論文2002-39SC-4-5

$GF(p^m)$상에서 모든 항의 계수가 0이 아닌 기약다항식에 대한 병렬 승산기의 설계

(Design of a Parallel Multiplier for Irreducible Polynomials with All Non-zero Coefficients over $GF(p^m)$)

朴 承 用 *, 黃 鍾 學 **, 金 興 壽 ***

(Seung-Yong Park, Jong-Hak Hwang, and Heung-Soo Kim)

요 약

본 논문에서는 유한체 $GF(P^m)$상에서 모든 항의 계수가 이 아닌 두 다항식의 승산 알고리즘을 제시하였다. 제시된 승산 알고리즘을 이용하여 모듈 구조의 병렬 입-출력 승산기를 구성하였다. 제시된 승산기는 $(m+1)^2$개의 동일한 셀로 구성되었으며, 각각의 셀은 1개의 $mod(p)$ 가산 게이트와 1개의 $mod(p)$ 승산 게이트로 구성되었다. 본 논문에서 제시된 승산기는 클럭이 필요하지 않고 m개의 $mod(p)$ 가산 게이트 지연시간과 1개의 $mod(p)$ 승산 게이트 소자 지연시간만을 필요로 한다. 또한, 제시된 승산기는 규칙성과 셀 배열에 의한 모듈성을 가지므로 VLSI 회로 실현에 적합할 것이다.

Abstract

In this paper, we proposed a multiplicative algorithm for two polynomials with all non-zero coefficients over finite field $GF(P^m)$. Using the proposed multiplicative algorithm, we constructed the multiplier of modular architecture with parallel in-output. The proposed multiplier is composed of $(m+1)^2$ identical cells, each cell consists of one mod(p) additional gate and one mod(p) multiplicative gate. Proposed multiplier need one mod(p) multiplicative gate delay time and m mod(p) additional gate delay time not clock. Also, our architecture is regular and possesses the property of modularity, therefore well-suited for VLSI implementation.

Keyword : 승산기, GF, 유한체, 병렬승산기, 다치논리

I. 서 론

유한체(Galois field)는 오류정정부호, 디지털 통신의 암호화 및 해독화를 요하는 보안 등에 많이 응용되고 있다. 이들 중 오류정정부호의 경우 유한체 $GF(2^m)$상의 연산에서 실제로 부호기 및 복호기 설계시 전체 시스템의 규모와 성능에 절대적인 영향을 미치므로 회로 경로의 연결, 시스템 구조의 복잡성과 동시성등의 문제점을 개선하기 위한 연구가 진행되어 왔다[1].

* 正會員, 才能大學 컴퓨터情報系列
(Dept. of Computer & Information, Jaenueng Collage)
** 正會員, 體育科學研究院
(Korea Sport Science Institute)
*** 正會員, 仁荷大學校 電子工學科
(Dept. of Electronic Eng., Inha University)
接受日字:2001年12月12日, 수정완료일:2002年6月25日

유한체 연산은 가산, 승산, 멱산, 제산 등인데, 가산은 매우 간단하여 유한체의 원소(field elements)들이 다항식 형태로 표현되는 경우 매우 간단한 회로로 수행될 수 있다.

1984년 Yet 등[2]은 유한체 $GF(2^m)$상에서 $AB+C$ 연산을 수행하는 병렬 입-출력 시스토릭(systolic)구조를 갖는 승산기를 개발하였다. 그 이후 많은 병렬 시스토릭 승산기가 제안되었으나,[3-5] 이 승산기들은 시스템의 복잡성으로 인해 암호 시스템 응용에는 비 효율적이었다. 그 후 Hasan 등[6]은 유한체 $GF(2^m)$상에서의 모듈 구조를 갖는 저 복잡성 병렬 승산기를 설계하였다.

