기약 All One Polynomial을 이용한 유한체 $GF(2^m)$상의 시스톨릭 곱셈기 설계†

정회원 권 순 학*, 김 창 훈**, 홍 춘 표**

Design of Systolic Multipliers in $GF(2^m)$ Using an Irreducible All One Polynomial

Soonhak Kwon*, Chang Hoon Kim**, Chun Pyo Hong** ***Regular Members***

요 약

본 논문에서는 AOP(All One Polynomial)에 의해 결정되는 유한체 $GF(2^m)$상의 곱셈을 위한 두 가지 종류의 시스톨릭 어레이를 제안한다. 제안된 두 시스톨릭 어레이 모두 패러럴 입출력 구조를 가진다. 첫 번째 제안된 곱셈기는 $O(m^2)$의 면적 복잡도와 $O(1)$의 시간 복잡도를 가진다. 다시 말하면, 이 곱셈기는 $m(m+1)/2$ 개의 동일한 셀들로 이루어지며 초기 $m/2+1$ 사이클 지연 후, 1 사이클 마다 곱셈의 결과를 출력한다. 첫 번째 제안된 곱셈기를 기존의 AOP를 사용하는 병렬형 시스톨릭 곱셈기와 비교 분석한 결과 하드웨어 및 계산지연 시간에 있어 각각 12% 및 50%의 성능 개선을 보인다. 두 번째 제안된 시스톨릭 곱셈기는 암호응용을 위해 선형 어레이로 설계되었으며, $O(m)$의 면적 복잡도와 $O(m)$의 시간 복잡도를 가진다. 즉, $m+1$ 개의 동일한 셀들로 이루어지며 $m/2+1$ 사이클 마다 곱셈의 결과를 출력한다. 두 번째 곱셈기를 기존의 선형 시스톨릭 곱셈기들과 비교 분석한 결과, 하드웨어, 계산지연 시간, 그리고 처리율에 있어 각각 43%, 83%, 그리고 50%의 성능 개선을 보인다. 또한 제안된 곱셈기들은 높은 규칙성과 모듈성을 가지기 때문에 VLSI 구현에 매우 적합하다. 따라서 $GF(2^m)$ 응용을 위해, 본 연구에서 제안된 곱셈기들을 사용하면 최소의 하드웨어 사용으로 최대의 성능을 얻을 수 있다.

Key Words : Finite field Multiplier, Systolic Array, All One Polynomial, VLSI

ABSTRACT

In this paper, we present two systolic arrays for computing multiplications in $GF(2^m)$ generated by an irreducible all one polynomial (AOP). The proposed two systolic arrays have parallel-in parallel-out structure. The first systolic multiplier has area complexity of $O(m^2)$ and time complexity of $O(1)$. In other words, the multiplier consists of $m(m+1)/2$ identical cells and produces multiplication results at a rate of one every 1 clock cycle, after an initial delay of $m/2+1$ cycles. Compared with the previously proposed related multiplier using AOP, our design has 12 percent reduced hardware complexity and 50 percent reduced computation delay time. The other systolic multiplier, designed for cryptographic applications, has area complexity of $O(m)$ and time complexity of $O(m)$, i.e., it is composed of $m+1$ identical cells and produces multiplication results at a rate of one every $m/2+1$ clock cycles. Compared with other linear systolic multipliers, we find that our design has at least 43 percent reduced hardware complexity, 83 percent reduced computation delay time, and has twice higher throughput rate. Furthermore, since the proposed two architectures have a high regularity and modularity, they are well suited to VLSI implementations. Therefore, when the proposed architectures are used for $GF(2^m)$ applications, one can achieve maximum throughput performance with least hardware requirements.

* 성균관대학교 수학과 (shkwon@math.skku.ac.kr), ** 대구대학교 컴퓨터정보공학과 (chkim@dsp.taegu.ac.kr)
논문번호 : 040022-0115, 접수일자 : 2004년 1월 19일
※이 논문은 성균관대학교의 성균학술연구비에 의하여 연구되었음

Ⅰ. 서 론

유한체 $GF(2^m)$상의 연산은 오류제어 코딩, 암호학 등 다양한 분야에 적용되고 있다[6]. $GF(2^m)$상의 중요한 연산으로는 덧셈, 곱셈, 나눗셈 그리고 지수 연산이 있다. 여기서 덧셈은 비트별 배타적 논리합 (XOR) 연산으로 간단하며, 적은 비용으로 구현할 수 있다. 그러나 나머지 연산들은 아주 복잡할 뿐 아니라 구현에 많은 비용이 든다. 여기서 곱셈은 가장 중요한 연산으로 취급된다. 이는 반복적인 곱셈을 통하여 나눗셈 및 지수 연산을 수행할 수 있기 때문이다[11,12,15]. 따라서 효율적인 곱셈기의 설계는 매우 중요하다.

