Journal of The Korea Knowledge Information Technology Society

ISSN 1975-7700

http://www.kkits.or.kr

Design of Hybrid Finite Field Multiplier over $GF(2^{163})$ for Elliptic Curve Cryptosystems

Yong-Suk Cho[1], Chang-Kyu Kim[*2]

[1]*Department of Information & Communication Security, Youngdong University*
[2]*Department of Information & Communication Engineering, Dong-eui University*

ABSTRACT

The multiplication over finite field $GF(2^m)$ is the main arithmetic operation in Elliptic Curve Cryptography (ECC). Therefore, the design of efficient dedicated finite field multiplier architectures can lead to dramatic improvement on the overall system performance. In this paper, a hardware implementation of hybrid multiplier over $GF(2^{163})$ is presented. The proposed multiplier operates in polynomial basis of $GF(2^{163})$. This multiplier's size of 163 bits is currently recommended by the National Institute of Standards and Technology (NIST) in their elliptic curve digital signature standard (ECDSS), and is used in practice for binary field multiplication in elliptic curve cryptography. The hybrid architecture is t-times faster than bit-serial architectures but with lower area complexity than bit-parallel ones, where the value for t, $2 \leq t \leq \lceil m/2 \rceil$, can be arbitrarily selected by the designer to set the tradeoff between area and speed. The most significant feature of the proposed architecture is that a trade-off between hardware complexity and delay time can be achieved. This makes the proposed multipliers suitable for applications where the value of m is large but space is of concern, e.g., resource constrained cryptographic systems such as smart cards and mobile phones. In addition, the proposed architecture is highly regular, simple, expandable and therefore, well-suited for VLSI implementation.

KEYWORDS: Elliptic curve cryptography, Finite fields, Galois fields, Polynomial basis, Multipliers

ARTICLE INFO: Received 30 July 2015, Revised 14 August 2015, Accepted 14 August 2015.

[*]Corresponding author is with the Department of Information & Communication Engineering, Dong-eui University, 176 Eomgwangno, Busanjin-gu Busan, KOREA.
E-mail address: ckkim@deu.ac.kr

1. 서 론

타원곡선 암호 시스템 (Elliptic Curve Cryptosystem)은 1985년 N. Koblitz와 V. Miller에 의해 제안된 공개키 암호 시스템으로 타원곡선 상에서 이산대수의 어려움에 안전성의 근거를 두고 있다[1][2]. 타원곡선 암호 시스템은 기존의 RSA와 Elgamal 공개키 암호시스템에 비하여 짧은 키 길이로 유사한 안전성을 제공한다는 장점을 가지고 있다. 또한 키의 길이가 짧기 때문에 스마트 카드와 같이 자원이 제한된 분야에서 효율적으로 사용될 수 있다[3]. 이러한 장점 때문에 IEEE와 NIST는 공개키 암호 시스템을 위해 ECC에 기반한 디지털 서명 알고리즘으로 IEEE 1363과 ECDSS (Elliptic Curve Digital Signature Standard)를 표준으로 채택하였다 [4][5].

타원곡선 암호 시스템에서는 소수체(prime field)와 이진체(binary field)의 유한체가 주로 사용된다. 소수체에서 사용되는 유한체 연산은 RSA에서 이용되는 연산과 유사하다. 이진체에서 사용되는 유한체 연산은 기저의 표현에 따라 달라지며, 주로 다항식기저와 정규기저를 사용한 구현이 많이 이루어지고 있다.

본 논문에서는 유한체 $GF(2^{163})$의 다항식기저에서 동작하는 하이브리드 곱셈기를 설계한다. 본 논문에서 선택한 유한체의 차수 163은 현재 NIST (National Institute of Standards and Technology)의 타원곡선 디지털 서명 표준인 ECDSS (Elliptic Curve Digital Signature Standard)에서 권고되고 있으며 2진 유한체 곱셈으로 실제 사용되고 있는 것이다[6]-[9]. 제안된 하이브리드 곱셈기는 비트직렬 곱셈기 보다 t배 빠르게 동작하며 비트병렬 곱셈기 보다는 더 낮은 회로 복잡도를 갖는다[10]. 여기에서 t는 $2 \le t \le \lceil m/2 \rceil$ 구간에서, 회로의 복잡도와 지연시간 사이에 절충을 고려하여 설계자가 임의로 선택할 수 있는 값이다. 본 논문에서는 t를 3으로 선택하여 설계하였다.

