# 유한 필드 $GF(2^m)$상의 모듈러 곱셈기 특성 분석

한 상 덕, 김 창 훈, 홍 춘 표
대구대학교 컴퓨터정보공학과
전화 : 053-850-4411 / 핸드폰 : 016-520-5287

# Characteristic Analysis of Modular Multiplier for $GF(2^m)$

Sang Duk Han, Chang Hoon Kim, Chun Pyo Hong
Dept. of Computer and Information Engineering, Taegu University
E-mail : sdhan@dsp.taegu.ac.kr

## Abstract

This paper analyze the characteristics of three multipliers in finite fields $GF(2^m)$ from the point of view of processing time and area complexity. First, we analyze structure of three multipliers; 1) LSB-first systolic array, 2) LFSR structure, and 3) CA structure. To make performance analysis, each multiplier was modeled in VHDL and was synthesized for FPGA implementation. The simulation results show that LFSR structure is best from the point of view of area complexity, and LSB systolic array is best from the point of view of processing time per clock.

## Ⅰ. 서론

유한 필드 $GF(2^m)$상의 연산들은 오류 제어 코딩, 암호화 시스템 등 여러 분야에서 널리 응용되고 있다[1]. 유한 필드상에서 덧셈은 벡터간의 XOR연산으로 처리되고, 곱셈은 원시 기약다항식 $P(x)$에 의해 $A(x)B(x)$ mod $P(x)$로 정의된다. 이때 곱셈 연산은 덧셈 연산에 비해 처리 시간이 길뿐만 아니라 연산 빈도가 높기 때문에 효율적인 곱셈 연산에 관한 관련 연구가 많이 이루어지고 있다[3][4][5].

본 논문에서는 타원 곡선 암호화 시스템 등에 응용되는 유한 필드 $GF(2^m)$상의 모듈러 곱셈기들을 FPGA로 구현하여 그 결과를 시간, 공간적으로 비교 분석하였다. 비교한 곱셈기는 LSB 우선 순차 시스톨릭 구조[3], Linear Feedback Shift Register (LFSR) 구조[4], 그리고 Celluar Automata (CA) 구조로서 3가지이다. 일차적으로 각 곱셈기의 구조를 분석한 결과 이들 곱셈기의 초기 지연 값은 입력 값이 연속적으로 입력될 경우 LSB 우선 순차 시스톨릭 구조는 $2m$, LFSR 구조는 $m$-2 클럭이고, CA 구조는 초기 지연이 생기지 않는다. 또한 3가지 구조 모두가 초기 지연 값 후에 $1/m$ 클럭 사이클 비율로 곱셈 결과값이 출력된다.

각 곱셈기에 대한 구조 해석을 한 다음, FPGA 구현을 위해 각각의 곱셈기들을 VHDL로 기술하였으며, ALTERA 사의 Quartus II 를 사용하여 functional 시뮬레이션 및 timing 시뮬레이션을 수행하였으며, 그 결과값이 이론값과 일치함을 확인하였다. 이때 논리 회로 합성은 Synopsys 사의 FPGA-Epress를 사용하였다. 구현 결과를 분석한 결과 공간 복잡도 특성에 있어서는 LFSR 구조가 가장 적은 칩 면적을 차지한다.

## Ⅱ. 곱셈기 구조

### 2.1 곱셈 알고리즘

$A(x)$와 $B(x)$는 $GF(2^m)$의 원소이고, $P(x)$는 차수 $m$인 원시 기약 다항식이다. $M(x)$는 원시 기약다항식 $P(x)$에 의해 $A(x)B(x)$ mod $P(x)$로 정의된다. 이때 다항식 $A(x)$, $B(x)$, $P(x)$ 및 $M(x)$는 다음과 같이 표현된다.

