셀룰라 오토마타를 이용한 GF(2^m)상의 곱셈기[1]

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

Modular Multiplier based on Cellular Automata over GF(2^m)

Hyoung-Mok Lee* Hyun-Sung Kim* Jun-Cheol Jeon* 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 유한 확대 체 GF(2^m)상에서 셀룰라 오토마타를 이용한 곱셈기 구조를 제안한다. 제안된 구조는 기약 다항식으로 AOP(All One Polynomial)의 특성을 사용하고 LSB방식으로 곱셈 연산을 수행한다. 제안된 곱셈기는 지연시간으로 $m+1$을 갖고 임계경로로는 $1\text{-}D_{AND}+1\text{-}D_{XOR}$를 갖는다. 특히 구조가 정규성, 모듈성, 병렬성을 가지기 때문에 VLSI구현에 효율적이다.

1. 서 론

암호학[1],[2]의 응용에서 갈로아 체(Galois Field, GF)[3],[4]의 연산은 아주 중요하다. 특히 GF(2^m)은 암호학에서 가장 관심을 가지는 유한 체이다.

본 논문에서는 기저의 변환이 필요 없는 GF(2^m)의 표준기저에 초점을 맞추었다. 지금까지 많은 비트 단위 직렬 및 병렬 곱셈기들이 제안되었으나 시스템의 복잡도 때문에 효과적이지는 못했다. 이런 시스템의 복잡도를 줄이기 위해서 Itoh는[3]에서 GF(2^m)상의 m차의 기약 다항식 AOP에 기초한 곱셈기와 m차의 ESP에 기초한 병렬 곱셈기로 발전시켰다. 또한, 논문[6]에서 Choudhury는 CA를 이용한 LSB방식의 곱셈기를 제안하였다.

본 논문에서는 기약 다항식으로 AOP의 속성을 사용한 새로운 모듈러 곱셈기 구조를 제안한다. 곱셈을 LSB방식으로 계산하는 제안된 구조의 기본 셀 구조는 하나의 AND와 하나의 XOR로 이루어진다. 제안된 구조는 전체 지연시간으로 $m+1$을 갖고 임계경로로는 $1\text{-}D_{AND}+1\text{-}D_{XOR}$를 갖는다. 또한 제안된 구조는 시간과 공간 복잡도 면에서 기존의 구조보다 효율적이다. 특히 이 구조를 기반으로 지수기, 나눗셈기 및 역원기를 보다 효율적으로 구현할 수 있다.

본 연구는 한국과학재단 목적기초연구 2000-2-51200-001-2 지원으로 수행되었음

2. 셀룰라 오토마타

셀룰라 오토마타(Cellular Automata, CA)는 규칙적으로 상호 연결된 많은 셀들로 구성되어져 있는 유한 상태 머신 (Finite State Machine)이다. CA의 각 셀들은 상호 연결된 이웃의 현재 상태 값과 특별한 법칙에 따라 이산적 시간에 동시에 새로운 상태 값으로 바뀌어진다. CA는 이웃 셀을 이용하여 셀을 갱신하기 위한 함수 즉 법칙과 자신을 포함하여 셀을 갱신하는데 직접적으로 관여하는 이웃의 개수에 의해 이루어진다. 다음은 2-상태 3-이웃 1-차원 CA의 예이다.

111	110	101	100	011	010	001	000
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
0	1	0	1	1	0	1	0
1	1	1	1	0	0	0	0

위에서 첫 번째 행은 3-이웃으로 셀을 나타낼 수 있는 모든 상태를 보여준다. 두 번째 행은 이와 관련된 상태 계수이다. 세 번째 행과 네 번째 행은 CA를 구성하는 원소 중에서 법칙을 나타낸다. 세 번째 행은 왼쪽 이웃과 오른쪽 이웃을 XOR한 결과로서 자신의 상태를 갱신한다. 이를 십진수로 나타내면 90이 된다. 이것을 법칙 90이라 한다. 네 번째 행은 십진수로 표현을 하면 240이다. 즉 법칙 240이다. 이 법칙은 왼쪽 이웃의 값으로 자기 자신을 갱신한다. 이처럼 CA는 이웃의 수와

적용된 법칙에 따라서 셀들의 상태 값이 갱신되어진다.