Koc와 Sunar[7]는 계수가 모두 1인 기약 다항식(irreducible All One Polynomial : AOP)을 기반으로 하는 저 복잡성 비트-병렬(bit-parallel) 정규 및 표준기저 승산기를 발표하였으며, Wu 등[8, 9]은 약한 이중 기저(weakly dual basis)를 이용한 저 복잡성 비트-병렬 승산기를 제안하였다. 위에서 제안된 저복잡성 승산기들이 암호시스템 응용에 적합하다 하더라도 시스토릭 기술을 이용하여 설계된 것이 아니기 때문에 m이 클 경우 $GF(2^m)$상에서 승산에 대한 지연시간은 매우 크다.

본 논문에서는 C.Y. Lee 등[10]이 제시한 AOP를 기반으로 하는 유한체 $GF(2^m)$상에서의 승산 알고리즘을 $GF(P^m)$상으로 확장하여 모든 항에 0이 아닌 계수가 존재하는 원시 기약다항식에 대한 승산 알고리즘을 제안하였다. 제시된 승산 알고리즘을 이용하여 병렬 입-출력 모듈구조의 승산기를 구성하였으며, 제시된 승산기는 $(m+1)^2$개의 동일한 셀로 구성되었으며, 1개의 셀은 1개의 2 입력 $mod(p)$ 가산 게이트와 1개의 2 입력 $mod(p)$ 승산 게이트로 구성되었다.

Ⅱ. 유한체 $GF(p^m)$상에서의 승산 알고리즘

유한체 $GF(P^m)$은 p가 임의의 소수이고, m이 양의 정수인 p^m개의 원소를 갖는다. 모든 항이 존재하는 원시 기약다항식은 다음과 같이 표현된다.

$$F(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{m-1} x^{m-1} + f_m x^m \quad (1)$$

$F(x)$는 최고 차수가 m이고, $f_i \in GF(p)$, $0 \le i \le m$이다. 본 논문에서는 식 (1)에 대하여 두 다항식을 승산하는 승산 알고리즘을 제시하고자 한다. α를 유한체 $GF(P^m)$상의 원시원이라 할 때 0원(zero element)을 제외한 p^m-1개의 모든 유한체 원소들은 α의 멱(power)으로 표현된다. 가 식 (1)의 근이라고 하면, $F(\alpha)=0$이므로

$$F(\alpha) = f_0 + f_1\alpha + f_2\alpha^2 + \cdots + f_{m-1}\alpha^{m-1} + f_m\alpha^m = 0 \quad (2)$$

로 표현된다. 식 (2)에서 최고차 항의 계수 $f_m = p-1$이면, α^m은 식 (3)과 같이 쓸 수 있다.

$$-(p-1)\alpha^m = f_0 + f_1\alpha + f_2\alpha^2 + \cdots + f_{m-1}\alpha^{m-1} \quad (3)$$

식 (3)에서 유한체의 성질에 의해서 $-(p-1)$은 1과 같으므로 식 (4)와 같이 쓸 수 있다.

$$\alpha^m = f_0 + f_1\alpha + f_2\alpha^2 + \cdots + f_{m-1}\alpha^{m-1} \quad (4)$$

식 (4)와 같이 유한체 $GF(P^m)$상의 각 원소들은 차수가 $m-1$ 이하의 α의 다항식으로 표현된다. 두 다항식을 승산하였을 때, α^m 보다 큰 차수들에 대하여 알아보기 위하여 먼저 α^{m+1}에 대한 식을 구하면 식 (5)와 같다.

$$\begin{aligned}\alpha^{m+1} &= \alpha^m \cdot \alpha \\ &= f_0\alpha + f_1\alpha^2 + f_2\alpha^3 + \cdots + f_{m-2}\alpha^{m-1} + f_{m-1}\alpha^m \end{aligned} \quad (5)$$

식 (5)에 식 (4)를 대입하면 식 (6)과 같다.

$$\begin{aligned}\alpha^{m+1} &= f_0\alpha + f_1\alpha^2 + f_2\alpha^3 + \cdots + f_{m-2}\alpha^{m-1} \\ &\quad + f_{m-1}(f_0 + f_1\alpha + f_2\alpha^2 + \cdots + f_{m-1}\alpha^{m-1}) \\ &= f_0 f_{m-1} + (f_0 + f_1 f_{m-1})\alpha + (f_1 + f_2 f_{m-1})\alpha^2 \\ &\quad + \cdots + (f_{m-2} + f_{m-1} f_{m-1})\alpha^{m-1} \end{aligned} \quad (6)$$

