Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.979

타입 II 최적 정규기저를 갖는 $GF(2^n)$의 곱셈기*

김 창 한,[1†] 장 남 수[2‡]
[1]세명대학교, [2]세종사이버대학교

Type II Optimal Normal Basis Multipliers in $GF(2^n)$*

Chang Han Kim,[1†] Nam Su Chang[2‡]
[1]Semyung University, [2]Sejong Cyber University

요 약

본 논문에서는 타입 II 최적 정규기저를 갖는 유한체 $GF(2^n)$의 Semi-Systolic 곱셈기를 제안한다. 본 곱셈기는 기존의 2012년에 발표된 Chiou 등의 곱셈기에 비해 공간복잡도 면 에서는 전체 트랜지스터가 $2n^2+44n+26$개 줄고 시간복잡도는 4 클럭 감소한다. 즉, NIST의 ECDSA를 위한 권장 유한체 $GF(2^{233})$인 경우 공간복잡도는 6.4% 줄고 시간복잡도는 2% 정도 줄어든다. 또한 이 구조는 2009년에 Chiou 등이 제안한 동시오류탐지 및 정정 방법을 그대로 적용할 수 있는 장점도 있다.

ABSTRACT

In this paper, we proposed a Semi-Systolic multiplier of $GF(2^n)$ with Type II optimal Normal Basis. Comparing the complexity of the proposed multiplier with Chiou's multiplier proposed in 2012, it is saved $2n^2+44n+26$ in total transistor numbers and decrease 4 clocks in time delay. This means that, for $GF(2^{233})$ of the field recommended by NIST for ECDSA, the space complexity is 6.4% less and the time complexity of the 2% decrease. In addition, this structure has an advantage as applied to Chiou's method of concurrent error detection and correction in multiplication of $GF(2^n)$.

Keywords: TYPE II Optimal Normal Basis, Semi-Systolic Multiplier, Error Detection

I. 서 론

유한체 $GF(2^n)$은 암호분야[5,10]와 리드-솔로몬 부호 분야[6]에 많이 응용된다. 최근 효율적인 유한체 연산 구현에 대한 연구[1-4] 가 활발하게 진행되고 있으며 특히 제곱 연산에 부담이 전혀 없는 정규기저 중 복잡도가 가장 낮은 최적 정규기저를 활용한 곱셈기가 활발하게 연구되고 있다[1-3,7,9]. 이중 타입 I 최적 정규기저의 경우 n이 짝수여서 응용분야에 활동도가 조금 미진한 반면 타입 II의 경우 n이 홀수로 암호 응용 분야에 널리 관심을 가지고 연구되는 경우이다[1,2,7,9]. NIST의 ECDSA를 위한 권장 유한체 $GF(2^{233})$의 n= 233도 이 경우의 하나이다.

2003년에 Kwon 등[1]이 처음으로 타입 II에 대한 시스톨릭 구조의 곱셉기를 제안하였으며 2009년에는 Chiou 등[7]이 일반적인 가우시안 정규기저(Gaussian Normal Bases)에 대한 세미 시스톨릭 구조의 곱셈기를 처음으로 제안하였다. 그 후 2012년에는 Chiou 등[9]이 2009년 곱셈기의 공간복잡도를 57% 개선하고 시간 복잡도가 다소 증가하는 세미 시스톨릭 곱셈기를 제안 하였다.

접수일(2015년 4월 21일), 수정일(1차: 2015년 9월 4일), 게재확정일(2015년 9월 7일)
* 이 논문은 2014학년도 세명대학교 교내학술연구비 지원에 의해 수행된 연구임.
† 주저자, chkim@semyung.ac.kr
‡ 교신저자, nschang@sjcu.ac.kr(Corresponding author)

본 논문에서는 타입 II 최적 정규기저를 갖는 유한체 $GF(2^n)$의 세미 시스톨릭 구조의 곱셈기를 제안하였다. 이 곱셈기는 기존 Chiou 등[9]의 곱셈기에 비하여 공간복잡도 면 에서는 전체 트랜지스터 수는 $2n^2+44n+26$ 개가 줄고 시간복잡도 도 4 클럭 감소하는 효율적인 곱셈기이다. 즉, NIST의 ECDSA를 위한 권장 유한체 $GF(2^{233})$인 경우 공간복잡도는 6.4% 줄고, 시간복잡도도 2% 정도 감소한다. 이 곱셈기는 Chiou등[7]이 제안한 오류 탐지 및 복구 방법을 그대로 적용할 수 있는 장점도 있다.

