Journal of The Korea Institute of Information Security & Cryptology(JKIISC) ISSN 1598-3986(Print)
VOL.23, NO.3, June 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.3.561

TBC에서 부채널공격을 고려한 효율적인 지수 연산*

박 영 호,† 장 남 수‡
세종사이버대학교

An efficient exponentiation method against side channel attacks in Torus-Based-Cryptosystem*

Young-Ho Park,† Nam Su Chang‡
Sejong Cyber University

요 약

본 논문은 Torus-Based-Cryptosystem 중 $T_2(p)$에서 부채널공격을 방지하는 효율적인 지수 연산방법을 제안한다. 제안한 지수 연산방법은 일반적인 지수 연산보다 더 효율적일 뿐만 아니라 제곱과 곱셈 연산의 계산량 차이를 없게하여 SPA 공격에 안전하다. 또한 상군(quotient group)의 특성을 이용하여 지수 연산시 메시지를 난수화하여 제1차 DPA 공격도 방어할 수 있다.

ABSTRACT

We propose an efficient exponentiation method which is resistant against some side channel attacks in $T_2(p)$, Torus-Based-Cryptosystem. It is more efficient than the general exponentiation method in $T_2(p)$ and is resistant against SPA by using that the difference of squaring and multiplication costs is negligible. Moreover, we can randomize a message in exponentiation step using the characteristic of quotient group which naturally protects against the first DPA.

Keywords: Torus-Based-Cryptosystem, Quotient Group, Side Channel Attack, SPA, DPA, Finite Field, Public Key Cryptosystem

I. 서 론

엘가말(ElGamal) 암호시스템[1]과 DSA[2]와 같이 유한체 곱셈군에서 이산대수문제를 이용한 많은 시스템들이 암호학적 응용으로 유용하게 제안되었다. 이들은 소수체(prime field)의 부분군을 사용하며, 이 시스템의 안전성은 큰 소수를 위수로 갖는 부분군에서의 이산대수문제는 유한체 전체 곱셈군의 이산대수문제만큼 어렵다는데 근거를 두고 있다[3]. 또한 소수체 대신에 확장체의 부분군을 사용하는 시스템들이 주목을 받고 있으며 LUC[4]와 XTR[9]이 공개키 암호법으로 소개되었다. 특히 2003년 Park외 2명[6]은 이차확창체의 상군에서의 이산대수문제를 고려한 암호시스템을 제안하였으며 이와 독립적으로 Rabin와 Silverberg[7]가 Torus based Cryptography(TBC)을 제안하였고 그 후 많은 연구가 진행되고 있다[8-13].

TBC는 공개키 파라메터의 크기를 줄여 통신량을 절약할 뿐만 아니라 효율적인 연산방법들이 가능하다. LUC와 XTR과 다르게 기존의 유한체의 부분군 이산대수 시스템에서의 스킴들을 사용할 수 있으며 따라서 기존의 ElGamal 암호시스템, DSA, DH 키교환 스

접수일(2013년 5월 22일), 게재확정일(2013년 5월 29일)
* 본 연구는 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업입니다. (No. 2010-0011511).
† 주저자, youngho@sjcu.ac.kr
‡ 교신저자, nschang@sjcu.ac.kr(Corresponding author)

킴들을 이용한 모든 프로토콜들에 큰 수정 없이 그대로 적용 가능하다. 또한 윈도우방법과 선계산방법을 사용하여 효율적인 지수 연산 뿐만 아니라 다승연산(multi-exponentiation)을 수행할 수 있는 장점도 있다.

한편 최근 스마트카드, RFID, NFC, 센서네트워크 등 스마트 기기들이 많이 사용되고 있으며 이러한 기기들에 대한 부채널공격(Side Channel Attack)[14]의 위협이 날로 증가하고 있다. XTR와 같은 sequence based 암호의 경우도 다양한 부채널 공격에 취약하다는 것이 발표되었다[15-17]. 따라서 Torus 기반의 암호(TBC)에서도 부채널공격을 막는 효율적인 연산의 연구가 필요한 실정이다.