※ 본 연구는 한국과학재단 목적기초연구(R01-2000-00402) 지원으로 수행되었음

$$A(x) = a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_1x+a_0$$
$$B(x) = b_{m-1}x^{m-1}+b_{m-2}x^{m-2}+\cdots+b_1x+b_0$$
$$P(x) = x^m+p_{m-1}x^{m-1}+p_{m-2}x^{m-2}+\cdots+p_1x+p_0 \quad (1)$$
$$M(x) = A(x)B(x) \bmod P(x)$$

$GF(2^m)$상에서 두 원소의 곱셈은 두 다항식을 곱한 뒤에 $P(x)$로 모듈러 연산을 취해주면 된다. 본 논문에서 구현한 곱셈기들은 모두 $B(x)$의 Least Significant Bit (LSB) 부터 곱셈을 시작한다. 식 (1)에서 $B(x)$의 LSB 부터 곱셈하는 방법은 식 (2) 와 같다.

$$\begin{aligned} M(x) &= A(x)B(x) \bmod P(x) \\ &= b_0A(x)+b_1[A(x)x \bmod P(x)] \\ &\quad +b_2[A(x)x^2 \bmod P(x)] \\ &\quad +\cdots+b_{m-1}[A(x)x^{m-1} \bmod P(x)] \end{aligned} \quad (2)$$

## 2.2 LSB 우선 순차 시스톨릭 구조

그림 1은 유한 필드 $GF(2^m)$상에서 $m$=4 로 하였을 때 LSB 순차 시스톨릭 곱셈기 구조를 나타낸 것이다 [3]. 입력값 $A(x)$, $P(x)$, 그리고 $M(x)$는 MSB 비트부터 순차적으로 입력되며, $B(x)$는 LSB 비트부터 순차적으로 입력된다. 이 구조에서는 연속적으로 입력 값을 주었을 경우 $2m$ 클럭 지연 후 $1/m$ 클럭 비율로 곱셈의 결과값이 출력된다. 지연 시간을 고려하여 $P(x)$와 $M(x)$는 한 클럭 지연 후 값을 입력한다.

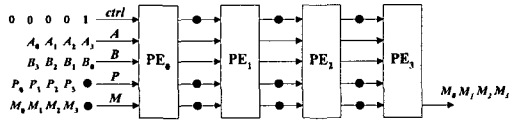



그림 1. 유한 필드 $GF(2^4)$상의 LSB 우선 순차 시스톨릭 곱셈기 구조 [3]

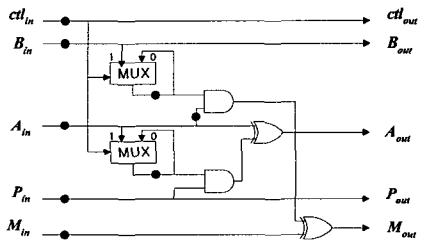



그림 2. 그림 1의 각 PE 구조

그림 1에서 '●' 는 시간 지연 소자이다. 그림 2는 그림 1의 한 Processing Element (PE) 의 구조를 나타낸 것이다. 그림에 기술된 것처럼 각 PE 는 2개의 2입력 AND 게이트와 2개의 2입력 XOR 게이트, 그리고 2개의 Multiplexer (MUX) 로 구성된다.

## 2.3 LFSR 구조

그림 3은 $GF(2^m)$상에서 LFSR 구조의 곱셈기를 나타낸 것이다[4]. 이때 입력 값 $a(x)$, $p(x)$, $M(x)$는 MSB 비트부터 순차적으로 입력되며, $b(x)$는 LSB 비트부터 순차적으로 입력된다. $GF(2^m)$상에서 $m$ 번째 클럭에서 $a(x)$의 모든 입력 값은 $a(x)$의 레지스터 $ar_{m-i}$에 입력되어, $b(x)$의 LSB 비트와 $ar_{m-i}$의 레지스터 값들이 동시에 연산 되며, 또한 $m$ 번째 클럭에서 $M(x)$의 레지스터 $Mr_{m-i}$ 은 모두 0으로 초기화 된다. 이 구조에서는 연속적으로 입력 값을 주었을 경우 $m$-2 클럭 지연 후 $1/m$ 클럭 비율로 곱셈의 결과값이 출력된다. 이 구조의 곱셈기는 $GF(2^m)$상에서 $m$=4 일 때 8개의 AND 게이트, 7개의 XOR 게이트, 그리고 8개의 MUX 로 구성된다.

