VCG를 사용한 GF(2^m)상의 고속병렬 승산기 설계에 관한 연구

성 현 경*

A Study on Design of High-Speed Parallel Multiplier over GF(2^m) using VCG

Hyeon-Kyeong Seong*

이 논문은 2008년도 상지대학교 교내 연구비 지원에 의해 연구되었음

요 약

본 논문에서는 $GF(2^m)$상의 표준기저를 사용한 새로운 형태의 VCG에 의한 고속병렬 승산회로를 제안하였다. 승산기의 구성에 앞서, 피승수 다항식과 기약다항식의 승산을 병렬로 수행하는 벡터 코드 생성기(VCG) 기본 셀을 설계하였고, VCG 회로와 승수 다항식의 한 계수와 비트-병렬로 승산하여 결과를 생성하는 부분 승산결과 셀(PPC)를 설계하였다. 제안한 승산기는 VCG와 PPC를 연결하여 고속의 병렬 승산을 수행한다. VCG 기본 셀과 PPC는 각각 1개의 AND 게이트와 1개의 XOR 게이트로 구성된다. 이러한 과정을 확장하여 m에 대한 일반화된 회로의 설계를 보였으며, 간단한 형태의 승산회로 구성의 예를 $GF(2^4)$를 통해 보였다. 또한 제시한 승산기는 PSpice 시뮬레이션을 통하여 동작특성을 보였다. 본 논문에서 제안한 승산기는 VCG와 PPC을 반복적으로 연결하여 구성하므로, 차수 m이 매우 큰 유한체상의 두 다항식의 곱셈에서 확장이 용이하며, VLSI에 적합하다.

ABSTRACT

In this paper, we present a new type high speed parallel multiplier for performing the multiplication of two polynomials using standard basis in the finite fields $GF(2^m)$. Prior to construct the multiplier circuits, we design the basic cell of vector code generator(VCG) to perform the parallel multiplication of a multiplicand polynomial with a irreducible polynomial and design the partial product result cell(PPC) to generate the result of bit-parallel multiplication with one coefficient of a multiplicative polynomial with VCG circuits. The presented multiplier performs high speed parallel multiplication to connect PPC with VCG. The basic cell of VCG and PPC consists of one AND gate and one XOR gate respectively. Extending this process, we show the design of the generalized circuits for degree m and a simple example of constructing the multiplier circuit over finite fields $GF(2^4)$. Also, the presented multiplier is simulated by PSpice. The multiplier presented in this paper uses the VCGs and PPCs repeatedly, and is easy to extend the multiplication of two polynomials in the finite fields with very large degree m, and is suitable to VLSI.

키워드

유한체, GF(2^m), 병렬 승산기, 표준기저, 벡터코드생성기

Key word

Finite fields, GF(2^m), Parallel multiplier, Standard basis, Vector code generator

* 상지대학교 컴퓨터정보공학부

접수일자 : 2010. 01. 07
심사완료일자 : 2010. 01. 13

Ⅰ. 서 론

유한체는 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.

$GF(2^m)$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 곱셈기는 비트-병렬 및 비트-직렬 구조 곱셈기로 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 곱셈기 설계에 관한 연구가 활발히 진행되고 있으며, 병렬 곱셈기 구조의 경우 회로는 복잡하지만 빠른 연산처리 능력을 가지고 있으므로 최근에 많이 연구되고 있다[6].