여기서, $\alpha^{m+1}=1$이 되기 위하여 식 (6)에서 식 (7)이 성립하여야 한다.

$$\begin{aligned} &f_0 f_{m-1} + (f_0 + f_1 f_{m-1})\alpha + (f_1 + f_2 f_{m-1})\alpha^2 + \cdots \\ &+ (f_{m-2} + f_{m-1} f_{m-1})\alpha^{m-1} = 1 \end{aligned} \quad (7)$$

따라서 식 (7)을 만족하기 위하여 각 계수들은

$$f_0 f_{m-1} = 1 \quad (8)$$

$$f_0 + f_1 f_{m-1} = 0 \quad (9)$$

$$f_1 + f_2 f_{m-1} = 0 \quad (10)$$

$$\vdots$$

$$f_{m-2} + f_{m-1} f_{m-1} = 0 \quad (11)$$

이 되어야 한다. 이제 [단계 1]~[단계 4]의 과정을 통

하여 식 (8)-(11)이 성립되기 위한 f_i 즉, f_0부터 $f_m=1$ 까지의 계수들을 구한다.

[단계 1] 식 (7)에서 $f_0 f_{m-1}=1$이 되기 위해서는 $f_0=1$, $f_{m-1}=1$이어야 한다.

[단계 2] 식 (8)에서 $f_0+f_1 f_{m-1}=0$이 되기 위해서 [단계 1]에서 구한 $f_0=1$을 대입하면 $f_1=p-1$이어야 한다.

[단계 3] 식 (9)에서 $f_1+f_2 f_{m-1}=0$이 되기 위해서 [단계 2]에서 구한 $f_1=p-1$을 대입하면 $f_2=1$이어야 한다.

[단계 4] 같은 방법으로 대입하여 구하면 $f_{m-2}=p-1$이어야 한다.

단계 1~단계 4에 의해서 α^{m+1}의 식 (6)는 상수 항 $f_0 f_{m-1}$만 1이고 나머지 계수들은 모두 0이 되어 α^{m+1}은 식 (12)와 같이 된다.

$$\alpha^{m+1}=\alpha^m\cdot\alpha=1 \tag{12}$$

따라서, 다음과 같이 정리할 수 있다.

[정리] $f_i\in GF(p)$일때

$$f_i=\begin{cases}1 & i\text{는 짝수}\\ p-1 & i\text{는 홀수}\end{cases}$$

$$0\le i\le m-1$$

m=홀수, p=임의의 소수

식 (12)를 이용하여 α^{m+2}, α^{m+3},…, α^{m+i},…, α^{2m}를 구하면 다음의 결과를 얻을 수 있다.

$$\begin{aligned}
&\alpha^{m+2}=\alpha^{m+1}\cdot\alpha=\alpha\\
&\alpha^{m+3}=\alpha^{m+2}\cdot\alpha=\alpha^2\\
&\alpha^{m+4}=\alpha^{m+3}\cdot\alpha=\alpha^3\\
&\cdot\\
&\alpha^{m+i}=\alpha^{i-1}\\
&\cdot\\
&\alpha^{2m}=\alpha^{m-1}
\end{aligned} \tag{13}$$

α가 유한체 $GF(P^m)$상에서 차 기약 다항식의 근이라 할 때, 두 다항식을 승산하기 위하여 승산 다항식 와 피승산 다항식 를 식 (14)와 같이 표현하였다.

$$\begin{aligned}
A&=a_0+a_1\alpha+a_2\alpha^2+\cdots+a_m\alpha^m\\
B&=b_0+b_1\alpha+b_2\alpha^2+\cdots+b_m\alpha^m
\end{aligned} \tag{14}$$

다항식 A, B를 승산하면 식 (15)와 같다.

$$\begin{aligned}
A\cdot B&=(a_0+a_1\alpha+a_2\alpha^2+\cdots+a_m\alpha^m)\\
&\cdot(b_0+b_1\alpha+b_2\alpha^2+\cdots+b_m\alpha^m)\\
&=(\sum_{i=0}^{m}a_i\alpha^i)(\sum_{i=0}^{m}b_i\alpha^i)
\end{aligned} \tag{15}$$

