전력분석 공격에 대응하는 타원곡선 상의 결합 난수 스칼라 곱셈 알고리즘

정석원*
목포대학교 정보보호학과 교수

A Combined Random Scalar Multiplication Algorithm Resistant to Power Analysis on Elliptic Curves

Seok Won Jung*
Professor, Department of Information Security Engineering, Mokpo National University

요 약 타원곡선 암호 알고리즘은 RSA 공개키 알고리즘에 비해 짧은 키의 길이와 적은 통신 부하 때문에 IoT 환경에서 인증용으로 많이 사용되고 있다. 타원곡선 암호 알고리즘의 핵심연산인 스칼라 곱셈이 안전하게 구현되지 않으면, 공격자가 단순 전력분석이나 차분 전력분석을 사용하여 비밀 키를 찾을 수 있다. 본 논문에서는 스칼라 난수화와 타원곡선 점 가리기를 함께 적용하고, 연산의 효율성이 크게 떨어지지 않으며 전력분석 공격법에 대응하는 결합 난수 타원곡선 스칼라 알고리즘을 제안한다. 난수 r과 랜덤 타원곡선 점 R에 대해 변형된 Shamir의 두 배 사다리 알고리즘을 사용하여 타원곡선 스칼라 곱셈 $kP=u(P+R)+vR$을 계산한다. 여기에서 위수 $n=2^l\pm c$ 일 때, $2^lP=\mp cP$를 이용하여 $l+20$ 비트 정도의 $u\equiv rn+k\,(\mathrm{mod}n)$과 $v\equiv rn-k\,(\mathrm{mod}n)$를 구한다.

주제어 : 사물인터넷, 인증, 타원곡선, 스칼라 곱셈, 차분 전력분석, 키 난수화, 타원곡선 점 가리기

Abstract The elliptic curve crypto-algorithm is widely used in authentication for IoT environment, since it has small key size and low communication overhead compare to the RSA public key algorithm. If the scalar multiplication, a core operation of the elliptic curve crypto-algorithm, is not implemented securely, attackers can find the secret key to use simple power analysis or differential power analysis. In this paper, an elliptic curve scalar multiplication algorithm using a randomized scalar and an elliptic curve point blinding is suggested. It is resistant to power analysis but does not significantly reduce efficiency. Given a random r and an elliptic curve random point R, the elliptic scalar multiplication $kP=u(P+R)+vR$ is calculated by using the regular variant Shamir's double ladder algorithm, where $l+20$-bit $u\equiv rn+k\,(\mathrm{mod}n)$ and $v\equiv rn-k\,(\mathrm{mod}n)$ using $2^lP=\mp cP$ for the case of the order $n=2^l\pm c$.

Key Words : IoT, Authentication, Elliptic Curve, Scalar Multiplication, DPA, Randomized Key, Point Blinding

본 논문은 2016년도 목포대학교 해외 장기연수 지원으로 수행되었음.
*교신저자 : 정석원(jsw@mokpo.ac.kr)
접수일 2020년 4월 27일 수정일 2020년 5월 29일 심사완료일 2020년 6월 12일

1. 서론

타원곡선 암호 알고리즘은 RSA 암호 알고리즘과 비교하여 키의 길이가 짧아 키 분배, 전자서명 등에 사용되고 있다[1]. 또한, IoT(Internet of Things) 환경에 적합하여 홈 네트워크, 차세대 ITS(Intelligent Transport Systems) 등의 환경에서 정보보호 서비스를 제공하는데 널리 사용되고 있다[2-3].

타원곡선 암호 알고리즘은 유한체 위에 정의된 타원곡선 점을 여러 번 더하는 스칼라 곱셈을 핵심연산으로 가지고 있다. 그런데 연산의 효율성만을 강조한 스칼라 곱셈 구현은 적용 환경에 따라 전력분석과 전자파 분석 등의 부채널 공격법에 대해 취약점이 있음이 알려져 있다[4].

