타원곡선 암호시스템에서 랜덤 분할 상수배를 이용한 전력 공격의 대응방법

김창균*, 이경근*, 하재철**, 문상재*

*경북대학교 전자전기공학부

**나사렛대학교 정보과학부

Power Attacks Resistant Countermeasure using Random Separation of Scalar Multiplication Method for ECC

ChangKyun Kim*, KyungKeun Lee*, JaeCheol Ha**, SangJae Moon*

*School of Electronics and Electrical Eng., Kyungpook National Univ.

**Division of Information Sicence, Korea Nazarene Univ.

요 약

본 논문에서는 전력 공격에 대응하는 효과적인 타원곡선 상수배 알고리즘을 제안하고 기존의 여러 대응방법과 비교해 몇가지 장점을 제시하였다. 타원곡선 암호시스템에 대한 전력 공격의 대응방법으로 스칼라 정수의 랜덤 분할을 이용한 다중 상수배 알고리즘을 사용하였으며 이 방법의 계산량은 기존의 대응방법과 비교해 적은 연산량을 가지고 있다. 윈도우 크기가 4인 제안된 대응방법은 기존의 대응방법들과 비교해 약 46.6% ~ 83.6%가 향상되었다.

I. 서론

부채널 공격(side-channel attack)은 암호시스템을 공격함에 있어 새롭게 분류되는 공격의 하나로 매우 효과적인 공격방법이다. 스마트카드와 같은 암호시스템이 비밀키에 대한 연산을 수행할 때 부채널 정보를 측정함으로써 공격자는 몇 가지 비밀 정보를 알아낼 수 있다. 이러한 부채널 공격은 시간 공격(timing attack) [1], 전력 공격(power attack) [2,3], 오류주입 공격(fault insertion attack) [4] 그리고 전자기 누출 공격(electromagnetic emission attack) [5] 등으로 나눌 수 있으며 그 중 전력 공격은 가장 강력한 부채널 공격의 하나로 이를 대응하기 위해 여러 가지 방법들이 많이 소개되고 있다.

공개키 암호시스템의 하나인 타원곡선 암호시스템(ECC)에 많은 대응방법들이 제안되었는데 Liardet과 Smart [6] 그리고 Joy와 Quisquater [7]는 하나의 형태로 타원곡선 점의 덧셈 연산과 두배 연산을 같이 수행할 수 있는 특별한 형태의 타원곡선을 각각 제안하였다. 이 외에도 Okeya와 Sakurai [8]가 Montgomery 형태의 타원곡선을 이용하여 부채널 공격을 방어하는 방법을 제안하였다. 하지만, 이들 방법은 특별한 형태의 타원곡선을 사용하므로 NIST [9] 및 SECG [10]와 같은 표준에서 추천하는 곡선에 사용할 수 없는 단점을 가지고 있다.

[11] 에서는 대수적인 접근에 의해 타원곡선의 동형사상(isomorphism)을 이용하여 DPA (differential power analysis) 공격을 효과적으로 방어하는 방법을 제안하였으며 Coron [12]은 아주 간단한 방법으로 SPA(simple power analysis)을 방어하였다. 이 두가지 방법이 합쳐진 형태가 전력 공격을 대응하는 가장 빠른 방법으로 나와 있지만 여전히 부가적인 연산이 많은 문제점이 남아있다.

본 논문에서는 전력 공격에 대응하는 기존의 대응방법을 연산측면에서 분석하고 이보다 효과적인 타원곡선 상수배 알고리즘을 제안한다. 연산량 비교에 있어서 제안된 방법이 기존에 알려진 가장 빠른 방법들에 비해 약 46.6% ~ 83.6%가 향상됨을 보인다.

II. 타원곡선 암호스시템 및 전력 공격

1. 타원곡선 암호시스템

$p > 3$인 소수에 대해서 유한체 GF(p)에서 정의된 non-supersingular 타원곡선 E(GF(p))는 식

(1)을 만족하는 점 (x,y)와 무한원점 O의 집합으로 정의 될 수 있다.

$$y^2 = x^3 + ax + b \quad (a, b \in GF(p),\ 4a^2 + 27b^3 \neq 0) \quad (3607)$$

Affine 좌표계에서 점 $P=(x_1, y_1)$, $Q=(x_2, y_2)$에 대해 $P+Q=(x_3, y_3)$를 계산하는 연산식은 다음과 같다.

