유한체 GF(2^m)상의 셀 배열 병렬 승산기의 설계

성 현 경†

요 약

본 논문에서는 유한체 GF(2^m)상에서 두 다항식의 승산을 실현하는 병렬-입력 및 병렬-출력을 갖는 셀 배열 병렬 승산기를 제시한다. 이 승산기는 승산연산부, 기약다항식연산부, MOD연산부로 구성한다. 승산연산부는 AND 게이트와 XOR 게이트로 설계한 기본 셀의 배열로 이루어지며, 기약다항식연산부는 XOR 게이트와 D 플립플롭회로를 사용하여 구성하며, MOD연산부는 AND 게이트와 XOR 게이트에 의한 기본 셀을 배열하여 구성하였다. 제시한 승산기는 PSpice 시뮬레이션을 통하여 동작특성을 보였으며, 클럭신호의 주기를 1μs로 하였다. 제시한 셀 배열 병렬 승산기는 $m=4$인 경우에 AND 게이트의 수가 24개, XOR 게이트의 수가 32개 필요하며, D 플립플롭회로가 4개 필요하다. 또한, AOP 기약다항식을 사용하면 AND 게이트와 XOR 게이트의 수가 24개 필요하며 D 플립플롭은 사용되지 않는다. 셀 배열 병렬 승산기의 승산연산부의 동작시간은 1 단위시간(클럭시간)이 소비되고, 기약다항식연산부에 의한 MOD연산부의 동작시간은 m 단위시간(클럭시간)이 소비되어 전체 동작시간은 $m+1$ 단위시간(클럭시간)이 소비된다. 본 논문에서 제시한 셀 병렬 승산기는 회선경로 선택의 규칙성, 간단성, 배열의 모듈성과 병렬 동작의 특징을 가지며, 특히 차수 m이 매우 큰 유한체상의 두 다항식의 승산에서 확장성을 갖는다.

A Design of Cellular Array Parallel Multiplier on Finite Fields GF(2^m)

Hyeon-Kyeong Seong†

ABSTRACT

A cellular array parallel multiplier with parallel-inputs and parallel-outputs for performing the multiplication of two polynomials in the finite fields $GF(2^m)$ is presented in this paper. The presented cellular array parallel multiplier consists of three operation parts: the multiplicative operation part (MULOP), the irreducible polynomial operation part (IPOP), and the modular operation part (MODOP). The MULOP and the MODOP are composed of the basic cells which are designed with AND gates and XOR gates. The IPOP is constructed by XOR gates and D flip-flops. This multiplier is simulated by clock period 1μs using PSpice. The proposed multiplier is designed by 24 AND gates, 32 XOR gates and 4 D flip-flops when degree m is 4. In case of using AOP irreducible polynomial, this multiplier requires 24 AND gates and XOR gates respectively, and not use D flip-flop. The operating time of MULOP in the presented multiplier requires one unit time(clock time), and the operating time of MODOP using IPOP requires m unit times(clock times). Therefore total operating time is $m+1$ unit times(clock times). The cellular array parallel multiplier is simple and regular for the wire routing and have the properties of concurrency and modularity. Also, it is expansible for the multiplication of two polynomials in the finite fields with very large m.

키워드 : 유한체 $GF(2^m)$(Finite fields $GF(2^m)$), 병렬 승산기(Parallel Multiplier), 시스토릭 승산기(Systolic Multiplier), 기약다항식(Irreducible Polynomial), Reed-Solomon 부호기(Reed-Solomon Decoder)

1. 서 론

유한체는 스위칭이론, 오류정정부호, 디지털신호처리 및 화상처리, 디지털통신의 암호화 및 해독화를 요하는 보안통신 등에서 많이 응용되고 있다. 특히 유한체 $GF(2^m)$는 신호처리와 화상처리 분야에서 특별한 계산을 요하거나 범용 컴퓨터계산의 고속화를 보조하는 고성능 전용 컴퓨터의 설계에 주목을 받고 있으며 Reed-Solomon 부호기 및 복호기의 VLSI 설계에 응용되고 있다[1-5]. 이들 중 오류정정부호의 설계는 유한체 $GF(2^m)$상의 연산을 사용한다. 실제로 오류정정부호기 및 복호기 설계는 전체 시스템의 규모와 성능에 절대적인 영향을 미치므로 유한체 $GF(2^m)$상의 연구는 회로경로의 연결, 시스템 구조의 복잡성과 동시성 등의 문제점을 개선하기 위하여 진행되고 있다[6-8].

유한체에서 중요한 연산은 가산, 승산, 멱승, 제산, 승법적 역원 등이며, 유한체 상에서 연산은 디지털 2진 산술연산과 현저하게 다르다. 가산은 매우 간단하여 유한체의 원소들이 다항식의 형태로 표현되는 경우 XOR 게이트에 의한 비트별 연산으로 회로를 간단히 구성할 수 있다. 반면에 가산을 제외한 연산은 연산과정이 복잡하며, 이들 연산 중 승산은 암호화 및 해독화 알고리즘에 자주 사용된다. 따라서 회로가 복잡하지 않으면서 용이하게 연산을 실현할 수

※ 이 논문은 2002년도 상지대학교 교내연구비 지원에 의해 연구되었음.
† 종신회원 : 상지대학교 컴퓨터·정보공학부 교수
논문접수 : 2003년 9월 3일, 심사완료 : 2003년 12월 23일

있는 빠른 승산 알고리즘의 개발이 중요하다.

유한체 승산기는 유한체상의 m 비트의 원소들에 대하여 어떻게 연산하는 가에 따라 비트-직렬 승산기와 비트-병렬 승산기로 분류될 수 있다. 최근 빠른 처리속도와 복잡도를 고려한 VLSI 구현에 있어 규칙성과 모듈화가 매우 중요시 되면서 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[9, 10].

Yeh 등[11]은 유한체 $GF(2^m)$상에서 표준기저를 사용하여 $A \cdot B + C$ 연산을 수행하는 병렬 입-출력 시스토릭 구조의 승산기를 개발하였다. 이 승산기는 하나의 셀에 2개의 2입력 AND 게이트와 2개의 2입력 XOR 게이트를 사용하여 VLSI화에 적합하도록 설계하였으나, 셀당 7개의 플립플롭 회로를 사용하기 때문에 회로가 복잡하고, 동작속도가 느린 단점이 있다. Wu 등[12]은 유한체에서 기약 AOP(All One Polynomial)와 기약 ESP(Equally Spaced Polynomial)를 기반으로 하는 약한 이중 기저를 이용한 복잡성이 낮은 비트-병렬 승산기를 제안하였으며, Drolet[13]은 $GF(2^m)$에서 나머지 다항식 링 모드 $x^n + 1$로 동형을 기반으로 하는 알고리즘을 제안하였다. 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 승산에 대한 지연시간은 매우 큰 것이 단점이다.