두 다항식의 승산결과인 식 (14)를 D로 놓으면, 식 (16)과 같이 표현할 수 있다.

$$\begin{aligned}
D&=d_0+d_1\alpha+d_2\alpha^2+\cdots+d_{2m}\alpha^{2m}\\
&=\sum_{i=0}^{2m}d_i\alpha^i\\
&=\sum_{i=0}^{m}d_i\alpha^i+\sum_{i=m+1}^{2m}d_i\alpha^i
\end{aligned} \tag{16}$$

식 (16)의 두 번째 항 $\sum_{i=m+1}^{2m}d_i\alpha^i$는 식 (13)을 이용하여 식 (17)과 같이 표현할 수 있다.

$$\begin{aligned}
D&=\sum_{i=0}^{m}d_i\alpha^i+\sum_{i=0}^{m-1}d_{m+i+1}\alpha^i\\
&=\sum_{i=0}^{m-1}(d_i+d_{m+i+1})\alpha^i+d_m\alpha^m
\end{aligned} \tag{17}$$

식 (17)에서 $d_i+d_{m+i+1}=D_i$, $d_m=D_m$이라 놓으면 식 (18)과 같이 표현된다.

$$\begin{aligned}
D&=\sum_{i=0}^{m-1}D_i\alpha_i+D_m\alpha^m\\
&=\sum_{i=0}^{m}D_i\alpha^i
\end{aligned} \tag{18}$$

이상과 같이 유도된 승산 알고리즘을 $GF(P^m)$상에서 $p=2$, $p=4$인 경우에 대하여 예를 들었다.

[예] $m=4$인 경우의 승산 다항식 A와 피승산 다항식 B가 다음과 같이 표현될 때,

$$\begin{aligned}
A&=a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3+a_4\alpha^4\\
B&=b_0+b_1\alpha+b_2\alpha^2+b_3\alpha^3+b_4\alpha^4
\end{aligned}$$

$GF(2^4)$상에서 두 다항식 A, B를 승산하면 다음과 같다.

$$
\begin{array}{cccccccccc}
 & \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 \\
\hline
 & a_0 & a_1 & a_2 & a_3 & a_4 & & & & \\
\times & b_0 & b_1 & b_2 & b_3 & b_4 & & & & \\
\hline
 & a_0b_0 & a_1b_0 & a_2b_0 & a_3b_0 & a_4b_0 & & & & \\
 & & a_0b_1 & a_1b_1 & a_2b_1 & a_3b_1 & a_4b_1 & & & \\
 & & & a_0b_2 & a_1b_2 & a_2b_2 & a_3b_2 & a_4b_2 & & \\
 & & & & a_0b_3 & a_1b_3 & a_2b_3 & a_3b_3 & a_4b_3 & \\
+ & & & & & a_0b_4 & a_1b_4 & a_2b_4 & a_3b_4 & a_4b_4 \\
\hline
 & d_0 & d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7 & d_8
\end{array}
$$

식 (13)으로부터 α^5, α^6, α^7, α^8은 다음과 같이 α^0, α^1, α^2, α^3로 변환할 수 있다.

$i=1$ 인 경우 $\alpha^5=\alpha^0$
$i=2$ 인 경우 $\alpha^6=\alpha^1$
$i=3$ 인 경우 $\alpha^7=\alpha^2$
$i=4$ 인 경우 $\alpha^8=\alpha^3$

따라서, α^5항 이하의 계수들은 α^0, α^1, α^2, α^3항의 계수들과 가산하여 구할 수 있다.