본 논문은 2장에서는 유한체의 기저에 관한 기본적인 이론 설명과 타입 II 최적 정규기저에 관한 정의를 하였고, 3장에서는 타입 II 최적 정규기저의 곱셈기 제안과 그 복잡도를 살펴보고, 4장에서는 결론을 제시하였다.

II. 유한체와 타입 II 최적 정규기저

유한체 $GF(2^n)$의 연산은 덧셈, 제곱, 곱셈과 역원으로 구성되어 있다. 덧셈과 제곱은 간단하게 구성되는 반면 곱셈은 유한체의 표현 방법에 따라 다양하게 구성된다. 유한체의 표현은 어떤 기저를 사용하여 표현하느냐에 따라 구분하는데, 대표적으로 다항식기저와 정규기저를 사용하고 있다. 즉, $GF(2^n)$을 구성하는 GF(2) 위의 기약다항식을

$$f(x)= x^n+f_{n-1}x^{n-1}+\cdots+f_1x+1$$

이라 할 때 $f(x)$의 근을 α라 하면 $GF(2^n)$의 원소

$$A= a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1},\quad a_i\in GF(2)$$

와 같이 표현하는 것이 다항식 기저를 이용한 표현이며, 이를 벡터로 표시하면 $A=(a_0,\cdots,a_{n-1})$이다.

반면에 정규기저를 이용한 표현은 $\beta\in GF(2^n)$의 켤레들이 $GF(2)$ 위에서 $GF(2^n)$ 의 기저가 될 때, 이 기저를 사용하는 것이다. 즉,

$$\{\beta,\beta^2,\cdots,\beta^{2^{n-1}}\}$$

이 기저가 되어 $GF(2^n)$의 원소

$$A=a_1\beta+a_2\beta^2+\cdots+a_n\beta^{2^{n-1}},\quad a_i\in GF(2)$$

와 같이 표현하는 것이다. 이때 β를 정규기저 생성자라 한다. 또한 A를 벡터로 표시하면

$$A=(a_1,a_2,\cdots,a_n)\quad .$$

정규기저를 이용할 경우 제곱 연산은 계수들의 위치이동으로 표시되므로 하드웨어적으로는 연산이 없는 장점이 있다. 정규기저를 구성하는 방법은 여러 방법이 있으나 정리 1에 제시된 가우시안 정규기저 방법이 가장 널리 쓰인다.

정규기저를 이용한 곱셈의 경우

$$C = A\cdot B,$$
$$A=\sum_{i=1}^{n}a_i\beta^{2^{i-1}},B=\sum_{i=1}^{n}b_i\beta^{2^{i-1}},C=\sum_{i=1}^{n}c_i\beta^{2^{i-1}}$$

라 하면

$$c_1=(a_1a_2\cdots a_n)\cdot M\cdot(b_1b_2\cdots b_n)^T,$$
$$M=(m_{ij}):n\times n$$

로 표시되고, 이때 행렬 M의 1의 개수(Weight)를 기저 $N=\beta,\ \beta^2,\ \cdots,\ \beta^{2^{n-1}}$의 곱셈에 대한 복잡도(Complexity) C_N이라 한다.

참고. 모든 정규기저 N의 복잡도는 $C_N\geq 2n-1$이다. 특히 $C_N=2n-1$인 경우 N을 최적 정규기저라 한다. 정리 1에서 k=1, 2인 경우 최적 정규기저이고 2인 경우를 타입 II라 한다[10].

정리 1. n, k는 nk+1이 2보다 큰 소수인 조건을 만족하는 양의 정수이고, α는 $GF(2^{nk})$에서 원시 nk+1 승근이라 하자. Z^*_{nk+1}에서 2의 위수(order)를 e라 할 때, $\gcd(nk/e,n)=1$ 라 하자. 그러면 Z_{nk+1}에서 원시 k 승근 τ 에 대하여

$$\beta=\sum_{i=0}^{k-1}\alpha^{\tau^i}$$

는 $GF(2)$ 위에서 $GF(2^n)$의 정규기저 생성자이다[10].

정리 2. $GF(2^n)$이 타입 II 최적 정규기저를 갖기 위한 필요충분조건은 2n+1은 소수이고

$$Z^*_{2n+1} = <-1, 2>$$

이다[10].