본 논문의 구성은 먼저 유한체 $GF(2^m)$에서 비트직렬 곱셈기 보다 t배 빠르게 동작하는 t배속 하이브리드 곱셈기를 설계하고, 타원곡선 암호시스템 용으로 권고되는 유한체 $GF(2^{163})$에서 55 클럭만에 곱셈의 결과를 출력하는 3배속 하이브리드 곱셈기를 설계한다. 그리고 결론을 맺는다.

2. 유한체 $GF(2^m)$ 상의 t 배속 하이브리드 곱셈기 설계

유한체 $GF(2^m)$ 상의 임의의 두 원소 A와 B를 다항식기저로 표현하면 다음과 같이 쓸 수 있다.

$$A = a_0 + a_1\alpha + \cdots\cdots + a_{m-1}\alpha^{m-1} \quad (1)$$

$$B = b_0 + b_1\alpha + \cdots\cdots + b_{m-1}\alpha^{m-1} \quad (2)$$

이 두 원소의 곱 Z는 다음과 같이 쓸 수 있다.

$$\begin{aligned} Z &= A \cdot B \\ &= A \cdot (b_0 + b_1\alpha + b_2\alpha^2 + \cdots \\ &\qquad \cdots\cdots + b_{m-1}\alpha^{m-1}) \end{aligned} \quad (3)$$

또한 식 (3)을 다시 정리하면 다음과 같이 된다.

$$\begin{aligned} Z = {} & b_0A + b_1[A\alpha] + b_2[A\alpha^2] + \cdots \\ & \cdots\cdots + b_{m-1}[A\alpha^{m-1}] \end{aligned} \quad (4)$$

여기에서 식 (4)를 t 개로 분할하면

$$Z = Z^{(0)} + Z^{(1)} + \cdots\cdots + Z^{(t-1)} \quad (5)$$

가 되고 $Z^{(0)}$, $Z^{(1)}$, ……, $Z^{(t-1)}$은 다음과 같이 정리할 수 있다.

$$\begin{aligned}
Z^{(0)} &= b_0[A] + b_t[A]\alpha^t \\
&\quad + b_{2t}[A]\alpha^{2t} + \cdots \\
Z^{(1)} &= b_1[A\alpha] + b_{t+1}[A\alpha]\alpha^t \\
&\quad + b_{2t+1}[A\alpha]\alpha^{2t} + \cdots\cdots \\
Z^{(2)} &= b_2[A\alpha^2] + b_{t+2}[A\alpha^2]\alpha^t \\
&\quad + b_{2t+2}[A\alpha^2]\alpha^{2t} + \cdots\cdots \\
&\vdots \\
Z^{(t-1)} &= b_{t-1}[A\alpha^{t-1}] + b_{2t-1}[A\alpha^{t-1}]\alpha^t \\
&\quad + b_{3t-1}[A\alpha^{t-1}]\alpha^{2t} + \cdots\cdots
\end{aligned} \tag{6}$$

식 (6)을 이용하면 <그림 1>과 같은 t배속 하이브리드 곱셈기를 설계할 수 있다.

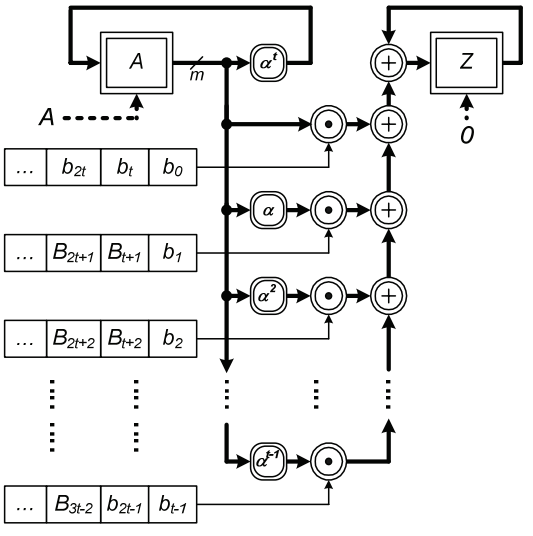

그림 1. $GF(2^m)$ 상의 t배속 하이브리드 곱셈기
Figure 1. The t-times fast hybrid multiplier over $GF(2^m)$