Yeh 등[7]은 유한체 $GF(2^m)$상에서 표준기저를 사용하여 $A \cdot B + C$ 연산을 수행하는 병렬 입-출력 시스토릭 구조의 곱셈기를 개발하였다. 이 곱셈기는 하나의 셀에 2개의 2입력 AND 게이트와 2개의 2입력 XOR 게이트를 사용하여 VLSI화에 적합하도록 설계하였으나 데이터의 역류 현상을 갖는 단점이 있다. Wang 등[8]은 Sunar와 Koc에 의해 제안된 병렬형 곱셈기로부터 유도된 직렬형과 병렬형 곱셈기의 일종인 타입 II 최적 정규기저에서 수행하는 새로운 종류의 곱셈기를 개발하였다. 이 곱셈기는 ModelSim 도구로 시뮬레이션하였고, Xilinx의 ISE로 합성하였다. Xilinx의 FPGA 장비로 실현된 회로기판 실험이 회로기판에서 80MHz에서 동작한다. Petra 등[9]은 Mastrovito 곱셈기의 첫 번째 블록의 최소-영역 실현과 Matrovito 곱셈기의 두 번째 블록의 고속 지연 유도 나무구조를 이용하여 새로운 곱셈기를 개발하였으며, 곱셈기의 복잡성과 지연시간에 대하여 여러 다항식을 분석적으로 평가하였다. 제안된 곱셈기는 실제 응용에서 사용할 수 있도록 (255, 239) Reed-Solomon 디코더를 해석할 수 있도록 0.25㎛ CMOS 기술로 실현함으로써 증명하였다. Wu 등[10]은 유한체에서 기약 AOP(All One Polynomial)와 기약 ESP(Equally Spaced Polynomial)를 기반으로 하는 약한 이중 기저를 이용한 저 복잡성 비트-병렬 곱셈기를 제안하였으며, Halbutogullari 등[11]은 일반적인 기약다항식에 대한 병렬 곱셈기를 제안하였다. 이들이 제안한 유한체상의 곱셈기들은 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 유한체 연산에 관한 기존의 연구 결과를 토대로, $GF(2^m)$상의 표준기저를 이용하여 VCG(Vector Code Generator)를 제안하였고, 이를 승산회로에 적용하여 보다 간략화 되고 고속의 연산이 가능한 새로운 승산기를 제안하였다. 본 논문에서 제안한 VCG는 벡터의 각 비트들의 병렬연산에 의해 동작되며, 회로모듈 내에 별도의 메모리소자를 필요로 하지 않으므로, 시간지연이 적게 발생하여 고속의 동작특성을 갖는다. 또한, 회로구성을 모듈화, 블록화 함으로써 m에 대한 확장과 VLSI에 유리하도록 하였다. 제안된 회로의 구성방법에 대하여 m에 대한 일반화된 수식과 이를 통한 회로의 구현을 보였다. 설계의 예로써 $GF(2^4)$상의 승산회로를 설계하였으며, 설계된 회로의 동작을 시뮬레이션을 통해 확인하였다. 본 논문에서 제안한 회로구성의 특징중 하나인 회로구성의 모듈화 및 블록화에 따라, 현재 통신분야에 널리 적용되고 있

는 $GF(2^8)$상의 승산회로를 포함하여 m에 대한 일반화된 회로설계가 용이하다.

Ⅱ. $GF(2^m)$상의 연산 알고리즘과 벡터코드의 생성

1. 유한체상의 덧셈

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 [3,13,14]. $GF(2^m)$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.

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

여기서 $F(x)$는 최고 차수 m의 계수 $f_m=1$인 모닉 다항식(monic polynomial)이다. 또한 $GF(2^m)$의 0이 아닌 원소들은 α의 승(power)으로서 표현이 가능하며 식 (2)와 같다.

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

원시 기약 다항식 $F(\alpha)=0$ 임으로 식 (3)과 같이 구할 수 있다.

$$F(\alpha)=\alpha^m+f_{m-1}\cdot\alpha^{m-1}+\cdots+f_1\cdot\alpha^1+f_0=0$$
$$\alpha^m=\sum_{i=0}^{m-1} f_i \cdot \alpha^i \tag{3}$$

그러므로 $GF(2^m)$상의 원소들은 m보다 더 낮은 차수를 갖는 α의 다항식으로 식 (4)와 같이 표현할 수 있다.

$$GF(2^m)=\sum_{i=0}^{m-1} a_i \cdot \alpha^i \ ; \alpha_i \in GF(2) \tag{4}$$

유한체 $GF(2^m)$에서 임의의 다항식 $A(x)$는 식 (5)와 같이 표현할 수 있다.

$$A(x)=a_{m-1}\cdot x^{m-1}+a_{m-2}\cdot x^{m-2}+\cdots+a_1\cdot x^1+a_0$$
$$=\sum_{i=0}^{m-1} a_i \cdot x^i \tag{5}$$

또한 임의의 다항식 $B(x)$는 식 (6)과 같이 표현할 수 있다.

$$B(x)=b_{m-1}\cdot x^{m-1}+b_{m-2}\cdot x^{m-2}+\cdots+b_1\cdot x^1+b_0$$
$$=\sum_{i=0}^{m-1} b_i \cdot x^i \tag{6}$$

임의의 두 다항식 $A(x)$와 $B(x)$의 덧셈은 식 (7)과 같이 나타낼 수 있다[3].

$$S(x)=A(x)+B(x)$$
$$=s_{m-1}\cdot x^{m-1}+s_{m-2}\cdot x^{m-2}+\cdots+s_1\cdot x^1+s_0$$
$$=\sum_{k=0}^{m-1} s_k \cdot x^k \tag{7}$$

여기서 $s_k=(a_i+b_i)\mathrm{mod}(2)$이고, $0\le k\le m-1$이다.