III. 제안하는 타입 II 최적 정규기저 곱셈기와 복잡도

타입 II인 경우 Z_{2n+1}에서 $\tau = -1$이므로 $\beta = \alpha + \alpha^{-1}$이다. 그리고 정리 2에 의하여 $Z^*_{2n+1} = \{\pm 2^i | 0 \le i \le n-1\}$ 이므로 $GF(2^n)$의 정규기저는 집합적으로 다음과 같다.

$$\begin{aligned} N &= \{\beta,\ \beta^2,\ \beta^{2^2},\ \cdots,\ \beta^{2^{n-1}}\} \\ &= \{\alpha+\alpha^{-1},\ \alpha^2+\alpha^{-2},\ \cdots,\ \alpha^n+\alpha^{-n}\} \\ &= \{\alpha+\alpha^{2n},\ \alpha^2+\alpha^{2n-1},\ \cdots,\ \alpha^n+\alpha^{n+1}\}. \end{aligned}$$

따라서 $GF(2^n)$ 원소 A의 계수 위치를 조정하면

$$A = \sum_{i=1}^{n} a_i(\alpha^i + \alpha^{-i})$$

이다. 또한, A를 $GF(2^{2n})$의 원소 $\overline{A}$로 표시하면 다음과 같다.

$$\begin{aligned} \overline{A} &= \sum_{k=1}^{2n} A_k \alpha^k \ , 1 \le i \le n, \\ A_i &= A_{2n+1-i} = a_i \quad . \end{aligned}$$

즉,

$$\begin{aligned} \overline{A} &= (a_1, a_2, \cdots, a_n, a_n, a_{n-1}, \cdots, a_1) \\ &= \sum_{i=1}^{n} a_i \alpha^i + (\sum_{i=1}^{n} a_{n+1-i}\alpha^i)\alpha^n \\ &= A1 + A2\alpha^n, \end{aligned}$$

$$A1 = \sum_{i=1}^{n} a_i \alpha^i,\ A2 = \sum_{i=1}^{n} a_{n+1-i}\alpha^i.$$

$C = A \cdot B$, $A, B \in GF(2^n)$을 구하기 위하여

$A \equiv \overline{A} = A1 + A2\alpha^n, B \equiv \overline{B} = B1 + B2\alpha^n$ 라 하면

$$\begin{aligned} C \equiv \overline{C} &= (A1 + A2\alpha^n)(B1 + B2\alpha^n) \\ &= A1 \cdot B1 + A1 \cdot B2\alpha^n \\ &\quad + A2 \cdot B1\alpha^n + A2 \cdot B2\alpha^{2n} \end{aligned}$$

이다.

한편,

$$A1 \cdot B1 = \sum_{i=1}^{n} a_i B1\alpha^i = \sum_{i=1}^{n} a_i B^{(i)},\ B^{(i)} = B1\alpha^i$$

라 하면

$$B^{(i)} = \sum_{j=1}^{n} b_j \alpha^{j+i},\ B^{(i+1)} = B^{(i)}\alpha = \sum_{j=1}^{n} b_j \alpha^{j+i+1}$$

이므로 $A1 \cdot B1$을 Fig.1.과 같이 세미 시스톨릭 (Semi-Systolic) 구조로 계산할 수 있다.

Network-XOR 에서는

(1) A1B2 와 A2B1 의 경우 :

AiBj 계산후 α^n 을 곱한 값을 출력하는 과정이다. 즉, $A1B2 = \sum_{i=2}^{2n} D_i\alpha^i$ 라 하면

$$\begin{aligned} A1B2\alpha^n = &(D_{n+1} + D_{n+2})\alpha + (D_{n+1} + D_{n+3})\alpha^2 + \\ &\cdots + (D_{n+1} + D_{2n})\alpha^{n-1} + D_{n+1}\alpha^n + \\ &D_{n+1}\alpha^{n+1} + (D_{n+1} + D_2)\alpha^{n+2} \\ &+ \cdots + (D_{n+1} + D_n)\alpha^{2n} \end{aligned}$$