<그림 1>에서 굵은 선은 m비트 버스이고, ▭는 m비트 레지스터를, ⊕는 m개의 2입력 XOR 게이트를, ⊙은 m개의 2입력 AND 게이트를, ⓐ는 $GF(2^m)$의 원시원 α를 곱하는 상수곱셈기(constant multiplier)를 나타내고 있다. 이와 같은 t배속 하이브리드 곱셈기는 $\lceil m/t \rceil$ 클럭 시간에 곱셈의 결과를 얻을 수 있다.

3. $GF(2^{163})$ 상의 3배속 하이브리드 곱셈기 설계

유한체 $GF(2^{163})$의 임의의 두 원소 A와 B의 곱 Z는 다음과 같이 쓸 수 있다.

$$\begin{aligned}
Z &= A \cdot (b_0 + b_1\alpha + \cdots\cdots + b_{162}\alpha^{162}) \\
&\equiv Z^{(0)} + Z^{(1)} + Z^{(2)}
\end{aligned} \tag{7}$$

여기에서 $Z^{(0)}$, $Z^{(1)}$, $Z^{(2)}$는 다음과 같이 된다.

$$\begin{aligned}
Z^{(0)} &= A \cdot (b_0 + b_3\alpha^3 + \cdots\cdots \\
&\qquad + b_{159}\alpha^{159} + b_{162}\alpha^{162}) \\
&= b_0[A] + b_3[A\alpha^3] + \cdots\cdots \\
&\quad + b_{159}[A\alpha^{159}] + b_{162}[A\alpha^{162}] \\
Z^{(1)} &= A \cdot (b_1\alpha + b_4\alpha^4 + \cdots\cdots \\
&\qquad + b_{160}\alpha^{160} + 0\alpha^{163}) \\
&= b_1[A\alpha] + b_4[A\alpha^4] + \cdots\cdots \\
&\quad + b_{160}[A\alpha^{160}] + 0[A\alpha^{163}] \\
Z^{(2)} &= A \cdot (b_2\alpha^2 + b_5\alpha^5 + \cdots\cdots \\
&\qquad + b_{161}\alpha^{161} + 0\alpha^{164}) \\
&= b_2[A\alpha^2] + b_5[A\alpha^5] + \cdots\cdots \\
&\quad + b_{161}[A\alpha^{161}] + 0[A\alpha^{164}]
\end{aligned} \tag{8}$$

식 (8)을 이용하면 <그림 2>와 같이 $GF(2^{163})$ 상의 3배속 하이브리드 곱셈기를 설계할 수 있다.

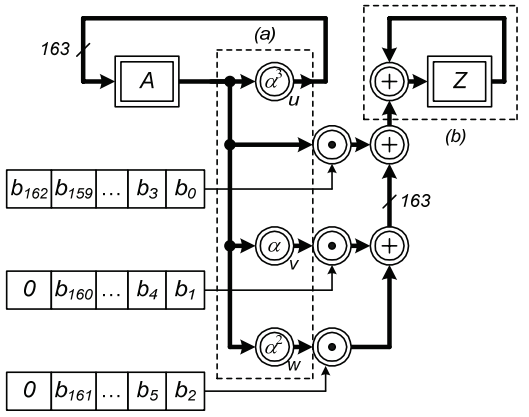

그림 2. $GF(2^{163})$ 상의 3배속 하이브리드 곱셈기
Figure 2. The 3 times fast hybrid multiplier over $GF(2^{163})$

<그림 2>의 곱셈기는 55(=⌈163/3⌉) 클럭 시간에 곱셈의 결과를 얻을 수 있다.