본 논문에서는 상군의 특성을 이용하여 TBC 중 $T_2(p)$에서 부채널공격을 막는 효율적인 알고리즘을 제안한다. SPA(Simple Power Analysis)를 막는 근본적인 방법 중 하나인 제곱연산과 곱셉연산의 계산량의 차이를 없게(negligible) 만들어 일반적인 SPA 대응 방법인 Square-and-Multiplication-Always Method(SMAM)과 Dummy Operations Method(DOM)와 달리 추가적인 연산량이 들지 않는 SPA 대응 연산방법을 제안한다. 또한 상군의 특성상 지수 연산에서도 자연스럽게 메시지를 난수화 하므로 제 1차 DPA 공격에도 추가적인 연산량 없이 효율적으로 방어할 수 있음을 보인다.

논문의 구성은 다음과 같다. 2절에서 상군과 상군에서의 연산에 대해 설명하고 3절에서 SPA를 막는 효율적인 알고리즘을 소개하고 4절에서 결론을 맺는다.

II. 상군(Quotient Group)과 상군에서의 연산

2.1 상군(Quotient Group)

양의 정수 m와 소수 p에 대해 $l=p^m$라 놓자. F_l를 l 개의 원소를 갖는 유한체라 하고, $F_l(\omega)$를 F_l에서 이차 기약다항식의 근 ω로 확장한 유한체라 하자. 이때 $F_l(\omega)$는 F_l 위에서 차수 2인 벡터공간으로 $\{1,\omega\}$는 기저(basis)가 된다. 따라서 $F_l(\omega)$의 모든 원소는 다음과 같은 일차결합으로 표현된다:

$$\alpha = x + y\omega, \quad x,y \in F_l \ .$$

$F_l(\omega)^*$는 위수가 l^2-1인 곱셈군으로 부분군 F_l^*를 포함하며 $|F_l(\omega)^*/F_l^*| = l+1$이다. $F_l(\omega)^*$의 곱으로 유도된 연산을 갖는 F_l^*의 상군(quotient group)을 $G := F_l(\omega)^*/F_l^*$라 하자. 더 명확하게, $\alpha \in F_l(\omega)^*$를 포함하는 류(class)를 $[\alpha]$라 표시하자. 여기서, $[\alpha]=[\beta] \in G \Leftrightarrow \alpha\beta^{-1} \in F_l^*$ 임을 알 수 있다. 그리고 G에서 연산을 $[\alpha][\beta]=[\alpha\beta]$로 정의한다. 자세한 내용은 [6]을 참조 바란다.

정리 1.

(1) G는 $F_l(\omega)^*$의 곱으로 유도된 연산을 갖는 위수가 $l+1$인 순환군이다.

(2) 만일 $\alpha \in F_l(\omega)^*$ 이고 $\alpha \notin F_l$ 이면 유일한 원소 $g \in F_l$가 존재하여 $[\alpha]=[g+\omega]$ 이다.

위 정리 1로부터 일대일 대응함수 $\phi : G \setminus [1] \rightarrow F_l$를 정의할 수 있다.

$$\phi([a_0 + a_1\omega]) = a_0 a_1^{-1}.$$

또한 $\phi([1]) = id$ 로 정의하면 함수 ϕ는 G의 모든 원소로 확장된다. 따라서 함수 ϕ는 상군의 모든 원소를 $F_l \bigcup id$ 로 표현할 수 있다.

2.2 소수체의 이차확장체에서의 연산

상군 $G = F_l(\omega)^*/F_l^*$에서의 이산대수문제를 기반한 암호는 정확히 TBC 중 $T_2(l)$에 해당된다. $T_2(l)$를 사용한 다양한 암호시스템들은 모두 $F_l(\omega)^*$에 있는 임의의 원소 α와 임의의 양의정수 n에 대한 지수연산 $[\alpha]^n$을 사용하며 이 연산이 암호시스템의 성능을 좌우하는 가장 중요한 부분이다. 상군의 특성상 $[\alpha]^n = [\alpha^n]$이기 때문에, 상군 G에 있는 원소의 지수연산은 $F_l(\omega)$에 있는 원소의 지수 연산으로 쉽게 변형하여 계산할 수 있다.

