Journal of The Korea Society of Computer and Information
Vol. 18, No. 2, February 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.2.009

유한체 GF(2^m)상의 기약다항식의 모든 계수가 1을 갖는 고속 병렬 승산기의 설계

성 현 경*

Design of High-Speed Parallel Multiplier with All Coefficients 1's of Primitive Polynomial over Finite Fields GF(2^m)

Hyeon-Kyeong Seong *

요 약

본 논문에서는 유한체 $GF(2^m)$상에서 모든 항에 0이 아닌 계수가 존재하는 기약 다항식을 이용한 두 다항식에 대한 승산 알고리즘을 제시하였으며, 제시된 승산 알고리즘을 이용하여 고속의 병렬 입-출력 모듈구조의 승산기를 설계하였다. 제시한 승산기의 구성은 m^2개의 동일한 기본 셀들로 설계되었으며, 제시한 기본 셀은 2입력 XOR 게이트와 2입력 AND 게이트로 구성하였다. 셀에 래치를 사용하지 않았으므로 회로가 간단하며, 셀당 지연시간이 $D_A + D_X$이다. 본 연구에서 제안한 승산기는 규칙성과 셀 배열에 의한 모듈성을 가지므로 m이 큰 회로의 확장이 용이하며 VLSI회로 실현에 적합할 것이다.

▸ Keywords : 유한체, $GF(2^m)$, 병렬승산기, 기약다항식, 셀배열

Abstract

In this paper, we propose a new multiplication algorithm for two polynomials using primitive polynomial with all 1 of coefficient on finite fields $GF(2^m)$, and design the multiplier with high-speed parallel input-output module structure using the presented multiplication algorithm. The proposed multiplier is designed m^2 same basic cells that have a 2-input XOR gate and a 2-input AND gate. Since the basic cell have no a latch circuit, the multiplicative circuit is very

• 제1저자 : 성현경 • 교신저자 : 성현경
• 투고일 : 2012. 11. 29, 심사일 : 2013. 2. 7, 게재확정일 : 2013. 2. 12.
* 상지대학교 컴퓨터정보공학부(School of Computer Information & Communication Eng., Sangji University)
※ 이 논문은 2011년도 상지대학교 교내 연구비 지원에 의해 연구되었음.

simple and is short the delay time $D_A + D_X$ per cell unit. The proposed multiplier is easy to extend the circuit with large m having regularity and modularity by cell array, and is suitable to the implementation of VLSI circuit.

▸ Keywords : Finite fields, $GF(2^m)$, Parallel multiplier, Primitive polynomials, Cell array

I. 서 론

유유한체는 오류정정부호, 스위칭이론 및 암호이론 등의 분야에 널리 적용되고 있는 연산체계이다. 유한체에서 중요하게 다루어지는 연산으로는 가산, 승산, 제산, 승산에 대한 역원 등이 있으며, 회로 복잡도와 처리속도를 고려한 최적의 연산 알고리즘을 찾기 위한 연구가 오랜 기간 지속되고 있다[1-3]. 특히, Galois field (GF) 연산은 Reed-Solomon 채널코딩과 디코딩 구조에 일반적으로 사용된다[4]. Reed-Solomon(RS) 코드는 무선통신 채널에 대하여 오류검출과 정정을 제공한다. 예를 들면, 3GPP/EDGE/E-TCH 블록 부호화/복호화는 보통 $GF(2^8)$으로 구현된다[5]. 그러나 RS 부호기와 복호기는 여러 가지 유한체 승산과 가산을 요구한다. 유한체 연산에서 가산은 간단하게 수행되는 반면에 승산은 상당한 계산량을 요구한다. 그러므로 승산에 대한 효과적인 구현을 갖는 것이 중요하게 되었다.

유한체에서 중요한 연산은 가산, 승산, 멱승, 제산, 승법적 역원 등이다. 이들 중 승산은 암호화 및 해독화 알고리즘에 자주 사용되며, 제산과 멱승, 승법적 역원 등은 승산을 반복적으로 적용하여 수행할 수 있기 때문에 승산은 가장 중요하다. 따라서 회로의 저복잡성이 용이하게 실현될 수 있는 빠른 승산 알고리즘 개발이 중요하다.

$GF(2^m)$의 원소를 표현할 때 표준 기저 표현법을 사용할 경우 곱셈 알고리즘은 승수의 처리 순서에 따라 LSB 우선과 MSB 우선 방법으로 구분되며, 일반적으로 LSB 우선 곱셈 알고리즘이 MSB 우선 곱셈 알고리즘에 비해 적은 계산 지연시간을 갖는다. 또한 $GF(2^m)$상의 승산기는 비트-병렬 및 비트-직렬 구조 승산기로 구분할 수 있으며, 일반적으로 비트-병렬형은 비트-직렬형에 비해 데이터 처리율이 높지만, 하드웨어가 복잡해지는 단점이 있다. 최근 빠른 처리속도와 복잡도를 고려한 VLSI 구현에 있어 규칙성과 모듈화가 매우 중요시되면서 이에 대한 적합한 유한체 승산기 설계에 관한 연구가 활발히 진행되고 있으며, 병렬 승산기 구조의 경우 회로는 복잡하지만 빠른 연산처리 능력을 가지고 있으므로 최근에 많이 연구되고 있다[6].