유한체 $GF(2^{163})$의 원시다항식이 $p(x)=x^{163}+x^7+x^6+x^3+1$일 때 $GF(2^{163})$ 상의 임의의 한 원소 A에 α, α^2, α^3을 곱하면 다음과 같이 된다.

$$\begin{aligned}A\cdot\alpha &= (a_0+a_1\alpha+\cdots+a_{162}\alpha^{162})\alpha\\ &= a_0\alpha+a_1\alpha^2+\cdots+a_{162}\alpha^{163}\\ &= a_0\alpha+a_1\alpha^2+\cdots\cdots\\ &\quad +a_{162}(1+\alpha^3+\alpha^6+\alpha^7)\\ &= a_{162}+a_0\alpha+a_1\alpha^2+(a_2+a_{162})\alpha^3\\ &\quad +a_3\alpha^4+a_4\alpha^5+(a_5+a_{162})\alpha^6\\ &\quad +(a_6+a_{162})\alpha^7+\cdots+a_{161}\alpha^{162}\end{aligned} \tag{9}$$

$$\begin{aligned}A\cdot\alpha^2 &= (a_0+a_1\alpha+\cdots+a_{162}\alpha^{162})\alpha^2\\ &= a_0\alpha^2+a_1\alpha^3+\cdots+a_{162}\alpha^{164}\\ &= a_0\alpha^2+a_1\alpha^3+\cdots\cdots\\ &\quad +a_{161}(1+\alpha^3+\alpha^6+\alpha^7)\\ &\quad +a_{162}(\alpha+\alpha^4+\alpha^7+\alpha^8)\end{aligned} \tag{10}$$

$$\begin{aligned}&= a_{161}+a_{162}\alpha+a_0\alpha^2+(a_1+a_{161})\alpha^3\\ &\quad +(a_2+a_{162})\alpha^4+a_3\alpha^5+(a_4+a_{161})\alpha^6\\ &\quad +(a_5+a_{161}+a_{162})\alpha^7+(a_6+a_{162})\alpha^8\\ &\quad +\cdots\cdots+a_{160}\alpha^{162}\end{aligned}$$

$$\begin{aligned}A\cdot\alpha^3 &= (a_0+a_1\alpha+\cdots+a_{162}\alpha^{162})\alpha^3\\ &= a_0\alpha^3+a_1\alpha^4+\cdots+a_{162}\alpha^{165}\\ &= a_0\alpha^3+a_1\alpha^4+\cdots\cdots\\ &\quad +a_{160}(1+\alpha^3+\alpha^6+\alpha^7)\\ &\quad +a_{161}(\alpha+\alpha^4+\alpha^7+\alpha^8)\\ &\quad +a_{162}(\alpha^2+\alpha^5+\alpha^8+\alpha^9)\\ &= a_{160}+a_{161}\alpha+a_{162}\alpha^2+(a_0+a_{160})\alpha^3\\ &\quad +(a_1+a_{161})\alpha^4+(a_2+a_{162})\alpha^5\\ &\quad +(a_3+a_{160})\alpha^6+(a_4+a_{160}+a_{161})\alpha^7\\ &\quad +(a_5+a_{161}+a_{162})\alpha^8+(a_6+a_{162})\alpha^9\\ &\quad +\cdots\cdots+a_{159}\alpha^{162}\end{aligned} \tag{11}$$

그러므로 식 (9)~(11)을 이용하면, <그림 2>에서 (a) 부분의 상수 곱셈기는 <그림 3>과 같이 9개의 2입력 XOR 게이트로 구현할 수 있다. 또한 (b) 부분의 유한체 누산기 (accumulator)는 $GF(2^m)$의 경우, m개의 D 플립플롭과 m개의 2입력 XOR 게이트로 구현할 수 있지만, 통합하여 m개의 T 플립플롭으로 구현할 수 있다[11]. <표 1>에 <그림 2>와 같은 $GF(2^{163})$ 상의 3배속 하이브리드 곱셈기의 구현에 소요되는 게이트 수를 정리하였다.