타원곡선 위의 점에 대한 스칼라 곱셈은 스칼라의 비트에 따라 두 배와 덧셈을 하는 Double-and-add 알고리즘, Addition-subtraction 알고리즘 등이 제안되었다. 그러나 이들은 단순 전력분석 공격법인 SPA (Simple Power Analysis)에 의해 스칼라가 노출되는 문제가 있다[4]. 이에 대한 대응책으로 두 배와 덧셈 연산에 같은 공식을 사용하는 방법, 두 배와 덧셈을 항상 사용하는 방법, Montgomery 사다리를 사용하는 방법, 덧셈만 사용하는 알고리즘 등이 제안되었다[4-6]. 그러나 이런 대응책도 Bauer 등의 HCCA(Horizontal Collision correlation Attack), Goubin의 RPA(Refined Power Analysis), Akishita 등의 ZPA(Zero-value Point Attack), Hanley 등의 상관 충돌(Correlation collision) 공격 등에 의해 취약점을 갖는다[7-10].

차분 전력분석 DPA(Differential Power Analysis)는 암호 장치에 여러 번의 입력을 주입하면서 소비전력을 측정하고, 중간 과정 값들의 연관성을 찾아 비밀 키 정보를 알아내는 공격법이다. 차분 전력분석 공격에 대응하는 방법으로 Coron의 스칼라 난수화, 타원곡선 점 숨기기와 사영좌표 사용, Clavier 등의 지수 분해(exponent splitting), Ciet 등의 난수 키 분해(random key splitting)와 두 배 연산 난수화, Smart의 잉여 모듈러 셈 방법 등이 제안되었다[4, 11-13]. 이런 대응책은 연산의 부하가 높거나 Doubling 공격, 2-Torsion 공격 등에 대해서 취약점을 보인다[14-15].

본 논문에서는 전력분석 공격법에 대응하기 위해 스칼라 난수 방법과 입력 타원곡선 점을 랜덤하게 만드는 두 가지 방법을 함께 사용하는 결합 난수 스칼라 곱셈 알고리즘을 제안한다. 그리고 연산의 효율성이 떨어지지 않게 타원곡선의 위수의 성질을 이용하여 난수화된 스칼라를 모듈러 감산하여 짧은 길이가 되도록 한다. 본 논문의 2장에서 타원곡선 스칼라 곱셈에 대한 전력분석 공격과 관련된 연구를 살펴본다. 3장에서 제안하는 결합 난수화 스칼라 곱셈 알고리즘을 설명하고 안전성을 분석한다. 4장에서 향후 연구 방향을 다룬다.

2. 관련 연구

정수 3보다 큰 소수 p에 대해 유한체 $\mathbb{F}_p$가 주어지고, 유한체 $\mathbb{F}_p$의 원소 a, b에 대해 타원곡선

$$E: y^2 = x^3 + ax + b$$

를 정의할 수 있다. 이때, 타원곡선 군을

$$E(\mathbb{F}_p) = \{(x, y) \mid y^2 = x^3 + ax + b\} \cup \{O\}$$

로 정의한다. 여기에서 O는 무한 원점으로 덧셈에 대한 항등원이다[16].

소수 유한체 $\mathbb{F}_p$ 위에 정의된 타원곡선 군 $E(\mathbb{F}_p)$의 점 P와 스칼라 k의 곱셈 kP는 스칼라 k를 이진수로 표현한 후 두 배와 덧셈을 반복하여 구할 수 있다[14]. 그러나 스칼라 비트의 값이 1일 때만 덧셈을 하도록 하여 연산의 효율성을 높이는 방법은 SPA에 의해 키가 노출되는 문제가 있다[4]. Coron은 SPA에 대응하는 방법으로 스칼라 비트의 값에 상관없이 항상 두 배와 덧셈 연산을 하는 Double-and-add resistant against SPA 알고리즘을 제안하였다. 그러나 Coron은 i-1번째 반복문에 사용된 결과와 i번째 반복문에 사용되는 값이 연관성이 있음을 보이고, Double-and-add 알고리즘이 차분 전력분석 DPA에 대해 안전하지 않음을 보였다. 그리고 DPA에 대응하는 방법으로 스칼라 난수화(randomized scalar), 입력 타원곡선 점 숨기기(blinding point), 랜덤한 사영좌표(randomized projective coordinates) 사용 방법을 제시하였다[4].