GF(2m)상의 곱셈 알고리즘은 basis의 선택에 의존적이다. 지금까지 사용된 대표적인 basis는 1) polynomial basis, 2) dual basis, 3) normal basis가 있다. 기존의 곱셈기들 중 Berlekamp 형태의 곱셈기들[1,2]은 dual basis를 사용하였고 Massey-Omura 형태의 곱셈기들[3,4,5,17,18]은 nomal basis를 사용하였다. 그러나 위에서 언급한 곱셈기들은 크게 다음과 같은 두 가지의 단점을 가진다. 첫 번째, 불규칙적인 회로 구조를 가진다. 다시 말하면, m의 선택을 달리할 경우 각각 다른 하드웨어 구조를 가진다. 암호 응용에서와 같이 두개의 유한체를 사용한다면(여기서 하나의 필드는 다른 필드의 하부 필드이다) 아주 큰 단점이 된다. 두 번째, 전역 신호를 가지기 때문에 m이 커질 경우 심각한 성능 저하를 야기 시킨다. 따라서 설계시 그 회로의 정확한 성능을 측정하기 어렵다. 그러나 시스톨릭 구조의 곱셈기들은 위에서 언급한 문제들을 가지지 않는다. 시스톨릭 곱셈기는 동일한 셀들의 반복적인 배치를 통하여 이루어지기 때문에 m의 선택에 의존적이지 않다. 또한 각각의 셀들은 단지 인근의 셀들과 연결되기 때문에 m이 커져도 신호전파 지연시간에 영향을 미치지 않는다. 따라서 신호들을 고속으로 전파시킬 수 있다.

지금까지 polynomial basis[7,8,10,11,13,15]와 dual basis[9]를 이용한 시스톨릭 곱셈기들이 많이 제안 되어졌다. 이중 Lee[10]등은 확장된 AOP basis를 이용하여, 다른 비트-패러럴 곱셈기들에 비해 훨씬 낮은 칩 면적 및 계산 지연시간을 가지는 구조를 제안하였다. 본 논문에서는 확장된 AOP basis를 이용하여 두 가지 종류의 시스톨릭 곱셈기를 제안한다. 첫 번째 제안하는 구조는 Lee[10]등이 제안한 비트-패러럴 곱셈기에 비해 12%의 낮은 칩 면적을 가지면서 계산 지연시간에 있어 50%의 성능 향상을 보인다. 또한 저자들은 암호와 같이 큰 m을 요구하는 응용을 위해 선형 시스톨릭 어레이도 제안한다. 제안된 선형 시스톨릭 구조는 기존의 유사한 시스톨릭 곱셈기들에 비해 훨씬 낮은 칩 면적을 가지면서 계산 지연시간에 있어 83% 그리고 처리율에 있어 50%의 성능 향상을 보인다. 더욱이, 본 연구에서 제안된 두 시스톨릭 어레이들은 높은 규칙성 및 모듈성을 가지기 때문에 VLSI 구현에 매우 적합하다. 따라서 GF(2m) 응용을 위해, 본 연구에서 제안된 곱셈기들을 사용하면 최소의 하드웨어 사용으로 최대의 성능을 얻을 수 있다.

Ⅱ. AOP를 이용한 $GF(2^m)$상의 곱셈

$GF(2^m)$을 2m개의 원소들로 구성된 유한체라 하자. $m+1=p$가 소수이고 2가 (mod p)에 대해 원시근(primitive root)일 때 $f(X)=1+X+X^2+\cdots+X^m \in GF(2)[X]$와 같은 형태의 기약 다항식은 존재한다. 이와 같은 다항식을 일반적으로 AOP(all one polynomial)라 부른다. α를 AOP f(X)의 근이라 하면 $GF(2^m)$은 $GF(2)$상에서 polynomial basis $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$를 가진다. α가 AOP $f(X)$의 근이라는 사실로부터 $\alpha^{m+1}-1=(\alpha-1)f(\alpha)=0$ 이기 때문에 우리는 $\alpha^{m+1}=1$ 이라는 좋은 속성을 얻을 수 있다. 따라서 차수 m의 AOP가 기약 일 때 x가 $GF(2^m)$상의 임의의 원소라면 확장된 AOP basis $\{1, \alpha, \alpha^2, \cdots, \alpha^m\}$에 대하여 $x=\sum_{i=0}^{m} x_i \alpha^i$와 같이 나타낼 수 있다. 즉, $\alpha^{m+1}=1$의 성질을 이용하여 우리는 $GF(2^m)$상의 효율적인 곱셈기를 설계할 수 있다. 위의 속성을 이용하여, [20,21]에서는 Berlekamp 형태의 비트-시리얼 곱셈기를 제안하였고, [3,5,18]에서는 Massey- Omura 형태의(Type-I optimal normal basis) 비트-패러럴 곱셈기를 제안하였다. 일반적으로, AOP basis는 무수히 많은 m에 대하여 존재하는데 $m \le 2000$ 경우 118개가 존재하는 것으로 알려져 있다. 예를 들면,

$m=2, 4, 10, 12, 18,$
$28, 36, 52, 58, 60, 66, 82, 100, 106, \cdots$
일 때 AOP basis는 존재한다. 지금부터 우리는 기약 AOP $f(X)=1+X+X^2+\cdots+X^m$가 존재한다고 가정한다.