D_0, D_1, D_2, D_3, D_4는 식 (18)을 이용하여 다음과 같이 쓸 수 있다.

$$
\begin{aligned}
D_0 &= d_0 + d_5 \\
D_1 &= d_1 + d_6 \\
D_2 &= d_2 + d_7 \\
D_3 &= d_3 + d_8 \\
D_4 &= d_4
\end{aligned}
$$

$D_0 \sim D_4$를 구하면 식 (19)과 같다.

$$
\begin{aligned}
D_0 &= a_0b_0 + a_4b_1 + a_3b_2 + a_2b_3 + a_1b_4 \\
D_1 &= a_1b_0 + a_0b_1 + a_4b_2 + a_3b_3 + a_2b_4 \\
D_2 &= a_2b_0 + a_1b_1 + a_0b_2 + a_4b_3 + a_3b_4 \\
D_3 &= a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 + a_4b_4 \\
D_4 &= a_4b_0 + a_3b_1 + a_2b_2 + a_1b_3 + a_0b_4
\end{aligned}
\qquad (19)
$$

Ⅲ. 승산기 구성

본 장에서는 2장에서 제시한 승산 알고리즘을 이용하여 승산기를 구성할 것이다. 먼저 [예]에서 구한 $GF(2^4)$에서의 승산기를 구성하기 위하여 그림 1과 그림 2에 표시한 1개의 2 입력 $mod(2)$ 가산 게이트와 1개의 2 입력 $mod(2)$ 승산 게이트로 구성된 셀이 필요

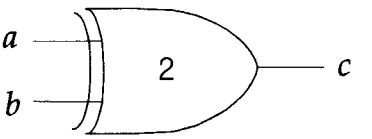


그림 1. $mod(2)$ 가산 게이트
Fig. 1. The $mod(2)$ additional gate.

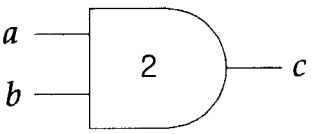


그림 2. $mod(2)$ 승산 게이트
Fig. 2. The $mod(2)$ multiplicative gate.

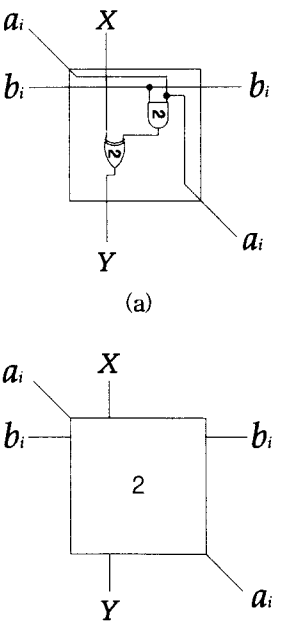


그림 3. $GF(2^4)$상의 승산기에 사용된 기본 셀
Fig. 3. The basic cell used in the multiplier on $GF(2^4)$.

하며, 승산기에 사용된 셀을 그림 3에 나타내었다. 여기서 a_i와 b_i는 각각 승산 다항식 A와 피승산 다항식 B의 계수를 뜻하며, 또한 셀 내부의 2는 $GF(P^m)$에서의 $p=2$를 의미한다. 그리고 X는 승산기 구성시 윗단 셀의 출력을 의미하며, Y는 셀의 출력을 나타낸다.

그림 4는 제시된 승산 알고리즘을 이용하여 [예]의 결과에 따라 구현한 $GF(2^4)$에서의 승산기 회로도이며, $D_0 \sim D_4$는 승산결과의 다항식에서 $\alpha^0 \sim \alpha^4$항의 계수이다. 이 승산기는 병렬 입-출력 모듈구조로서, $(m+1)^2$개 즉, 36개의 동일한 셀로 구성되었으며, 회로는 클럭(clock)신호에 의해 동작하는 것이 아니고 각 셀의 소자 지연시간에 의해 결과가 출력되므로 이 승산기는 $m+1$의 지연시간을 갖는다. 또한 이 구조는 전체적으로 매우 적은 결선이 요구된다.

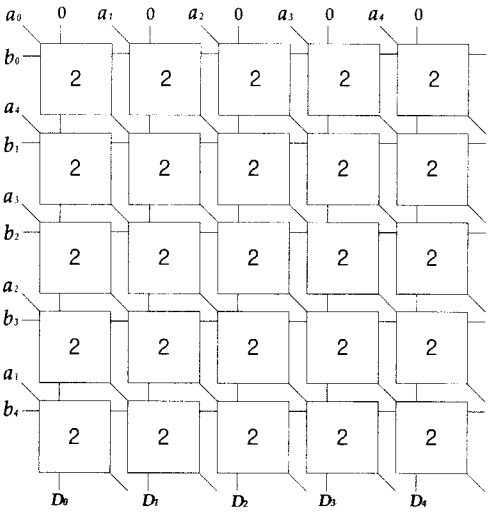


그림 4. $GF(2^4)$상의 제안된 승산기
Fig. 4. The proposed multiplier on $GF(2^4)$.