Yeh 등[7]은 표준기저를 사용하여 유한체 $GF(2^m)$상에서 $AB+C$ 연산을 수행하는 병렬 입-출력 시스토릭 구조의 승산기를 개발하였다. 이 승산기는 하나의 셀에 2개의 2-입력 AND 게이트와 2개의 2-입력 XOR 게이트를 사용하였다. 그러나 이 승산기는 VLSI화에는 적합하였으나 데이터가 역류하는 현상을 갖는다. Itoh와 Tsujii[8]는 시스템의 복잡성을 줄이기 위하여 $GF(2^m)$상에서 다항식의 계수가 모두 1인 m차 기약 AOP(All One Polynomial)와 m차 기약 ESP(Equally Spaced Polynomial)를 기반으로 하는 모듈 구조의 저복잡성 승산기를 설계하였다. Wang과 Lin[9]은 Yeh 등이 제안한 시스토릭 승산기의 회로 복잡성을 개선하기 위하여 2개의 2-입력 XOR 게이트 대신에 1개의 3-입력 XOR 게이트를 사용하였다.

Lee 와 Lu[10]은 유한체 $GF(2^m)$상에서 기약 AOP를 기반으로 하는 순환이동과 내적이라는 두 연산을 이용한 승산 알고리즘을 제안하였다. 그리고 그 알고리즘을 기반으로 저복잡성 비트-병렬 시스토릭 승산기를 구성하였다. 첫 번째 승산기는 1개의 2-입력 AND 게이트와 1개의 2-입력 XOR 게이트, 3개의 1 비트 래치회로로 이루어진 $(m-1)^2$개의 동일한 셀들로 구성하였고, 또 하나의 승산기는 $(m+1)^2$개의 동일한 셀들과 m개의 XOR 게이트로 구성하였는데, 각 셀은 1개의 2-입력 AND 게이트와 1개의 2-입력 XOR 게이트, 4개의 1 비트 래치회로로 구성하였다. 각각의 승산기는 각 셀에서의 지연시간이 짧기 때문에 속도가 빠르다.

Wang 등[11]은 Sunar와 Koc에 의해 제안된 병렬형 승산기로부터 유도된 직렬형과 병렬형 승산기의 일종인 타입 II 최적 정규기저에서 수행하는 새로운 종류의 승산기를 개발하였다. 이 승산기는 ModelSim 도구로 시뮬레이션하였고, Xilinx의 ISE로 합성하였다. Xilinx의 FPGA 장비로 실현된 회로기판 실험이 회로기판에서 80MHz에서 동작한다. Petra 등[12]은 Mastrovito 승산기의 첫 번째 블록의 최소-영역 실현과 Matrovito 승산기의 두 번째 블록의 고속 지연

유도 나무구조를 이용하여 새로운 승산기를 개발하였으며, 승산기의 복잡성과 지연시간에 대하여 여러 다항식을 분석적으로 평가하였다. 제안된 승산기는 실제 응용에서 사용할 수 있도록 (255, 239) Reed-Solomon 디코더를 해석할 수 있도록 0.25㎛ CMOS 기술로 실현함으로써 증명하였다. Wu 등[13]은 유한체에서 기약 AOP(All One Polynomial)와 기약 ESP(Equally Spaced Polynomial)를 기반으로 하는 약한 이중 기저를 이용한 저 복잡성 비트-병렬 승산기를 제안하였으며, Halbutogullari 등[14]은 일반적인 기약다항식에 대한 병렬 승산기를 제안하였다. 이들이 제안한 유한체상의 승산기들은 보안 및 암호시스템 응용에 적합하다 할지라도 시스토릭 기술을 이용하여 설계된 것이 아닌 경우에는 m이 클 경우 $GF(2^m)$상의 곱셈에 대한 지연시간은 매우 큰 것이 단점이다. 이들의 연구 이외에도 많은 연구결과들이 도출되어 왔으며, 이들은 각각 독특한 회로설계 알고리즘과 회로구성으로 그 효용성을 입증 받았으며, 보다 개선된 회로구현을 위한 연구는 계속될 것으로 전망된다.