◆ 덧셈 연산 ($P \neq \pm Q$)

◆ $x_3 = \lambda^2 - x_1 - x_2$

S $y_3 = \lambda(x_1 - x_3) - y_1$ M

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

I+M

두배 연산 ($P = Q$)

$x_3 = \lambda^2 - 2x_1$

S $y_3 = \lambda(x_1 - x_3) - y_1$

M $\lambda = \frac{3x_1^2 + a}{2y_1}$

I+M+S

여기서, M은 체 곱셈, S는 체 제곱 그리고 I는 체 역원을 말한다. 좌표계에 대해서는 Affine 좌표계, Projective 좌표계, Jacobian 좌표계, Chudnobsky Jacobian 좌표계 그리고 변형된 Jacobian 좌표계를 각각 A, P, J, J^C, J^m로 나타낸다. 표 2는 각 좌표계에 대한 타원곡선 점의 덧셈 및 두배 연산의 연산량을 나타낸 것이다.

표 1. 덧셈 연산 및 두배 연산에 대한 연산량

	두배 연산		덧셈 연산	
	$a \neq -3$	$a = -3$	$Z_1 \neq 1$	$Z_1 = 1$
A	1I+2M+2S		1I+2M+S	
P	7M+5S	7M+3S	12M+2S	9M+2S
J	4M+6S	4M+4S	12M+4S	8M+3S
J^C	5M+6S	5M+5S	11M+3S	8M+3S
J^m	4M+4S	-	13M+6S	9M+5S

2. 타원곡선 암호시스템

P. Kocher는 SPA와 이보다 더욱 강력한 공격방법인 DPA 공격을 소개하였다 [2,3]. SPA는 단순히 소비 전력을 관측하여 공격하는 방법이고 DPA 공격은 SPA와 함께 통계적인 분석(statistical analysis)과 에러 정정(error correction) 기술을 함께 사용한 공격방법이다.

Coron은 타원곡선 암호시스템에 그림 1과 같이 이전 멱승 알고리즘을 변형하여 간단한 SPA 대응방법(SSPA: simple SPA counteremeasure)을 제시하였다 [12]. 그림 1은 각 비트마다 항상 덧셈 연산과 두배 연산을 계산하도록 하였으나 이는 상당한 연산량의 증가를 가져오며 여전히 DPA 공격에는 대응할 수 없다.

INPUT : point P and integer d
OUTPUT : $Q = dP$

1. $Q \leftarrow P$
2. for i from $l-2$ to 0 do
2.1 $Q[0] \leftarrow 2Q[0]$
2.2 $Q[1] \leftarrow Q[0] + P$
2.3 $Q[0] \leftarrow Q[d_i]$
3. output Q

그림 1. SPA에 대응하는 두배-덧셈 알고리즘

비록 SPA에 대응한 방법이더라도 항상 DPA 공격을 방어하지는 못한다. DPA 공격을 방어하기 위해서는 몇 개의 매개 변수 혹은 계산 과정을 랜덤하게 함으로서 방어가 가능하다. Coron은 DPA 공격에 대한 대응방법으로 3가지를 제안하였는데 그중 세 번째 방법의 기본 개념은 랜덤한 사영좌표를 사용한다는 것이다. 즉, 난수 r에 대해서 점 $P=(X, Y, Z)$가 (rX, rY, r)과 같음을 이용한 것이다. Joy-Tymen은 Coron의 세 번째 방법을 향상시킨 random morphism을 이용한 DPA 공격 대응 방법을 제안하였다 [11]. 그 외에도 특별한 형태의 타원곡선을 이용한 전력 공격의 대응 방법이 제안되었지만 표준 형태의 타원곡선에 적용을 못하는 단점이 있다. 제안하는 방법은 표준 형태뿐만 아니라 특별한 형태에도 사용이 가능하며 기존의 전력 공격에 대한 대응방법에 비해 효과적인 연산량을 가지고 있다.

Ⅲ. 제안된 전력 공격 대응방법

이 장에서는 제안된 대응방법에 대해 알아 볼 것이다. 상수배 과정을 랜덤화 하기 위해서 멱지수의 랜덤 분할을 이용할 것이며 랜덤 분할된 멱지수를 수정된 다중 상수배 알고리즘에 적용하여 전력 공격에 대응하는 방법을 소개한다.

1. 스칼라 정수의 랜덤 분할 방법

타원곡선 암호시스템에서 DPA 공격을 방어하기 위해서 일반적으로 상수배 과정을 랜덤화 한다. 제안된 대응방법에서는 랜덤화 과정의 방법으로 스칼라 정수의 랜덤 분할을 이용하였다.