최근 Lee 등[15]은 유한체 $GF(2^m)$상에서 기약 AOP를 기반으로 하는 순환이동과 내적의 두 연산을 이용한 승산 알고리즘을 제안하였으며, 이를 기반으로 복잡성이 낮은 비트-병렬 시스토릭 승산기를 구성하였다. 제안된 승산기는 1개의 2입력 AND 게이트와 1개의 2입력 XOR 게이트, 3개의 1비트 래치회로로 구성하였다. Lee 등이 제안한 승산기는 각 셀에서 D 플립플롭회로에 의한 지연시간 때문에 시스템의 속도가 느린 것이 단점이다. Masoleh 등[20]은 AOP를 기반으로 하는 Massey-Omura 병렬 승산기를 제안하였으며, 제안된 승산기는 원래의 병렬 Massey-Omura 승산기보다 복잡성을 감소시키며, XOR 게이트를 상당히 감소시키는 장점을 갖는다. Wu[21]은 유한체상의 다항식 기반의 비트-병렬 승산기와 제곱 연산기를 제안하였으며, 이 승산기는 AND-XOR 네트워크와 XOR 네트워크로 구성되어 있어 간단한 구조를 갖는 장점이 있으나, 기약다항식을 계산하는데 있어서 3항만을 갖는 기약다항식을 사용하고 있어 일반성을 갖지 못하는 단점이 있다. 또한, Wang 등[23]은 유한체상에서 곱의 합 연산 $C+AB^2$을 수행하는 단일 방향성 데이트 흐름의 병렬입력-병렬출력의 시스토릭 배열 승산기를 제안하였다. 이 승산기는 셀의 구조가 AND-XOR 구조로 되어 있어 규칙성과 모듈성을 갖는 장점이 있으며, 전단의 셀 데이터를 래치시키는 1비트 래치회로가 셀 당 13개를 포함하고 있는 단점이 있다.

본 논문에서는 유한체 $GF(2^m)$상에서 두 다항식의 승산 $R = A \cdot B$을 실현하는 새로운 한 방식인 병렬-입력 및 병렬-출력을 갖는 셀 배열 병렬 승산기를 제시하였다. 이 승산기는 승산연산부, 기약다항식연산부, MOD연산부로 구성된다. 승산연산부는 AND와 XOR 게이트로 설계한 기본 셀의 배열을 이루며, 기약다항식연산부는 XOR게이트들과 D 플립플롭 회로들을 사용하여 구성하며, MOD연산부는 AND와 XOR 게이트의 기본 셀을 배열하여 구성한다.

2. 유한체의 기본 성질과 승산 알고리즘

2.1 유한체의 기본성질

유한체 $GF(p^m)$은 p가 소수(prime number)이고 m이 양의 정수인 p^m개의 원소들을 갖는다. 유한체 $GF(2^m)$은 2개의 원소들을 갖는 기초체(ground field) $GF(2)$의 확대체이다. 즉, 유한체 $GF(2)$는 {0, 1}의 원소들을 구성한다[3, 18, 19]. $GF(2^m)$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.

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

유한체 $GF(2^m)$의 유용한 성질들을 증명 없이 설명하면 다음과 같다[3].

① $GF(2^m)$에서 임의의 한 원소 α에 대하여 식 (5)와 같은 값을 갖는다.

$$\alpha^{2^m} = \alpha \text{이고, } \alpha^{2^m-1} = 1 \tag{5}$$

여기서 모든 원소 α는 $\{\alpha \in GF(2)\}$이다.

② $GF(2^m)$에서 임의의 두 원소들 α와 β에 대하여 식 (6)과 같다.

$$(\alpha + \beta)^2 = \alpha^2 + \beta^2 \tag{6}$$

여기서 모든 원소 α와 β는 $\{\alpha, \beta \in GF(2^m)\}$이다.

③ $GF(2^m)$에서 $\alpha^i \cdot \alpha^j$는 식 (7)과 같다.

$$\begin{aligned} \alpha^i \cdot \alpha^j &= \alpha^{(i+j) \bmod (2^m-1)} \\ &= \alpha^{(r) \bmod (2^m-1)} \end{aligned} \tag{7}$$

여기서 모든 원소 $\alpha^i, \alpha^j, \alpha^r$는 $\{\alpha^i, \alpha^j, \alpha^r \in GF(2^m)\}$이다.

2.2 가산 알고리즘

유한체 $GF(2^m)$에서 임의의 다항식 $A(x)$는 식 (8)과 같이 표현할 수 있다.

$$A(x) = \sum_{i=0}^{m-1} a_i \cdot x^i \tag{8}$$

또한 임의의 다항식 $B(x)$는 식 (9)와 같이 표현할 수 있다.

$$B(x) = \sum_{j=0}^{m-1} b_j \cdot x^j \tag{9}$$

임의의 두 다항식 $A(x)$와 $B(x)$의 가산은 식 (10)과 같이 나타낼 수 있다[3].

$$\begin{aligned} S(x) &= A(x) + B(x) \\ &= \sum_{k=0}^{m-1} s_k \cdot x^k \end{aligned} \tag{10}$$

여기서 $s_k = (a_i + b_j) \bmod (2)$이고, $0 \le k \le m-1$이다.

그러므로 $GF(2^m)$상에서 임의의 두 다항식의 가산은 직접적이고 m개의 비트 독립적인 XOR 게이트들에 의하여 디지털 2진 가산보다 쉽게 실현된다.

2.3 승산 알고리즘

유한체 $GF(2^m)$상에서 두 다항식 $A(x)$와 $B(x)$의 병렬-입력 및 병렬-출력을 수행하는 승산 알고리즘을 제시하며, 먼저 유한체 $GF(2^m)$에서 임의의 두 다항식 $A(x)$와 $B(x)$의 승산에서 다음과 같이 승산 계수 원소들을 정의한다.

[정의 1] $GF(2^m)$에서 임의의 두 다항식 $A(x)$와 $B(x)$의 승산은 원시 기약 다항식 $F(x)$를 mod 계산하지 않은 경우 식 (11)과 같이 표현할 수 있다.

$$\begin{aligned} P(x) &= A(x) \cdot B(x) \\ &= \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} (a_i \cdot b_j) \cdot X^{(i+j)} \\ &= \sum_{n=0}^{2m-1} p_n \cdot x^n \end{aligned} \tag{11}$$

식 (11)에서 승산 다항식 $P(x)$의 계수원소 p_n을 표현하면 식 (12)와 같다.

$$p_n = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i \cdot b_j \tag{12}$$

여기서 $n = i + j$이며, $0 \le n \le 2^m - 2$로서 계수원소의 밑수 i와 j의 합이 승산 결과 계수원소 p의 밑수 n과 같으며, n인 계수원소 항들만 mod(2) 연산한다.