본 논문에서는 Lee 등이 제시한 AOP를 기반으로 하는 유한체 $GF(2^m)$상에서 모든 항에 0이 아닌 계수가 존재하는 기약다항식의 두 원소에 대한 승산 알고리즘을 제안하였다. 먼저 $GF(2^m)$상에서 AOP를 기반으로 하여 확장기저를 이용한 기약다항식에 대한 두 원소의 승산 알고리즘을 제시하고, $GF(2^4)$상에서 예를 들어 승산결과를 구하였다. 또한 $GF(2^m)$상에서 제시된 승산 알고리즘을 이용하여 고속의 병렬 입-출력 모듈구조의 승산기를 설계하였다. 본 논문에서 제안한 회로구성의 특징중 하나인 회로구성의 모듈화 및 블록화에 따라, 현재 통신분야에 널리 적용되고 있는 $GF(2^8)$상의 승산회로를 포함하여 m에 대한 일반화된 회로설계가 용이하다.

II. 유한체 $GF(2^m)$상에서의 승산 알고리즘

유한체 $GF(2^m)$은 p가 소수(prime number)이고 m이 양의 정수인 p^m개의 원소들을 갖는다. 유한체 $GF(2^m)$은 2개의 원소들을 갖는 기초체 $GF(2)$의 확대체이다. 즉, 유한체 $GF(2)$는 {0,1}의 원소들을 구성한다[3,15,16]. $GF(2^m)$에서 모든 산술연산은 그 결과를 mod(2) 연산을 함으로써 이루어진다. $GF(2^m)$의 0이 아닌 모든 원소들은 원시원소 α에 의해 생성되며, α는 $GF(2^m)$의 원시 기약 다항식 $F(x)=0$의 근이다.

$$F(x)=\sum_{i=0}^{m} f_i \cdot x^i = f_0+f_1x+f_2x^2+\cdots+f_{m-1}x^{m-1}+f_mx^m \quad (1)$$

여기서, $f_i=1$인 경우를 m차의 AOP(All One Polynomial)라고 하며[6], x가 m차의 기약 AOP의 근이라고 하면 유한체 $GF(2^m)$상에서 임의의 원소 $A(x)$ 는 식 (2)와 같이 표현된다.

$$A(x)=\sum_{i=0}^{m-1} a_i \cdot x^i = a_0+a_1x+a_2x^2+\cdots+a_{m-1}x^{m-1} \quad (2)$$

여기서, $a_i \in GF(2)$이며, $0 \le i \le m-1$이다. $\{1, x, x^2, \cdots, x^{m-1}\}$ 는 $GF(2^m)$의 정규기저이다. 또한, 원소 $A(x)$는 식 (3)과 같이 표현할 수 있다.

$$A(x)=\sum_{i=0}^{m} a_i \cdot x^i = a_0+a_1x+a_2x^2+\cdots+a_{m-1}x^{m-1}+a_mx^m \quad (3)$$

식 (3)에서는 정규기저에 x^m이 추가된 기저 $\{1, x, x^2, \cdots, x^{m-1}, x^m\}$이 원소 $A(x)$를 표현하기 위하여 사용되었는데, 이것을 정규기저 $\{1, x, x^2, \cdots, x^{m-1}\}$의 확장기저라고 한다. 따라서 원소 $A(x) \in GF(2^m)$는 두 가지로 표현될 수 있다. 예를 들어 원소 $A(x)=1+x+x^3 \in GF(2^4)$은 정규기저를 사용한 원소 $A(x)=1+x+x^3$와 확장기저를 사용한 원소 $A(x)=x^2+x^4$로 표현할 수 있다. 본 논문에서는 확장기저를 이용하여 알고리즘을 구현한다. $GF(2^m)$상에서 모든 항이 존재하는 m차 모닉 기약 AOP는 다음과 같이 표현된다.

$$F(x)=\sum_{i=0}^{m} f_i \cdot x^i = 1+x+x^2+\cdots+x^m \quad (4)$$

x를 $F(x)=1+x+x^2+\cdots+x^m$이 되는 $F(x)=0$의 근이라 하자. 그러면 식 (5)와 같이 유한체 $GF(2^m)$상의 각 원소들은 차수가 $m-1$이하의 x의 다항식으로 표현된다.

$$x^m = 1+x+x^2+\cdots+x^{m-1} \quad (5)$$

두 다항식을 승산하였을 때, x^m 보다 큰 차수들의 승산에 대하여 구하면 식 (6)과 같다.

$$\begin{aligned} x^{m+1} &= x^m \bullet x \\ &= x + x^2 + x^3 + \cdots + x^{m-1} + x^m \end{aligned} \tag{6}$$

식 (6)에서 x^m 항에 식 (5)를 대입하면 식 (7)과 같다.

$$\begin{aligned} x^{m+1} &= (x + x^2 + x^3 + \cdots + x^{m-1}) \\ &\quad + (1 + x + x^2 + \cdots + x^{m-1}) \end{aligned} \tag{7}$$

식 (7)에서 1을 제외한 나머지 항 즉, $x, x^2, x^3, \cdots, x^{m-1}$의 계수들은 모두 2가 되며, $GF(2^m)$상에서 유한체의 수학적 성질에 의하여 2는 0과 같으므로 식 (8)이 된다.

