암호공격에 안전한 Koblitz 타원곡선 암호시스템의 스칼라 곱셈 알고리즘

장용희*, 高木直史*, 高木一義*, 권용진†

*일본나고야대학 정보과학연구과, †한국항공대학교 항공전자 및 정보통신공학부

A Scalar Multiplication Algorithm Secure against Side-Channel Attacks for Koblitz Curve Cryptosystems

Yong-Hee Jang*, Naofumi Takagi*, Kazuyoshi Takagi*, Yong-Jin Kwon†

*Nagoya University, †Hankuk Aviation University.

Abstract

Recently, many power analysis attacks have been proposed. Since the attacks are powerful, it is very important to implement cryptosystems securely against the attacks. We propose countermeasures against power analysis attacks for elliptic curve cryptosystems based on Koblitz curves (KCs), which are a special class of elliptic curves. That is, we make our countermeasures be secure against SPA, DPA, and new DPA attacks, specially RPA, ZPA, using a random point at each execution of elliptic curve scalar multiplication. And since our countermeasures are designed to use the Frobenius map of KC, those are very fast.

I. Introduction

Elliptic curve cryptosystem (ECC) has been attracted much attention because of its short key size. The key length of ECC is currently chosen smaller than those of RSA cryptosystems. The small key size of ECC is suitable for mobile devices like smart cards, mobile phones and PDAs [8]. However, if an implementation is careless, an attacker can recover the secret key of ECC by using side-channel attacks (SCAs) such as timing attack, fault attack and power analysis attack. Thus, it is very important to defend SCAs on ECC.

P. Kocher et al.[12] proposed attacks based on simple and differential power analysis (SPA and DPA, respectively) to recover the secret key by monitoring and analyzing the power consumption signals [2]. Since power attacks are known to be the most practical and powerful [13], many countermeasures have been proposed to prevent power analysis attacks. For ECC, Coron[5] proposed three types of countermeasure: randomization of the private exponent, blinding the point, randomized projective(or Jacobian) coordinates. And Joye-Tymen[9] proposed countermeasures using random elliptic curve isomorphisms. The above methods are the most typical types of countermeasures in ECC. However, these countermeasures have some security weaknesses.

Okeya-Sakurai[7] showed some weaknesses of Coron's first two countermeasures and asserted that his 3rd countermeasure was secure. However, Coron's 3rd and Joye-Tymen's countermeasures can be broken by a refined power analysis (RPA) as proposed by Goubin[4] [3]. And RPA is generalized to zero-value point attack (ZPA) by [11]. ZPA makes use of the fact that even if a point has no zero-value coordinate, auxiliary registers used in the definition field might take zero value. The Coron's third and Joye-Tymen's countermeasures do not protect against ZPA attacks.

Cryptosystems based on Koblitz curves (KCs)

This paper was supported by the JSPS(the Japan Society for the Promotion of Science) Postdoctoral Fellowship.

were proposed by N. Koblitz in [14]. Since such cryptosystems offer significant advantage in terms of reduced processing time, the cryptosystems are quite attractive for practical applications [2]. And specific parameters for Koblitz curves have been proposed by NIST (the National Institute of Standards and Technology)[15] and SECG (the Standards for Efficient Cryptography Group)[16].

In this paper, we propose countermeasure against SPA, DPA, and new DPA attacks, that is, RPA and ZPA for KC-based cryptosystems. Our countermeasure uses a random point to protect the above SCA attacks. By using a random point at each execution of elliptic curve scalar multiplication, we can make any point or any register be changed at each execution. Thus, our countermeasure is resistant against DPA, RPA, and ZPA attacks. Also we compute the scalar multiplication to be secure against SPA. Our countermeasure is designed to eliminate elliptic curve point doubling operation using the Frobenius map of KC. Thus, our countermeasure is more faster than the existing ones. That is, we accomplish both security against the above attacks and improvement of the speed by using the random point and the Frobenius map.

II. Preliminaries

2.1 Elliptic Curve Cryptosystems

An elliptic curve cryptosystem is the set of points satisfying a bivariate cubic equation over a field. For the finite field $GF(2^n)$, the standard equation for an elliptic curve is the Weierstrass equation as below:

$$y^2+xy=x^3+\alpha^2+\beta, \quad (1)$$

where $\alpha,\beta\in GF(2^n)$ and $\beta\neq 0$. The points on the curve are of the form $P=(x,y)$, where x and y are elements of $GF(2^n)$. The curve has a special point O at infinity. The set of points on the curve forms a commutative finite group under the addition operation. And the point O is the group identity.

Elliptic curve scalar multiplication is the basic operation in elliptic curve cryptosystems. If a k is a positive integer and P is a point on elliptic curve, then the scalar multiplication kP is the operation of adding a point P to itself k times. The standard algorithm to compute kP is called as a binary algorithm as Algorithm 1.