[예 1] $GF(2^4)$ 상의 두 다항식 $A(x)$와 $B(x)$의 승산에서 식 (12)에 의하여 $n = i + j = 4$인 승산 계수원소 p_4는 식 (13)과 같이 나타낼 수 있다.

$$\begin{aligned} p_4 &= \sum_{i=0}^{3} \sum_{j=0}^{3} a_i \cdot b_j \\ &= a_1 \cdot b_3 + a_2 \cdot b_2 + a_3 \cdot b_1 \end{aligned} \tag{13}$$

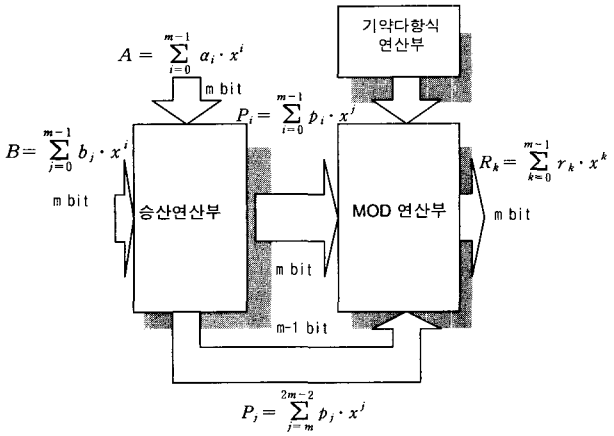
[정의 1]을 이용하여 $GF(2^m)$상에서 임의의 두 다항식 $A(x)$와 $B(x)$의 승산은 식 (14)와 같이 표현할 수 있다.

$$\begin{aligned} R(x) &= \{A(x) \cdot B(x)\} \bmod (F(x)) \\ &= \left\{ \sum_{j=0}^{m-1} A(x) \cdot (b_j \cdot x^j) \right\} \bmod (F(x)) \\ &= \left\{ \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} (a_i \cdot b_j) \cdot x^{(i+j)} \right\} \bmod (F(x)) \\ &= \left\{ \sum_{n=0}^{2m-2} p_n \cdot x^n \right\} \bmod (F(x)) \\ &= \left\{ \sum_{i=0}^{m-1} p_i \cdot x^i + \sum_{j=m}^{2m-2} p_j \cdot x^j \right\} \bmod (F(x)) \\ &= \sum_{i=0}^{m-1} p_i \cdot x^i + \left\{ \sum_{j=m}^{2m-2} p_j \cdot x^j \right\} \bmod (F(x)) \\ &= \sum_{k=0}^{m-1} r_k \cdot x^k \end{aligned} \tag{14}$$

여기서 r_k는 원시 기약 다항식 $F(x)$에 의해 생성된 승산 결과의 계수 원소이다.

3. 유한체상의 병렬 승산기의 설계

이 장에서는 앞장에서 논한 $GF(2^m)$상의 승산 알고리즘 $R(x) = \{A(x) \cdot B(x)\} \bmod (F(x))$를 실행하는 병렬-입력 및 병렬-출력을 갖는 셀 배열 병렬 승산기의 설계를 논한다. (그림 1)은 $GF(2^m)$상의 두 다항식의 승산을 실행하는 셀 배열 병렬 승산기의 구성도이다.



(그림 1) $GF(2^m)$상의 셀 배열 병렬 승산기

(그림 1)의 셀 배열 병렬 승산기는 $GF(2^m)$상의 두 다항식의 계수들의 승산을 실행하는 승산연산부와 기약다항식을 산술연산 처리한는 기약다항식연산부와 승산연산부의 출력을 입력으로 하여 기약 다항식에 의한 $\bmod(F(x))$ 연산을 행하는 MOD연산부로 구성되며, 이들의 구성은 다음과 같다.

3.1 승산연산부

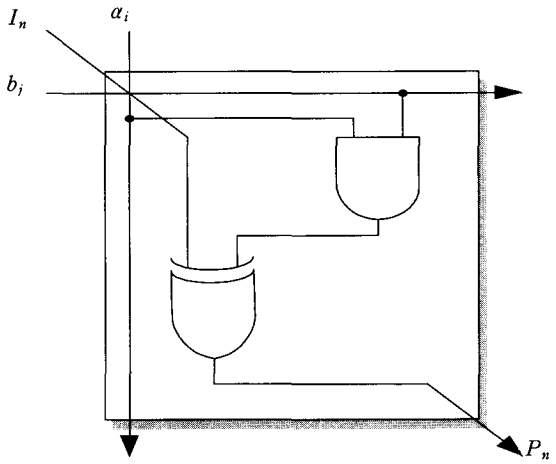
유한체 $GF(2^m)$ 상의 두 다항식의 승산 알고리즘에서 [정의 1]을 실행하는 승산연산부는 AND 게이트와 XOR 게이트로 설계된 기본 셀의 배열에 의해 구성된다. (그림 2)는 기본 셀의 회로도이다. 이 기본 셀은 계수 a_i 비트와 계수 b_j 비트의 AND 연산 결과와 전단의 출력 I_n을 XOR 연산을 행하며, 식 (12)로부터 이 기본 셀의 출력 p_n을 구할 수 있다.

$$p_n = (a_i \cdot b_j) \oplus I_n \tag{15}$$

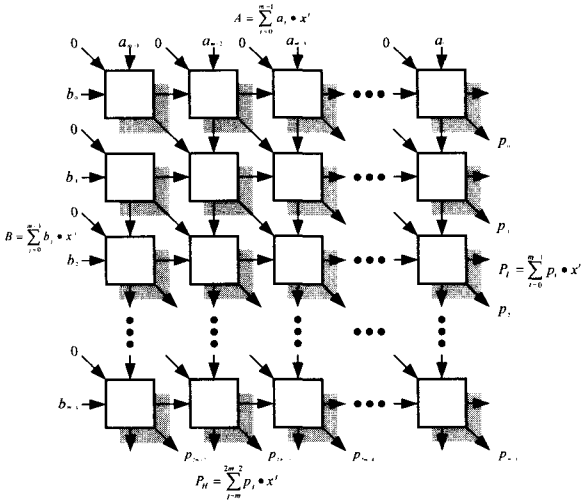
$$I_n = \sum_{t=i+1}^{n} \sum_{s=j-1}^{0} (a_t \cdot b_s) \tag{16}$$

여기서 $n = i+j = t+s$ 이며, p_n의 출력은 i 번째 열과 j 번째 행의 기본 셀의 출력이다. 식 (16)의 I_n은 전단의 기본 셀의 출력을 나타낸다.