$GF(2^m)$상에서 임의의 두 다항식의 덧셈은 모듈러-2 덧셈을 $\oplus$ 기호로 나타낼 때, 식 (7)의 각 계수 $s_i=a_i\oplus b_i$ $(0\le i\le m-1)$와 같이 간단히 구할 수 있다. 그러므로 유한체 $GF(2^m)$상의 덧셈회로는 m개의 비트 독립적인 XOR 게이트들에 의해 쉽게 구현된다.

2. 곱셈 알고리즘

유한체 $GF(2^m)$상의 곱셈은 덧셈에 비해 매우 복잡하게 구현되며, 곱셈의 전개방식에 따라 다양한 회로 구현이 가능하다. 유한체 $GF(2^m)$상에서 두 다항식 $A(x)$와 $B(x)$의 곱셈 결과를 $P(x)$는 식 (8)과 같이 나타낼 수 있다.

$$P(x)=\{A(x)\cdot B(x)\}\mathrm{mod}(F(x))$$
$$=p_{m-1}\cdot x^{m-1}+p_{m-2}\cdot x^{m-2}+\cdots+p_1\cdot x^1+p_0$$
$$=\sum_{i=0}^{m-1} p_i \cdot x^i \tag{8}$$

식 (8)을 자세히 표현하기 위하여 기약다항식을 $F(x)$라 하였을 때 비트-병렬을 수행하는 곱셈 알고리즘은 다음과 같다.

$$\begin{aligned} P(x) &= \{A(x) \cdot B(x)\}\mathrm{mod}(F(x)) \\ &= \left\{A(x) \cdot \left(\sum_{i=0}^{m-1} b_i \cdot x^i\right)\right\}\mathrm{mod}(F(x)) \\ &= \left\{\sum_{i=0}^{m-1} b_i \cdot (A(x) \cdot x^i)\right\}\mathrm{mod}(F(x)) \\ &= \sum_{i=0}^{m-1} b_i \cdot \left\{\left(\sum_{k=0}^{m-1} a_k^{(i)} \cdot x^{(i+k)}\right)\right\}\mathrm{mod}(F(x)) \end{aligned} \tag{9}$$

식 (9)의 오른쪽 항인 $\left\{\left(\sum_{k=0}^{m-1} a_k^{(i)} \cdot x^{(i+k)}\right)\right\}\mathrm{mod}(F(x))$은 식 (2)의 $F(x)$에 의하여 계수항의 연산을 식 (10)과 같이 나타낼 수 있다.

$$\begin{aligned} a_k^{(i+1)} &= \left(f_k \cdot a_{m-1}^{(i)}\right) \oplus a_{k-1}^{(i)} \quad (1 \le k \le m-1) \\ &= f_k \cdot a_{m-1}^{(i)} \qquad (k=0) \end{aligned} \tag{10}$$

식 (10)에서 $k=0$인 경우 $a_{k-1}^{(i)}=0$이다.

그리고 식 (9)에 식 (10)을 대입하면 식 (11)과 같이 나타낼 수 있다.

$$P(x) = \sum_{i=0}^{m-1}\sum_{k=0}^{m-1}\left\{\left(b_i \cdot a_k^{(i+k)}\right) \oplus p_{k-1}^{(i)}\right\} \cdot x^i \tag{11}$$

식 (11)에서 $i=0$일 때 오른쪽 항 $p_{k-1}^{(i)}$은 0이다.

식 (11)에서 곱셈결과 $P(x)$의 계수항을 나타내면 식 (12)와 같다.

$$\begin{aligned} p_k^{(i+1)} &= \left(b_i \cdot a_k^{(i+1)}\right) \oplus p_{k-1}^{(i)} \\ &= \left\{b_i \cdot \left(f_k \cdot a_{m-1}^{(i)}\right) \oplus a_{k-1}^{(i)}\right\} \oplus p_{k-1}^{(i)} \end{aligned} \tag{12}$$

그러므로 식 (10)은 다항식 $A(x)$와 기약다항식 $F(x)$을 병렬로 연산을 구현하고, 식 (11)에서 i를 0에서 $m-1$까지 순차적으로 대입하여 반복적으로 구할 수 있다.

