PBCA를 이용한 MSB곱셈기 설계[1]

전준철* 김현성* 이형목* 하경주** 구교민*** 김남연* 유기영*
* 경북 대학교
** 경산 대학교
*** 대구 교육 대학교
(jcjeon33, hskim, hmhl01)@purple.knu.ac.kr

MSB Multiplier Design based on Periodic Boundary Cellular Automata

Jun-Cheol Jeon* Hyun-Sung Kim* Hyoung-Mok Lee* Kyeoung-Ju Ha**
Kyo-Min Ku*** Nam Yeun Kim* Kee-Young Yoo*
*Dept. of Computer Engineering, Kyungpook National University
**Dept. of Information Processing, Kyungsan University
*** Daegu National University of Education

요 약

본 논문에서는 셀룰라 오토마타(Cellular Automata, CA)를 이용한 MSB곱셈기를 제안한다. 본 논문에서 제안한 구조는 PBCA(Periodic Boundary CA)의 특성을 AOP의 특성과 조화시킴으로써 정규성을 높이고 시간지연을 줄일 수 있는 장점을 가지고 있다. 이 곱셈기는 지수연산을 위한 하드웨어 설계에 효율적으로 이용될 수 있을 것이다.

1. 서 론

암호학을 포함하는 여러 응용들이 유한체 GF(2^m)상에서 이루어지고 있다[1]. 특히 RSA와 같은 공개키 암호 시스템 등의 응용[2]에서 유한체 상의 나눗셈이나 지수연산 및 곱셈의 역원과 같은 연산들을 요구한다. 이러한 연산들은 AB곱셈기나 AB^2연산구조를 기본으로 구현할 수 있다.

많은 연구에서 AOP의 특성을 이용한 효율적인 구조를 제안하고 있다. Fenn은 GF(2^m)상에서 LFSR(Linear Feedback Shift Register)구조를 이용하는 AB곱셈기를 두 가지 형태의 비트 순차구조(bit-serial)로 디자인하였다[3]. Von Neumann에 의해 소개된 셀룰라 오토마타는 수리적 이론에서의 많은 문제들과 병렬처리 연산처럼 다양한 응용에 사용되고 있다[4].

본 논문에서는 PBCA를 이용하여 MSB알고리즘에 기반한 곱셈기를 제안한다. 또한 모듈러로써 AOP를 적용함으로써 효율적인 구조를 유도할 수 있다. 제안된 구조의 각 셀은 1-AND와 1-XOR의 복잡도를 가지며 m+1의 시간지연만에 연산결과를 출력한다.

2. 셀룰라 오토마타

CA는 규칙성을 가지고 서로 연결된 여러 셀들로 구성된다. CA를 구성하는 중요한 요소는 각 셀의 상태 갱신에 적용되는 법칙과 여기에 직접적으로 관여하여 셀의 갱신에 직접적으로 영향을 미칠 수 있는 이웃 셀의 개수이다. 본 논문에서는 두 가지 상태를 가진 3-이웃 1차원 CA를 고려한다. 표 1은 3-이웃으로 가능한 모든 상태와 두 가지 법칙을 보여준다.

표 1 법칙에 따른 상태 변화의 예

	111	110	101	100	011	010	001	000
법칙150	1	0	0	1	0	1	1	0
법칙240	1	1	1	1	0	0	0	0

법칙 150: 왼쪽 이웃⊕ 자신⊕오른쪽 이웃 → 상태갱신
법칙 240: 왼쪽 이웃 값에 의존적으로 상태갱신

CA는 해당 법칙 연산에 따라서 선형CA, 비선형CA로 구분된다. 해당 법칙이 XOR연산만으로 이루어진 것을 선형CA, 그 외의 연산으로 이루어진 것을 비선형CA라 한다. 특히 XOR와 XNOR연산이 사용되는 CA는 추가적(Additive)CA라고 한다. 또한 한가지 법칙을 모든 셀에 적용한 것을 균등(Uniform)CA, 두 가지 이상의 법칙이 사용된 CA를 하이브리드(Hybrid) CA라고 한다.