이 기본 셀의 배열에 의한 $GF(2^m)$ 상의 두 다항식의 계수 원소들의 승산을 실행하는 승산연산부는 (그림 3)과 같다. (그림 3)의 상측에는 $A(x) = \sum_{i=0}^{m-1} a_i \cdot x^i$의 계수원소들이 입력으로 가해지고 좌측에는 $B(x) = \sum_{j=0}^{m-1} b_j \cdot x^j$의 계수원소들이 입력으로 가해진다. $P(x) = A(x) \cdot B(x)$의 계수원소인 $p_n = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} a_i \cdot b_j$는 분할되어 (그림 3)의 우측에 $P_L(x) = \sum_{i=0}^{m-1} p_i \cdot x^i$의 계수원소가 출력으로 나타나고, 아래쪽에는 $P_H(x) = \sum_{j=m}^{2m-2} p_j \cdot x^j$의 계수원소가 출력으로 나타난다.



(그림 2) 승산연산부의 기본 셀

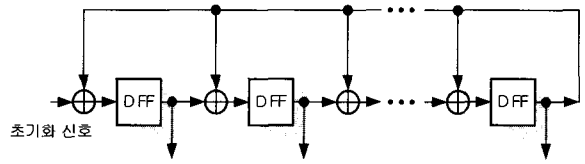


(그림 3) $GF(2^m)$상의 승산연산부

3.2 기약다항식연산부

$GF(2^m)$ 상의 기약다항식 $F(x) = 0$이고 모닉 다항식이므로 $x^m = \sum_{i=0}^{m-1} f_i \cdot x^i$ 이다. 이 기약다항식에 의해 두 다항식의 승산에서 m이상의 차수를 $m-1$이하로 감소시킨다. $GF(2^m)$

상의 기약다항식연산부는 (그림 4)와 같다. (그림 4)의 기약다항식연산부는 XOR 게이트들, D 플립플롭 회로들에 의해 구성되며, 이 연산부의 동작은 기플롭 회로의 출력이 한 비트씩 좌측으로 이동하면서 MOD 연산부의 각 셀내의 AND 게이트들을 동작시킨다.



(그림 4) $GF(2^m)$상의 기약다항식 연산부

3.3 MOD연산부

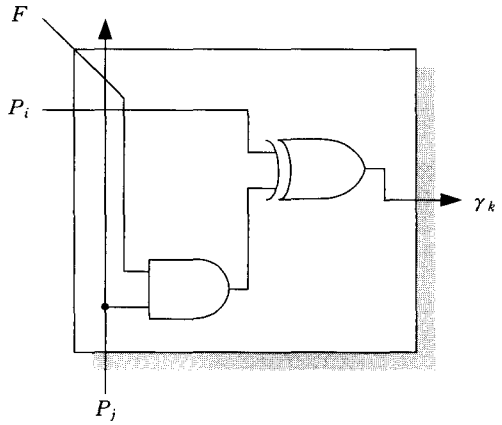
유한체 $GF(2^m)$상의 두 다항식의 승산 알고리즘의 식 (14)에서 승산 결과 $R(x)$는 다음과 표현된다.

$$R(x) = \sum_{i=0}^{m-1} p_i \cdot x^i + \left\{ \sum_{j=m}^{2m-2} p_j \cdot x^j \right\} \bmod (F(x)) \qquad (17)$$

식 (17)을 수행하는 MOD연산부는 승산연산부의 출력을 입력으로 하며, AND 게이트와 XOR 게이트로 설계된 기본 셀의 배열에 의해 구성된다. (그림 5)는 기본 셀의 회로도이며 이 기본 셀은 다항식의 계수들만을 계산하며, 기본 셀의 출력 r_k는 식 (17)로부터 계수만을 구할 수 있다.

$$r_k = (p_j \cdot F) \oplus p_i \qquad (18)$$

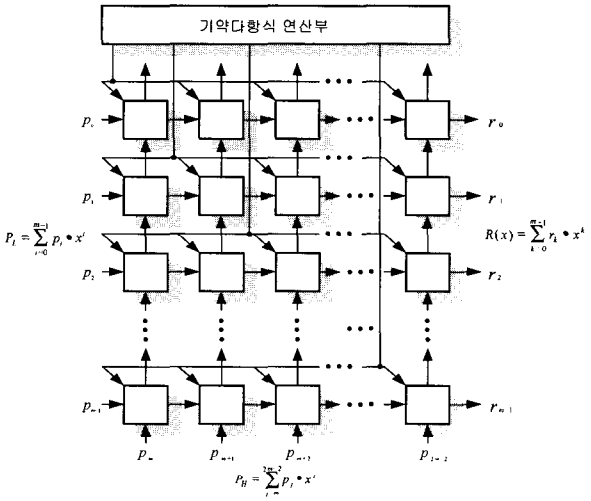
여기서 p_i는 승산연산부의 우측단의 출력인 $P_L(x)$의 계수이고, p_j는 승산연산부의 하단의 출력인 $P_H(x)$의 계수이며, F는 기약다항식연산부의 출력이다. 또한 i는 $\{0, 1, \cdots, m-1\}$이고 j는 $\{m, m+1, \cdots, 2m-2\}$이다.



(그림 5) MOD연산부의 기본 셀

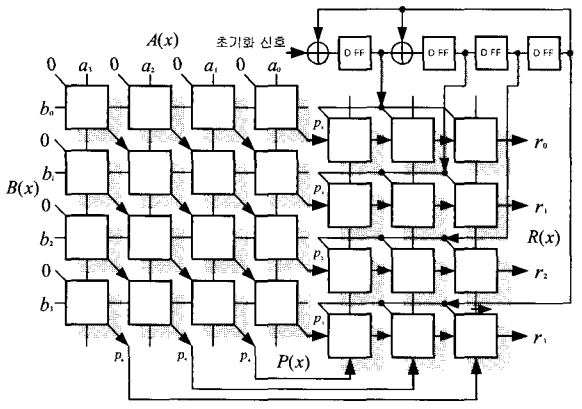
이 기본 셀의 배열에 의한 $GF(2^m)$상의 승산연산부와 기약다항식연산부의 출력을 입력으로 하는 MOD연산부는 (그림 6)과 같다.