점 P와 $Q=kP$가 타원곡선의 점이라 하고, 이때 k는 정수이다. 제안된 방법은 일반적인 상수배 형태인 $Q=kP$와는 달리 k를 k_1과 k_2로 랜덤하게 분리하여 $Q=k_1P+k_2P$의 형태로 계산한다.

INPUT : 정수 k OUTPUT : k_1, k_2
1. k보다 작은 난수 k_1을 선택 2. $k_2=k-k_1$ 를 계산 3 만약 $k=k_1+k_2$이면 (k_1, k_2)출력 후 마침. 4 단계 (1)로 간다.

그림 2. 스칼라 정수의 랜덤 분할 방법

그림 2에서 분할된 스칼라 정수 k_1과 k_2는 랜덤한 비트열로 간주할 수 있으므로 각각의 Hamming weight는 총 비트 길이의 약 50%가 된다.

2. 제안된 타원곡선 상수배 알고리즘

제안된 상수배 알고리즘은 동시 다중 상수배 방법(simultaneous multi-scalar multiplication method)[13]을 수정한 것에 스칼라 정수의 랜덤 분할을 이용한 것으로 SPA와 DPA 공격을 동시에 방어하는 방법이다. 그림 3은 비트값에 상관없이 항상 같은 계산 과정을 반복하기 때문에 SPA에 방어할 수 있으며, 스칼라 정수의 랜덤 분할로 인하여 계산되는 중간 값이 항상 랜덤하게 변하므로 DPA 공격을 방어할 수 있다.

INPUT : 윈도우 크기 w, $k=(k_{t-1},\ldots,k_1,k_0)_2, P$ OUTPUT : kP
Precomputation Stage 1. $i\in[0,2^w-1]$ 대해서 iP 계산. **Evaluation Stage** 2. 그림 2를 이용하여 $k_1=(k_1^{d-1},\ldots,k_1^1,k_1^0)$, $k_2=(k_2^{d-1},\ldots,k_2^1,k_2^0)$ 계산. 여기서 k_1^i, k_2^i는 길이 w인 비트열, $d=\lceil t/w \rceil$. 3 R=0. 4 $d-1$부터 0까지 i를 -1씩 감소하면서 수행. 4.1 $R=2^wR$. 4.2 $R=R+(k_1^iP)+(k_2^iP)$. 5 출력 R.

그림 3. 전력 공격에 대응하는 상수배 알고리즘

그림 3에서 사전계산 단계 1에서는 무한원점 O과 점 P를 알고 있으므로 2^w-2번의 덧셈 연산이 필요하며 2^w-1개의 점을 저장할 메모리가 필요하다. 주요계산 단계에 들어서면 그림 2를 이용하여 k를 랜덤 분할하고 단계 4를 거친다. 주요계산 단계에서 필요한 계산량은 $(2d-3)$번의 덧셈 연산과 $(d-1)w$번의 두배 연산이 필요하다.

Ⅳ. 연산량 비교

이 장에서는 제안된 상수배 알고리즘의 연산량을 분석하고 기존의 대응방법과 비교할 때 향상된 정도를 따져 볼 것이다.

1. 연산량

A와 D를 각각 타원곡선 점의 덧셈 연산과 두배 연산으로 나타낼 때 제안된 상수배 방법의 총 연산량은 $(2d-3)A+(d-1)wD$가 된다.

표 2는 160 비트 타원곡선 상수배 연산에 대해서 연산 량을 나타낸 것이다. 총 연산량을 체 곱셈(M)으로 표현하기 위해 체 역원(I)과 체 제곱(S)을 각각 I=30M, S=0.8M로 이림잡았다 [14]. 여기서 좌표계는 Jacobian 좌표계를 사용한다고 가정한다. k가 160 비트인 경우, 제안된 상수배 알고리즘의 연산량은 표 2와 같다.

표 2. 제안된 방법의 연산량 (k=160 bits)

w	General	$a=-3$, $Z_1=1$
2	2582M+1594S+I	1926M+1117S+I (2849.6M)
3	2214M+1564S+I	1714M+1085S+I (2612.0M)
4	1748M+1310S+I	1374M+905S+I (2128.0M)
5	1742M+1304S+I	1370M+901S+I (2120.8M)

2. 연산에 대한 효율성 비교

현재까지 전력 공격 대응방법으로 가장 빠른 상수배 방법은 Coron의 SSPA와 Joye-Tymen의 방법을 합친 방법(SSPA/Joye-Tymen)이다 [15].