표 1. 제안된 곱셈기의 소요 게이트 수
Table 1. Gate counts for the proposed multiplier

구 분	게이트 수
레지스터	$3m=3\times163=$ 489
2-input AND	$tm=3\times163=$ 489
2-input XOR	$(t-1)m=2\times163=$ 326
상수 곱셈기	2-input XOR 9
CLOCK	$\lceil m/t\rceil=\lceil 163/3\rceil=$ 55

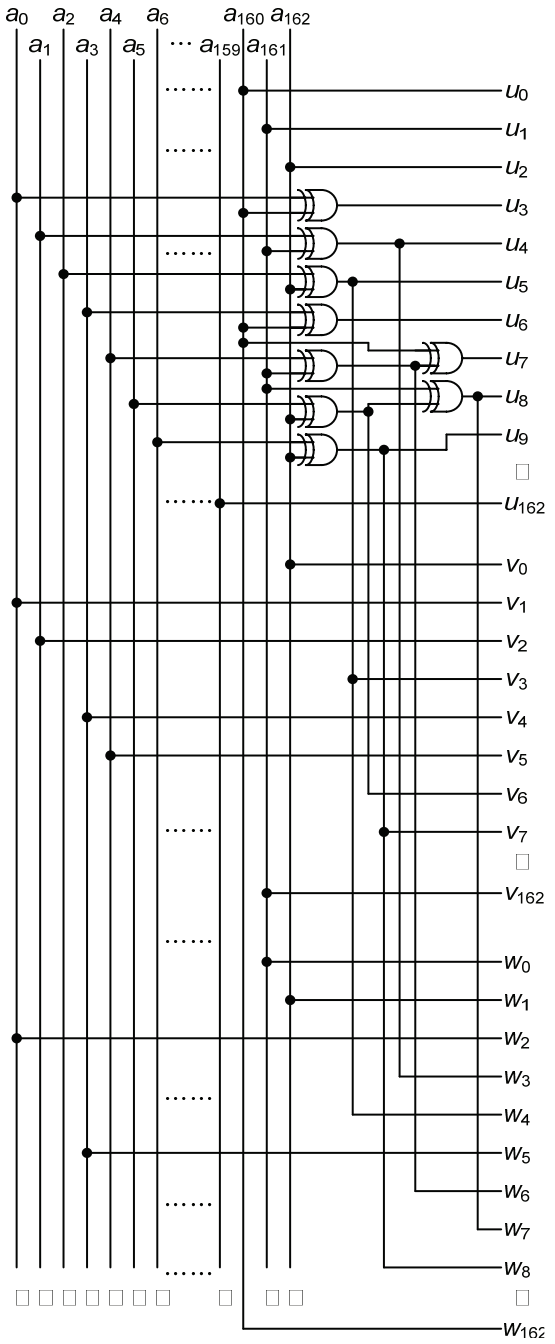

그림 3. <그림 2>의 상수곱셈기
Figure 3. The constant multiplier in Fig. 2

4. 결 론

본 논문에서는 유한체 $GF(2^m)$의 다항식기저 상에서 기존의 비트직렬 곱셈기에 비해 t배 빠르게 곱셈의 결과를 계산할 수 있는 t배속 하이브리드 곱셈기를 설계하고, 실제 예로서 타원곡선 암호 시스템에서 사용되는 유한체 $GF(2^{163})$에서 55클럭만에 곱셈의 결과를 출력할 수 있는 3배속 하이브리드 곱셈기를 설계하였다.

설계된 곱셈기는 비트직렬 곱셈기의 긴 지연시간과 비트병렬 곱셈기의 복잡한 회로 사이를 적절하게 절충함으로써, 비트직렬 곱셈기보다는 짧은 지연시간에 결과를 얻을 수 있으며 비트병렬 곱셈기보다는 더 적은 하드웨어로 구현할 수 있는 장점을 가지고 있다.

References

[1] N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation, 48, pp. 203-209, 1987.

[2] V. S. Miller, *Use of elliptic curves in cryptography*, Springer-Verlag, Advances in Cryptology - Proceedings of Crypto'85, LNCS 218, pp. 417-426, 1986.

[3] D. Hankerson, A. Menezes and S. Vanstone, *Guide to elliptic curve cryptography*, Springer-Verlag, 2004.

[4] IEEE 1363, *IEEE standard specifications for public-key cryptography*, Jan. 2000.

[5] NIST, *Digital signature standard*, FIPS Publication, 186-2, Feb. 2000.

[6] C. H. Kim, S. Kwon, and C. P. Hong, *FPGA implementation of high performance elliptic curve cryptographic processor over GF(2^{163})*, Journal of Systems Architecture,

Vol. 54, No. 10, pp. 893-900, 2008.