Coron의 스칼라 난수 방법은 타원곡선 군의 위수를 n이라 할 때, 타원곡선 위의 점 P는

$$nP = O$$

임을 사용한다. 이 사실을 사용하면 난수 r을 선택한 후 스칼라 곱셈이

$$kP = (rn + k)P$$

이므로, kP를 계산하는 대신 $(rn+k)P$를 계산하여 같은 스칼라 k와 P가 입력되어도 항상 다른 연산을 하게 하여 DPA를 막고자 했다. 그러나 이 방법은 $rn+k$가 스칼라 k비트보다 두 배 이상 커지기 때문에 스칼라 곱

셈의 연산이 두 배 이상 많아져 효율성이 많이 떨어지게 된다. Coron은 연산의 효율성을 위해 20-비트 길이 정도의 난수 r을 사용하도록 권고하였다[4]. 그런데 SECG (Standards for Efficient Cryptography Group)와 NIST(National Institute of Standards and Technology)에서 권고하는 표준 타원곡선 군의 위수 n이 l비트 길이로 $n = 2^l \pm c$ 꼴로 나타나는 경우가 많다. 이 경우 $rn+k$의 값이 스칼라 k의 일부를 난수로 만들지 못한다. 이러한 사실을 바탕으로 Feix 등은 소비전력에 대한 상관관계를 이용하여 스칼라 k를 찾는 데 성공하였다[17].

Ciet과 Joye는 난수 r에 대해 $S = rP$, $k_1 = k \bmod r$, $k_2 = \left\lfloor \frac{k}{r} \right\rfloor$ 로 놓고, 타원곡선 스칼라 곱셈을

$$kP = k_1 P + k_2 S$$

로 계산하는 방법을 제안하였다. 그리고 double and add 알고리즘과 연산량이 같은 Algorithm 1을 제안하였다[12].

Algorithm 1. Regular variant of Shamir's double ladder[12]

Inputs: Point P and S, $k = (k_{n-1}, \cdots, k_0)_2$, $d = (d_{n-1}, \cdots, d_0)_2$
Output: $Q = kP + dS$
1. $R_1 \leftarrow P; R_2 \leftarrow S; R_3 \leftarrow P + S;$
   $c \leftarrow 2d_{n-1} + k_{n-1}; R_0 \leftarrow R_c$
2. for i from $n-2$ to 0 do
   2.1 $R_0 \leftarrow 2R_0$
   2.2 $b \leftarrow \neg(k_i \vee d_i); c \leftarrow 2d_i + k_i; R_b \leftarrow R_b + R_c$
3. return R_0

그러나 Ciet과 Joye의 방법도 2-torsion 점을 이용하여 $S = rP$를 계산하는 과정에서 r을 찾은 후, k_1과 k_2를 찾는 방법이 알려졌다. 그리고 Algorithm 1의 중간에 계산되는 일부 값들이 서로 연관성을 갖게 되어 차분 전력분석에 취약함이 알려졌다[15, 18].

Coron의 입력 타원곡선 점을 숨기는 방법(blinding point)은 입력 타원곡선 점 P와 랜덤 타원곡선 점 R을 더한 값에 대해 스칼라 곱셈을

$$kP = k(P+R) - kR$$

로 계산하는 것이다. 이 방법은 공격자가 입력 타원곡선 점을 임의로 선택하지 못하도록 하여 RPA와 ZPA 같은 공격을 막는다. 그러나 Okeya 등이 $P, 2P, 4P, \ldots$점들을 암호 장치에 순차적으로 입력하고 소비전력을 측정한 후 이들의 연관성을 찾아 스칼라 k를 알아내는 데 성공하였다[19].