또한 CA는 셀 사이에 적용된 법칙이 어떤 연산으로 이루어지는가에 따라서 선형 셀룰라 오토마타(Linear CA), 비선형 셀룰라 오토마타(Non-Linear CA), Additive CA로 이루어진다. 선형 셀룰라 오토마타는 각 셀들간의 다음 상태를 갱신 하기 위한 법칙이 XOR연산 만으로 이루어진 것을 말하며, 비선형 셀룰라 오토마타는 그 이외의 연산으로 이루어진 것을 말한다. 비선형 셀룰라 오토마타 중 XOR와 XNOR 연산 만으로 이루어진 CA를 Additive CA라 한다.

그리고 CA는 적용된 법칙들이 동일한 것으로 이루어지는 Uniform CA와 두개 이상의 법칙들로 이루어진 Hybrid CA로 구분된다. 또한 각 셀들의 배열 구조에 따라서 1-차원, 2-차원, 3-차원 CA가 있다.

CA를 구성하는데 있어서 다른 중요한 요소 중의 하나는 경계 조건이다. CA는 가장 왼쪽 셀의 왼쪽 이웃과 가장 오른쪽 셀의 오른쪽 이웃이 존재하지 않는다. 이를 해결하기 위한 Null, Periodic, Intermediate 경계 조건이 존재한다. 이 경계 조건을 각각 적용한 CA를 NBCA(Null Boundary CA), PBCA(Periodic Boundary CA), IBCA(Intermediate Boundary CA)라 부른다. NBCA는 가장 왼쪽 셀과 가장 오른쪽 셀에서의 입력을 0으로 부여하는 것이고, PBCA는 가장 왼쪽 셀과 가장 오른쪽 셀이 이웃 한 것으로 간주함으로써 두 입력을 부여하는 것이다. IBCA는 가장 왼쪽(오른쪽) 셀의 왼쪽(오른쪽) 이웃을 두 번째 오른쪽(왼쪽) 이웃으로 간주하여 값을 입력하는 것이다.

또한 CA의 특성 중에서 다음 셀의 상태를 결정하기 위한 특성화 행렬이 있다. 법칙 240 즉, 자기 자신의 왼쪽 이웃을 1로 표현 하고 나머지 이웃은 0으로 표현하는 PBCA의 (4×4)특성화 행렬은 다음과 같이 나타낼 수 있다.

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

3. GF(2^m)상의 AOP(All One Polynomial)

유한 체 GF(2)의 유한 확대 체를 GF(2^m)이라 하자. 그러면 GF(2^m)을 생성하는 기약 다항식 즉, GF(2)의 원소를 계수로 갖는 기약 다항식 $f(x)$를 $f(x)=a_mx^m+a_{m-1}x^{m-1}+\cdots+a_1x+a_0$로 나타낼 수 있다. 이러한 $f(x)$중에서 계수가 모두 1인 기약 다항식을 AOP라 한다. 이 AOP $f(x)=x^m+x^{m-1}+\cdots+x+1$의 근을 α라 하면 다음 방정식을 만족한다.

$$\alpha^{m+1}+1=0 \quad (2)$$

그리고 위의 AOP $f(x)$의 근 α에 의해 생성된 집합 {1, α, α^2, ⋯, α^{m-1}}은 GF(2^m)상의 표준기저가 되고 GF(2^m)상의 한 원소 A는 $A=a_{m-1}\alpha^{m-1}+a_{m-2}\alpha^{m-2}+\cdots+a_1\alpha+a_0$로 표현된다. 이 표준기저에서 확장된 기저를 {1, α, α^2, ⋯, α^{m-1}, α^m}라 하면 GF(2^m)의 원소 A는 $A=a_m\alpha^m+a_{m-1}\alpha^{m-1}+\cdots+a_1\alpha+a_0(a_m=0)$로 표현할 수 있다. 그리고 GF($2^4$)상의 두 원소 A와 B를 확장된 기저로 표현하고 확장된 체 상에서 AOP 속성이 적용된 $P=\alpha^{m+1}+1$를 모듈러로 사용해서 A와 B의 곱 즉, AB mod P (LSB방식)를 다음과 같이 표현할 수 있다.