본 논문에서는 편의를 위해 $l=p$ 이고 소수 $p \equiv 2 \pmod 3$인 $T_2(p)$의 경우만을 다룬다. 만일 $F_p(\omega)$의 원소를 표현하기 위해 F_p위의 이차 기약다항식 X^2+X+1과 다항식기저(polynomial basis)를 사용하면 다음과 같은 보조정리를 얻을 수 있다([18,19] 참조). 본 논문에서 연산량을 측정하기 위해 [18]에서 사용한 것처럼 F_p에서의 연산 기호 M,S,D를 사용하는데 M과 S는 모듈러 감산을 사용하지 않는 두 개의 정수의 곱셈과 제곱을 각각 의미하며, D는 모듈러 감산 연산을 의미한다. F_p에서의 곱

셈연산은 M+D 연산으로 계산된다. 따라서 일반적인 지수 연산의 계산모델을 사용하여 F_p에서의 덧셈과 뺄셈 연산은 무시하며 지수 연산의 계산량 측정단위로 M=D=0.5 와 S=0.3 을 사용한다[18].

보조정리 1. 소수 $p \equiv 2 \pmod 3$인 $F_p(\omega)$의 원소 α, β는 다음을 만족한다.

(1) α^p 계산량은 거의 없다.
(2) α^2 계산량은 2M+2D 이다.
(3) $\alpha\beta$ 계산량은 3M+2D 이다.

또한 $[\alpha] \in G$에서 $[\alpha]^{p+1} = id$ 이므로 $[\alpha]^{-1} = [\alpha]^p = [\alpha^p]$이며 역원 $[\alpha]^{-1}$은 보조정리 1에 의해 계산량이 들지 않으므로 signed binary 방법을 사용하여 지수 연산을 효율적으로 계산할 수 있다.

보조정리 2. 소수 $p \equiv 2 \pmod 3$이고 $[\alpha] \in G$, $\alpha = x + y\omega$, $\phi[\alpha] = g \in F_p$이면

(1) $[x+y\omega]^{-1} = [(x-y) - y\omega]$.
(2) $\phi([\alpha]^{-1}) = 1 - g \in F_p$.

증명.

(1) $(x+y\omega)((x-y)-y\omega) = x^2 - xy + y^2 \in F_p$
(2) $\phi([\alpha]^{-1}) = \phi([(x-y)-y\omega])$
$= \phi([-y((-xy^{-1}+1)+\omega)])$
$= \phi([(-xy^{-1}+1)+\omega]) = -xy^{-1}+1$
$= 1 - \phi[\alpha] = 1 - g$. □

상군 $G = F_p(\omega)^*/F_p^*$에서 k비트를 갖는 지수 n에 대하여 $[\alpha]^n$ 의 효율적인 연산을 위해 signed binary 방법과 NAF window 방법을 사용할 수 있다([11] 참조). 일반적인 left-to-right binary method 의 running time은 $k/2$ 곱셈과 k의 제곱연산이 소요된다. 반면 윈도우 사이즈 w의 NAF의 running time은 선계산량이 $2^{w-2}-1$ 곱셈과 한 번의 제곱연산 그리고 $\frac{k}{w+1}$ 곱셈과 k의 제곱연산이 소요된다. 따라서 보조정리 1과 2에 의해서 다음과 같은 정리를 얻는다.

정리 2. 소수 $p \equiv 2 \pmod 3$, $[\alpha] \in G$ 이면 $\lceil \log_2 n \rceil = k$ 인 양의 정수 n에 대하여 $[\alpha]^n$ 은

(1) Left-to-right binary method에 의해 $((7/2)M+3D)k$ 연산량이 필요하며 F_p에서의 평균 $3.25k$ 곱셈으로 계산된다.
(2) 윈도우 사이즈 w의 NAF에 의해
$(3 \cdot 2^{w-2}-1)M + 2^{w-1}D$
$+ k((\frac{3}{w+1}+2)M + (\frac{2}{w+1}+2)D)$
연산량이 필요하며 F_p에서의 평균
$(5 \cdot 2^{w-3} - \frac{1}{2}) + k((\frac{5}{2(w+1)}+2))$
곱셈으로 계산된다.