위 에서는 $GF(2^4)$상에 대하여 예를 들었지만 제시된 승산 알고리즘은 $GF(P^m)$상의 p치에 대해서도 그대로 확장 적용할 수 있다. $GF(P^m)$상에서의 승산기를 구성하기 위하여 1개의 2 입력 $mod(p)$ 가산 게이트와 1개의 2 입력 $mod(p)$ 승산 게이트로 구성된 셀이 필요하며, p치 승산에 사용된 셀은 그림 7과 같이 셀 내부에 P로 표시하였다. 여기서 $mod(p)$ 가산 게이트와 $mod(p)$ 승산 게이트는 두 원소를 $mod(p)$가산 및 승산하기 위한 게이트를 말하며, a_i와 b_i는 각각 승산 다항식 A와 피승산 다항식 B의 계수를 의미한다.

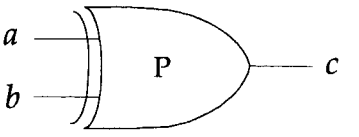


그림 5. $mod(p)$가산 게이트
Fig. 5. The $mod(p)$ additional gate.

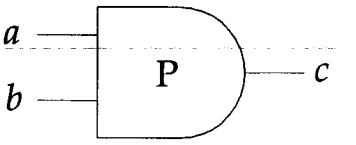


그림. 6. $mod(p)$승산 게이트
Fig. 6. The $mod(p)$ multiplicative gate.

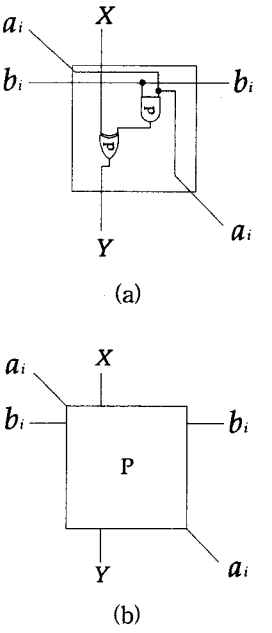


그림 7. $GF(P^m)$상의 승산기에 사용된 기본 셀
Fig. 7. The basic cell used in the multiplier on $GF(P^m)$.

그림 8은 제시된 승산 알고리즘을 이용한 $GF(P^m)$상에서의 승산기 회로도이다. 이 승산기는 $(m+1)^2$ 개의 동일한 셀로 구성되었으며, 모듈구조를 갖는 병렬 입-출력 승산기이다. 그림 8에서 b_i는 가로 위치에 놓인 모든 셀과 연결되어 있고 a_i는 우측방향으로 내려가는 대각선 위치에 놓인 셀들과 연결되어 있으며, $m+1$의 지연시간을 갖는다.

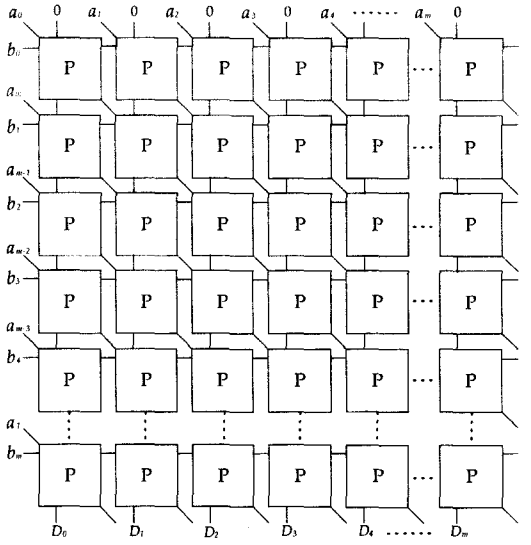


그림 8. $GF(P^m)$상의 제안된 승산기
Fig. 8. The proposed multiplier on $GF(P^m)$.