$$x^{m+1} = 1 \tag{8}$$

식 (8)을 이용하여 x^{m+1}보다 큰 차수들에 대하여 구하면 다음과 같은 식들을 얻을 수 있다.

$$\begin{aligned} x^{m+2} &= x^{m+1} \bullet x = x \\ x^{m+3} &= x^{m+2} \bullet x = x^{m+1} \bullet x \bullet x = x^2 \\ x^{m+i} &= x^{m+i-1} \bullet x = x^{i-1} \\ x^{2m} &= x^{m+m-1} \bullet x = x^{m-1} \end{aligned} \tag{9}$$

x가 유한체 $GF(2^m)$상에서 m차 기약 다항식의 근이라 할 때, $GF(2^m)$상의 원소인 2개의 다항식을 승산하기 위하여 승산 다항식 $A(x)$와 피승산 다항식 $B(x)$를 식 (10)과 같이 표현하였다.

$$\begin{aligned} A(x) &= a_0 + a_1 x + a_2 x^2 + \cdots + a_{m-1} x^{m-1} \\ &= \sum_{i=0}^{m-1} a_i \bullet x^i \\ B(x) &= b_0 + b_1 x + b_2 x^2 + \cdots + b_{m-1} x^{m-1} \\ &= \sum_{i=0}^{m-1} b_i \bullet x^i \end{aligned} \tag{10}$$

여기서, $a_i, b_i \in GF(2)$이며, $0 \le i \le m-1$이다. 식 (10)의 다항식 $A(x)$, $B(x)$를 승산하면 식 (11)과 같다.

$$\begin{aligned} A(x) \bullet B(x) &= \left(a_0 + a_1 x^1 + a_2 x^2 + \cdots + a_{m-1} x^{m-1}\right) \\ &\quad \bullet \left(b_0 + b_1 x + b_2 x^2 + \cdots + b_{m-1} x^{m-1}\right) \\ &= \left(\sum_{i=0}^{m-1} a_i x^i\right) \bullet \left(\sum_{i=0}^{m-1} b_i x^i\right) \end{aligned} \tag{11}$$

식 (11)에서 $D(x) = A(x) \bullet B(x)$로 놓으면, 식 (12)와 같이 표현할 수 있다.

$$\begin{aligned} D(x) &= (d_0 + d_1 x + d_2 x^2 + \cdots + d_{2m-2} x^{2m-2}) \\ &= \left(\sum_{i=0}^{2m-2} d_i x^i\right) \end{aligned} \tag{12}$$

식 (12)를 $m-1$차를 기준으로 2개의 항으로 나누어 다시 쓰면 식 (13)과 같다.

$$D(x) = \left(\sum_{i=0}^{m-1} d_i x^i\right) + \left(\sum_{i=m}^{2m-2} d_i x^i\right) \tag{13}$$

식 (13)의 두 번째 항 $\sum_{i=m}^{2m-2} d_i x^i$는 식 (8), (9)를 이용하여 $\sum_{i=0}^{m-1} d_{m+i} x^i$로 표현할 수 있으며, 식 (13)은 식 (14)와 같이 다시 쓸 수 있다.

$$D(x) = \left(\sum_{i=0}^{m-1} d_i x^i\right) + \left(\sum_{i=0}^{m-1} d_{m+i} x^i\right) \tag{14}$$

식 (14)에서 m차 항을 분리하여 다시 정리하면 식 (15)와 같이 표현된다.

$$\begin{aligned} D(x) &= \sum_{i=0}^{m-1} d_i x^i + \sum_{i=0}^{m-1} d_{m+i} x^i \\ &= \sum_{i=0}^{m-1} (d_i + d_{m+i}) x^i \end{aligned} \tag{15}$$

식 (15)에서 $d_i + d_{m+i} = D_i$ 이라 놓으면 식 (16)과 같이 표현된다.

$$D(x) = \sum_{i=0}^{m-1} D_i x^i \tag{16}$$

여기서, $D_i \in GF(2)$이다.

식 (16)은 식 (12)와 같은 형태의 승산식으로 표현되었으며, m이상의 차수에 대하여 $m-1$차 이하의 승산식으로 표현되었음을 보여준다. 이상과 같이 유도된 승산 알고리즘을 $GF(2^m)$상에서 $m=4$인 경우에 대하여 예를 들었다.