3. 제안 방법

2장에서 살펴보았듯이 20-비트 길이의 난수 r을 사용하는 Coron의 스칼라 난수 방법은 SECG와 NIST가 권고하는 타원곡선에 대해서 스칼라의 상당 부분이 난수화되지 않는다. 따라서 난수 r을 l비트 크기를 사용하여 스칼라 k의 모든 비트를 난수화 해야 한다. 그러나 이 경우 스칼라 곱셈 연산이 많아져서 효율성이 떨어진다. 그런데 위수 n이 $n = 2^l \pm c$ 꼴인 경우, $2^l P = \mp cP$라는 사실을 이용하여 l비트 이상의 난수 값을 적당히 모듈러 감산시켜

$$rn + k \equiv u \pmod{n}$$

을 얻을 수 있다. 여기에서 u는 $l+20$ 비트 정도가 되도록 한다. 그러면 난수 r이 스칼라 k의 모든 비트에 영향을 주게 되고, 난수 값 전체를 사용하여 $(rn+k)P$를 계산하는 대신에 uP를 계산하면 되므로 연산의 효율성을 가져올 수 있다[20].

제안하는 알고리즘은 스칼라 난수화와 타원곡선 점 숨기기를 동시에 적용하여 여러 가지 전력분석 공격에 대응하도록 한다. 이를 위해 먼저 난수 r과 랜덤 타원곡선 점 R을 생성한다. 랜덤 점 R로 타원곡선 점 P를 $P+R$로 가리고, 난수 스칼라 곱 $(rn+k)(P+R)$을 한 후, 랜덤 점 R의 계산량을 $(rn-k)R$로 상쇄한다. 즉,

$$kP = (rn+k)(P+R) + (rn-k)R$$

을 얻을 수 있다. 여기에서 $2^l P = \mp cP$ 인 성질을 사용하여 스칼라 $rn+k$와 $rn-k$를 $l+20$ 비트 정도가 되도록 반복적으로 모듈러 감산을 시행한다. 즉,

$$rn+k \equiv u \pmod{n},\ rn-k \equiv v \pmod{n}$$

으로 u와 v의 길이가 $l+20$ 비트 정도가 되도록 계산한다. 이때, $P+R = P'$라 하면

$$kP = uP' + vR$$

이 된다. 이에 대해서 Algorithm 1을 적용하여 스칼라 곱셈을 구한다.

이상에서 설명한 스칼라 난수화와 타원곡선 점 숨기기를 방법을 함께 적용한 결합 난수 스칼라 곱셈 알고리즘은 다음 Algorithm 2와 같이 정리할 수 있다.

Algorithm 2. combined random scalar multiplication

Inputs: Point P, $k=(k_{l-1}, \cdots, k_0)_2$, order n, reduction depth ϵ
Output: $Q=kP$
1. generate a random r and a point R
2. $P \leftarrow P+R$
3. $u \leftarrow rn+k \bmod n$; $v \leftarrow rn-k \bmod n$
4. $R_1 \leftarrow P$; $R_2 \leftarrow R$; $R_3 \leftarrow P+R$;
   $c \leftarrow 2v_{l+\epsilon-1}+u_{l+\epsilon-1}$; $R_0 \leftarrow R_c$
5. for i from $n+\epsilon-2$ to 0 do
   5.1 $R_0 \leftarrow 2R_0$
   5.2 $b \leftarrow \neg(u_i \vee v_i)$; $c \leftarrow 2v_i+u_i$; $R_b \leftarrow R_b+R_c$
6. return R_0

모듈러 감산의 정도는 ϵ으로 정의한다. 예를 들어 $\epsilon=l+20$ 이다. 제안하는 Algorithm 2의 단계 1에서는 스칼라를 난수화 하는 난수 r과 타원곡선 점을 가릴 때 사용하는 랜덤 타원곡선 점 R을 만든다.