Definition 1. $x=\sum_{i=0}^{m} x_i\alpha^i$가 $GF(2^m)$상의 한 원소라 하자. 만약 $i\equiv j \pmod{m+1}$ 이라면, $x_i\in GF(2)$는 $x_i=x_j$로 정의하자. 여기서 i는 임의의 정수이고 j는 $0,1,2,\cdots,m$에 속하는 정수이다. Definition 1과 $\alpha^{m+1}=1$을 이용하면, 우리는 아래의 Lemma 1을 쉽게 얻을 수 있다.

Lemma 1. $x=\sum_{i=0}^{m} x_i\alpha^i$와 $y=\sum_{i=0}^{m} y_i\alpha^i$가 $GF(2^m)$상의 두 원소라 두면, 두 원소의 곱은 $xy=\sum_{k=0}^{m}(xy)_k\alpha^k$로 나타낼 수 있다. 여기서 k번째 계수 $(xy)_k$는 $(xy)_k=\sum_{i=0}^{m} y_i x_{k-i}$로 쓸 수 있다. 위의 Lemma 1은 식(1)에 의해 쉽게 증명될 수 있다.

$$xy=\sum_{i=0}^{m} x_i\alpha^i \sum_{j=0}^{m} y_j\alpha^j=\sum x_i y_j\alpha^{i+j} = \sum_{i=0}^{m}\sum_{j=0}^{m} y_j x_{\langle i-j\rangle}\alpha^i \quad (1)$$

여기서 $\langle i-j\rangle$는 $\langle i-j\rangle\equiv i-j \pmod{m+1}$을 만족하는 $0,1,2,\cdots,m$에 속하는 유일한 정수이다. $m+1=p$가 홀수인 소수이므로 $0, 2, 4, \cdots, 2m$ 와 $0, 1, 2, \cdots, m$는 $(\mathrm{mod}\ m+1)$에 대하여 동일한 집합이다. 따라서 Definition 1에 의해 $x\in GF(2^m)$에 대하여, 식(2)를 얻을 수 있다.

$$\{x_0, x_2, x_4, \cdots, x_{2m}\} = \{x_0, x_1, x_2, \cdots, x_m\} \quad (2)$$

Lemma 1로부터, k번째 계수 $(xy)_k$는 식(3)과 같이 행벡터와 열벡터의 행렬 곱셈으로 나타낼 수 있다

$$(xy)_k=(x_k, x_{k-1}, \cdots, x_{k-m})(y_0, y_1, \cdots, y_m)^T \quad (3)$$

식 (3) 에서 $(y_0, y_1, \cdots, y_m)^T$ 는 열 벡터 $(y_0, y_1, \cdots, y_m)$ 의 전치 행렬이다.

Theorem 1. $x=\sum_{i=0}^{m} x_i\alpha^i$ 와 $y=\sum_{i=0}^{m} y_i\alpha^i$ 가 $GF(2^m)$상의 두 원소라 두면, 임의의 정수 k에 대하여, 우리는 식(4)를 얻을 수 있다.

$$(xy)_{2k}=\sum_{i=0}^{m} y_{k+i}x_{k-i} \quad (4)$$

Proof. Definition1과 Lemma1을 이용하면 식 (5)를 얻을 수 있다.

$$\begin{aligned}(xy)_{2k} &= \sum_{i=0}^{m} y_i x_{2k-i}\\ &=(x_{2k}, x_{2k-1}, \cdots, x_{2k-m})(y_0, y_1, \cdots, y_m)^T\\ &=(x_k, x_{k-1}, \cdots, x_{k-m})(y_k, y_{k+1}, \cdots, y_{k+m})^T\\ &=\sum_{i=0}^{m} y_{k+i}x_{k-i} \end{aligned} \quad (5)$$

식(5)의 3번째 등식은 두 번째 등식에서 벡터를 k만큼 왼쪽으로 쉬프트 시키면 된다. Theorem 1 으로부터 $GF(2^m)$상의 시스톨릭 곱셈기는 쉽게 얻을 수 있으며, 이미 Lee[10]등이 제안 하였다. 그러나 Lee[10]등의 논문에서는 $GF(2^m)$상의 두 원소의 내적이라는 익숙하지 않은 정의와 시스톨릭 어레이를 유도하는 과정이 매우 복잡하다. 그러나 본 논문의 Theorem 1의 설명은 아주 간단하고 이해하기 쉽다. Theorem 1로부터, 비트-패러럴 시스톨릭 곱셈기의 기본 셀은 그림 1과 같이 쉽게 유도 할 수 있다. 완전한 곱셈기 구조는 [10]에 나타난다.