[7] Y. Zhang, D. Chen, Y. Choi, L. Chen, and S. Ko, *A high performance ECC hardware implementation with instruction-level parallelism over GF(2^{163})*, Microprocessors and Microsystems, Vol. 34, No. 6, pp. 228-236, October 2010.

[8] H. Mahdizadeh, and M. Masoumi, *Novel architecture for efficient FPGA implementation of elliptic curve cryptographic processor over GF(2^{163})*, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 21, No. 12, pp. 2330-2333, 2013.

[9] K. C. Cinnati Loi, and Seok-Bum Ko, *Improvements for high performance elliptic curve cryptosystem processor over GF(2^{163})*, 2012 International Symposium on Electronic System Design, pp. 140-144, 2012.

[10] Yong-Suk Cho, and Kyoung-Il Min, *Hardware implementation of t-times fast hybrid polynomial basis multiplier over GF(2^m)*, Journal of The Korea Knowledge Information Technology Society(JKKITS), Vol. 10, No. 2, pp. 271-277, 2015.

[11] P. K. Meher, *On efficient implementation of accumulation in finite field over GF(2^m) and its applications*, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 17, No. 4, pp. 541-550, 2009.

타원곡선 암호시스템을 위한 유한체 $GF(2^{163})$ 상의 하이브리드 곱셈기 설계

조용석[1], 김창규[2]

[1] *영동대학교 정보통신보안학과*

[2] *동의대학교 정보통신공학과*

요 약

유한체 상의 곱셈은 타원곡선 암호(Elliptic Curve Cryptography)에 있어서 핵심이 되는 연산이다. 그러므로 효율적인 구조를 갖는 유한체 상의 곱셈기를 설계하면 전체적인 시스템의 성능을 대폭 향상시킬 수 있다. 본 논문에서는 유한체 $GF(2^{163})$ 상의 하이브리드 곱셈기를 설계한다. 설계된 곱셈기는 유한체 $GF(2^{163})$의 다항식기저 상에서 동작한다. 본 논문에서 선택한 유한체의 차수 163은 현재 NIST(National Institute of Standards and Technology)의 타원곡선 디지털 서명 표준인 ECDSS(Elliptic Curve Digital Signature Standard)에서 권고되고 있으며 2진 유한체 곱셈으로 실제 사용되고 있는 것이다. 제안된 하이브리드 곱셈기는 비트직렬 곱셈기 보다 t배 빠르게 동작하며 비트병렬 곱셈기 보다는 더 낮은 회로 복잡도를 갖는다. 여기에서 t는 $2 \le t \le \lceil m/2 \rceil$로 설계자가 회로 면적과 속도 사이에서 적절하게 절충하여 임의로 선택할 수 있는 값이다. 제안된 곱셈기의 가장 큰 장점은 회로의 복잡도와 지연시간 사이에 적절한 절충을 꾀할 수 있는 점이다. 따라서 본 곱셈기는 자원이 한정된 암호 시스템, 예를 들어 스마트 카드나 이동전화와 같이, m값은 크지만 회로의 면적이 문제가 되는 암호 응용에 적합한 장점을 가지고 있다. 또한 제안된 곱셈기는 회로의 구조가 규칙적이고 간단하며 쉽게 확장할 수 있어서 VLSI 구현에 적합하다.

Yong-Suk Cho received the B.S., M.S., and Ph.D. degree in the Department of Electronic Communication Engineering from Hanyang University in 1986, 1988 and 1998, respectively. From 1989 to 1996, he was a researcher at Korea Telecom. He has been a professor in the Department of Information & Communication Security at Youngdong University since 1996. His current research interests include finite field arithmetic, cryptography, and error-control coding.

E-mail address: yscho@yd.ac.kr

Chang-Kyu Kim received the B.S., M.S., and Ph.D. degree in the Department of Electronic Communication Engineering from Hanyang University in 1981, 1984 and 1989, respectively. He has been a professor in the Department of Information & Communication Engineering at Dong-eui University since 1988. His current research interests include finite field arithmetic, cryptography, and error-control coding. (Corresponding author of this paper)

E-mail address: ckkim@deu.ac.kr