단계 2에서 입력 타원곡선 점 P가 랜덤 타원곡선 점 R과 더해지므로 매번 알고리즘에서 연산 되는 값이 바뀐다. 따라서 공격자가 같은 타원곡선 점 P를 암호 장치에 입력하고, 점 P를 계산할 때 소비전력을 분석하여 스칼라를 찾는 차분 전력분석 공격은 가능하지 않다. 또한, 공격자가 특별한 타원곡선 점에 대해 연산 과정을 추정하고, 특별한 점을 입력한 후 전력분석을 측정하여 스칼라를 찾아내는 RPA와 ZPA 공격을 시행할 수 있다. 그러나 입력되는 특별한 점은 단계 2에서 랜덤한 타원곡선 점과 더해지며 특성이 없어지므로 특별한 점의 연산 과정 추정이 의미 없어지므로 차분 전력분석이 가능하지 않다.

단계 3에서는 입력된 모듈러 감산의 수준 ϵ에 따라 모듈러 감산을 수행한다. 즉, l비트 크기의 r을 이용하여 계산된 $2l$ 비트 크기의 스칼라 $rn+k$와 $rn-k$를 $l+\epsilon$ 크기로 감산한다. 이 과정에서 난수 r의 비트 값들이 스칼라 k의 모든 비트에 영향을 주고, 알고리즘이 실행될 때마다 k의 값을 바꾸는 효과를 보게 된다. 또한, u와 v가 $l+\epsilon$ 크기이므로 $2l$ 비트를 계산할 때보다 스칼라 곱셈의 계산량을 줄일 수 있다.

단계 5에서 각 스칼라 비트 값에 대해 항상 두 배와 덧셈을 수행하므로 단순 소비전력 분석에 대응함을 알 수 있다.

단계 3의 결과 u와 v는 알고리즘이 실행될 때마다 새로운 난수 r값에 의해 갱신된다. 그래서 단계 4의 R_0 값과 단계 5.2의 R_b 값이 랜덤한 타원곡선 점 R의 영향을 받는다. 공격자가 차례로 Algorithm 2의 입력값으로 P, $2P$, $4P$, $\cdots$, 2^iP, $\cdots$ 를 입력한 후 연산에 소비되는 모든 전력 파형을 수집하여 분석하는 공격을 고려해 볼 수 있다. 그런데 단계 2에서 랜덤 타원곡선 점이 더해지므로 Algorithm 2의 단계 5.1과 단계 5.2에서 계산되는 $2^{i-1}P$를 입력으로 한 스칼라 곱셈 중간 값과 2^iP를 입력으로 한 스칼라 곱셈 중간값 사이의 연관성을 찾을 수 없다. 따라서 알고리즘이 실행할 때마다 수집한 전력소비량 사이의 상관관계를 찾을 수 없어 차분 전력분석 공격이 가능하지 않다.

4. 결론

사물인터넷 환경의 구축 확대로 인해 사물들이 유·무선으로 연결되고 지능형으로 바뀌고 있다. 이러한 환경변화에 따라서 정보 침해와 유출도 증가하는 상황이다. 인증은 정보보호를 위한 핵심 요소 중 하나이고, 타원곡선 알고리즘은 인증을 제공하는 중요한 암호 프리미티브 중 하나이다. 그러나 타원곡선 알고리즘의 핵심연산인 스칼라 곱셈을 안전하게 구현하지 않으면 부채널 공격법에 따라 키가 노출될 수 있다. 본 논문에서는 스칼라 난수화와 타원곡선 점 가리기를 동시에 적용하여 전력분석 공격에 대응하는 결합 난수 스칼라 곱셈 알고리즘을 제안하였다. 향후 다른 알고리즘과의 연산 효율성 비교와 사영좌표를 사용한 환경에서 알고리즘 개선에 관한 연구가 필요하다.

REFERENCES

[1] Ministry of the Interior and Safety, *Guideline for introduction of government internet of things*, pp.19-22, 2019.