$$\begin{aligned} &AB \bmod P \\ &=A(b_0+b_1\alpha+b_2\alpha^2+b_3\alpha^3+b_4\alpha^4) \bmod P \\ &=(Ab_0+Ab_1\alpha+Ab_2\alpha^2+Ab_3\alpha^3+Ab_4\alpha^4) \bmod P \end{aligned}$$

이 곱셈 연산을 수행하는데 있어서 위에서 언급한 AOP의 속성이 모듈러로서 사용된다. 즉, 모듈러 연산은 원소 A의 각 비트들을 한 비트 서큘러 시프트(Circular Shift)함으로써 수행된다. 그림 1에서 보여주는 바와 같이 GF(2^4)상에서 법칙 240이 적용된 (5×5)특성화 행렬을 가지는 3-이웃 1-차원 PBCA구조를 이용하여 $A\alpha$ mod P연산을 수행할 수 있다.

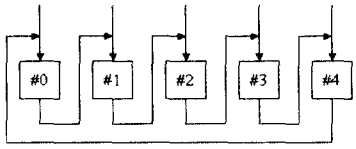


그림 1. 법칙 240이 적용된 PBCA

4. 효율적인 셀룰라 오토마타 곱셈기 설계

이 장에서는 셀룰라 오토마타에 기반하고 기약 다항식으로 AOP의 특성을 사용하는 곱셈기 구조를 제안한다. GF(2^m)상의 두 원소 A와 B를 확장된 기저로 표현해서 A와 B의 곱, AB mod P(LSB방식)를 다음과 같이 표현할 수 있다.

$$\begin{aligned} &AB \bmod P \\ &=A(b_0+b_1\alpha+\cdots+b_{m-1}\alpha^{m-1}+b_m\alpha^m) \bmod P \\ &=(Ab_0+Ab_1\alpha+\cdots+Ab_{m-1}\alpha^{m-1}+Ab_m\alpha^m) \bmod P \\ &= r_0+r_1\alpha+\cdots+r_{m-1}\alpha^{m-1}+r_m\alpha^m \end{aligned} \quad (3)$$

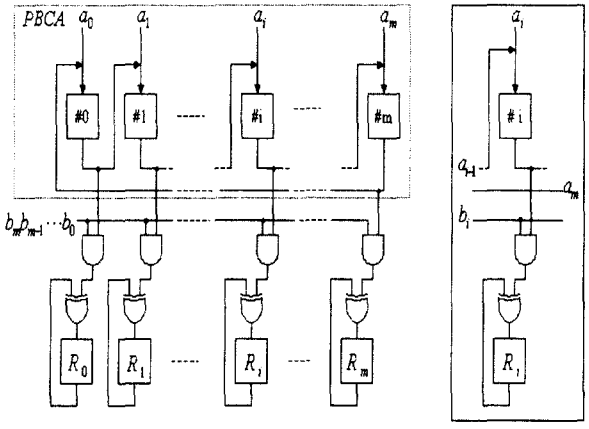
위 식은 크게 두 가지 연산으로 나뉘어진다. CA를 이용해서 승수의 자리 수, $A\alpha$ mod P를 구하는 연산과 구해진 자리 수를 이용해서 실제 곱셈 연산인 $R_i=R_i+Ab_i(0\le i\le m)$를 구하는 연산이다.

먼저 CA를 이용한 $A\alpha$ mod P의 연산은 레지스터에서 원소 A의 각 비트들을 한 비트 서큘러 시프트 함으로써 얻을 수 있다. 이 때 AOP의 이런 특성을 CA에 적용하면 왼쪽 이웃의 값에만 의존적인 법칙 240을 따라야 한다. 그리고 마지막 셀과 처음 셀이 이웃 한 것으로 간주해서 입력을 처리하는 PBCA를 이용함으로써 $A\alpha$ mod P를 계산할 수 있다. (4)식은 (3)식을 계산하기 위해 법칙 240을 적용한 PBCA의 $(m+1)\times(m+1)$특성화 행렬이다.