정리 2는 $T_2(p)$에서의 지수 연산이 같은 보안강도를 갖는 소수체에서의 원래 지수 연산보다 효율적인 것을 나타낸다. 소수 p가 512비트인 경우 1024비트의 소수체에서의 지수 연산보다 $G = F_p(\omega)^*/F_p^*$에서의 지수 연산이 대략 40%의 속도가 향상됨을 알 수 있다[6].

III. 부채널 공격을 막는 효율적인 알고리즘

부채널공격 중 SPA(Simple Power Analysis)를 막는 대표적인 방법으로 지수의 비트 값에 상관없이 항상 곱셈과 제곱연산을 수행하는 SMAM과 추가적인 계산을 수행하는 DOM이 주로 사용된다. 하지만 이들 방법은 추가적인 계산량의 증가를 가져온다. 본 논문에서는 SPA를 막는 근본적인 방법 중 하나인 제곱연산과 곱셈연산의 계산량의 차이를 없게 만들어 (negligible) 추가적인 연산량이 들지 않는 연산방법을 제안한다. 만일 소수 $p \equiv 2 \pmod 3$이며 $[\alpha] \in G$, $\alpha = x + yw$ 일 때 $[\alpha] = [g+w], g = \phi[\alpha] = xy^{-1}$라 하자. 제안된 방법의 주 아이디어는 연산 시 반복적으로 곱셈에 사용되는 $\alpha = x + yw$ 대신 같은 값을 갖는 $g+w$를 사용하여 곱셈 연산량을 감소시키는 것이다. 따라서 binary NAF 방법을 사용하여 다음과 같은 지수 연산 알고리즘을 제안한다.

[알고리즘 1]에서 $A \cdot (g+w)$와 $A \cdot (1-g+w)$의 연산량을 계산하면 다음과 같다. 임의의 $A = x + yw \in F_p(w)$에 대하여

$$(x+yw)(g+w) = (xg-y) + (x+yg-y)w$$
$$(x+yw)(1-g+w) = (x-xg-y) + (x-yg)w$$

이므로 각각 $2M+2D$의 연산으로 계산할 수 있다.

〔알고리즘 1〕 SPA를 막는 효율적인 지수 연산

Input : $[\alpha]=[g+w]$, 양의 정수 n
Output: $[\alpha]^n$

1. $NAF(n)=\sum_{i=0}^{k-1} d_i 2^i, d_i \in \{-1,0,1\}$를 계산한다.
2. $A \leftarrow 1$
3. For i from $k-1$ downto 0 do
   3.1 $A \leftarrow A^2$
   3.2 If $d_i = 1$ then $A \leftarrow A \cdot (g+w)$
   3.3 If $d_i = -1$ then $A \leftarrow A \cdot (1-g+w)$
4. Return : $[A]$

그러므로 〔알고리즘 1〕의 3.1 단계의 제곱연산과 3.2와 3.3 단계의 연산 모두 $2M+2D$으로 동일한 연산량으로 계산되며 두 연산량의 차이는 없게 된다. 따라서 위 제안된 알고리즘은 추가연산 없이 SPA 공격을 막는 효율적인 알고리즘일 뿐만 아니라 $F_p(\omega)$의 일반적인 지수 연산을 사용하는 것보다 더 효율적임을 알 수 있다. 또한 위 제안된 알고리즘은 선계산을 이용한 윈도우 사이즈 w의 NAF 알고리즘으로 쉽게 변형할 수 있다. 〔표 1〕은 기존 알고리즘과 제안 알고리즘의 지수 연산에 대한 연산량을 비교한 것이다.