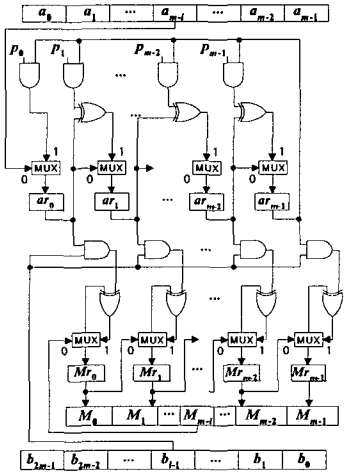



그림 3. $GF(2^m)$상의 LFSR 구조 [4]

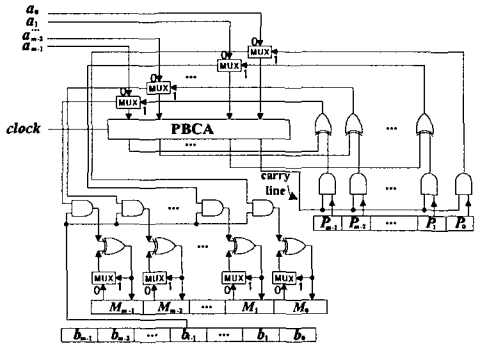



그림 4. $GF(2^m)$일 때 CA 구조 [5]

### 2.4 CA 구조

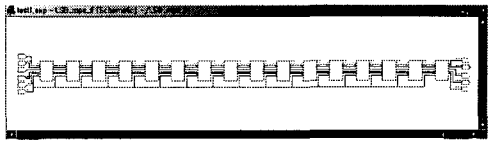
그림 4는 $GF(2^m)$상에서 CA구조의 곱셈기를 나타낸 것이다. $a(x)$의 입력 값은 왼쪽 순환 Periodic Boundary Cellular Automata (PBCA) 에 의해 매 클럭마다 한 비트씩 왼쪽으로 순환된다 [5]. PBCA 에서 계산된 $a(x)$의 LSB 비트가 1이면, $a(x)$의 LSB 비트와 $P(x)$를 연산한다. 이때 MUX 의 출력 값은 $b(x)$를 연산하는 부분과, PBCA 에 입력되는 부분으로 나눠지며, MUX 는 제어 신호에 의해 제어된다. CA 구조는 $a(x)$, $P(x)$, $M(x)$가 동시에 병렬로 입력되어 $b(x)$의 LSB 비트와 연산된다. 곱셈 결과 값은 초기 지연 값 없이 첫 번째 클럭부터 출력되기 시작하며, 결과 값은 $1/m$ 클럭 비율로 출력된다. 이 구조의 곱셈기는 $GF(2^m)$상에서 $m$=4 일 때 8개의 AND 게이트, 7개의 XOR 게이트, 그리고 8개의 MUX 로 구성된다.

## III. FPGA 구현

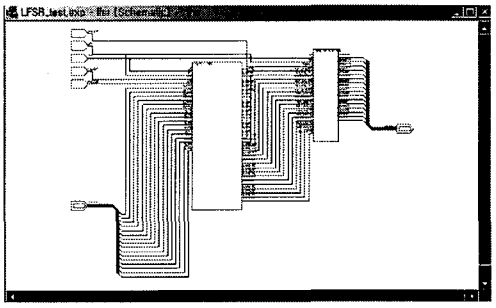
본 절에서는 3 절에서 해석한 각각의 곱셈기들을 FPGA로 구현하기 위해 이들을 VHDL로 기술한 다음, Synopsys사의 합성 툴(FPGA-Express Version : 2000.11-FE 3.5.1)을 사용하여 논리 회로를 합성하였다. 회로의 정확성을 검증하기 위해 ALTERA사의 Quartus II 1.0 을 사용하여 funtional 시뮬레이션, place & routing, 그리고 timing 시뮬레이션을 수행하였으며, FPGA 칩상의 핀 배치도와 결과 값이 정확히 일치함을 확인하였다.

그림 5는 $GF(2^m)$상에서 $m$=16 일 때 각 곱셈기들의 회로 합성 결과이다. 그림 5.(a)는 16 개의 PE 로 구성된 LSB 우선 순차 시스톨릭 곱셈기 구조를 나타낸다. 그림 5.(b)는 LFSR 곱셈기 구조를 나타내는데, 그림에 표시된 것처럼 $a(x)$와 $P(x)$를 연산하는 부분과, 이 결과값을 받아 $b(x)$와 $M(x)$를 연산하는 부분으로 모듈화하여 나타내었다. 그림 5.(c)는 CA 곱셈기 구조를 나타내는데, PBCA부분, $P(x)$와 PBCA의 결과 값 연산부분, $a(x)$의 MUX 부분, $B(x)$와 $a(x)$의 MUX 결과값 연산부분, $M(x)$의 MUX부분, 그리고 $M(x)$의 MUX 결과값과 $B(x)$와 $a(x)$의 MUX 결과값 연산부분으로 모듈화하여 나타내었다. VHDL로 기술한 파일을 Quartus II 에서 $m$=16 일 때 회로의 정확성을 검증하기 위해 functional 및 timing 시뮬레이션을 수행했으며, 그 결과값이 일치함을 확인하였다. 이때 시뮬레이션 과정에서 입력 값으로 식 (3)을 이용했다.