Algorithm 1. The binary algorithm.

```
Input: $k=(k_{n-1},\cdots,k_1,k_0)_2$, a point $P$
Output : $Q=kP$
  1. $Q$ := $O$
  2. for $i=n-1$ downto 0 do
       $Q$ := $2Q$
       if $k_i=1$ then $Q$ := $Q+P$
  3. Return $Q$.
```

2.2 Koblitz Curves

Koblitz curves are a special class of elliptic curves with following forms:

$$y^2+xy=x^3+\alpha x^2+1, \quad (2)$$

where $\alpha\in GF(2)$. Since the Koblitz curves are defined over $GF(2)$, if $P=(x,y)$ is a point on Koblitz curve, then so is the point (x^2,y^2). Using the addition rule of elliptic curve, we can verify that

$$(x^4,y^4)+2(x,y)=(-1)^{1-\alpha}(x^2,y^2) \quad (3)$$

for every point (x,y) on Koblitz curve. Using (3), we can then obtain

$$\tau(x,y)=(x^2,y^2), \quad (4)$$

where τ is a complex number which satisfies

$$\tau^2-(-1)^{1-\alpha}\tau+2=0. \quad (5)$$

Equation (4) is referred to as the Frobenius map over $GF(2)$ [2].

A important meaning of (4) is as follows: If the scalar k is represented with radix τ, then, in the computation of kP using Algorithm 1, the operation $Q:=2Q$ is replaced by $Q:=\tau Q$.

The latter corresponds to two squaring operations over $GF(2^n)$ and completely eliminates much more costly elliptic curve point doubling operations [2].

To take advantage of the Frobenius map in the computation of scalar multiplication, the scalar k is converted into a τ-adic representation. Let us denote this representation $k=\sum_{i=0}^{l-1}\kappa_i\tau^i$. If we limit κ_i to be 0 or ±1 only, then $l\approx 2n$ [6]. If we compute the Algorithm 1 with the τ-adic representation of k, the loop will be executed approximately $2n$ times; hence, about $2n$ elliptic operations (only additions, no doubling) are needed. Thus, τ-adic representation of k does not appear to provide computational advantages to the Koblitz curves. However, we can alleviate this problem by reducing the k in mod $\tau^n - 1$ [2].

2.2 Power Analysis Attacks

Simple Power Analysis. A SPA consists in observing the power consumption of one single execution of a cryptographic algorithm. Algorithm 1 is vulnerable to the SPA. To resist against the SPA, Coron[5] proposed a simple countermeasure as in Algorithm 2, which is called as a double-and-add-always algorithm.

Algorithm 2. Double-and-add-always algorithm

```
Input: $k=(k_{n-1},\cdots,k_1,k_0)_2$, a point $P$
Output : $Q=kP$
  1. $Q[0]$ := $O$
  2. for $i=n-1$ downto 0 do
       $Q[0]$ := $2Q[0]$
       $Q[1]$ := $Q[0]+P$
       $Q[0]$ := $Q[k_i]$.
  3. Return $Q[0]$.
```

The double-and-add-always algorithm always computes elliptic curve addition whether $k_i = 0$ or 1. However, even though this algorithm is resistant against the SPA attack, it remains vulnerable to a DPA attack.

Differential Power Analysis. A DPA attack is based on the same basic concept as a SPA attack, but use statistical and digital signal processing techniques to extract very small differences in the power consumption signals. In order to be resistant against DPA, power consumption should be changed at each new execution of the scalar multiplication. Coron[5] proposed three countermeasures to resist against DPA attacks: randomizing the private exponent k, blinding the point, and randomizing the projective(or Jacobian) coordinates. Okeya-Sakurai[7] showed the bias in Coron's 1st and 2nd countermeasures and asserted that Coron's 3rd countermeasure is secure enough [8]. Coron's 3rd countermeasure is to randomize the representation of a point $P=(X:Y:Z)$ in the Jacobian(or projective) coordinates by using the relationship $(X:Y:Z)=(\lambda^2X:\lambda^3Y:\lambda Z)$ for λ in the finite field [8]. An enhanced version of Coron's 3rd countermeasure has been proposed by Joye-Tymen[9]. Joye-Tymen's countermeasure maps an underlying curve to a random isomorphic curve. However, all these countermeasures are still vulnerable against RPA, ZPA [3].

Refined Power Analysis and Zero-value Point Analysis. Goubin[4] proposed a new analysis using a special elliptic curve point with zero value, which is defined as $(x,0)$, $(0,y)$. The points $(x,0)$ or $(0,y)$ has still a zero value even if it is converted into $(\lambda^2X:0:\lambda Z)$ or $(0:\lambda^3Y:\lambda Z)$ by using Coron's 3rd countermeasure. Similarly, the randomized isomorphisms of Joye-Tymen cannot randomize these points [1]. And also the method of Joye-Tymen does not apply for elliptic curves over binary fields because the x-coordinate of a point is invariant through isomorphism [9].