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad (4)$$

그리고 이렇게 계산된 결과 값, 즉 $A\alpha \bmod P$와 b_i값을 AND 연산하고 그 결과 값을 누적 변수 R_i에 누적하면 원하는 곱셈 결과를 얻을 수 있다.

그림 2의 (a)에서는 셀룰라 오토마타를 이용한 제안된 곱셈기 구조를 보여주고 각 셀들은 (b)구조를 기반으로 한다. 단, $\#i\ (0 \le i \le m)$는 PBCA의 각 셀을 나타낸다.



(a) 곱셈기 구조 (b) 곱셈기의 기본 셀

그림 2. GF(2^m)상의 PBCA를 이용한 곱셈기

5. 비 교 및 분 석

본 논문에서 제시한 구조와 기존에 제시된 구조인 Choudhury [6] 구조 및 Fenn [7] 구조와 비교한다.

표1. 구조 비교

구조 / 항목	Choudhury [6]	Fenn [7]	제안된 구조
기 능	$AB+C$	AB	$AB+C$
셀 수	m	m	$m+1$
셀 복잡도	2 AND 2 XOR	1 AND 1 XOR	1 AND 1 XOR
지 연 시 간	m	$2m+1$	$m+1$
임 계 경 로	$2\text{-}D_{AND}+2\text{-}D_{XOR}$	$1\text{-}D_{AND}+1\text{-}D_{XOR}$	$1\text{-}D_{AND}+1\text{-}D_{XOR}$

위의 표에서 D_{AND}와 D_{XOR}를 각각 AND와 XOR gate의 지연시간 이라 할 때, 논문 [6]에서 지연시간은 m이고 임계경로는 $2\text{-}D_{AND}+2\text{-}D_{XOR}$이다. 제안된 구조에서는 비록 연산시간은 1증가 하지만 $1\text{-}D_{AND}+1\text{-}D_{XOR}$의 임계경로를 가진다.

따라서 논문 [6]의 구조보다 임계경로 면에서 더 효율적이다. 논문 [7]에서는 지연시간이 $2m+1$이고 임계경로는 제안된 구조와 같다. 제안된 구조는 논문 [7]과 비교할 때, 같은 임계경로를 가지지만 시간 면에서는 m만큼 더 효율적이다. 결국 본 논문에서 제안된 구조가 기존의 구조인 논문 [6]과 [7]에 비해서 각각 임계경로와 지연시간 면에서 더 효율적임을 알 수 있다. 제안된 구조는 GF(2^m) 상에서 효율적인 나눗셈기, 지수기 및 역원기를 설계하는데 기본 구조로 사용될 수 있을 것이다.

6. 결 론

본 논문에서는 유한 확대 체 GF(2^m)상의 셀룰라 오토마타를 이용한 곱셈기를 제안하였다. 그리고 모듈러 연산을 위해 일반 기약 다항식을 사용하지 않고 AOP의 특성을 사용함으로써 $m+1$의 지연시간과 $1\text{-}D_{AND}+1\text{-}D_{XOR}$의 임계경로를 가졌다. 본 논문에서 제시된 구조는 기존의 구조보다 시간과 임계경로 면에서 더 효율적인 장점을 제공한다. 그래서 제안된 구조는 GF(2^m) 상에서의 효율적인 나눗셈기, 지수기 및 역원기를 설계하는데 기본 구조로 사용될 수 있다.

더욱이 제안된 구조 자체가 정규성, 모듈성, 병렬성을 가지기 때문에 VLSI구현에 효율적이다.

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. AMC.* Vol. 21, pp. 120-126, 1978.

[3] E. R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw-Hill, 1986.

[4] R. J. McEliece, *Finite fields for Computer Scientists and Engineers*, New York: Kluwer-Academic,1987.

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

[6] P. Pal. Choudhury, "Cellular Automata Based VLSI Architecture for Computing Multiplication And Inverses In GF(2^m)," *IEEE 7th Interna tional Conference on VLSI Design*, January 1994.

[7] S. T. J. Fenn *et al*, "Bit-serial Multiplication in GF(2^m) using irreducible all one polynom- ials,"*IEE. Proc. Comput. Digit. Tech.*, Vol. 144. No. 6. November 1997.