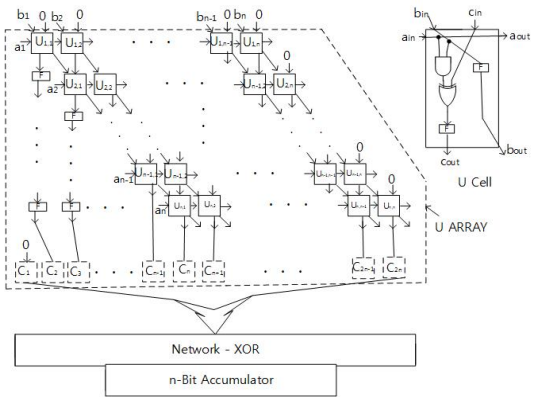

Fig. 1. Semi-systolic architecture

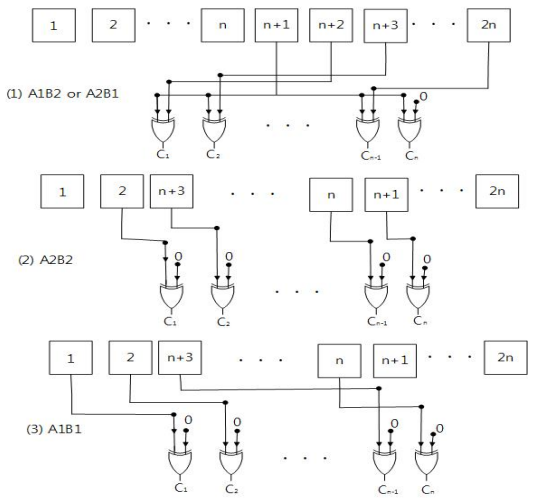

Fig. 2. Network-XOR

이므로

$$(D_{n+1}+D_{n+2})\alpha+(D_{n+1}+D_{n+3})\alpha^2+\cdots \\ +(D_{n+1}+D_{2n})\alpha^{n-1}+D_{n+1}\alpha^n$$

의 과정이 필요하다.

(2) A2B2 의 경우 :

$A2B2=\sum_{i=2}^{2n} D_i\alpha^i$라 하면 $A2B2\alpha^{2n}=\sum_{i=1}^{2n-1} D_{i+1}\alpha^i$

이므로 실제적으로는 쉬프팅이다.

(3) A1B1 경우는 C_1 부터 C_n 까지 그대로 연결이다.

(1), (2), (3)을 통합하기 위하여 n번의 XOR로 구성하였다(Fig.2. 참고).

전체적인 연산 구성을 구체적으로 보면, Cell의

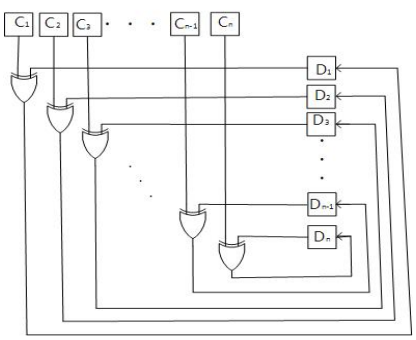

Fig. 3. Accumulator

n 클럭 후, 즉, A1B2를 U Array가 계산한 후, A2B1이 U Array 계산을 마치는 순간 A1B2는 Network-XOR을 계산 후 Accumulator의 Register C로 이동, A2B2가 U Array계산을 마친 경우, A1B2는 Accumulator 계산 후 Register D로 이동, A2B1은 Network-XOR 후 Accumulator C로 이동, 그 후 A1B1이 U Array 계산을 마친 경우는 A2B2는 Network-XOR 계산 후, Accumulator C로 이동, A1B2와 A2B1은 XOR 후 D로 이동, 이후 XOR 한번으로 A2B2와 (A1B2⊕A2B1)의 XOR 후 D로 이동, A1B1은 Network-XOR 후 C로 이동, 마지막으로 한번의 XOR에 의하여 AB의 값을 출력한다. 전체적으로 (n+3)번의 Cell Delay와 2번의 XOR Delay로 구성된다. 클럭 통일을 위하여 1번의 XOR도 Cell 과 같은 클럭으로 움직이면 n+5번의 Cell Delay 발생한다. 또한, Accumulator D에 $E\in GF(2^n)$의 값을 넣으면 $AB+E$의 연산도 가능하다. 그리고 Accumulator를 유한체 덧셈기로 대체 가능하다.

전체적인 연산 시스템을 구체적으로 보면 Cell의 n 클럭 후 A1B2를 U Array가 계산한 후, A2B1이 U Array 계산을 마치는 순간 A1B2는 Network-XOR을 계산 후 Accumulator의 Register C로 이동, A2B2가 U Array 계산을 마친 경우, A1B2는 Accumulator 계산 후 Register D로 이동, A2B1은 Network-XOR 후 Accumulator C로 이동, 그 후 A1B1이 U Array 계산을 마친 경우는 A2B2는 Network-XOR 계산 후, Accumulator C 로 이동, A1B2와 A2B1은 XOR 후 D로 이동, 이후 XOR 한번으로 A2B2와 (A1B2⊕A2B1)의 XOR 후 D로 이동, A1B1은 Network-XOR 후 C로 이동, 마지막으로 한번의 XOR에 의하여 AB의 값을 출력한다. 공간복잡도의 경우 AND, XOR은 6개, Latch(Flop-Flip)은 8개의 transistor로 구성 된 것[8]으로 전체 복잡도를 제시하였다. 또한 C_1 부터 C_{2n}의 Flip-Flop은 불필요한 것으로 그림의 이해를 위하여 추가하였다.