3. 행렬방정식

$GF(2^m)$상의 원소들은 $F(x)$를 통해 m개 기저들의 선형결합에 의해 벡터로 표현될 수 있다. $GF(2^m)$상의 임의의 두 원소들의 벡터표현 x, y에 대하여, 이들이 일정한 규칙 T에 의해 각각 입출력의 관계를 가질 때 이를 $y = T \cdot x$와 같이 표현할 수 있다. 여기서 x, y를 각각 $m \times 1$구조를 갖는 m-튜플(tuple)벡터로 가정할 때, T는 $m \times m$구조를 가지며, 전달행렬이라 할 수 있다.

주어진 조건에 대한 전달행렬에 대하여 이를 상사변환(similar transform)에 의해 식(13)와 같이 표현될 수 있다. 식 (13)의 P는 상사변환행렬이라 하며 $m \times m$ 구조를 갖는다. 한편, T가 $m \times m$구조를 갖는 행렬이므로 T의 특성다항식의 차수는 m이 되고 특성다항식의 최고사항 λ^m의 계수는 1이 된다.

$$T' = P^{-1}TP = \begin{pmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C_s \end{pmatrix} \tag{13}$$

이 성질을 갖는 다항식을 모닉(monic)다항식이라 하며, 모든 모닉다항식은 어떤 행렬의 특성다항식임을 보여준다. 특성다항식 $\lambda(x) = c_0 + c_1\lambda + \cdots + c_{m-1}\lambda^{m-1} + \lambda^m$는 식(14)의 행렬로 나타낼 수 있으며, 이때의 행렬 C를 특성다항식 $c(\lambda)$의 동반행렬이라 한다.

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & -c_0 \\ 1 & 0 & 0 & \cdots & -c_1 \\ 0 & 1 & 0 & \cdots & -c_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & -c_{n-1} \end{pmatrix} \tag{14}$$

$GF(2^m)$상의 원시다항식 $F(x)$를 통해 표준기저의 다항식표현으로 나타내어진 임의의 원소 α^i $(0 \le i \le m-2)$로부터 α^{i+1}의 다항식표현을 구하면 식 (15)과 같다.

$$\begin{aligned} \alpha^{i+1} &= \alpha^i \cdot \alpha \\ &= (x_{m-1}\alpha^{m-1} + \cdots + x_1\alpha^1 + x_0)\alpha \\ &= x_{m-1}\alpha^m + \cdots + x_1\alpha^2 + x_0\alpha \\ &= x_{m-1}(f_{m-1}\alpha^{m-1} + \cdots + f_1\alpha^1 + f_0) \\ &\quad + (x_{m-2}\alpha^{m-1} + \cdots + x_1\alpha^2 + x_0\alpha \\ &= (x_{m-2} \oplus x_{m-1}f_{m-1})\alpha^{m-1} + \cdots + (x_1 \oplus x_{m-1}f_2)\alpha^2 \\ &\quad + (x_0 \oplus x_{m-1}f_1)\alpha + x_{m-1}f_0 \end{aligned} \tag{15}$$

원시다항식 $F(x)$는 모닉 다항식의 조건을 만족한다. 또한, 유한체의 성질에 의해 식(16)와 같이 동반행렬로 표현된다.

$$T=\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & 0 & \cdots & 0 & -f_1 \\ 0 & 1 & 0 & \cdots & 0 & -f_2 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -f_{m-1} \end{pmatrix} \tag{16}$$

이에 따라 식 (15)을 행렬표현 형식으로 나타내면 식 (17)과 같다.