(그림 6)의 MOD연산부에서 상측은 기약다항식연산부의 출력이 가해지고, 좌측은 승산연산부의 출력 $P_L(x) = \sum_{i=0}^{m-1} p_i \cdot x^i$의 계수원소들이 가해지고, 아래쪽은 $P_H(x) = \sum_{j=m}^{2m-2} p_j \cdot x^j$의 계수원소들이 가해진다. MOD연산부의 우측은 $R(x) = \sum_{k=0}^{m-1} r_k \cdot x^k$의 승산결과 계수원소들이 출력된다. 이때 MOD연산부의 동작은 기약다항식연산부에서 한 비트씩 좌측으로 이동할 때마다 $\bmod(F(x))$ 연산을 실행하도록 동기화되어 있다면 MOD연산부의 동작시간은 m 단위시간이 소비된다.



(그림 6) $GF(2^m)$상의 MOD연산부

위에서 논한 $GF(2^m)$상의 승산기 구성에 의하여 $GF(2^m)$의 두 다항식 $A(x)$와 $B(x)$의 승산을 실행하는 병렬-입력 병렬-출력을 갖는 셀 배열 병렬 승산기는 (그림 7)과 같다. (그림 7)의 셀 배열 병렬 승산기는 $GF(2^m)$상의 기약다항식 중 $F(x) = x^4 + x + 1$을 사용하였다. (그림 7)의 $R(x)$가 유한체 $GF(2^m)$상의 두 다항식의 승산 결과이다.



(그림 7) GF(24)상의 셀 배열 병렬 승산기

4. 시뮬레이션 및 비교 검토

본 논문에서 제안한 셀 배열 병렬 승산기를 포함하여 참고문헌의 승산기들은 독특한 성질과 장점을 갖는다. 일반적으로 사용되는 회로비교의 척도들은 간략화된 회로구성, 빠른 동작속도, 저전력 등을 들 수 있다. 회로의 간략화를 평가하기 위해서는 구성소자의 개수 및 소자간 결선의 수, 입출력단자의 수, 기타 부속회로 및 게이트의 존재여부 등을 고려해야 한다. 또한 동작 속도는 입력이 인가되면서 회로의 동작출력이 나타나기까지의 소자에 의한 지연시간과 클럭시간 등이 중요한 고려 요소이다. 이외에도 주변회로 블록과의 호환 및 신호전달의 적합성 등 다양한 항목을 통해 종합적으로 평가될 수 있으며, 적용하고자 하는 목적에 따라 일부항목에 대한 상충(trade-off) 조건을 고려할 수 있다. 따라서 일부 항목만을 통해 단편적으로 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 따랐다.

여기서는 3장에서 제시한 유한체 $GF(2^m)$상의 승산 알고리즘 $R(x) = \{A(x) \cdot B(x)\} \bmod (F(x))$를 실행하는 병렬-입력 및 병렬-출력을 갖는 셀 배열 병렬 승산기를 구성하는 승산연산부, 기약다항식 연산부, MOD 연산부와 기약다항식 $F(x) = x^4 + x + 1$에 의한 셀 배열 승산기에 대하여 시뮬레이션을 통하여 동작특성을 보였다. 시뮬레이션은 Pspice를 사용하여 수행하였고, 클럭시간은 회로 동작의 안정성을 위하여 1μs에서 수행하였다.

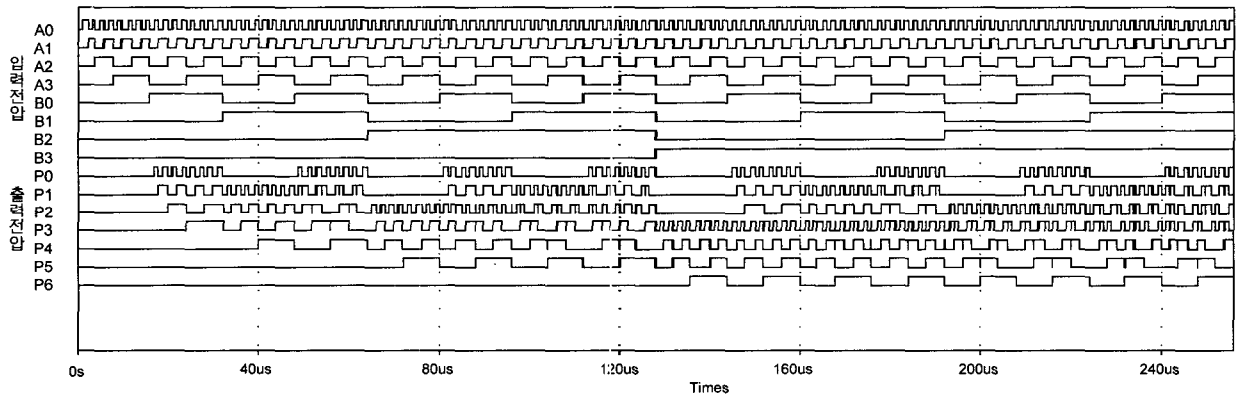
4.1 시뮬레이션 결과

4.1.1 승산 연산부

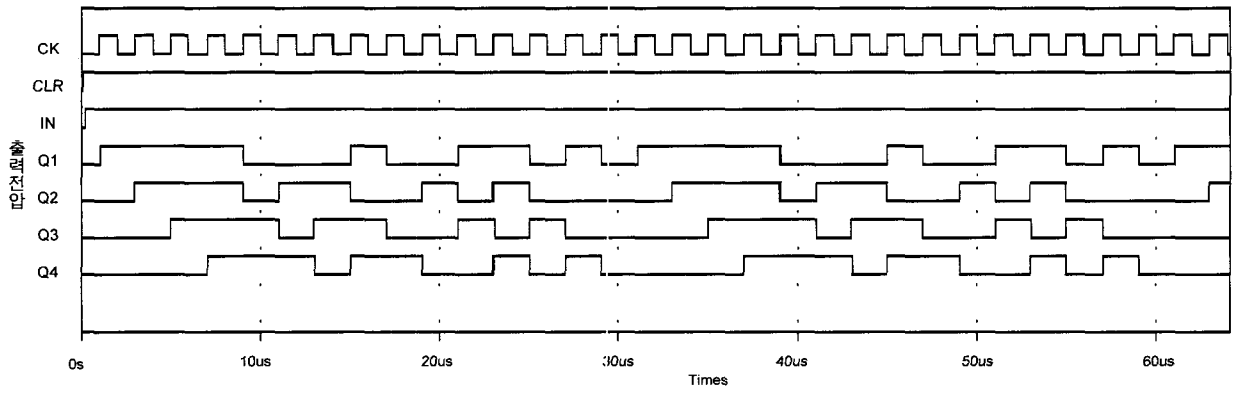
(그림 3)의 승산연산부의 시뮬레이션 결과를 그림 8에서 보였다. (그림 8)은 두 다항식 $A(x)$와 $B(x)$의 계수에 대한 256개의 파형을 입력으로 하였을 때 $P(x)$의 계수의 파형을 나타내었다. (그림 8)에서 200μs에서 입력전압 $A(x)$=(1 0 0 0)이고 $B(x)$=(1 1 0 0)일 때 출력전압 $P(x)$=(1 1 0 0 0 0 0)를 보인다. 승산연산부의 입력 파형의 주기는 1μs이며, 승산연산부의 동작시간은 1 단위시간(1μs)이 소비된다.