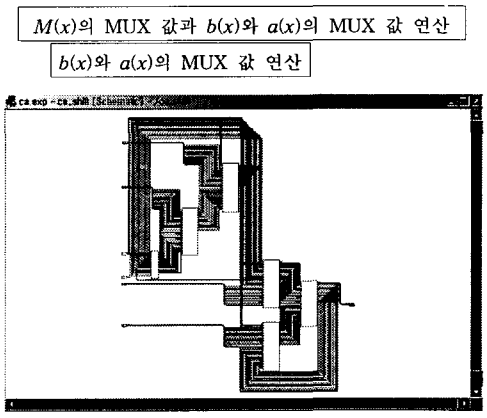
$$\begin{aligned} A(x) &= x^{15}+x^{14}+x^{13}+x^{12}+x^7+x^6+x^5+x^4 \\ B(x) &= x^{11}+x^{10}+x^9+x^8+x^3+x^2+x+1 \\ P(x) &= x^{16}+x^5+x^3+x^2+1 \\ M(x) &= 0 \end{aligned} \tag{3}$$



(a) LSB 우선 순차 시스톨릭 구조




(b) LFSR 구조

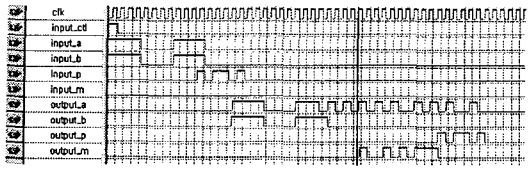



(c) CA 구조

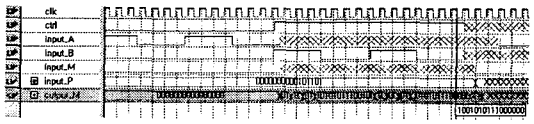
그림 5. $GF(2^{16})$ 상에서 각 곱셈기 회로 합성 결과

Timing 시뮬레이션 결과는 각각 그림 6에 나타내었다. 그림 6.(a)는 LSB 우선 순차 시스톨릭 곱셈기 구조에 대한 timing 시뮬레이션 결과이고, 6.(b)는 LFSR 곱셈기 구조에 대한 timing 시뮬레이션 결과이고, 6.(c)는 CA 곱셈기 구조에 대한 timing 시뮬레이션 결과를 각각 나타낸다. Timing 시뮬레이션 결과 입력 값이 연속적으로 공급이 될 경우 6.(a), (b)구조는 $2m$ , $m$-2 클럭 지연 후에 $1/m$ 클럭 비율로 곱셈 결과값이 출력되고, 6.(c)는 지연 없이 첫 클럭에 결과값이 출력되기 시작하여, $1/m$ 클럭 비율로 곱셈 결과값이 출력된다. 이때 출력 결과 값은 $M(x) = x^{15}+x^{12}+x^{10}+x^8+x^7+x^6$ 임을

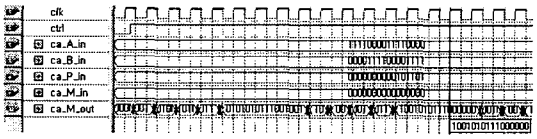
확인하였다. 이는 3절에서 각 곱셈기에 대한 구조 해석으로 얻은 해석적인 결과와 동일함을 알 수 있다.