Ⅳ. 비교 및 검토

본 논문에서는 $GF(P^m)$상에서 임의의 p(p는 소수)치로 승산하는 승산 알고리즘을 제안하였다. p치 승산 알고리즘을 위하여 원시 기약다항식에 대한 정리를 새롭게 제시하였으며, Yeh[2]와 Wei[3], 그리고 Lee[10]의 논문과 비교하기 위하여 p가 2인 경우로 하였다. 이들 중 특히 p가 2인 경우에 대하여 기존에 제안한 Lee의 논문과 비교해 볼 때, Lee의 논문은 두 가지 연산 즉, 순환이동(cyclic shifting)과 내적(inner product)을 이용한 2치 승산 알고리즘을 제시하였으나, 본 논문에서는 2치를 확장하여 임의의 p치로 승산하는 회로를 구성하기 위하여 병렬 입-출력 승산 알고리즘을 제안하였다. 또한 Lee가 제시한 승산기 구성도에는 1 비트 래치를 사용하였으나 본 논문에서는 사용하지 않았다. 왜냐하면 입력 값이 미리 입력되어 있어도 결과는 마찬가지이기 때문이다. 이들 승산기들의 비교결과는 표 1과 같다.

표 1. 비교표
Table 1. The table of comparison.

승산기 / 항 목	Yeh[2]	Wei[3]	Lee[10]	본 논문
셀당 회로 복잡성				
2 입력 AND게이트	2	3	1	1
2 입력 XOR게이트	2	1	1	1
3 입력 XOR게이트	0	1	0	0
1 비트 latch	7	10	3	0
전체 게이트 수				
2 입력 AND게이트	$2m^2$	$3m^2$	$(m+1)^2$	$(m+1)^2$
2 입력 XOR게이트	$2m^2$	m^2	$(m+1)^2$	$(m+1)^2$
3 입력 XOR게이트	0	m^2	0	0
1 비트 latch	$7m^2$	$10m^2$	$4(m+1)^2$	0
셀당 지연시간	T_A+T_X $+2T_L$	T_A+T3_X $+2T_L$	T_A+T_X $+T_L$	T_A+T_X
전체 지연시간	3m	3m	m+1	m+1

[주] T_A = 2 입력 AND 게이트의 지연시간
T_X = 2 입력 XOR 게이트의 지연시간
$T3_X$ = 3 입력 XOR 게이트의 지연시간
T_L = 래치의 지연시간

Ⅴ. 결 론

본 논문에서는 유한체 $GF(P^m)$상에서 모든 항에 0이 아닌 계수가 존재하는 원시 기약 다항식에 대한 승산 알고리즘을 제시하였으며, 제시된 승산 알고리즘을 이용하여 병렬 입-출력 모듈구조의 승산기를 구성하였다. 제시된 승산 알고리즘은 2치 뿐만 아니라 다항식의 계수가 $p-1$인 다치 승산기로 확장 적용할 수 있다.

제시된 승산기는 $(m+1)^2$개의 동일한 셀로 구성되었으며, 1개의 셀은 1개의 $mod(p)$ 가산 게이트와 1개의 $mod(p)$ 승산 게이트로 구성되었고, 클럭이 필요하지 않고 소자 지연시간만 필요하므로, m개의 $mod(p)$ 가산 게이트 지연시간과 1개의 $mod(p)$ 승산 게이트 소자 지연시간 만을 필요로 한다. 또한 제시된 승산기는 규칙성과 셀 배열에 의한 모듈성을 가지므로 VLSI회로 실현에 적합할 것이다. 향후 연구는 m이 홀수인 경우가 아닌 짝수인 경우까지 확대하여 그에 대한 승산 알고리즘과 회로를 구현하고 집적회로를 제작하여야 할 것이다.

참 고 문 헌

[1] S.L. Hurst, "Multiple-Valued Logic-its Future," IEEE Trans. Computers, vol 30, pp. 1161-1179, Dec. 1984.