RPA is generalized to zero-value point analysis (ZPA) by [11]. RPA uses a special point which has a zero-value coordinate. In a ZPA attack, on the other hand, it makes use of any zero-value register in addition formula. Coron's or Joye-Tymen's countermeasure do not protect against ZPA attacks. The addition and doubling formulae have a lot of each different operations stored in auxiliary registers, one of which may become zero.

III. Proposed Countermeasure against Side-Channel Attacks

In this section, we show our new countermeasure for Koblitz curve. By using a random point at each execution of the elliptic curve scalar multiplication, any point or any register used in the addition formulae changes at each execution. Thus, it is resistant against DPA, RPA, and ZPA. And also, since our countermeasure can the Frobenius map of KC, those are computationally more efficient than the existing alternative ones.

From now, we describe the idea of the proposed countermeasure. Since the solutions (x,y) to (2) are over $GF(2^n)$, we have $x^{2^n} \equiv x$. Consequently, we can get the following equation:

$$\tau^n(x,y) = (x^{2^n}, y^{2^n}) \equiv (x,y)$$

$$(\tau^n - 1)(x,y) \equiv O. \qquad (6)$$

Thus, for the scalar multiplication kP, instead of using k, we can use $k(\bmod\ \tau^n - 1)$. And we can represent $k(\bmod\ \tau^n - 1)$ into τ-adic NAF representation of n-tuple (see [6] in details).

From (6), we can write

$$(\tau - 1)(\tau^{n-1} + \tau^{n-2} + \cdots + \tau + 1)(x,y) \equiv O,$$

implying that

$$(\tau^{n-1} + \tau^{n-2} + \cdots + \tau + 1)(x,y) \equiv O. \qquad (7)$$

Our countermeasure uses (7), a random point R, and the reduced $k(\bmod\ \tau^n - 1)$ of τ-adic NAF representation of n-tuple to compute

$$\begin{aligned} & kP + (\tau^{n-1} + \tau^{n-2} + \cdots + \tau + 1)R = \\ & (\kappa_{n-1}\tau^{n-1} + \kappa_{n-2}\tau^{n-2} + \cdots + \kappa_1\tau + \kappa_0)P + \\ & (\tau^{n-1} + \tau^{n-2} + \cdots + \tau + 1)R \\ & = (R + \kappa_{n-1}P)\tau^{n-1} + (R + \kappa_{n-2}P)\tau^{n-2} + \cdots + \\ & (R + \kappa_1 P)\tau + (R + \kappa_0 P). \end{aligned} \qquad (8)$$

In (8), since $(\tau^{n-1} + \tau^{n-2} + \cdots + \tau + 1)R \equiv O$, finally we can get kP. Algorithm 3 shows our idea in details. Algorithm 3 makes all variables Q, $T[0]$, $T[1]$, and $T[2]$ dependent on a random point R, and thus let all variables of each addition differ at each execution.

Algorithm 3. The proposed scalar multiplication algorithm

```
Input: A point $P$ and $k$ $=k(\bmod\ \tau^n - 1) = (\kappa_{n-1}, \cdots, \kappa_1, \kappa_0)_\tau$, $\kappa_i \in \{-1,0,1\}$, that is, $\tau$-adic NAF.
Output: $Q = kP$
  1. $R$ := randompoint()
  2. $T[0]$ := $R$, $T[1]$ := $R+P$, $T[2]$ := $R-P$
  3. $Q$ := $O$
  4. for $i = n-1$ downto 0 do
       $Q$ := $\tau Q$
       if $\kappa_i = 0$ then          $Q$ := $Q + T[0]$
       elseif $\kappa_i = 1$ then      $Q$ := $Q + T[1]$
       else                            $Q$ := $Q + T[2]$.
  5. Return $Q$.
```

That is, by choosing R randomly, Algorithm 3 can be resistant against DPA, RPA, and ZPA, since any special point or zero-value register used in addition formulae changes at each execution. Also, since Algorithm 3 lets the power-consumption pattern be fixed regardless of the bit pattern of the scalar k, it is resistant against SPA. And algorithm 3 is very fast because it can use the Frobenius map of KC.

IV. Comparison

From the point of view of computation and memory amount, we compare our scalar multiplication algorithm with previously reported algorithms, that is, [3] and [10], which are secure against SPA, DPA, RPA and ZPA. In [3], Mamiya et al. recently proposed the countermeasure which uses a random initial point R. The basic idea of Mamiya et al. is to let 1 express $1 = (1\bar{1}\bar{1}\cdots\bar{1})_2$ and computes $kP + (1\bar{1}\bar{1}\cdots\bar{1})R$. In [3], however, it is impossible to use the Frobenius map because $1 \neq (1\bar{1}\bar{1}\cdots\bar{1})_\tau$.