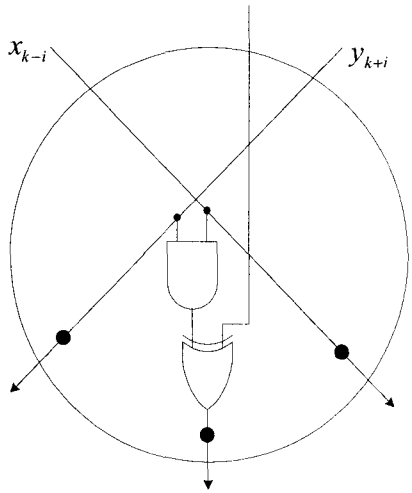


그림 1. (i, k) 기본 셀의 회로도 [10]

Ⅲ. AOP를 이용한 $GF(2^m)$상의 새로운 비트-패러럴 시스톨릭 곱셈기 설계

본 절에서, 우리는 Theorem 1을 수정하여, Lee[10]등이 제안한 구조보다 계산 지연시간 및 칩 면적에 있어 개선된 비트-패러럴 시스톨릭 어레이를 설계한다.

Theorem 2. $x=\sum_{i=0}^{m} x_i\alpha^i$ 와 $y=\sum_{i=0}^{m} y_i\alpha^i$ 가 $GF(2^m)$상의 두 원소라 두면, 임의의 정수 k에 대하여, 우리는 식(6)을 얻을 수 있다.

$$(xy)_{2k}=\sum_{i=0}^{m/2-1}(y_{k+i}x_{k-i}+y_{k-i-1}x_{k+i+1}) + y_{k+m/2}x_{k-m/2} \quad (6)$$

Proof. Theorem 1을 이용하면, 아래의 식(7)을 얻을 수 있다.

$$\begin{aligned}(xy)_{2k} &= \sum_{i=0}^{m} y_{k+i}x_{k-i}\\ &= \sum_{i=0}^{m/2-1} y_{k+i}x_{k-i}+\sum_{i=m/2+1}^{m} y_{k+i}x_{k-i}\\ &\quad + y_{k+m/2}x_{k-m/2}\\ &= \sum_{i=0}^{m/2-1} y_{k+i}x_{k-i}+\sum_{i=0}^{m/2-1} y_{k+m-i}x_{k-(m-i)}\\ &\quad + y_{k+m/2}x_{k-m/2} \quad (7)\\ &= \sum_{i=0}^{m/2-1} y_{k+i}x_{k-i}+\sum_{i=0}^{m/2-1} y_{k-i-1}x_{k+i+1}\\ &\quad + y_{k+m/2}x_{k-m/2}\\ &= \sum_{i=0}^{m/2-1}(y_{k+i}x_{k-i}+y_{k-i-i}x_{k+i+1})\\ &\quad + y_{k+m/2}x_{k-m/2}\end{aligned}$$

식 (7)로부터, 각각의 $(xy)_{2k}$에 대하여 우리는 아래의 열벡터를 정의한다.

$$W_k=(\omega_{0k},\ \omega_{1k},\ \cdots,\ \omega_{(m/2-1)k},\ \omega_{(m/2)k})^T \quad (8)$$

여기서

$$\omega_{ik}=y_{k+i}x_{k-i}+y_{k-i-1}x_{k+i+1},\ \text{if}\ 0\le i\le m/2-1 \quad (9)$$

$$\omega_{(m/2)k}=y_{k+m/2}x_{k-m/2},\ \text{if}\ i=m/2 \quad (10)$$

따라서, 열벡터 W_k의 모든 성분의 합은 정확히 $(xy)_{2k}$이고 W_k는 아래의 $(m/2+1\times m+1)$ 행렬 $W=(w_{ik})$의 k번째 $(0\le k\le m)$ 열벡터로 나타난다.

$$W=\begin{pmatrix}\omega_{00} & \omega_{01} & \cdot & \cdot & \omega_{0m}\\ \omega_{10} & \omega_{11} & \cdot & \cdot & \omega_{1m}\\ \omega_{20} & \omega_{21} & \cdot & \cdot & \omega_{2m}\\ \cdot & \cdot & \cdot & \cdot & \cdot\\ \cdot & \cdot & \cdot & \cdot & \cdot\\ \omega_{(m/2-1)0} & \omega_{(m/2-1)1} & \cdot & \cdot & \omega_{(m/2-1)m}\\ \omega_{(m/2)0} & \omega_{(m/2)1} & \cdot & \cdot & \omega_{(m/2)m}\end{pmatrix} \quad (11)$$

각각의 $0\le i\le m/2-1$와 $0\le k\le m$에 대하여 아래의 관계식을 이용하면,

$$\omega_{ik}=y_{k+i}x_{k-i}+y_{k-i-1}x_{k+i+1} \quad (12)$$

식 (13)을 얻을 수 있다.