전체적으로 (n+3)번의 Cell Delay와 2번의 XOR Delay로 구성되며, XOR도 Cell과 같은 클럭으로 움직이면 n+5번의 Cell Delay가 발생한다. 구체적인 복잡도는 Table 1.에 제시하였다.

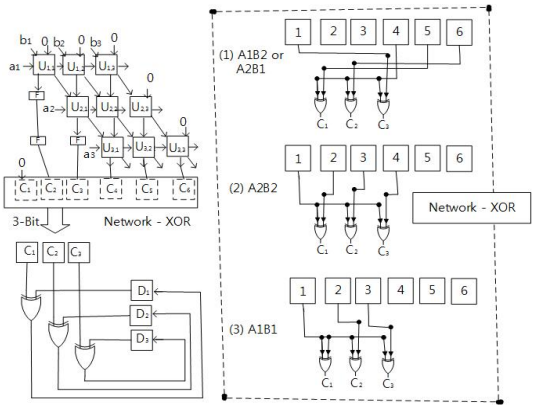

Fig. 4. The proposed multiplier over $GF(2^3)$

예제) $GF(2^3)$ 의 경우를 보자

$$A1 = a_1\alpha + a_2\alpha^2 + a_3\alpha^3, B1 = b_1\alpha + b_2\alpha^2 + b_3\alpha^3$$

이므로

$$\begin{aligned} A1 \cdot B1 = {} & a_1(b_1\alpha^2 + b_2\alpha^3 + b_3\alpha^4) \\ & + a_2(b_1\alpha^3 + b_2\alpha^4 + b_3\alpha^5) \\ & + a_3(b_1\alpha^4 + b_2\alpha^5 + b_3\alpha^6) \end{aligned}$$

$$\begin{aligned} A1 \cdot B2 = {} & a_1(b_3\alpha^2 + b_2\alpha^3 + b_1\alpha^4) \\ & + a_2(b_3\alpha^3 + b_2\alpha^4 + b_1\alpha^5) \\ & + a_3(b_3\alpha^4 + b_2\alpha^5 + b_1\alpha^6) \\ = {} & d_2\alpha^2 + d_3\alpha^3 + d_4\alpha^4 + d_5\alpha^5 + d_6\alpha^6 \end{aligned}$$

라 하면

$$\begin{aligned} A1B2\alpha^3 = {} & (d_4 + d_5)\alpha + (d_4 + d_6)\alpha^2 + d_4\alpha^3 \\ & + (d_4 + d_2)\alpha^5 + (d_4 + d_3)\alpha^6. \end{aligned}$$

$A2B2 = e_2\alpha^2 + e_3\alpha^3 + e_4\alpha^4 + e_5\alpha^5 + e_6\alpha^6$라 하면

$$A2B2\alpha^6 = e_2\alpha + e_3\alpha^2 + e_4\alpha^3 + e_5\alpha^4 + e_6\alpha^5$$

이다.

IV. 결 론

유한체는 정보보호 분야와 코드 분야에 많이 응용되는 분야이다. 이와 관련하여 유한체 연산에 관한 연구가 활발하게 진행되고 있는 상황이다. 가장 최근에 발표된 Chiou 등[9]이 제시한 곱셈기 보다 공간 복잡도면에서 전체 트랜지스터가 $2n^2+44n+26$ 개 줄어 약 6% 정도 줄고 시간 복잡도는 4 사이클 감소하는 곱셈기를 제안하였다. 구체적으로 NIST[5]의 ECDSA를 위한 권장 유한체인 $GF(2^{233})$ 인 경우는 공간 복잡도는 기존의 6.4% 줄고 시간 복잡도는 2 % 감소하는 곱셈기 이다. 또한 최근에 오류