〔표 1〕에서 SMAM 이나 DOM 는 지수의 비트 값에 상관없이 동일하게 곱셈과 제곱연산이 수행되어야 하므로 NAF 방법이 효율적이지 않으므로 binary 지수 연산 방법을 사용하는 것이 효율적이다. 일반적으로 w-NAF 알고리즘을 사용할 때 가장 효율적인 윈도우 사이즈는 $\lceil \log_2 n \rceil = k$의 크기에 따라 다르다. 제안된 알고리즘과 일반적인 w-NAF 알고리즘 모두 $k=160$, 224 또는 256 일 경우 $w=5$인 NAF 방법이 가장 효율적이다. 따라서 〔표 2〕에서는 $w=5$인 NAF 방법을 사용하였을 때 기존의 알고리즘과 제안

〔표 1〕 지수 연산량 비교

	F_p에서의 평균 곱셈량	방법
일반적인 지수 연산 알고리즘	$(5 \cdot 2^{w-3}-(1/2))+k((5/(2(w+1))+2))$	w-NAF
SMAM (DOM)	4.5k	binary SMAM
제안된 알고리즘	$2^{w-1}+k(\frac{2}{(w+1)}+2)$	w-NAF

〔표 2〕 $w=5$인 NAF 방법을 사용한 지수 연산량 비교

	F_p에서의 평균 곱셈량	방법
일반적인 지수 연산 알고리즘	$2.4k+19.5$	5-NAF
SMAM (DOM)	4.5k	binary SMAM
제안된 알고리즘	$2.3k+16$	5-NAF

된 알고리즘의 효율성을 비교한 것이다.

또한 상군 G의 원소 $[\alpha],[\beta] \in G$에 대하여 $[\alpha]=[\beta] \Leftrightarrow \alpha\beta^{-1} \in F_p^*$ 이므로 임의의 0이 아닌 난수 $r \in F_p$에 대하여 $[\alpha]=[r\alpha]$을 만족하므로 $[\alpha]^n$의 계산을 $[r\alpha]^n$으로 바꾸어 계산할 수 있다. 따라서 주어진 메시지가 〔α〕라 할 때 $[\alpha]^n=[r\alpha]^n$ 으로 〔α〕를 〔$r\alpha$〕로 랜덤화하여 계산할 수 있으므로 제1차 DPA(Differential Power Analysis)를 쉽게 막을 수 있다. 물론 이때는 〔알고리즘 1〕을 사용할 수 없으며 $F_p(\omega)$의 일반적인 지수 연산 알고리즘을 사용하게 된다.

IV. 결론

본 논문에서는 TBC 중에 가장 기본적인 이차확장체에서의 상군 $T_2(p)$에 대한 연산방법과 부채널공격에 안전한 효율적인 알고리즘을 제안하였다. 제안된 알고리즘은 SPA 공격을 막을 뿐만 아니라 지수 연산도 더 효율적으로 수행할 수 있다는 장점이 있다. 또한 상군의 특성상 지수 연산에서도 자연스럽게 메시지를 난수화할 수 있으므로 제 1차 DPA 공격에도 추가적인 연산량 없이 효율적으로 방어할 수 있음을 알았다. 본 연구에서 제안된 방법은 모든 TBC에 자연스럽게 확장할 수 있을 것으로 예상되며 따라서 TBC은 키 크기의 감소뿐 만 아니라 부채널공격을 고려한 연산의 효율성에서도 다른 암호에 비해 장점을 갖고 있음을 알 수 있다.

참고문헌

〔1〕 T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. on Information Theory, vol. 31, no 4, pp. 469-472, July 1985.