〔예 1〕 $GF(2^m)$상에서 $m=4$인 경우의 승산 다항식 $A(x)$와 피승산 다항식 $B(x)$가 다음 같이 표현될 때, $GF(2^4)$상에서 두 다항식 $A(x)$, $B(x)$를 승산하면 그림 1(a)와 같다.

$$A(x)=\sum_{i=0}^{m-1}a_i x^i = a_0+a_1x^1+a_2x^2+a_3x^3 \tag{17}$$

$$B(x)=\sum_{i=0}^{m-1}b_i x^i = b_0+b_1x^1+b_2x^2+b_3x^3 \tag{18}$$

여기서, a_i, $b_i \in GF(2)$이다.

$$\begin{aligned} D(x) &= A(x)\cdot B(x)\\ &=\left(\sum_{i=0}^{m-1}a_i x^i\right)\cdot\left(\sum_{i=0}^{m-1}b_i x^i\right)\\ &=(d_0+d_1x+d_2x^2+\cdots+d_{2m-2}x^{2m-2})\\ &=\left(\sum_{i=0}^{2m-2}d_i x^i\right) \end{aligned} \tag{19}$$

$$\begin{array}{cccccccc} & x^0 & x^1 & x^2 & x^3 & x^4 & x^5 & x^6\\ \hline & a_0 & a_1 & a_2 & a_3 & & & \\ \times & b_0 & b_1 & b_2 & b_3 & & & \\ \hline & a_0b_0 & a_1b_0 & a_2b_0 & a_3b_0 & & & \\ & & a_0b_1 & a_1b_1 & a_2b_1 & a_3b_1 & & \\ & & & a_0b_2 & a_1b_2 & a_2b_2 & a_3b_2 & \\ + & & & & a_0b_3 & a_1b_3 & a_2b_3 & a_3b_3\\ \hline & d_0 & d_1 & d_2 & d_3 & d_4 & d_5 & d_6 \end{array}$$

(a) 단계 1

$$\begin{array}{ccccc} & x^0 & x^1 & x^2 & x^3\\ \hline & a_0 & a_1 & a_2 & a_3\\ \times & b_0 & b_1 & b_2 & b_3\\ \hline & a_0b_0 & a_1b_0 & a_2b_0 & a_3b_0\\ & a_3b_1 & a_0b_1 & a_1b_1 & a_2b_1\\ & a_2b_2 & a_3b_2 & a_0b_2 & a_1b_2\\ + & a_1b_3 & a_2b_3 & a_3b_3 & a_0b_3\\ \hline & D_0 & D_1 & D_2 & D_3 \end{array}$$

(b) 단계 2

그림 1. $GF(2^4)$상에서의 승산

Fig. 1. Multiplication over $GF(2^4)$.

그림 1(a)에 나타낸 두 다항식 $A(x)$와 $B(x)$의 승산을 정리하면 식 (20)과 같다.

$$\begin{aligned} d_0 &= a_0b_0\\ d_1 &= a_1b_0+a_0b_1\\ d_2 &= a_2b_0+a_1b_1+a_0b_2\\ d_3 &= a_3b_0+a_2b_1+a_1b_2+a_0b_3\\ d_4 &= a_3b_1+a_2b_2+a_1b_3\\ d_5 &= a_3b_2+a_2b_3\\ d_6 &= a_3b_3 \end{aligned} \tag{20}$$

식 (9)의 $x^m=x^{i-1}$로부터 $m=4$이므로 x^4, x^5, x^6은 다음 같이 x^0, x^1, x^2로 변환할 수 있다. 즉, $i=1$인 경우 $x^4=x^0$, $i=2$인 경우 $x^5=x^1$, $i=3$인 경우 $x^6=x^2$이다.

따라서, x^4항 이하의 계수들은 그림 1(b)와 같이 x^0, x^1, x^2항 계수들과 가산하여 구할 수 있다. $m=4$이므로 식 (16)의 m에 4를 대입하고 $A(x)$와 $B(x)$의 승산결과인 $D(x)$를 구하면 식 (21)과 같다.

$$\begin{aligned} D(x) &= \sum_{i=0}^{3}D_i x^i\\ &= D_0x^0+D_1x^1+D_2x^2+D_3x^3 \end{aligned} \tag{21}$$

식 (21)에서 D_0, D_1, D_2, D_3는 식 (13)을 이용하여 다음과 같이 쓸 수 있다.

$$\begin{aligned} D_0 &= d_0+d_4\\ D_1 &= d_1+d_5\\ D_2 &= d_2+d_6\\ D_3 &= d_3 \end{aligned} \tag{22}$$

식 (22)에 식 (21)을 대입하여 $D_0 \sim D_4$를 다시 쓰면 식 (23)과 같다.

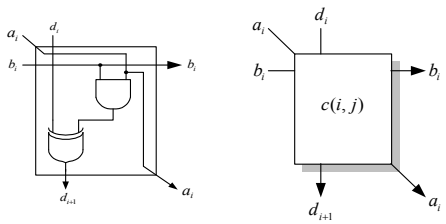
$$\begin{aligned} D_0 &= a_0b_0 + a_3b_1 + a_2b_2 + a_1b_3 \\ D_1 &= a_1b_0 + a_0b_1 + a_3b_2 + a_2b_3 \\ D_2 &= a_2b_0 + a_1b_1 + a_0b_2 + a_3b_3 \\ D_3 &= a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \end{aligned} \quad (23)$$

III. 유한체 $GF(2^4)$상에서의 고속 병렬 승산기 구성

이 장에서는 앞장에서 제시한 승산 알고리즘 $D(x) = A(x) \cdot B(x)$을 이용하여 $GF(2^4)$상의 두 다항식 $A(x)$와 $B(x)$을 실행하는 고속 병렬 승산기의 설계를 논한다.