4.1.2 기약다항식 연산부

(그림 4)의 기약다항식 연산부의 시뮬레이션 결과를 (그림 9)에서 보였으며, 기약 다항식은 $F(x) = x^4 + x + 1$를 사용하였다. (그림 9)에서 D 플립플롭의 출력전압은 40μs에서



(그림 8) 승산연산부의 시뮬레이션 결과



(그림 9) 기약다항식연산부의 시뮬레이션 결과

$Q_4\ Q_3\ Q_2\ Q_1$ = (1 0 1 0)이며, 클럭신호의 주기는 1μs로 하였다. 동작시간은 기약다항식의 계수원소들이 이미 기약다항식 연산부의 각 D 플립플롭에 입력되었다고 가정하면 m 단위시간(클럭시간)이 소요된다.

4.1.3 MOD 연산부

(그림 6)의 MOD 연산부의 시뮬레이션 결과를 (그림 10)에서 보였다. (그림 9)에서 입력전압은 승산연산부의 출력인 $P(x)$의 계수들 p_0부터 p_6의 파형이며, 128개의 파형을 입력으로 하고, 기약다항식 $F(x) = x^4 + x + 1$를 사용한 (그림 9)의 기약다항식 연산부의 출력의 계수들 Q_1부터 Q_4의 파형을 입력으로 하였을 때 출력파형을 보였다. 그림 10에서 MOD연산부의 동작은 80μs에서 입력전압 $P(x)$ = (1 0 1 0 0 0 1)일 때 출력전압 $R(x)$ = (1 1 1 0)를 보인다. MOD 연산부의 입력 파형과 클럭신호의 주기를 1μs로 하였다.

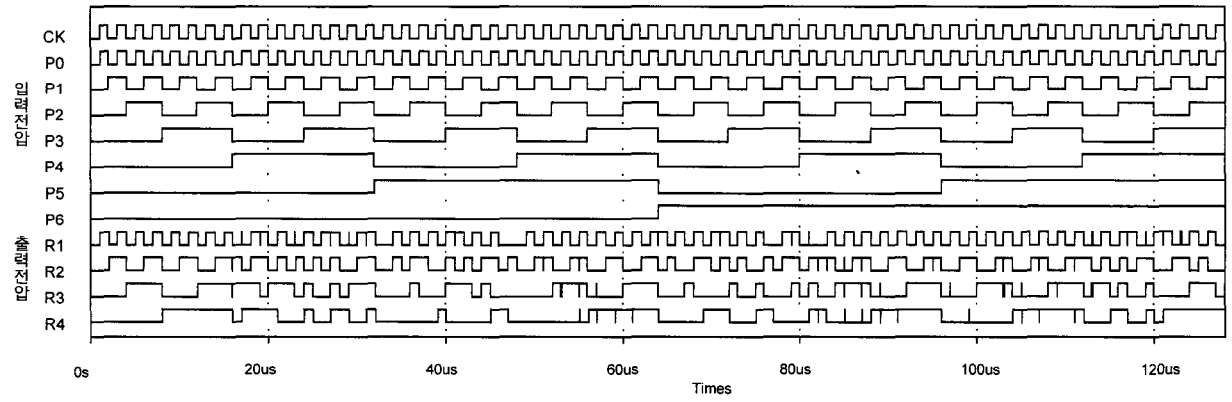
4.1.4 셀 배열 승산기

(그림 7)의 유한체 GF(2^4)에 대한 두 다항식 $A(x)$와 $B(x)$의 승산을 실현하는 병렬-입력 및 병렬-출력을 갖는 셀 배열 승산기의 시뮬레이션 결과를 (그림 11)에서 보였다. (그림 11)에서 $A(x)$와 $B(x)$의 계수에 대한 256개의 파형을 입력으로 하고, 기약다항식은 $F(x) = x4 + x + 1$를 입력으로 하였을 때 출력 $R(x)$의 계수들에 대한 파형을 보였다. (그림 11)에서 셀 배열 병렬 승산기의 동작은 200μs에서 입력전압 $A(x)$=(1 0 0 0)이고 $B(x)$=(1 1 0 0)일 때 출력전압 $R(x)$=(1 0 1 0)를 보인다. 셀 배열 승산기의 입력 파형과 클럭신호의 주기는 1μs이다.

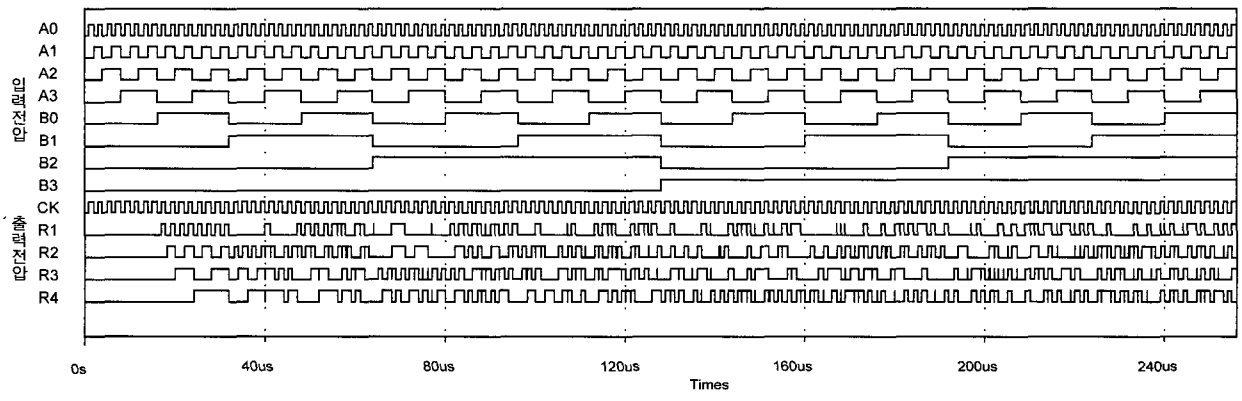
위의 Pspice를 사용한 시뮬레이션 동작파형을 통하여 본 논문에서 제시한 유한체 GF (2^4)에 대한 두 다항식 $A(x)$와 $B(x)$의 승산을 실현하는 새로운 방식의 병렬-입력 및 병렬-출력을 갖는 셀 배열 승산기가 클럭주기 1μs에서 안정하게 동작함을 보였으며, m을 증가하였을 경우 셀만을 증가시킬 수 있어 확장성이 용이한 장점이 있다. 다만, Pspice의 AND 및 XOR 게이트의 속도가 약 20ns 정도여서 클럭 속도를 높였을 때 오동작하기 때문에 이에 대한 연구가 요구된다.