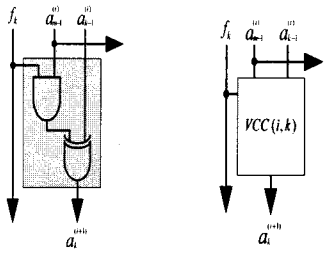
$$\alpha^{i+1} = T \cdot \alpha^i$$

$$\begin{pmatrix} x_0^{(i+1)} \\ x_1^{(i+1)} \\ \vdots \\ x_{m-2}^{(i+1)} \\ x_{m-1}^{(i+1)} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & -f_0 \\ 1 & 0 & \cdots & 0 & -f_1 \\ 0 & 1 & \cdots & 0 & -f_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -f_{m-1} \end{pmatrix} \begin{pmatrix} x_0^{(i)} \\ x_1^{(i)} \\ \vdots \\ x_{m-2}^{(i)} \\ x_{m-1}^{(i)} \end{pmatrix} \tag{17}$$

식 (17)의 열벡터 표현에서 x는 아래첨자 0, 1, ..., $m-1$로 표현된 기저들의 가중치 비트를 의미하며, 위첨차 (i), $(i+1)$은 원소 α의 지수를 의미한다.

Ⅲ. VCG에 의한 고속병렬 승산회로의 설계

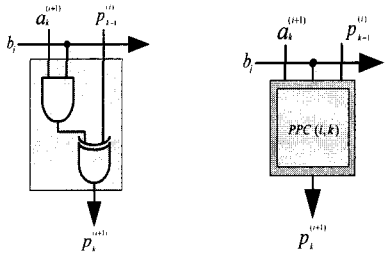
이 장에서는 앞장에서 논한 $GF(2^m)$상의 곱셈 알고리즘 $P(x)=\{A(x) \cdot B(x)\}\mathrm{mod}(F(x))$를 실행하는 비트-병렬 승산기의 설계를 논한다. 유한체상의 피승수 다항식과 기약다항식의 계수항만을 병렬로 연산하고, 승수 다항식의 한 계수와 비트-병렬로 연산을 수행하는 벡터 코드 생성기(Vector Code Generator; VCG)의 기본 셀은 그림 1과 같다.



(a) (b)

그림 1. VCG의 기본 셀회로 (a) 회로 (b) 기호
Fig. 1. Basic Cell circuit of VCG. (a) circuit (b) sign

그림 2는 VCG의 기본 셀회로에서 구한 값을 부분 승산결과를 구하는 기본 셀(Partial Product Cell; PPC) 회로이다. 그림 1의 VCG의 기본 셀은 1개의 AND 게이트와 1개의 XOR 게이트로 구현하였으며, 그림 2의 PPC의 셀도 1개이 AND 게이트와 1개의 XOR 게이트로 구현하며, VCG와 PPC를 연결하면 식 (18)과 같은 단일 승수 b_i에 의한 승산결과를 수행한다.



(a) (b)

그림 2. PPC 셀 회로 (a) 회로 (b) 기호
Fig. 2. Partial product result cell circuit.
(a) circuit (b) sign

$$\begin{aligned} p_k^{(i+1)} &= \left(b_i \cdot a_k^{(i+1)}\right) \oplus p_{k-1}^{(i)} \\ &= \left\{b_i \cdot \left(f_k \cdot a_{m-1}^{(i)}\right) \oplus a_{k-1}^{(i)}\right\} \oplus p_{k-1}^{(i)} \end{aligned} \tag{18}$$

그림 1의 VCG의 기본 셀과 그림 2의 PPC 셀을 사용하여 식 (11)에서 $m=4$인 유한체 $GF(2^4)$상의 다항식 $B(x)$의 임의의 계수 b_i를 구하는 VCG를 구현하면 그림 3과 같다. 그림 3의 VCG는 기약다항식과 피승수 다항식 $A(x)$를 병렬로 연산을 수행한 결과와 승수 다항식 $B(x)$의 한 계수와 병렬로 연산을 수행한다. 그림 3은 VCG의 1비트 연산회로를 보였다.

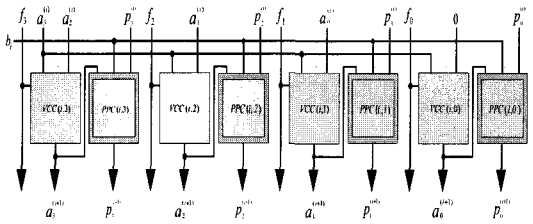


그림 3. $GF(2^4)$의 VCG circuit.
Fig. 3. VCG circuit of $GF(2^4)$

그림 4은 유한체 $GF(2^4)$상의 VCG 회로의 시뮬레이션 결과를 보인 것이다.