3.1 $GF(2)$ 승산기의 기본 셀 설계

$GF(2^4)$상에서의 승산기를 구성하기 위하여 기본 게이트는 mod(2) 연산을 수행하는 2입력 XOR 게이트와 AND 게이트를 사용한 기본 셀을 그림 2에서 보였다. 여기서, a_i와 b_i는 각각 승산 다항식 $A(x)$와 피승산 다항식 $B(x)$의 계수들을 나타낸다. 그리고 d_i는 셀의 입력으로 전단 셀의 출력을 의미하며 d_{i+1}는 셀의 출력을 나타낸다.



(a) 회로도 (b) 기호

그림 2. $GF(2)$상 승산기의 기본 셀
Fig. 2. The basic cell of the multiplier on $GF(2)$.

3.2 $GF(2^4)$상에서의 고속 병렬 승산기 설계

그림 3은 앞장에서 제시된 $GF(2^m)$상의 승산 알고리즘을 이용하여 유한체 $GF(2^4)$에서 고속으로 승산하는 병렬 승산기 구성도이다. 최하단의 $D_0 \sim D_3$는 다항식의 승산결과에 대한 각 항의 계수이며, 최상단에 위치한 셀들에 입력되는 0은 셀에 대한 초기값이다. 이 승산기는 병렬 입-출력 모듈구조로서 m^2개 즉, 16개의 동일한 셀로 구성되었으며, 메모리 소자는 필요하지 않으며, 클럭신호에 의해 동작하는 것이 아니고 각 셀의 소자 지연시간에 의해 결과가 출력되므로, 이 승산기는 전체 지연시간은 m 단위 시간을 갖는다. 또한 이 구조는 전체적으로 매우 적은 결선이 요구된다.

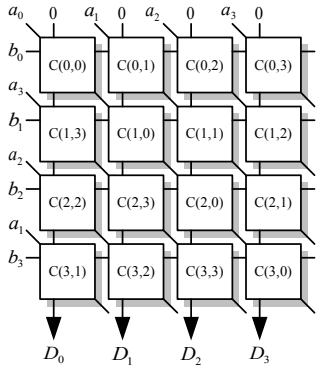


그림 3. $GF(2^4)$상의 고속 병렬 승산기
Fig. 3. The high-speed parallel multiplier on $GF(2^4)$.

IV. 비교 및 검토

본 논문에서 제안한 모든 항의 계수가 0이 아닌 기약다항식을 이용한 두 원소를 승산하는 고속 병렬 승산기 회로를 포함하여 참고문헌의 승산회로들은 저마다의 독특한 성질과 장점을 갖는다. 일반적으로 사용되는 회로비교의 척도들은 간략화된 회로구성, 빠른 동작속도, 저전력 등이다. 회로의 간략화를 평가하기 위해서는 구성소자의 개수 및 소자 간 결선의 수, 입출력 단자의 수, 기타 부속회로 및 게이트의 개수, VLSI 구현시 필요한 면적 등을 고려하여야 한다. 또한 동작속도는 입력이 인가되면서 회로의 동작출력이 나타나기까지의 소자에 의한 지연시간과 클럭시간 등이 중요한 고려 요소이다. 이외에도 주변회로 블록과의 호환 및 신호전달의 적합성, 예를 들면 부호기, 복호기의 필요 여부 등 다양한 항목을 통해 종합적으로 평가될 수 있다. 적용하고자 하는 목적에 따라 일부 항목에 대한 트레이드-오프 조건을 고려할 수도 있다. 따라서 일부 항목만의 단편적 비교를 통해 구성회로의 우열을 논하기는 쉽지 않은 문제이다. 그러나 대략적으로 회로의 비교를 위해 여러 참고문헌들은 구성회로의 소자 수와 시간지연에 대한 비교를 행하고 있으며, 본 논문에서도 이에 따

라 비교하였다.

