture for modulo multiplication,' IEEE Transactions on Circuits and Systems II, pp.715-729, Vol. 42, Issue 11, 1995.

저 자 소 개

박 춘 명(평생회원)
전자공학회 논문지 제51권 제6호 (Vol.51, No.6) 참조
<주관심분야 : 차세대 디지털논리시스템 및 컴퓨터구조, 차세대 회로 및 시스템, 임베디드컴퓨터시스템, 차세대 e-learning 시스템 등>