$GF(2^4)$의 기약다항식 중 $F(x)=x^4+x+1$를 사용하였다. 그림 4에서 시간이 60μs에서 $A(x)$=(1 0 1 1)이고, $B(x)$= (1)의 1 비트만을 곱하였을 경우 시뮬레이션 결과 $P(x)$= (1 0 1 1)를 보인다.

그림 3의 유한체 $GF(2^4)$의 VCG 회로를 사용하여 유한체 $GF(2^4)$상의 임의의 두 다항식에 대한 VCG에 의한 고속 병렬 승산기 회로를 구성하면 그림 5와 같다. 그림 3의 VCG는 피승수 다항식 $B(x)$의 계수항 만큼 반복적으로 사용되며, 유한체 $GF(2^4)$상의 고속 병렬 승산 연산을 위해 소요되는 기본 셀은 $m=4$인 경우 $4\times4(m\times m)$개가 필요하며, 메모리 소자는 필요하지 않는다.

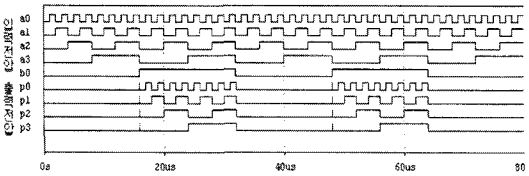


그림 4. $GF(2^4)$의 VCG 회로 시뮬레이션 결과
Fig. 4. Simulation result of VCG circuit over $GF(2^4)$

그림 5의 VCG에 의한 고속 병렬 승산기 회로는 $GF(2^4)$의 기약다항식 중 $F(x)=x^4+x+1$를 사용하였다.

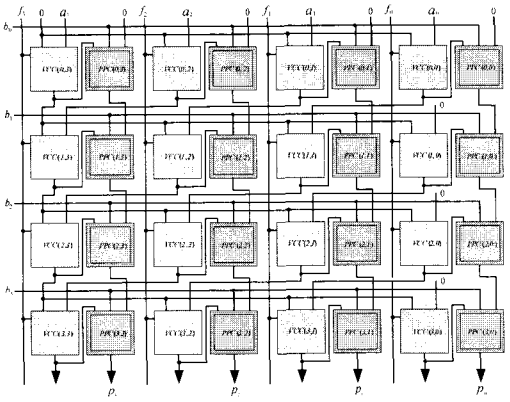


그림 5. $GF(2^4)$의 VCG에 의한 고속 병렬 승산기 회로
Fig. 5. High speed parallel multiplier circuit using VCG on $GF(2^4)$

그림 5에서 승수 다항식 $B(x)$의 첫 번째 계수 b_0가 입력으로 들어가는 VCG 회로에서 곱셈 결과 다항식의 계수항 $p_k^{(0)}$는 모두 0이 가해진다. 이는 전단으로부터 곱셈 결과가 없기 때문이다.

그림 6은 $GF(2^4)$의 VCG에 의한 고속 병렬 승산기 회로에 대한 시뮬레이션 결과이다. 그림 6에서 VCG에 의한 고속 병렬 승산기 회로의 동작은 48μs에서 피승수 입력전압 $A(x)$는 (1 1 0 0)이고, 승수 입력전압 $B(x)$의 첫 번째 비트 b_0는 48μs에서 (0)이고, b_1은 52μs에서 (0), b_2은 56μs에서 (1)이고, b_3는 60μs에서 (1)의 값인 $B(x)$는 (1 1 0 0)을 가하면 출력전압 $P(x)$는 60μs에서 (1 1 1 1)을 보인다.

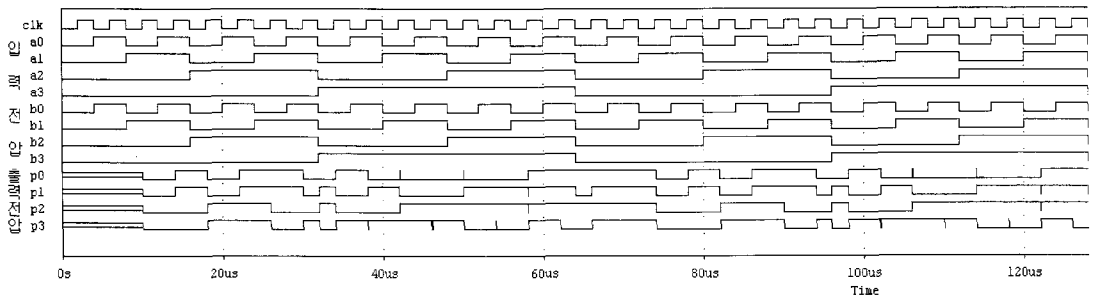


그림 6. VCG에 의한 고속 병렬 승산기 회로의 시뮬레이션 결과
Fig. 6. Simulation result of high speed parallel multiplier circuit using VCG.