$$\omega_{(i-1)(k-1)}=y_{k+i-2}x_{k-i}+y_{k-i-1}x_{k+i-1} \quad (13)$$

즉, w_{ik}의 x_{k-i}와 y_{k-i-1}신호는 $w_{(i-1)(k-1)}$로부터 얻을 수 있고, 또한 식(14) 로부터 x_{k+i+1}과 y_{k+i} 신호는 $w_{(i-1)(k+1)}$ 로부터 얻을 수 있다.

$$\omega_{(i-1)(k+1)}=y_{k+i}x_{k-i+2}+y_{k-i+1}x_{k+i+1} \quad (14)$$

마지막 행의 신호들은 $m/2-1$ 번째 행으로부터 얻을 수 있다. 즉, $w_{(m/2)0}=y_{m/2}x_{-m/2}=y_{m/2}x_{m/2+1}$는 $w_{(m/2-1)1}=y_{m/2}x_{2-m/2}+y_{1-m/2}x_{m/2+1}$의 $y_{m/2}$와 $x_{m/2+1}$로부터 얻을 수 있다. 그리고 각 $1\le k\le m$에 대하여 $w_{(m/2)k}=y_{k+m/2}x_{k-m/2}$는 $w_{(m/2)k}=y_{k+m/2}x_{k-m/2}+y_{k-m/2-1}x_{k+m/2-1}=y_{k+m/2-2}x_{k-m/2}+y_{k+m/2}x_{k+m/2-1}$의 $y_{k+m/2}$와 $x_{k-m/2}$ 로부터 얻을 수 있다. 따라서 지금까지 설명된 내용을 바탕으로 우리는 basis $\{1,\alpha^2,\alpha^4,\cdots,\alpha^{2m}\}$에 대하여 비트-패러럴 시스톨릭 곱셈기를 설계할 수 있다. 여기서 $\alpha^{m+1}=1$

이다. 기본 셀의 구조는 그림 2와 같다. 그림 2에서 '•'은 1-비트 1-사이클 지연소자 이다.

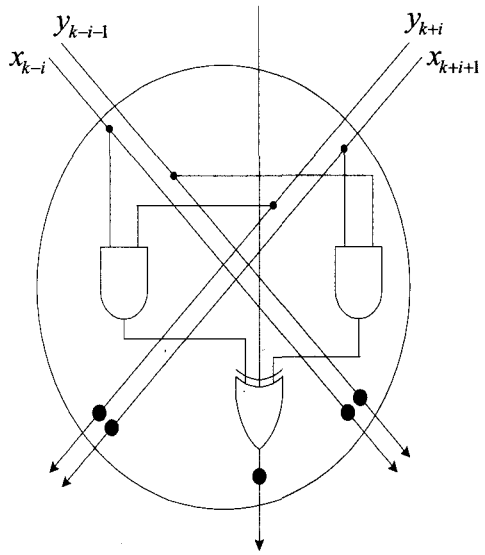


그림 2. 새로운 (i, k) 기본 셀의 회로도

그림 3은 완전한 비트-패러럴 시스톨릭 곱셈기이고 $m=4$로 가정하였다. 따라서 행렬 W는 아래의 식 (15)와 같다. $z=\sum_{i=0}^{m} z_i \alpha^i$를 $GF(2^m)$상의 또다른 원소라 하면, 곱의 합연산 $xy+z$은 그림 3의 시스톨릭 곱셈기를 이용하여 계산 할 수 있다.

표 1에 본 절에서 제안된 구조와 관련된 기존의 시스톨릭 곱셈기들과 하드웨어 및 계산 시간 측면에서 비교분석 하였다. 조금 더 자세한 비교를 위하여, 우리는 [22]에 따라 3-입력 AND 게이트와 3입력 XOR 게이트는 각각 2개의 2-입력 AND 게이트 그리고 2-입력 XOR 게이트로 구성된다고 가정하였고 2-입력 AND 게이트, 2-입력 XOR 게이트, 2-to-1 MUX, 그리고 1-비트 래치는 각각 4, 6, 6, 그리고 8개의 트랜지스터(TR)로 구성된다고 가정하였다. 또한 D_A, D_X, 그리고 D_L은 각각 AND, XOR, 그리고 래치의 계산 지연시간을 나타낸다. 표 1 로부터 Lee 등이 제안한 곱셈기가 본 논문에서 제안된 구조보다 기본 셀에 대해서는 낮은 하드웨어 복잡도를 가지지만 셀의 개수가 2배 이상이기 때문에 전체적으로는 약 12%의 더 많은 TR을 요구한다. 또한 최대 처리기 지연시간 측면에서 보면, 본 연구에서 제안한 구조가 Lee 등이 제안한 구조보다 D_X만큼 많지만, 계산 지연시간을 약 50% 감소시키기 때문에 전체적인 계산 지연시간은 훨씬 적다.