4.2 비교 검토

본 논문에서 제시한 셀 배열 병렬 승산기의 구성과 참고문헌의 승산기들의 구성을 <표 1>에 정리하였다. <표 1>에서 보인 것처럼 Mastrovito[17], Koc[7], Masoleh[20] 및 본 논문에서는 유한체상의 두 다항식 A와 B의 승산함수는 시스토릭 구조를 갖지 않기 때문에 전단에서 들어오는 초기치 C가 없어서 $R = A \cdot B$이며, Yeh 등[11], Wei 등[16]



(그림 10) MDO연산부의 시뮬레이션 결과



(그림 11) 셀 배열 병렬 승산기의 시뮬레이션 결과

〈표 1〉 셀 배열 병렬 승산기의 비교표

Multiplier Item	Yeh[11]		Wei[16]	Mastrovito [17]	Koc[7]	Masoleh [20]	Lee[15]		This Paper	
	1-D	2-D					Type 1	Type 2		
1. Function	AB+C	AB+C	AB+C	AB	AB	AB	AB+C	AB+C	AB	AB
2. F(x)	x^4+x+1	x^4+x+1	x^4+x+1	x^4+x+1	AOP	AOP	AOP	AOP	x^4+x+1	AOP
3. I/O Format	Serial	Parallel	Parallel	Parallel	Parallel	Parallel	Parallel	Parallel	Parallel	Parallel
4. AND	3m (12)	$2m^2$ (32)	$3m^2$ (48)	$2m^2$ (32)	$2m^2$ (32)	m^2 (16)	$(m+1)^2$ (25)	$(m+1)^2$ (25)	2m(m-1) (24)	2m(m-1) (24)
5. XOR	2m (8)	$2m^2$ (32)	$2m^2$ (32)	$(m+1)^2$ (25)	$(m+1)^2$ (25)	$(m+1)^2$ (25)	$(m+1)^2$ (25)	(m+1)(m+2) (30)	$2m^2$ (32)	2m(m-1) (24)
6. D Flip-Flop	10m+2 (42)	$7m^2+16$ (128)	$10m^2$ (160)	$(m+1)^2$ (25)	-	-	$4(m+1)^2$ 100	$5(m+1)^2$ (125)	m (4)	-
7. Propagation time	$2m^2$	2m	2m	2m	2m	m	2m	m+1	m+1	m
Comment	( ) = the total gate number of generalization for degree m = 4 AOP means All One Polynomial of degree m									

과 Lee 등[15]의 승산기는 시스토릭 구조를 갖고 동작하기 때문에 승산함수 $R = A \cdot B + C$이다.

GF(2^4)상의 기약다항식 $F(x)$는 x^4+x+1, x^4+x^3+1와 $x^4+x^3+x^2+x+1$이 있으며, Lee은 AOP로서 $F(x) = x^4+x^3+x^2+x+1$를 적용하여 회로를 구성하였으며, 본 논문과 Yeh, Wei, Mastrovito의 승산기는 $F(x) = x^4+x+1$을 적용하여 회로를 구성하였다. I/O 형식은 Yeh는 직렬형(1D)과 병렬형(2D)의 승산기를 제안하였으며, 본 논문과 비교의 일관성을 위해 병렬형 승산기에 대해서 논의하였다. 다만, 직렬형의 예를 보인 것은 전체 동작시간이 상당히 증가함을 보이기 위한 것이다. 유한체상에서 승산은 기약다항식에 따라 계산량이 많아지거나 적어진다. 그러므로 임의의 기약다항식에서 동작할 수 있는 일반성을 갖는 승산기를 설계하는 것이 연구의 목적이다. 그러므로 본 논문은 기약다항식 연산부를 D 플립플롭과 XOR 게이트를 사용하여 일반성을 갖게 설계하였다. 다만 회로 구성상 기약다항식의 D 플립플롭과 XOR 게이트의 연결에 사용되는 스위치를 생략하였다.

승산기를 구성하는 게이트의 수를 비교하면 $m=4$인 경우 AND 게이트는 Masoleh, 본 논문과 Lee의 논문은 16개, 25개 및 24개로 우수하며, 타 연구는 다소 증가한다. XOR 게이트는 타 논문의 경우 25개로 우수하며, 본 연구는 약간 증가하는 단점이 있다. Koc과 Masoleh는 D 플립플롭을 전혀 사용하지 않으며, 본 논문은 기약다항식 연산부에서 4개가 필요하다. 그러나 Wei, Mastrovito, Lee의 논문은 많은 수의 D 플립플롭이 필요하다. 동작시간은 D 플립플롭을 사용하지 않는 Masoleh가 가장 우수하며, 본 논문과 Lee의 Type 2 승산기가 약간 우수하다. AOP 기약다항식은 수많은 기약다항식 중에서 특수한 기약다항식이며, 본 논문의 경우 AOP 기약다항식을 사용할 경우 기약다항식 연산부가 사용되지 않기 때문에 D 플립플롭과 XOR 게이트가 각각 m 개씩 감소한다. 그러므로 m = 4인 경우 AND 게이트와 XOR 게이트는 각각 24개이고, D 플립플롭이 사용되지 않는다.

승산기의 구조를 비교하면 Masoleh는 D 플립플롭을 사용하지 않는 간단한 AND와 XOR의 배열 구조로 구성되어 있으며 모듈성이 있으나 규칙성이 없어 소자가 증가하는 단점과 각 소자들 간의 연결이 매우 복잡한 단점이 있다. 반면에 Lee, Wei, Mastrovito는 시스토릭 구조로 동작하며, AND-XOR 셀 배열의 모듈성과 규칙성이 있으나 게이트 수가 증가하는 단점이 있다. 본 논문은 AND-XOR 셀 배열로 구성되어 있어 배열의 모듈성과 규칙성을 가지며, 소자간의 연결이 간단하고, 확장성이 용이한 장점이 있다. AOP 기약다항식을 사용하는 경우 XOR 게이트가 감소되고, D 플립플롭이 사용되지 않는 장점이 있으며, 기약다항식이 변경되었을 경우 기약다항식 연산부에서 기약다항식의 계수들을 입력하는데 많은 시간이 요구되는 단점이 있다.