(a) LSB 우선 시스톨릭 구조의 timing 시뮬레이션 결과




(b) LFSR 구조의 timing 시뮬레이션 결과




(c) CA 구조의 timing 시뮬레이션 결과

그림 6. $GF(2^{16})$ 상에서 timing 시뮬레이션 결과

## Ⅳ. 성능 분석

본 절에서는 FPGA로 구현된 세 가지 곱셈기의 특성을 비교, 분석 하였다. <표 1>은 $GF(2^m)$ 상에서 각 곱셈기의 하드웨어 복잡도 및 데이터 처리 지연시간을 비교한 것이다. <표 1>에 기술된 것처럼 하드웨어 복잡도 측면에선 LFSR 구조가 가장 간단하며, 데이터 처리 지연시간 측면에선 CA 구조가 가장 빠르다는 것을 알 수 있다. <표 2>는 $GF(2^{160})$ 일 때 FPGA 구현 결과를 비교한 것이다. 이때 FPGA 구현을 위해 ALTERA사의 Quartus II 1.0 에서 APEX20KC 군의 EP20K1500CF33C-7 디바이스를 target 으로 하였다. $GF(2^{160})$ 일 때 CA 곱셈기의 입출력 핀 수는 808 개로서, 본 연구에서는 150만 게이트 급인 EP20K1500CF 33C-7 를 선택하였다[6]. <표 2>에서 FPGA 로 구현하였을 때 칩 이용률은 APEX20KC 군의 가장 작은 단위인 LE 단위로 표시하였으며, 한 개의 LE 는 한 개의 4입력 LUT, 한 개의 programmable register, 한 개의 carry, 그리고 한 개의 cascade chain 으로 구성된다[6]. <표 2>에 나타낸 것처럼 공간 복잡도 측면에서는 LFSR 구조가 가장 간단하며, LSB 우선 순차 시스톨릭 구조가 가장 복잡함을 알 수 있다. 또한 한 클럭 당 처리 시간은 LSB 우선 순차 시스톨릭 구조가 가장 빠르며, CA 구조가 가장 느리다는 것을 알 수 있다.

<표 1> $GF(2^m)$ 일 때 곱셈기의 특성 비교

| | 곱셈기 1 [3] | 곱셈기 2 [4] | 곱셈기 3 [5] |
|---|---|---|---|
| AND | $2m$ | $2m$ | $2m$ |
| XOR | $2m$ | $2m-1$ | $2m-1$ |
| MUX | $2m$ | $2m$ | $2m$ |
| Latency(cycles) | $3m$ | $2m-1$ | $m$ |
| Throughput | $m$ | $m$ | $m$ |

<표 2> $GF(2^{160})$ 일 때FPGA 구현 결과

| | 곱셈기 1 [3] | 곱셈기 2 [4] | 곱셈기 3 [5] |
|---|---|---|---|
| LEs | 1759 | 480 | 1119 |
| Frequency(MHz) | 200.80 | 117.92 | 99.67 |
| Clock Period(ns) | 4.980 | 8.480 | 10.033 |
| LEs = Logic Elements | | | |

## Ⅴ. 결론

본 논문에서는 타원 곡선 암호화 시스템 등에 널리 이용되는 유한 필드 $GF(2^m)$상의 모듈러 곱셈기들에 대한 처리시간과 공간 복잡도를 비교 분석하였다. 비교한 곱셈기는 세 가지로서 LSB 우선 순차 시스톨릭 구조, Linear Feedback Shift Register (LFSR) 구조, 그리고 Celluar Automata (CA) 구조이다. 각 곱셈기들을 FPGA 로 구현한 다음 특성을 비교, 분석하였다. 그 결과 공간 복잡도 측면에서는 LFSR 구조가 가장 우수하며, 또한 한 클럭 당 처리 시간은 LSB 우선 순차 시스톨릭 구조가 가장 빨랐다.

## 참고문헌

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

[2] S. Y Kung, *VLSI Array Processors*, Prentice-Hall, 1987.

[3] 유기영, 김정준, "유한 필드 $GF(2m)$상의 시스톨릭 곱셈기 및 곱셈/제곱기", 제 11회 정보보호와 암호에 관한 학술대회 WISC'99 논문집, pp. 375-389, 1999.

[4] C. Paar, P. Fleischmann and S. Pedro, Fast Arithmetic for Public-Key Algorithms in Galois Fields with Composite Exponents, *IEEE Trans. on Computers.*, vol. 48, no. 10, pp. 1025-1034, Oct. 1999.

[5] 하경주, 구교민, "셀룰러오토마타를 이용한 LSB 곱셈기 설계", 한국산업정보학회 2001 추계공동학술대회, pp.850-859, November, 2001.

[6] Altera, *APEX 20KC Programmable Logic Device Data Sheet*, ver. 1.2, Oct. 2001.