CA는 경계조건에 따라 NBCA(Null Boundary CA), PBCA(Periodic Boundary CA), IBCA(Intermediate Boundary CA)로 나눌 수 있다. 본 논문에서는 PBCA(주기적 경계 셀룰러 오토마타)의 속성을 이용한다. 이 구조에서

1. 본 연구는 한국과학재단 목적기초 연구 2000-2-51200-001-2 지원으로 수행되었음

는 가장 왼쪽의 셀과 가장 오른쪽의 셀이 이웃 한 것으로 간주한다. 이 구조에 법칙 240을 사용하면 기약다항식으로 AOP를 사용할 때 효율적인 모듈러 감소 연산을 수행할 수 있다.

셀의 다음 상태를 나타내기 위하여 특성화 행렬(characteristic matrix)을 사용한다. CA의 다음 상태는 현재 상태벡터와 행렬의 곱으로 표현한다. 아래는 법칙 240을 적용한 특성화 행렬의 일반적인 표현이다.

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad (1)$$

행렬(1)의 $m \times m$ 의 값들이 해당 셀의 상태 값을 표시하고 이들의 왼쪽 값과 오른쪽 값이 각각 왼쪽 셀과 오른 쪽 셀의 상태 값을 표시한다. 아래는 PBCA구조의 일반화된 표현이다

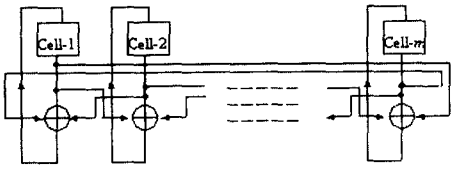

그림1 PCBA구조의 일반화

제안된 구조에서는 법칙 2400이 적용된 PBCA구조를 이용한다. 따라서, 각 셀들은 왼쪽 셀들의 값에 의존적이므로 그림 1에서는 XOR연산이 불필요하다.

3. 유한체

유한체 혹은 갈로아 체(Galois Field, GF)는 교환, 결합, 분배 법칙에 대해 닫혀 있고, 덧셈, 뺄셈, 곱셈, 나눗셈 연산이 가능한 유한 개의 원소들의 집합이다. 유한체에서 원소를 표기하기 위해서 정규기저(Normal Basis)표기법, 이원기저(Dual Basis)표기법 그리고 다항식 기저(Polynomial Basis)표기법등이 있다. 본 논문에서는 기저의 변환 단계가 필요 없는 다항식 기저 표기법으로 원소를 표시한다. 유한체 GF(2)의 유한 확대체 GF(2^m)은 2^m 개의 원소를 갖는다. GF(2)의 원소를 계수로 갖는 m 차의 기약 다항식을 $f(x)$ 할 때, 다항식의 계수가 모두 '1'인 다항식 $f(x)= x^m + x^{m-1} + \ldots + x + 1$ 을 AOP(all one polynomial)이라고 한다. 이 방정식의 근을 α라고 하면 $\alpha^{m+1}+1=0(m+1$ 은 소수)의 속성을 가진다[6].

GF(2^m)상의 한 원소 A 는 $A= a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \ldots + a_1\alpha + a_0$ 이고 $a_i, (0 \le i \le m-1)$는 GF(2)의 원소이다. 또한 $\{\alpha^{m-1}, \alpha^{m-2}, \ldots, \alpha, 1\}$은 GF($2^m$)상의 표준기저(standard basis)이다. GF(2^{m+1})상의 한 원소 A는 $A = A_m\alpha^m + A_{m-1}\alpha^{m-1} + \ldots + A_1\alpha + A_0, (A_m=0)$으로 표현된다. 또한 확장된 기저 $\{\alpha^m, \alpha^{m-1}, \alpha^{m-2}, \ldots, \alpha, 1\}$은 GF($2^m$)상의 표준기저에서 하나 확장된 기저이다. 따라서 A_i와 a_i의 관계를 식으로 나타내면 아래와 같다.

$$A_i = a_i + A_m \quad (i= 0, 1, 2, \ldots, m-1) \quad (2)$$

이러한 속성은 곱셈연산을 수행하는데 있어 정규성과 하드웨어 복잡도를 보다 효과적으로 제공한다.