본 논문에서 제시한 고속 병렬 승산기의 구성과 참고문헌의 승산기들의 구성을 표 2에 정리하였다. 표 2에서 보인 것처럼 Mastrovito[17], Koc[6], Masoleh[18], Petra[12] 및 본 논문에서는 유한체상의 두 다항식 A와 B의 곱셈함수는 시스토릭 구조를 갖지 않기 때문에 전단에서 들어오는 초기치 C가 없어서 $D=A \cdot B$이며, Kumar[19]와 Namin[20]의 승산기는 시스토릭 구조를 갖고 동작하기 때문에 곱셈함수 $D=A \cdot B+C$이다. $GF(2^4)$상의 기약다항식 $F(x)$는 x^4+x+1, x^4+x^3+1와 $x^4+x^3+x^2+x+1$ 등이 있으며, Koc, Masoleh, Namin은 AOP로서 $F(x)=x^4+x^3+x^2+x+1$를 적용하여 회로를 구성하였으며, Kumar, Petra는 Trinomial을 기약다항식을 사용하였고, 본 논문의 승산기는 모든 계수가 0이 아닌 기약다항식 $F(x)=x^4+x^3+x^2+x+1$을 적용하여 회로를 구성하였다. 유한체상에서 곱셈은 기약다항식에 따라 계산량이 많아지거나 적어진다. 그러므로 임의의 기약다항식에서 동작할 수 있는 일반성을 갖는 승산기를 설계하는 것이 연구의 목적이다. 그러므로 본 논문은 AND 게이트와 XOR 게이트를 사용하여 기본 셀들이 일반성을 갖게 설계하였다.

승산기를 구성하는 게이트의 수를 비교하면 $m=4$인 경우 AND 게이트는 Masoleh의 논문과 본 논문은 16개로 우수하며, 타 연구는 32개로 다소 증가한다. XOR 게이트는 타 논문의 경우 25개이며, 본 연구는 16개로 약간 우수하다. Mastrovito, Kumar, Namin, Petra 의 논문은 많은 수의 D 플립플롭이 필요한 반면에 Koc, Masoleh 및 본 논문은 D 플립플롭을 전혀 사용하지 않는다. 동작시간은 D 플립플롭을 사용하지 않는 Koc, Masoleh 및 본 논문이 가장 우수다.

승산기의 구조를 비교하면 Koc와 Masoleh 논문은 D 플립플롭을 사용하지 않는 간단한 AND 와 XOR 의 배열 구조로 구성되어 있으며 모듈성이 있으나 규칙성이 없어 소자가 증가하는 단점과 각 소자들 간의 연결이 매우 복잡한 단점이 있다. 반면에 Mastrovito, Kumar, Namin, Petra는 비트 시스토릭 구조로 동작하며, AND-XOR 셀 배열의 모듈성과 규칙성이 있으나 게이트 수가 증가하는 단점이 있다. 본 논문은 각 1개의 AND-XOR 셀 배열로 구성되어 있어 배열의 모듈성과 규칙성을 가지며, 소자간의 연결이 간단하고, 확장성이 용이한 장점이 있으며, 동작속도가 빠르다. 또한 AOP 기약 다항식을 사용하므로 임의의 기약다항식에서도 동일한 동작속도를 갖는 장점이 있다.

표 2. $GF(2^4)$상의 승산기들의 비교표

Table 2. Comparison table of multipliers on $GF(2^4)$

Multiplier Item	Mastrovito [17]	Koc[6]	Masoleh [18]	This Paper
1. Function	AB	AB	AB	AB
2. F(x)	x4+x+1	AOP	AOP	AOP
3. I/O Format	Bit-Parallel	Parallel	Parallel	Parallel
4. AND	2m2 (32)	2m2 (32)	m2 (16)	m2 (16)
5. XOR	(m+1)2 (25)	(m+1)2 (25)	(m+1)2 (25)	m2 (16)
6. D Flip-Flop	(m+1)2 (25)	-	-	-
7. Minimum clock period	DA+3DX +5DL	DA+3DX	DA+2DX	DA+DX

Multiplier Item	Kumar [19]	Namin [20]	Petra [12]	This Paper
1. Function	AB+C	AB+C	AB	AB
2. F(x)	Trimonial	AOP	Trinomial	AOP
3. I/O Format	Bit-Parallel	BSWP	Bit-Parallel	Parallel
4. AND	2m2 (32)	2m2 (32)	2m2 (32)	m2 (16)
5. XOR	(m+1)2 (25)	2m2 (32)	(m+1)2 (25)	m2 (16)
6. D Flip-Flop	(m+1)2 (25)	(m+1)2 (25)	2m(m-1) (24)	-
7. Minimum clock period	DA+DX+ 5DL	DA+2DX + 5DL	DA+2DX+ 4DL	DA+DX
Comment	DA = the propagation delay of one 2-input AND gate DX = the propagation delay of one 2-input XOR gate DL = the propagation delay of one latch ( ) = the total gate number of generalization for degree m=4 AOP means All One Polynomial of degree m BSWP = Bit-Serial Word-Parallel			

V. 결 론

본 논문에서는 유한체 $GF(2^m)$상에서 모든 항에 0이 아닌 계수가 존재하는 기약 다항식에 대한 승산 알고리즘을 제시하

였으며, 제시된 승산 알고리즘을 이용하여 고속의 병렬 입-출력 모듈구조의 승산기를 구성하였다. 제시한 승산기의 구성은 m^2개의 동일한 셀로 설계되었으며, 1개의 셀은 2입력 XOR 게이트와 AND 게이트로 구성하였다.