Table 1. Comparison of space and time complexity

Multipliers	Kwon[1]	Chiou [7]	Chiou[9]	Proposed Multiplier
Array Type	Systolic	Semi-Systolic	Semi-Systolic	Semi-Systolic
Function	AB+C	AB+C	AB+C	AB+C
Number of Cells	n^2	$n(2n+1)$	n^2	n^2
Space Complexity 2-Input AND	$2n^2+n$	$2n^2+n$	n^2	n^2
2-Input XOR		$2n^2+5n+1$	n^2+4n+1	n^2+2n
3-Input XOR 1-bit Latch or Flip -Flop	n^2+n		2n+1(multiplexer)	
Total transistor counts	$5n^2+2n-2$	$9n(n+1)/2+2$	$2n^2+2n+1$	$5n(n+1)/2$
	$64n^2+34n-16$	$60n^2+56n+22$	$34n^2+76n+26$	$32n(n+1)$
Time Complexity Cell Delay	$T_A+T_{X3}+T_L$	$T_A+T_X+T_L$	$T_A+T_X+T_L$	$T_A+T_X+T_L$
Latency	n+1	n+1	n+8	n+5
Total Delay	(n+1) $(T_A+T_{X3}+T_L)$	(n+1) $(T_A+T_X+T_L)$	(n+8) $(T_A+T_X+T_L$	(n+5) $(T_A+T_X+T_L)$

주입 공격과 관련 하여 유한체 연산의 오류 탐지에 대한 관심 집중되고 있는 상황에서 Chiou 등[7]이 제안한 오류 탐지 및 복구 방법을 그대로 적용할 수 있는 장점도 있다.

References

[1] S. Kwon, "A Low Complexity and a Low Latency Bit Parallel Systolic Multiplier over $GF(2^m)$ Using an Optimal Normal Basis of Type II," Proc. 16th IEEE Symp. Computer Arithmetic, pp. 196-202, June. 2003.

[2] C.H. Kim, Y. Kim, S.Y. Ji and I. Park, "A New Parallel Multiplier for Type II Optimal Normal Basis," CIS 2006, pp. 460-469, 2006.

[3] A. Reyhani-Masoleh, "Efficient Algorithms and Architecture for Finite Multiplication Using Gaussian Normal Bases," IEEE Trans. computers, vol. 55, no. 1, pp. 34-47, Jan. 2006.

[4] A. Reyhani-Masoleh and M.H. Hasan, "A New Construction of Massey- Omura Parallel Multiplier over $GF(2^m)$," IEEE Trans. computers, Vol. 51, no. 5, pp. 512-520, May. 2002.

[5] Nat'1 Inst. of Standard and Technology, Digital Signature Standard, FIPS Publication 182-2, Jan. 2000.

[6] E.R. Berlekamp, "Bit-Serial Reed-Solomon Encoders," IEEE Trans. on info. Theory, vol. 28, pp. 869-874, Nov. 1982.

[7] C.W. Chiou, C.C. Chang, C.Y. Lee, and T.W. Hou, "Concurrent Error Detection and Correction in Gaussian Normal Basis Multiplier over GF(2^m)," IEEE Trans. computers, vol. 58, no. 6, pp. 851-857, June. 2009.

[8] N. Weste and K. Eshraghian, "Principles of CMOS *VLSI* Design : A system perspective," Addison-Wesley, 1985.

[9] C.W. Chiou, H.W. Chang, W.Y. Liang, C.Y. Lee, J.M. Linand Y.C. Yeh, "Low-Complexity Gaussian Normal Basis Multiplier over GF(2^m)," IET Information Security, vol. 6, Iss. 4, pp. 310-317, 2012.

[10] A.J. Menezes, I.F. Blake, X. Gao, R.C. Muliin, S.A. Vanstone, and T. Yaghoobian, "Applications of Finite Fields," Kluwer Academic Publishers, 1993.

〈저자소개〉

김 창 한 (Chang Han Kim) 종신회원
1985년 2월: 고려대학교 수학과 이학사
1987년 2월: 고려대학교 수학과 이학석사
1992년 2월: 고려대학교 수학과 이학박사
1992년 8월~현재: 세명대학교 정보통신학부 교수
〈관심분야〉 정수론, 공개키암호, 암호프로토콜

장 남 수 (Nam Su Chang) 종신회원
2002년 2월: 서울 시립대학교 수학과 이학사
2004년 8월: 고려대학교 정보보호대학원 공학석사
2010년 2월: 고려대학교 정보경영공학전문대학원 공학박사
2010년 7월~현재: 세종사이버대학교 정보보호학과 조교수
〈관심분야〉 암호칩 설계 기술, 부채널 공격, 공개키 암호 알고리즘, 공개키 암호 암호분석