4. MSB우선 곱셈

유한 확대체 GF(2^m)상의 곱셈은 크게 LSB(Least Significant Bit)우선곱셈과 MSB(Most Significant Bit)우선곱셈의 두 가지로 나눌 수 있다. 본 논문에서는 지수기 구현에 효율적인 MSB우선 곱셈을 제안한다.

피연산자 B의 MSB부터 먼저 연산을 시작하는 것을 MSB우선곱셈 알고리즘이라 한다. 곱셈은 차수 m의 원시 다항식에 의해서 정의된다. 두 원소의 곱셈은 단순히 두 다항식을 곱한 뒤 기약다항식 P로 모듈러 연산을 취한다. A와 B는 GF(2^m)상의 원소이고, P는 차수 m의 원시 다항식이라 하면, 각 다항식은 다음과 같이 표현된다.

$$A = a_m\alpha^m + a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + a_0$$
$$B = b_m\alpha^m + b_{m-1}\alpha^{m-1} + \ldots + b_1\alpha + b_0$$
$$P = \alpha^{m+1}+1$$

다음 식에서 다항식 R을 A와 B의 MSB부터 처리한 곱셈을 모듈러 연산한 결과이다.

$$\begin{aligned} R &= AB \bmod P \\ &= \{\ldots[Ab_m \bmod P + Ab_{m-1}]\alpha \bmod P \\ &\quad + \ldots + Ab_1\}\alpha \bmod P + Ab_0 \end{aligned} \quad (3)$$

식(3)에서 각 연산을 비트별 연산으로 고친 후 AOP의 속성을 적용한 비트별 모듈러 곱셈 알고리즘으로 유도한다.

<MSB 우선곱셈 알고리즘>

입력 : $A = (a_m, a_{m-1}, a_{m-2}, \ldots, a_1, a_0)$
$B = (b_m, b_{m-1}, b_{m-2}, \ldots, b_1, b_0)$
$P = \alpha^{m+1}+1$

출력 : $R = AB \bmod \alpha^{m+1}+1$

초기식 : $R^{(-1)} = (R^{(-1)}_m, R^{(-1)}_{m-1}, \ldots, R^{(-1)}_1, R^{(-1)}_0)$
$= (0, 0, \ldots, 0, 0)$

단계 1 for i =0 to m

단계 2 $R^{(i)}$= Circular_Right_Shift($R^{(i-1)}$)

단계 3 for j =0 to m

단계 4 $R^{(i)}_{(m-1)-j} = R^{(i)}_{(m-1)-j} + b_{(m-1)-i}\, a_{(m-1)-j}$

단계 2에서 AOP의 특성이 적용된 모듈러 연산($R\alpha \bmod P$)이 이루어진다. 즉, GF(2^m)상의 한 원소 R의 각 비트를 한 비트 우측 순회함으로써 구해진다. 따라서 이 연산은 PBCA에 법칙 2400이 적용된 구조로 구현이

가능하다. 단계 2는 그림 1의 연산을 수행하고 단계 3,4는 그림 2의 part 2에 해당되는 연산을 한다. 제안된 곱셈 알고리즘과 PBCA에 기반한 곱셈기 구조는 그림 2와 같다.

5. PBCA를 이용한 MSB곱셈기

본 논문에서 제안한 구조는 그림 1에서 제시한 PBCA를 이용하여 연산하는 곱셈기이다. 이 구조는 크게 두 부분, part 1과 part 2로 나눌 수 있다. part 1은 $R\alpha \bmod p$를 구하는 PBCA구조이다. part 2는 $R_i = R_i + a_i b_j$을 구하는 구조이다. 이 구조의 연산과정을 보면 다음과 같이 진행된다.

PBCA안의 각 셀들은 결과값 R_i=0으로 초기화된다. a_i, $(0 \le i \le m)$셀에도 해당되는 연산자의 값으로 초기화된다. 첫 스텝에서 미리 입력된 a_i의 값들과 이 스텝에 입력된 피연산자 b_j값을 이용하여 $a_i \times b_j$, $(0 \le i \le m, j$는 스텝을 의미한다.)연산을 수행한다. 다시 이 값들은 R_i셀로 입력된다. R_i의 값들은 각각 1-비트 우측순환을 한다. 이러한 과정이 m번 반복되면서 결과값 R_i를 구한다. 아래의 그림은 GF(2^4)상에서 MSB곱셈기의 구조를 나타낸다.