본 논문에서 제시된 승산기는 클럭이 필요하지 않고 m개의 XOR 게이트 소자 지연시간과 1개의 AND 게이트 소자의 지연시간만을 필요로 한다. 또한 셀에 래치를 사용하지 않았으므로 회로가 간단하며, 셀 당 게이트 수는 2개, 승산기에 사용된 전체 게이트의 수는 m^2로서 비교 논문들 중에 가장 적은 수의 게이트가 사용되었다. 이것은 VLSI 제조시 보다 작은 실리콘 면적이 필요함을 의미한다. 또한 셀 당 지연시간도 $D_A + D_X$로서 가장 적으므로 승산기의 전체 지연시간도 적다. 본 연구에서 구성한 승산기는 규칙성과 셀 배열에 의한 모듈성을 가지므로 확장이 용이하며 VLSI회로 실현에 적합할 것이다.

참고문헌

〔1〕 B. A. Laws and C. K. Rushforth, "A Cellular Array Multiplier for $GF(2^m)$," IEEE Trans. Computers, vol. C-20, pp. 1573-1578, Dec. 1971.

〔2〕 H. M. Shao, T. K. Truong, L. J. Deutsch, J. H. Yaeh and I. S. Reed, "A VLSI Design of a Pipelining Reed-Solomon Decoder," IEEE Trans. Computers, vol. C-34, pp. 393-403, May 1985.

〔3〕 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 $GF(2^m)$," IEEE Trans. Computers, vol. C-34, pp. 709-717, Aug. 1985.

〔4〕 S. B. Wicker and V. K. Bhargava, Reed-Solomon Codes and Their Applications, IEEE Press, 1994.

〔5〕 3rd Generation Partnership Project., "Technical specification group GSM/EDGE radio access network; channel coding (release 5)," Tech. Rep. 3GPP TS 45.003 V5.6.0, June 2003.

〔6〕 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.

〔7〕 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.

〔8〕 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.

〔9〕 C. L. Wang and J. L. Lin, "Systolic Array Implementation of Multipliers for Finite Fields $GF(2^m)$," IEEE Trans. Circuits and Systems, vol. 38, no. 7, July 1991.

〔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〕 Y. Wang, Z. Tian, X. Bi and Z. Niu, "Efficient Multiplier over Finite Field Represented in Type II Optimal Normal Basis," Proceedings of the Sixth International Conference on Intelligent Systems Design and Applications (ISDA '06), 2006.

〔12〕 N. Petra, D. de Caro and A. G.M. Strollo, "A Novel Architecture for Galois Fields $GF(2^m)$ Multipliers Based on Mastrovito Scheme," IEEE Trans. Computers, vol. 58, no. 11, pp. 1470-1483, Nov. 2007.

〔13〕 H. Wu and H. 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.

〔14〕 A. Halbutogullari and C. K. Koc, "Mastrovito Multiplier for General Irreducible Polynomials," IEEE Trans. Computers, vol. 49, no. 5, pp. 503-518, May 2000.

〔15〕 R. Lidl, H. Niederreiter and P. M. Cohn, *Finite Fields*, Addison-Wesley, Reading, Massachusetts, 1983.

〔16〕 S. B. Wicker and V. K. Bhargava, *Error*

Correcting Coding Theory, McGraw-Hill, New York, 1989.

〔17〕 E. D. Mastrovito, "VLSI Design for Multiplication on Finite Field $GF(2^m)$," Proc. International Conference on Applied Algebraic Algorithms and Error-Correcting Code, AAECC-6, Roma, pp. 297-309, July 1998.

〔18〕 A. R. Masoleh and M. A. Hasan, "A New Construction of Massey-Omura Parallel Multiplier over $GF(2^m)$," IEEE Trans. Computers, vol. 51, no. 5, pp. 511-520, May 2002.

〔19〕 S. Kumar, T. Wollinger and C. Paar, "Optimum Digit Serial $GF(2^m)$ Multipliers for Curve-Based Cryptography," IEEE Trans. Computers, vol. 55, no. 10, pp. 1306-1311, Oct. 2006.

〔20〕 A. H. Namin, H. Wu and M. Ahmadi, "Comb Architectures for Finite Field Multiplication in IF_{2^m}," IEEE Trans. Computers, vol. 56, no. 7, pp. 909-916, July 2007.

저 자 소 개

성 현 경

1982: 인하대학교 전자공학과 공학사.

1984: 인하대학교 전자공학과 공학석사.

1991: 인하대학교 전자공학과 공학박사.

현 재: 상지대학교 컴퓨터정보공학부 교수

관심분야: Multiple-Valued Logic Design, Computer Architecture Design, Information & Coding Theory, Cryptography Theory & Security, RFID/WSN 설계 및 응용 등

Email : hkseong@sangji.ac.kr