$$W=\begin{pmatrix} y_0x_0+y_4x_1 & y_1x_1+y_0x_2 & y_2x_2+y_1x_3 & y_3x_3+y_2x_4 & y_4x_4+y_3x_0 \\ y_1x_4+y_3x_2 & y_2x_0+y_4x_3 & y_3x_1+y_0x_4 & y_4x_2+y_1x_0 & y_0x_3+y_2x_1 \\ y_2x_3 & y_3x_4 & y_4x_0 & y_0x_1 & y_1x_2 \end{pmatrix} \quad (15)$$

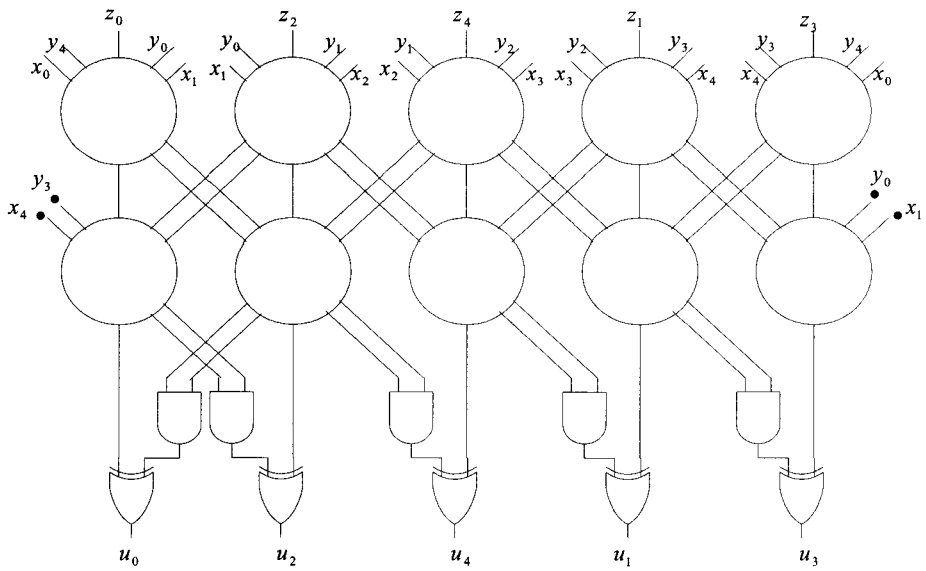


그림 3. $GF(2^4)$상의 $u=xy+z$ 계산을 위한 새로운 시스톨릭 어레이

표 1. $GF(2^m)$상의 비트-패러럴 시스톨릭 곱셈기들의 특성 비교

	Wang [7]	Yeh [8]	Fenn [9]	Wei [11]	Lee [10]	Fig. 3
Basis	Polynomial	Polynomial	Dual	Polynomial	AOP	AOP
기능	AB	AB+C	AB	AB^2+C	AB+C	AB+C
셀 구성요소						
AND	2	2	2	3	1	2
XOR	2	2	2	2	1	2
Latch	7	7	7	10	3	5
셀의 갯수	m^2	m^2	m^2	m^2	$(m+1)^2$	$m(m+1)/2$
TR 갯수	$76m^2$	$76m^2$	$76m^2$	$104m^2$	$34m^2+116m+58$	$30m^2+30m$
지연시간	$3m$	$3m$	$3m$	$3m$	$m+1$	$m/2+1$
최대 처리기 지연시간	$D_A+2D_X+D_L$	$D_A+D_X+D_L$	$D_A+D_X+D_L$	$D_A+2D_X+D_L$	$D_A+D_X+D_L$	$D_A+D_{3X}+D_L$

Ⅳ. 암호응용을 위한 선형 시스톨릭 어레이

비록 3절에서 제안된 비트-패러럴 시스톨릭 어레이가 기존의 곱셈기들에 비해서 낮은 칩 면적을 가지지만 암호응용에는 적합하지 않다. 최근 타원곡선 암호시스템이 비트당 높은 안전도를 보이지만 최소한 m이 163보다 커야한다. 따라서 본 절에서는 암호응용을 위한 선형 시스톨릭 어레이를 설계한다. 이를 위하여, 2절의 Theorem 2를 이용하면 우리는 그림 4와 같은 지연시간 $m/2+1$을 가지는 선형 시스톨릭 어레이를 구성할 수 있다. 그림 5는 k번째 $(0 \le k \le m)$ 기본 셀 구조이다. 그림 5에서 부분적인 합 s_i는 $0 < i \le m/2$ 일 경우 $s_i = z_{2k} + \sum_{j=0}^{i-1}(y_{k+j}x_{k-j} + y_{k-j-1}x_{k+j+1})$과 같고 마지막 출력 $(xy+z)_{2k}$는 $s_{m/2} + y_{k+m/2}x_{k-m/2}$이다. 그림 5에 보이는 바와 같이, 이 두 연산을 구분하기 위하여 $m/2+1$ 비트 길이의 콘트롤 시퀀스 $(11\cdots10)$를 추가하였다. 본 절에서 제안된 선형 시스톨릭 곱셈기는 $m/2+1$의 계산 지연시간 및 $1/(m/2+1)$의 처리율을 가진다.