[2] C.S. Yeh, I.S. Reed, and T.K. Truong, "Systolic Multipliers for Finite Fields $GF(2^m)$," IEEE Trans. Computers, vol. 33, no. 4, pp. 357-360, Apr. 1984.

[3] S.W. Wei, "A Systolic Power-Sum Circuit for $GF(2^m)$," IEEE Trans. Computers, vol. 43, no. 2, pp. 226-229, Feb. 1994.

[4] C.L. Wang, "Bit-Level Systolic Array for fast Exponentiation in $GF(2^m)$," IEEE Trans. Computers, vol. 43, no. 7, pp. 838-841, July 1994.

[5] J.J. Wonziak, "Systolic Dual Basis Serial Mutiplier," IEE Proc. Computers and Digital Technology, vol. 145, no. 3, pp. 237-241, July 1998.

[6] M.A. Hasan, M.Z. Wang, and V.K. Bhargava, "Moduler Construction of Low Complexity Parallel Multipliers for a Class of Finite Fields $GF(2^m)$," IEEE Trans. Computers, vol. 41, no. 8, pp. 961-971, Aug. 1992.

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

[8] H. Wu and M.A. Hasan, "Low Complexity Bit-Paralell Multipliers for a Class of Finite Fields," IEEE Trans. Computers, vol. 47, no. 8, pp. 883-887, Nov. 1998.

[9] H. Wu and M.A. Hasan and L.F. Blake, "New Low-Complexity Bit-Parallel Finite Fields Multipliers Using Weekly Dual Basis," IEEE Trans. Computers, vol. 47, no. 11 pp. 1223-1234, Nov. 1998.

[10] 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. Computers, vol. 50, no. 5, pp. 385-392, May 2001.

[11] 황종학, 박승용, 신부식, 김홍수 "멀티플렉서를 이용한 $GF(2^m)$ 상의 승산기," 전자공학회 논문지, 제37권, SC편, 제7호, pp. 35-41, 2000년 7월

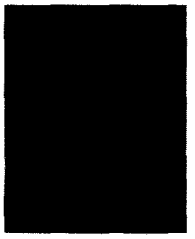
[12] T,Itoh and S.Tsujii, "Structure of Parallel Multipliers for a Class of Fields $GF(2^m)$," Inform. Comp., vol. 83, pp.21-40, 1989.

[13] 황종학, 심재환, 최재석, 김홍수, "$GF(2^m)$상의 기약 3 항식을 이용한 승산기 설계," 전자공학회 논문지, 제37권, SC편, 제1호, pp. 27-34, 2000년 1월

[14] P.E. Scott, S.e. Tavares, L.E. Peppard, "A Fast VLSI Multiplier for $GF(2^m)$," IEEE Journal Selected Areas in Comunications, SAL-4, no. 1, pp. 62-65, Jan. 1986.

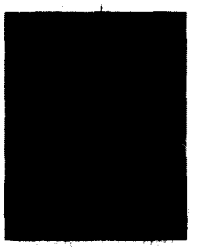
[15] 성현경, 김홍수, "$GF(2^m)$상의 셀배열 승산기의 구성." 전자공학회 논문지, 제26권, 제4호, pp. 81-87, 1989년 4월

저 자 소 개



朴 承 用(正會員)

1979년 : 인하대학교 전자공학과 학사. 1982년 : 인하대학원 전자공학과 석사. 1999년 : 인하대학원 전자공학과 박사과정수료. 1985년~현재 : 재능대학 컴퓨터정보계열 교수. <주관심분야 : 컴퓨터시스템 및 네트워크>



黃 鐘 學(正會員)

1988년 : 인하대학교 전자공학과 학사. 1990년 : 인하대학원 전자공학과 석사. 2001년 : 인하대학원 전자공학과 공학박사. 1990~1992년 : ㈜필코 부설연구소 연구원. 1992~1995년 : 나우정밀 전임연구원. 1996년~현재 : 체육과학연구원 선임연구원. <주관심분야 : 이동통신, 체육기자재, FPGA설계>

金 興 壽(正會員) 第37卷 SC編 第4號 參照