[2] S.Park, K.Han and K.Kim, "The Simplified V2V Communication Authentication Service for Privacy Protection", *Jour. of The Korea Internet of Things Society*, Vol.2, No.1, pp.35-40, 2016.

[3] T.Kim and S.Jung, "Test Vector Generator of timing simulation for 224-bit ECDSA hardware", *Jour. of The Korea Internet of Things Society*, Vol.1, No.1, pp.33-38, 2015.

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

[5] E.Brier and M.Joye, "Weirstrass elliptic curves and side-channel attacks", *PKC 2002*, LNCS 2274, pp.335-345, 2002.

[6] M.Joye, "Highly regular right-to-left algorithms for scalar multiplication", *CHES 2007*, LNCS 4727, pp.135-147, 2007.

[7] A.Bauer, E.Jaulmes, E.Pruff, J.R.Reinhard and J.Wild, "Horizontal collision correlation attack on elliptic curves:-Extended Version-", *Cryptography and Communications*, Vol.7, No.1, pp.91-119, 2014.

[8] L.Goubin, "A refined power-analysis attack on elliptic curve cryptosystem", *PKC 2003*, LNCS 2567, pp.199-211, 2002.

[9] T.Akishita and T.Takagi, "Zero-value point attacks on elliptic curve cryptosystem", *ISC 2003*, LNCS 2851, pp.218-233, 2003.

[10] N.Hanley, H.S.Kim and M.Tunstall, "Exploiting collisions in addition chain-based exponentiation algorithms using a single trace", *CT-RSA 2015*, LNCS 9048, pp.431-448, 2015.

[11] C.Clavier and M.Joye, "Universal exponentiation algorithm", *CHES 2001*, LNCS 2162, pp.300-308, 2001.

[12] M.Ciet and M.Joye, "(Virtually) Free randomization techniques for elliptic curve cryptography", *ICICS 2003*, LNCS 2836, pp.348-359, 2003.

[13] N.Smart, E.Oswald and D.Page, "Randomised representations", *IET Information Security*, Vol.2, pp.19-27, 2008.

[14] P-A.Fouque and R.Valette, "The doubling attack why upwards is better than downloads", *CHES 2003*, LNCS 2779, pp.269-280, 2003.

[15] J.Ha, J.Park, S.Moon and S.Yen, "Provably secure countermeasure resistant to several types if power attack for ECC", *WISA 2007*, LNCS 4867, pp.333-344, 2007.

[16] D.Hankerson, A.Menezes, and S.Vanstone, *Guide to Elliptic Curve Cryptography*, pp.75-97, 2004.

[17] B.Feix, M.Roussellet and A.Vnelli, "Side-channel analysis on blinded regular scalar multiplications", *INDOCRYPT 2014*, LNCS 8885, pp.3-20, 2014.

[18] N.M.Ebeid, *Key randomization countermeasures to power analysis attacks on elliptic curve cryptosystems,* University of Waterloo, Phd.D. Electrical and Computer Engineering, 2007.

[19] K.Okeya and K.Sakurai, "Power analysis breaks elliptic curve cryptosystems even secure against the timing attack", *INDOCRYPT 2000*, LNCS 1977, pp.178-190, 2000.

[20] S.Jung, "A Method for Scalar Multiplication on Elliptic Curves against Differential Power Analysis using Efficient Key-Randomization", *Jour. of the Korea contents association*, Vol.20, No.1, pp.356-363, 2019.

정 석 원(Seok Won Jung) [종신회원]

- 1993년 2월 : 고려대학교 일반대학원 수학과 (이학석사)
- 1997년 2월 : 고려대학교 일반대학원 수학과 (이학박사)
- 1999년 2월 ~ 2001년 2월 : ㈜텔리맨 책임연구원
- 2004년 4월 ~ 현재 : 목포대학교 정보보호학과 교수

〈관심분야〉

암호알고리즘 구현, 암호프로토콜 설계, 부채널공격법