Ⅳ. 비교 및 검토

본 논문에서 제안한 VCG에 의한 고속 병렬 승산기 회로를 포함하여 참고문헌의 승산회로들은 저마다의 독특한 성질과 장점을 갖는다. 일반적으로 사용되는 회로 비교의 척도들은 간략화된 회로구성, 빠른 동작속도, 저전력 등이다. 회로의 간략화를 평가하기 위해서는 구성 소자의 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 따라 비교하였다.

본 논문에서 제시한 VCG에 의한 고속 병렬 승산기의 구성과 참고문헌의 승산기들의 구성을 표 2에 정리하였다. 표 2에서 보인 것처럼 Mastrovito[12], Koc[6], Masoleh[15], Petra[9] 및 본 논문에서는 유한체상의 두 다항식 A와 B의 곱셈함수는 시스토릭 구조를 갖지 않기 때문에 전단에서 들어오는 초기치 C가 없어서 $P=A \cdot B$이며, Kumar[16]와 Namin[17]의 곱셈기는 시스토릭 구조를 갖고 동작하기 때문에 곱셈함수 $P=A \cdot B+C$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 논문과 Mastrovito의 곱셈기는 $F(x)=x^4+x+1$을 적용하여 회로를 구성하였다. 유한체상에서 곱셈은 기약다항식에 따라 계산량이 많아지거나 적어진다. 그러므로 임의의 기약다항식에서 동작할 수 있는 일반성을 갖는 곱셈기를 설계하는 것이 연구의 목적이다. 그러므로 본 논문은 AND 게이트와 XOR 게이트를 사용하여 기본 셀들이 일반성을 갖게 설계하였다.

표 2. $GF(2^4)$상의 곱셈기들의 비교표
Table 2. Comparison table of multipliers on $GF(2^4)$

Multiplier Item	Mastrovito [12]	Koc[6]	Masoleh [15]	Kumar [16]	Namin [17]	Petra [9]	This Paper
1. Function	AB	AB	AB	AB+C	AB+C	AB	AB
2. F(x)	x^4+x+1	AOP	AOP	Trimonial	AOP	Trinomial	x^4+x+1 or AOP
3. I/O Format	Bit-Parallel	Parallel	Parallel	Bit-Parallel	BSWP	Bit-Parallel	Bit-Parallel
4. AND	$2m^2$ (32)	$2m^2$ (32)	m^2 (16)	$2m^2$ (32)	$2m^2$ (32)	$2m^2$ (32)	$2m^2$ (32)
5. XOR	$(m+1)^2$ (25)	$(m+1)^2$ (25)	$(m+1)^2$ (25)	$(m+1)^2$ (25)	$2m^2$ (32)	$(m+1)^2$ (25)	$2m^2$ (32)
6. D Flip-Flop	$(m+1)^2$ (25)	-	-	$(m+1)^2$ (25)	$(m+1)^2$ (25)	2m(m-1) (24)	-
7. Minimum clock period	$D_A+3D_X+5D_L$	D_A+3D_X	D_A+2D_X	$D_A+D_X+5D_L$	$D_A+2D_X+5D_L$	$D_A+2D_X+4D_L$	D_A+2D_X
Comment	D_A = the propagation delay of one 2-input AND gate D_X = the propagation delay of one 2-input XOR gate D_L = 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						

곱셈기를 구성하는 게이트의 수를 비교하면 $m=4$인 경우 AND 게이트는 Masoleh의 논문은 16개로 우수하며, 타 연구와 본 연구는 32개로 다소 증가한다. XOR 게이트는 타 논문의 경우 25개로 우수하며, 본 연구는 32개로 약간 증가한다. Mastrovito, Kumar, Namin, Petra 의 논문은 많은 수의 D 플립플롭이 필요한 반면에 Koc, Masoleh 및 본 논문은 D 플립플롭을 전혀 사용하지 않는다. 동작시간은 D 플립플롭을사용하지 않는 Koc, Masoleh 및 본 논문이 가장 우수다. AOP 기약다항식은 수 많은 기약다항식 중에서 특수한 기약다항식이며, 본 논문의 경우 AOP 기약다항식을 사용할 경우도 동일하게 소자들이 소요되는 장점이 있다.