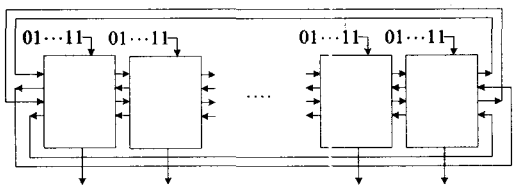


그림 4. $GF(2^m)$상의 $u = xy + z$ 계산을 위한 새로운 선형 시스톨릭 어레이

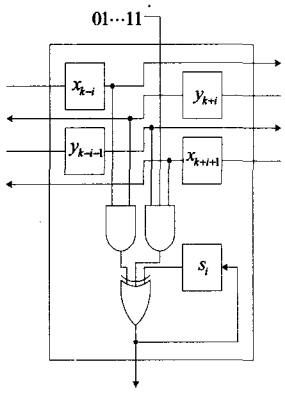


그림 5. 그림 4의 k번째 기본셀 회로도

표 2에 본 절에서 제안된 구조와 관련된 기존의 선형 시스톨릭 곱셈기들과 하드웨어 및 계산 시간 측면에서 비교분석 하였다. 표 2에서 DM은 2-1 멀티플렉서의 지연시간을 나타낸다. 표 2로부터 알 수 있듯이 제안된 모든 구조가 거의 동일한 최대 처리기 지연시간을 가지나 본 절에서 제안된 시스톨릭 어레이가 기존의 연구결과들에 비해 훨씬 낮은 칩 면적을 가지면서 계산 지연시간에 있어 83% 그리고 처리율에 있어 50%가 개선됨을 알 수 있다.

Ⅴ. 결 론

본 논문에서는 AOP가 만드는 유한체 $GF(2^m)$상의 곱셈을 위한 두 가지 종류의 시스톨릭 어레이를 제안하였다. 제안된 두 어레이 모두 병렬 입출력 구조이지만, 첫 번째 제안된 곱셈기는 $m(m+1)/2$ 개의 동일한 셀로 이루어지며 초기 $m/2+1$ 사이클의 지연 후, 매번 1 사이클 마다 곱셈의 결과를 출력하

표 2. $GF(2^m)$상의 선형 시스톨릭 곱셈기들의 특성 비교

	Wang [7]	Yeh [8]	Fenn [9]	Fig. 4
Basis	Polynomial	Polynomial	Dual	AOP
셀 구성요소				
AND	3	3	3	3
XOR	2	2	2	2
MUX	1	1	1	0
Latch	8	10	8	5
셀의 갯수	m	m	m	m+1
지연시간	$3m$	$3m$	$3m$	$m/2$+1
최대 처리기 지연시간	D_A+2D_X+D_L+D_M	D_A+D_X+D_L+D_M	D_A+D_X+D_L+D_M	2D_A+2D_X+D_L
처리율	$1/m$	$1/m$	$1/m$	$1/(m/2+1)$

고, 두 번째 구조는 m+1 개의 동일한 셀로 이루어지며 $m/2$+1 사이클 마다 곱셈의 결과를 출력한다. 표 2와 표 3으로부터, 본 연구에서 제안된 두 곱셈기 모두 기존의 동일한 형태의 연구결과들과 비교했을 때, 계산 지연시간 및 칩 면적 모두에 있어 상당한 성능 향상을 보였다. 특히, 선형 시스톨릭 어레이는 상당히 낮은 칩 면적, 계산 지연시간, 그리고 높은 처리율을 가지기 때문에 저 면적 및 실시간 암호응용에 매우 적합하다 할 수 있다. 뿐만 아니라 제안된 곱셈기들은 높은 규칙성과 모듈성을 가지기 때문에 VLSI 구현에 매우 적합하다.

참 고 문 헌

[1] E.R. Berlekamp, "Bit-serial Reed- Solomon encoders," *IEEE Trans. Inform. Theory*, vol. 28, pp. 869-874, 1982.

[2] M. Wang and I.F. Blake, "Bit serial multiplication in finite fields," *SIAM J. Disc. Math.*, vol. 3, pp. 140-148, 1990.

[3] M.A. Hasan, M.Z. Wang and V.K. Bhargava, "A modified Massey-Omura parallel multiplier for a class of finite fields," *IEEE. Trans. Computers*, vol. 42, pp. 1278-1280, 1993.

[4] B. Sunar and C.K. Koc, "An efficient optimal normal basis type II multiplier," *IEEE Trans. Computers*, vol. 50, pp. 83-87, 2001.

[5] T. Itoh and S. Tsujii, "Structure of parallel multipliers for a class of finite fields $GF(2^m)$," *Information and computation*, vol. 83, pp. 21-40, 1989.