〔2〕 FIPS PUB 186-3, "Digital Signature

Standard (DSS)," Information Technology Laboratory, NIST. June 2009.
〔3〕 C.P. Schnorr, "Efficient signature generation by smart cards," Journal of Cryptology, vol. 4, no. 3, pp. 161-174, Feb. 1991.
〔4〕 P. Smith and C. Skinner, "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms," Adv. Crypto.- Asiacrypt'94, LNCS 917, pp. 355-364. Nov. 1994.
〔5〕 A.K. Lenstra and E.R. Verheul, "The XTR public key system," Adv. Cryptol.-CRYPTO 2000, LNCS 1880, pp. 1-19, Aug. 2000.
〔6〕 박영호, 오상호, 주학수, "공개 파라메터 키 크기를 줄인 새로운 이산대수문제," 한국정보보호학회논문지, 13(2), pp. 91-98, 2003년 4월.
〔7〕 K. Rubin and A. Silverberg, "Torus-based cryptography," Adv. Crypto.-CRYPTO, LNCS 2729, pp. 349 - 365, Aug. 2003.
〔8〕 M. van Dijk and D. Woodruff, "Asymptotically optimal communication for torus-based cryptography," Adv. Cryptol.-CRYPTO, LNCS 3152, pp. 151 - 178, Aug. 2004.
〔9〕 M. van Dijk, R. Granger, D. Page, K. Rubin, A. Silverberg, M. Stam, and D. Woodruff, "Practical cryptography in high dimensional tori," Adv. Crypto.-EUROCRYPT, LNCS 3494, pp. 234 - 250, May 2005.
〔10〕 K. Rubin and A. Silverberg, "Compression in finite fields and torus based cryptography," SIAM J. Comput., vol. 37, no 5. pp. 1401 - 1428, Jan. 2008.
〔11〕 D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. New York: Springer-Verlag, 2004.
〔12〕 R. Granger, D. Page, and M. Stam, "On small characteristic algebraic tori in pairing-based cryptography," LMS J. Comput. Math., vol. 9, pp.64 - 85, March 2006.
〔13〕 K. Karabina, "Torus-Based Compress ion by Factor 4 and 6," Trans. on Information Theory, vol 58, no 5, pp. 3293-3304, May 2012.
〔14〕 P Kocher, J Jaffe and B Jun, "Differential Power Analysis," Adv. Cryptol.-CRYPTO, LNCS 1109, pp. 388 - 397, Aug. 1999.
〔15〕 J. Chung and A. Hasan, "Security Analysis of XTR Exponentiation Algorithms against Simple Power Analysis Attack," Preprint of CACR, Univ. of Waterloo, CACR 2004-05.
〔16〕 D. Page and M. Stam, "On XTR and Side-Channel Analysis," Selected Areas in Cryptography (SAC 2004), LNCS 3357, pp. 54-68, Aug. 2004.
〔17〕 D.-G. Han, T. Izu, J. Lim, and K. Sakurai, "Side Channel Cryptanalysis on XTR Public Key Cryptosystem," IEICE Trans. Fund. S. S. on Disc. Math. and Its Applications, vol. E88-A, no. 5, pp.1214-1223, May 2005.
〔18〕 M. Stam and A. K. Lenstra, "Efficient Subgroup Exponentiation in Quadratic and Sixth Degree Extensions," CHES 2002, LNCS 2523, pp. 318-332. Aug. 2002.
〔19〕 A.K. Lenstra and E.R. Verheul, "The XTR public key system," Advances in Cryptology - CRYPTO 2000, LNCS 1880, pp. 1-19, Aug. 2000.

〈저 자 소 개〉

박 영 호 (Young-Ho Park) 종신회원
1990년 2월: 고려대학교 수학과 이학사
1993년 2월: 고려대학교 수학과 이학석사
1997년 2월: 고려대학교 수학과 이학박사
2002년 3월 ~ 현재: 세종 사이버 대학교 부교수
〈관심분야〉 정수론, 공개키 암호, 암호 프로토콜, 부채널 공격

장 남 수 (Nam Su Chang) 종신회원
2002년 2월: 서울 시립대학교 수학과 이학사
2004년 8월: 고려대학교 정보보호 대학원 공학석사
2010년 2월: 고려대학교 정보경영공학전문대학원 공학박사
2010년 3월~2010년 6월 : 고려대학교 정보보호연구원 연구교수
2010년 7월 ~ 현재: 세종사이버대학교 조교수
〈관심분야〉 암호칩 설계 기술, 부채널 공격, 공개키 암호 알고리즘, 공개키 암호 암호분석