표 2. 제안된 방법의 연산량 (k=160 bits)
방법 1 : L-R 이진 멱승 방법
방법 2 : Sliding window (w=4)
방법 3 : SSPA/Coron's 3rd
방법 4 : SSPA/Joye-Tymen
방법 5 : 제안된 방법 (w=4)
부가연산 : 방법 1에 대한 각 방법의 연산 비율

방법	Immunity	연 산 량	비 고
1	NO	1282M+878S+I (2014.4M)	100%
2	SPA	951M+754S+I (1584.2M)	78.6%
3	SPA/DPA	2550M+1574S+I (3839.2M)	190.6%
4	SPA/DPA	1916M+1434S+I (3093.2M)	153.6%
5	SPA/DPA	1402M+905S+I (2156.0M)	107.0%

표 2는 전력 공격에 대응하지 않은 순수한 L-R 이진 멱승방법, 윈도우 크기가 4인 Sliding widnow 방법, 그리고 제안된 상수배 알고리즘을 포함하여 대표적인 기존의 대응방법들의 연산량을 분석한 것이다.

제안된 상수배 방법은 윈도우 크기가 4일 때 SSPA/Joye-Tymen의 연산량에 비해 약 46.6%가 향상되었으며 순수한 L-R 이진 멱승 방법에 비해서 약 7.0%의 부가적인 연산만으로 전력 공격을 대응할 수 있었다.

Ⅳ. 결론

기존에 제안된 전력 공격의 대응방법은 많은 부가 연산이 필요하였다. 본 논문에서는 타원곡선 암호시스템에서 전력 공격에 대응하는 효과적인 상수배 알고리즘을 제안하였다. 기존에 제안된 방법과 비교했을 때 제안된 방법이 가장 빠르며 윈도우 크기 4를 가지는 제안된 방법은 기존에 알려진 가장 빠른 상수배 방법(SSPA/Joye-Tymen)에 비해 약 46.6%가 향상되었다.

참고문헌

[1] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", *Advances in Cryptology-CRYPTO'96*, LNCS 1109, pp.104-113, Springer-Verlag, 1996.

[2] P. Kocher, J. Jaffe and B. Jun, "Introduction to Differential Power Analysis and Related Attacks", Available at http://www.cryptography.com/dpa/technical/index.html/

[3] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis", *Advances in Cryptology - CRYPTO'99*, LNCS 1666, pp.388-397, Springer-Verlag, 1999.

[4] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems", *Advances in Cryptology-CRYPTO'97*, LNCS 1294, pp.513-525, Springer-Verlag, 1997.

[5] J. R. Rao and P. Rohatgi, "EMpowering Side-Channel Attacks", Available at http://eprint.iacr.org/complete/

[6] P. Liardet and N. Smart, "Preventing SPA/DPA in ECC systems using the Jacobi form", *CHES2001*, LNCS 2162, pp.391-401, Springer-Verlag, 2001.

[7] M. Joye and J. Quisquater, "Hessian elliptic curves and side-channel attacks", *CHES2001*, LNCS 2162, pp.402-410, Springer-Verlag, 2001.

[8] K. Okeya and K. Sakurai, "Power analysis breaks elliptic curve cryptosystems even secure agaisnt the timing attack", *Advances in Cryptology-INDOCRYPT'00*, LNCS 1977, pp.178-190, Springer-Verlag, 2000.

[9] National Institute of Standards and Technology, *Digital Signature Standard*, FIPS 186-2, February 2000.

[10] SECG SECG2: *Recommended Elliptic Curve Cryptography Domain Parameters*, v1.0, Sep. 20, 2000.

[11] M. Joye and C. Tymen, "Protections against Differential Analysis for Elliptic Curve Cryptography", *CHES2001*, LNCS 2162, pp.377-390, Springer-Verlag, 2001.

[12] J. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems", *CHES'99*, LNCS 1717, pp.292-302, Springer-Verlag, 1999.

[13] M. Brown, D. Hankerson, J. Lopez and A. Menezes, "Software Implementation of the NIST Elliptic Curves Over Prime Fields", Proc. of *CT-RSA'2001*, LNCS 2020, pp.250-265, Springer-Verlag, 2001.

[14] K. Okeyam and K. Sakurai, "Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve", *CHES2001*, LNCS 2162, pp.126-141, Spriger-Verlag, 2001.

[15] T. Izu and T. Takagi, "A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks", *PKC2002*, LNCS 2274, pp.280-296, Springer-Verlag, 2002.