And the method proposed in [10] splits an exponent and computes $kP = \lfloor k/r \rfloor rP + (k \bmod r)P$ by using a random number r. The method of [10] computes by the same cost as the add-and-double-always algorithm (Algorithm 2) with an extra point (rP) for computation.

Table 1 shows the comparison, where A D, or F shows elliptic curve addition, doubling, or Frobenius map, respectively.

	(#point, #scalar)	#D	#A	#F
ES[10]	(4, 2)	n	n	0
BRIP [3]	(3, 0)	n	n	0
Algorithm 3	(4, 0)	0	n	n

Table 1. Comparison with the existing countermeasures

Our countermeasure, Algorithm 3, don't require elliptic curve doubling operations. The Frobenius map is the squaring of the x and y coordinates of the point. In a normal basis representation, squaring is as simple as a cyclic shift of the bits of the operand. Thus, using a normal basis representation, our countermeasures can compute the elliptic curve scalar multiplication at very more high speed than those of [3] and [10].

V. Conclusion

Side channel attacks such as power analysis attacks have become serious threats. Thus, it is very important to implement cryptosystems securely against the attacks. And also, it is important to design cryptosystems so that those can be computed at high speed. In this paper, we have proposed countermeasure for elliptic curve cryptosystems based on Koblitz curves. Using the random point and (7), we let our countermeasure be resistant against ZPA, RPA, DPA, and SPA attacks. Also since our countermeasure can the Frobenius map of KC, those are computed very fast.

[References]

[1] Toru Akishita and Tsuyoshi Takagi, "Zero-Value Register Attack on Elliptic Curve Cryptosystem," IEICE Trans. Fundamentals, Vol. E88-A, No. 1, pp. 132-139, January 2005.

[2] M. A. Hasan, "Power Analysis Attacks and Algorithmic Approaches to Their Countermeasures for Koblitz Curve Cryptosystems," IEEE Trans. on Computers, Vol. 50, No. 10, pp. 1071-1083, October 2001.

[3] H. Mamiya, A. Miyaji, and H. Morimoto, "Efficient countermeasure against RPA, DPA and SPA," CHES'04, LNCS 3156, pp. 343-356, Springer-Verlag, 2004.

[4] L. Goubin, "A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems," PKC2003, LNCS 2567, pp. 199-211, Springer-Verlag 2003.

[5] J. Coron, "Resistance against differential Power Analysis for Elliptic Curve Cryptosystems," CHES'99, LNCS 1717, pp. 292-302, Springer-Verlag 1999.

[6] J. Solinas, "An Improved Algorithm for Arithmetic on a Family of Elliptic Curves," CRYPTO'97, pp. 357-371, 1997.

[7] K. Okeya and K. Sakurai, "Power analysis breaks elliptic curve cryptosystems even secure against the timing attack," INDOCRYPT2000, LNCS 1977, pp. 178-190, Springer-Verlag, 2000.

[8] Tetsuya IZU and Tsuyoshi Takagi, "Fast Elliptic Curve Multiplications Resistant against Side Channel Attacks," IEICE Trans. Fundamentals, Vol. E88-A, No. 1, January 2005.

[9] M. Joye and C. Tymen, "Protections against differential analysis for elliptic curve cryptography," CHES2001, LNCS 2162, pp. 377-390, Springer-Verlag, 2001.

[10] M. Ciet and M. Joye, "(Virtually) Free randomization technique for elliptic curve cryptograph," ICICS2003, LNCS 2836, pp. 348-359, Springer-Verlag, 2003.

[11] T. Akishita and T. Takagi, "Zero-value Point Attacks on Elliptic Curve Cryptosystem," ISC2003, LNCS 2851, pp. 218-233, Springer-Verlag, 2003.

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

[13] Jae Cheol Ha and San Jae Moon, "Randomized Signed-Scalar Multiplication of ECC to Resist Power Attacks," CHES2002, LNCS 2523, pp. 551-563, Springer-Verlag 2003.

[14] N. Koblitz, "CM-Curves with Good Cryptographic Properties," CRYPTO'91, LNCS 576, pp. 279-287, Springer-Verlag, 1992.

[15] US Dept. of Commerce/NIST, Digital Signature Standards (DSS), Federal Information Processing Standards Publications, http://csrc.nist.gov/cryptoval, Jan. 2000.

[16] Standards for Efficient Cryptography Group (SECG), SEC2: Recommended Elliptic Curve Domain Parameters, Version 1.0, 2000. http://www.secg.org/