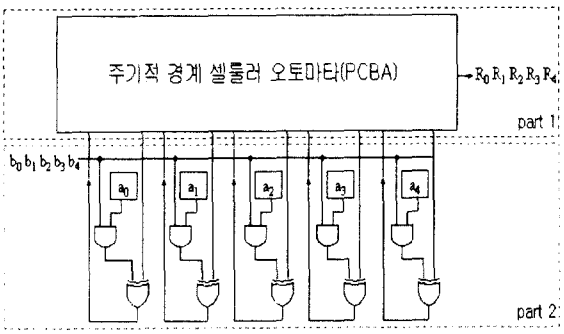

그림 2 PCBA를 이용한 MSB곱셈기 구조

6. 분석

본 논문에서 제안한 구조를 기존의 구조[3], [5], [6]과 비교, 분석한다.

표 2 곱셈기 구조 비교

	Fenn[3]	Chang[5]	Choudhury [6]	그림 2
기본 셀 수	m+1	m	m	m+1
셀 복잡도	1-AND +1-XOR	3-AND +2-XOR	2-AND +2-XOR	1-AND +1-XOR
지연시간	2m+1	m	M	m+1

Fenn[3]이 제안한 LFSR구조는 m+1개의 기본 셀로 구성되어 있고 2m+1의 지연을 가진다. Chang[5] 이 제안한 PCA기반의 구조와 Choudhury[6]이 제안한 CA기반의 LSB 곱셈구조는 각각 3-AND + 2-XOR와 2-AND + 2-XOR의 복잡도를 가진다. 이에 비해 제시된 구조는 m+1개의 기본 셀을 가지며 1-AND + 1-XOR의 셀 복잡도를 가지고 단지 m+1의 시간지연을 가진다.

본 논문에서 제안된 구조는 [3]의 구조에 비해 지연 시간을 줄일 수 있었고, [5]와 [6]의 구조에 비해서는 셀 복잡도가 줄었다. 따라서 기존의 여러 다른 구조와 비교했을 때 하드웨어 복잡도와 지연 시간면에서 각각 효율적임을 알 수 있다.

7. 결 론

본 논문에서는 유한체 GF(2^m)상에서 임의의 원소에 대한 모듈러 곱셈연산 $AB \bmod P$을 수행하는 PBCA기반의 곱셈기를 구현하였다. 기존의 곱셈기 구조 구현에 자주 사용되던 LFSR은 기저가 자주 변경되는 구조에 적합하지 않은 단점이 있다. 제안된 구조는 CA의 특성에 AOP의 특성이 고려된 효율적인 하드웨어 구조를 제시하였다. 이 구조는 기존의 시스템에 비하여 시간지연과 하드웨어 구조 복잡도면에서 각각 장점을 제시하였다. 제안된 구조는 정규적인 특성이 있고 모듈화 할 수 있는 특성이 있다. 따라서 이 구조를 이용하여 나눗셈이나 지수연산 및 곱셈의 역원을 구하기 위한 효율적인 구조 구현이 가능할 것으로 기대된다.

참 고 문 헌

[1] D. E. R. Denning, *Cryptography and data security Reading*, MA: Addison-Wesley, 1983.

[2] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," *Comm. ACM.* vol. 21, pp. 120-126, 1978.

[3] S.T.J. Fenn, M.G. Parker, M. Benaissa, and D. Tayler, "Bit-serial multiplication in GF(2^m) using irreducible all-one opolynomial," *IEE Proc. Comput. Digit. Tech.*, vol. 144, no.6 pp. 391-393, 1997.

[4] J. von Neumann, *The theory of self-reproducing automata*, University of Illinois Press, Urbana and London, 1666.

[5] Chang N. Zhanag and Ming Y.Deng, and Ralph Mason, "A VLSI Prorammable Cellular Automata Array for Multiplication in GF(2^n)," *PDPTA '99 International Conference.*.

[6] P. Pal. Choudhury and R. Barua, "Cellular Automata Based VLSI Architecture for Computing Multiplication And Inverses In GF(2^m)," *IEEE 7th International Conference on VLSI Design*, January 1991.

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