곱셈기의 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 2개의 AND-XOR 셀 배열로 구성되어 있어 배열의 모듈성과 규칙성을 가지며, 소자간의 연결이 간단하고, 확장성이 용이한 장점이 있으며, 동작속도가 빠르다. 또한 AOP 기약 다항식을 사용하는 경우도 동일한 회로가 사용되므로 임의의 기약다항식에서도 동일한 동작속도를 갖는 장점이 있다. 또한 PSpice를 사용하여 제안한 고속 병렬 곱셈기의 동작을 확인하기 위해 시뮬레이션을 하였으며, 승산기가 정상적으로 동작함을 보였다.

V. 결 론

본 논문에서는 유한체상에서 곱셈을 수행하는 여러 가지 방법 중에서 한 가지 방법인 유한체 $GF(2^4)$상에서 두 다항식의 곱셈을 실현하는 VCG에 의한 고속 병렬을 갖는 승산기를 제시하였다. 이 승산기는 먼저 피승수 다항식과 기약다항식의 곱셈을 병렬로 수행한 후 승수 다항식의 한 계수와 병렬로 곱셈하여 결과를 생성하는 VCG을 제안하였다. VCG의 기본 셀과 PPC 회로는 각각 1개의 AND 게이트와 1개의 XOR 게이트로 구성되며, 이들로부터 두 다항식의 고속 병렬 승산을 수행하여 승산 결과를 얻도록 설계하였다. 또한 PSpice에 의한 시뮬레이션을 통하여 제안한 VCG에 의한 고속 병렬 승산기가 정상적으로 동작함을 보였다.

제시한 VCG에 의한 고속 병렬 승산기는 $m=4$인 경우 AND 게이트가 32개, XOR 게이트의 수가 32개 소요된다. 제안한 VCG에 의한 고속 병렬 승산기의 VCG는 1 단위시간(클럭시간)이 소비된다. 그러므로 제시한 VCG에 의한 고속 병렬 승산기의 전체 시스템 동작시간은 1 단위시간이 소요되어 타 연구의 승산기보다 전체 지연시간이 빠른 장점이 있다. 또한 유한체상에서 수많은 기약다항식 중 특수한 기약다항식인 AOP 기약다항식을 사용할 경우도 동작속도는 변화가 없는 장점이 있다.

본 논문에서 제시한 VCG에 의한 고속 병렬 승산기는 각 1개의 AND-XOR로 구성되는 VCG 기본 셀과 PPC들의 배열로 구성되기 때문에 회선경로선택의 규칙성, 단순성, 배열의 모듈성, 병렬 동작의 이점을 가지며 특히 차수 m이 증가하는 유한체상의 두 다항식의 승산에서 확장성을 가지므로 다양한 유한체 연산회로에 적용할 수 있을 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 Field $GF(2^m)$," IEEE Trans. Computers, vol. C-33, pp. 357-360, Apr. 1984.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

[13] R. Lidl, H. Niederreiter and P. M. Cohn, Finite Fields, Addison-Wesley, Reading, Massachusetts, 1983.

[14] S. B. Wicker and V. K. Bhargava, Error Correcting Coding Theory, McGraw-Hill, New York, 1989.

[15] 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.

[16] 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.

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

[18] K. Sakiyama, L. Batina, B. Preneel and I. Verbauwhede, "Multicore Curve-Based Cryptoprocessor with Reconfigurable Modular Arithmetic Logic Units over $GF(2^m)$," IEEE Trans. Computers, vol. 56, no. 9, pp.1269-1282, Sep. 2007.

저자소개

성현경(Hyeon-Kyeong Seong)

1982년 인하대학교 전자공학과 공학사
1984년 인하대학교 대학원 전자공학과 공학석사
1991년 인하대학교 대학원 전자공학과 공학박사
2005년 ~ 2006년 미국 Naval Postgraduate School 방문교수
1991년 ~ 현재 상지대학교 컴퓨터정보공학부 교수
※ 관심분야 : Multiple-Valued Logic Design, Computer Architecture Design, Information & Coding Theory, Cryptography Theory & Security, RFID/WSN 설계 및 응용 등