[6] A.J. Menezes, *Applications of finite fields*, Kluwer Academic Publisher, 1993.

[7] C.L. Wang and J.L. Lin, "Systolic array implementation of multipliers for finite fields $GF(2^m)$," *IEEE Trans. Circuits Syst.*, vol. 38, pp. 796-800, 1991.

[8] C.S. Yeh, I.S. Reed and T.K. Troung, "Systolic multipliers for finite fields $GF(2^m)$," *IEEE Trans. Computers*, vol. C-33, pp. 357-360, 1984.

[9] S.T.J. Fenn, M. Benaissa and D. Taylor, "Dual basis systolic multipliers for $GF(2^m)$," *IEE Proc. Comput. Digit. Tech.*, vol. 144, pp. 43-46, 1997.

[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, pp. 385-393, 2001.

[11] C.W. Wei, "A systolic power sum circuit for $GF(2^m)$," *IEEE Trans. Computers*, vol. 43, pp. 226-229, 1994.

[12] S.K. Jain, L. Song and K.K. Parhi, "Efficient semisystolic architectures for finite field arithmetic," *IEEE Trans. VLSI Syst.*, vol. 6, pp. 101-113, 1998.

[13] J.H. Guo and C.L. Wang, "Systolic array implementation of Euclid's algorithm for inversion and division in $GF(2^m)$," *IEEE*

Trans. Computers, vol. 47, pp. 1161-1167, 1998.

[14] C.C. Wang, T.K. Truong, H.M. Shao, L.J. Deutsch, J.K. Omura and I.S. Reed, "VLSI architectures for computing multiplications and inverses in $GF(2^m)$," *IEEE Trans. Computers*, vol. 34, pp. 709-716, 1985.

[15] C.Y. LEE, E.H. Lu and L.F. Sun, "Low complexity bit parallel systolic architecture for computing AB^2+C in a class of finite field $GF(2^m)$," *IEEE Trans. Circuits Syst. II*, vol. 48, pp. 519-523, 2001.

[16] W.C. Tsai, C.B. Shung and S.J. Wang, "Two systolic architectures for modular multiplication," *IEEE Trans. VLSI Syst.*, vol. 8, pp. 103-107, 2000.

[17] A. Reyhani-Masoleh and M.A. Hasan, "A new construction of Massey-Omura parallel multiolier over $GF(2^m)$," *IEEE Trans. Computers*, vol. 51, pp. 511-520, 2002.

[18] 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, pp. 353-356, 1998.

[19] C. Paar, P. Fleischmann and P. Roelse, "Efficient multiplier architectures for Galois fields $GF(2^{4n})$," *IEEE Trans. Computers*, vol. 47, pp. 162-170, 1998.

[20] G. Drolet, "A new representation of elements of finite fields $GF(2^m)$ yielding small complexity arithmetic circuits," *IEEE Trans. Computers*, vol. 47, pp. 938-946, 1998.

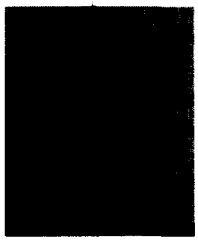
[21] S.T.J. Fenn, M.G. Parker, M. Benaissa and D. Taylor, "Bit-serial multiplication in $GF(2^m)$ using irreducible all one polynomials," *IEE Proc. Comput. Digit. Tech.*, vol. 144, pp. 391-393, 1997.

[22] N. Weste and K. Eshraghian, *Principles of CMOS VLSI Design: A System Perspective*, 2nd ed. Reading, MA: Addison-Wesley, 1993.

권 순 학(Soonhak Kwon) 정회원

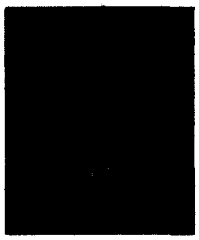
1990년 2월 : KAIST 수학과, 학사
1992년 2월 : 서울대학교 수학과, 석사
1997년 5월 : Johns Hopkins University, 박사
1998년 3월~현재 : 성균관대학교 수학과, 부교수
<관심분야> 정수론, 암호론, Cryptographic Hardware

김 창 훈(Chang Hoon Kim) 정회원



2001년 2월 : 대구대학교 컴퓨터정보공학부, 학사
2003년 2월 : 대구대학교 컴퓨터정보공학과, 석사
2003년 3월~현재 : 대구대학교 컴퓨터정보공학과, 박사과정
<관심분야> 암호 시스템, Embedded System

홍 춘 표(Chun Pyo Hong) 정회원



1978년 2월 : 경북대학교 전자공학과, 학사
1986년 12월 : Georgia Institute of Technology ECE, 석사
1991년 12월 : Georgia Institute of Technology ECE, 박사
1994년 9월~현재 : 대구대학교 정보통신공학부, 교수
<관심분야> DSP 하드웨어 및 소프트웨어, 컴퓨터 구조, VLSI 신호처리, Embedded System