5. 결 론

본 논문에서는 유한체상에서 승산을 수행하는 여러 가지 방법 중에서 한 가지 방법인 유한체 $GF(2^m)$상에서 두 다항식의 승산을 실현하는 병렬-입력 및 병렬-출력을 갖는 셀 배열 병렬 승산기를 제시하였다. 이 승산기는 승산연산부, 기약다항식연산부, MOD연산부로 구성된다. 승산연산부는 AND 게이트와 XOR 게이트로 설계한 기본 셀들을 행렬로 배열하여 구성하며, MOD연산부는 AND 게이트와 XOR 게이트의 기본 셀들을 행렬로 배열하여 구성하였다. 기약다항식 연산부는 XOR 게이트들과 D플립플롭 회로들을 사용하여 구성하였다. 또한 PSpice에 의한 시뮬레이션을 통하여 제안한 셀 배열 병렬 승산기가 정상적으로 동작함을 보였

으며, 승산기의 안정한 동작을 위해 클럭신호의 주기를 1μs로 하였다.

제시한 셀 배열 병렬 승산기는 $m=4$인 경우 AND 게이트가 24개, XOR 게이트의 수가 32개 소요되며, D 플립플롭회로가 4개 소요된다. D 플립플롭회로의 감소는 전체 시스템 구성을 단순화하는 장점이 있으며, 전체 지연시간을 감소시킨다. 또한 제시한 셀 배열 병렬 승산기의 전체 지연시간은 승산연산부는 1단위시간(클럭시간)이 소비되며, MOD 연산부와 기약다항식 연산부의 지연시간은 기약다항식의 계수원소들이 이미 기약다항식연산부에 입력되었다고 가정하면 D 플립플롭회로가 m개 소요되기 때문에 m 단위시간(클럭시간)이 소비된다. 그러므로 제시한 셀 배열 병렬 승산기의 전체 시스템 동작시간은 $m+1$ 단위시간이 소요되어 타 연구의 승산기보다 전체 지연시간이 빠른 장점이 있다. 또한 유한체상에서 수많은 기약다항식 중 특수한 기약다항식인 AOP 기약다항식을 사용할 경우 기약다항식 연산부가 사용되지 않기 때문에 D 플립플롭과 XOR 게이트가 각각 m 개씩 감소한다. 그러므로 m=4인 경우 AND 게이트와 XOR 게이트는 각각 24개이고, D 플립플롭은 사용되지 않는 장점이 있다. 그러나 기약다항식이 변경되었을 경우 기약다항식 연산부에서 기약다항식의 계수들을 입력하는데 많은 시간이 요구되는 단점이 있다.

본 논문에서 제시한 셀 배열 병렬 승산기는 AND-XOR 셀들의 배열로 구성되기 때문에 회선경로선택의 규칙성, 단순성, 배열의 모듈성, 병렬 동작의 이점을 가지며 특히 차수 m이 증가하는 유한체상의 두 다항식의 승산에서 확장성을 갖는다.

향후 연구과제는 기약다항식의 변경에 대하여 기약다항식 연산부의 일반성이 없는 단점이 있기 때문에 일반성을 갖는 기약다항식 연산부의 설계가 요구되며, Pspice의 AND 및 XOR 게이트의 속도가 약 20ns 정도여서 클럭 속도를 높였을 때 오동작하기 때문에 이에 대한 연구가 요구된다.

참 고 문 헌

[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] P. A. Scott, S. E. Tarvares and L. E. Peppard, "A Fast Multiplier for GF(2^m)," *IEEE J. Select. Areas Communications*, Vol.SAC-4, No.1, pp.707-717, Jan., 1986.

[5] I. S. Hsu, T. K. Truong, L. J. Deutsch and I. S. Reed, "A Comparison of VLSI Architecture of Finite Field Multipliers Using Dual, Normal, or Standard Bases," *IEEE Trans. Computers*, Vol.C-37, No.6, pp.735-739, Jun., 1988.

[6] 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.

[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] Kiamal Z. Pekmestzi, "Multiplexer-Based Array Multipliers," *IEEE Trans. Computers*, Vol 48, No.1, pp. 15-23, Jan., 1999.

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

[10] J. J. Wonziak, "Systolic Dual Basis Serial Multiplier," *IEE Proceeding Computers and Digital Technology*, Vol.145, No.3, pp.237-241, July., 1998.

[11] C. S. Yeh, I. S. Reed and T. K. Truong, "Systolic Multipliers for Finite Field GF(2m)," *IEEE Trans. Computers*, Vol.C-33, pp.357-360, Apr., 1984.

[12] 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.

[13] G. Drolet, "A New Representation of Finite Fields GF(2^m) Yielding Small Complexity Arithmetic," *IEEE Trans. Computers*, Vol.47, No.9, pp.938-946, Sept., 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] 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.

[16] S. W. Wei, "A Systolic Power-Sum Circuit for GF(2^m)," *IEEE Trans. Computers*, Vol.43, No.2, pp.226-229, Feb., 1994.

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

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

[20] 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.

[21] H. Wu, "Bit-Parallel Finite Field Multiplier and Squarer Using Polynomial Basis," *IEEE Trans. Computers*, Vol. 51, No.7, pp.750-758, July., 2002.

[22] C. L. Wang and J. H. Guo, "New Systolic Arrays for C+AB^2, Inversion, and Division in GF(2^m)," *IEEE Trans. Computers*, Vol.49, No.10, pp.1120-1125, Oct., 2000.

[23] C. H. Kim, S. Oh and J. Lim, "A New Hardware Architecture for Operation in GF(2^n)," *IEEE Trans. Computers*, Vol.51, No.1, pp.90-92, Jan., 2002.

성 현 경

e-mail : hkseong@mail.sangji.ac.kr

1982년 인하대학교 전자공학과(공학사)

1984년 인하대학교 대학원 전자공학과 (공학석사)

1991년 인하대학교 대학원 전자공학과 (공학박사)

1989년~1991년 부천전문대학 전자계산과 조교수

1991년~현재 상지대학교 컴퓨터·정보공학부 부교수

관심분야 : Multiple-Valued Logic Design, Computer Architecture & VLSI 설계, Information & Coding Theory Cryptography Theory & Security, Digital Signal Processing