情報保護學會論文誌
第17卷 第3號, 2007. 6

# A Blinding-Based Scalar Multiplication Algorithm Secure against Power Analysis Attacks*

ChangKyun Kim,[1†‡] JaeCheol Ha,[2] SangJae Moon[3]
[1]National Security Research Institute, [2]Hoseo University, [3]Kyungpook National University.

## ABSTRACT

Most existing countermeasures against classical DPA are vulnerable to new DPA, e.g., refined power analysis attack (RPA), zero-value point attack (ZPA), and doubling attack. More recently, Mamiya et al proposed a new countermeasure (so-called BRIP) against RPA, ZPA, classical DPA and SPA. This countermeasure, however, also has a vulnerability of scalar multiplication computations by exploiting specially chosen input message. Therefore, to prevent various power analysis attacks like DPA and new SPA, we propose an enhanced countermeasure by developing a new random blinding technique.

**Keywords** : *DPA, BRIP, ECC, Countermeasure*

## I. Introduction[1)]

Since Kocher introduced power analysis attacks against cryptographic devices[1], many countermeasures have been proposed to prevent power analysis attacks based on various hardware and software techniques. Specifically, for implementations of elliptic curve cryptosystems (ECC), there are several types of countermeasures that have been suggested, including random scalar multiplication algorithm, random blinding on a point, random projective coordinate algorithm, and some approaches using special forms of elliptic curves[2-5]. However, these above countermeasures suffer from some disadvantages; they have either large computational overhead or some security weaknesses against new types of power analysis attack including RPA[6], ZPA[7], and doubling attack[8].

More recently, two new countermeasures have been proposed to protect against the different types of DPA attacks. First, Smart analyzed RPA and presented two defending methods (randomization of the private key and point blinding)[9]. However, none of these methods are efficient from a viewpoint of computational load. Second, to prevent various power analysis attacks like DPA, Mamiya et al proposed a new countermeasure (called BRIP) which uses a random initial point (RIP)[10]. This method, however, is vulnerable to a simple power analysis (SPA) by exploiting specially chosen input messages[11]. Moreover, the countermeasure is not suitable for RSA implementation because it requires an inversion computation and almost similar to the proposed countermeasure to prevent fault analysis attacks and power analysis attacks[12]. To solve the above mentioned problem of new vulnerability and computational inefficiency, we propose an enhanced countermeasure by developing a

접수일: 2006년 11월 6일; 채택일: 2007년 2월 12일
* This research was supported by the MIC of Korea, under the ITRC support program supervised by the IITA(IITA-2006-C1090-0603-0026).
† 주저자, kimck@etri.re.kr
‡ 교신저자, kimck@etri.re.kr

new random blinding technique.

## Ⅱ. New Proposed Countermeasure

### 2.1 Proposed Scalar Multiplication Algorithm

The basic idea of the proposed countermeasure is to blind a point using a random point $R$. We finally compute $dP+\#\varepsilon R$ instead of $dP$, where $d$, $P$, and $\#\varepsilon$ is the secret key, the input point, and the number of points of the curve, respectively. Now, let $s = \#\varepsilon - d$, then we compute both $d(P+R)$ and $sR$. The core of the algorithm is the simultaneous scalar multiplication of the above two operations $d(P+R)$ and $sR$ as described in Fig. 1. By using a random blinding point technique, the intermediate values of points and registers used in each iteration are randomly changed.

In Fig. 1, to compute $d(P+R)$ and $sR$ simultaneously we applied to the Shamir's trick. In this case the final result $dP$ is obtained by computing

$$\begin{aligned} dP &= \sum_i (d_i(P+R)+s_iR) \qquad (1)\\ &= \sum_i d_iP+\sum_i (d_i+s_i)R \\ &= dP+(d+s)R \\ &= dP+\varepsilon R \end{aligned}$$

where $\#\varepsilon R$ is equal to a point $O$ at infinity. Although the proposed idea seems to be a simple analogy of the previously known countermeasure BRIP and the exponent splitting[13], this idea is more secure and efficient than the above two countermeasures.

Even if an attacker inputs special points to attempt an attack using RPA and ZPA, he cannot bypass the proposed countermeasure because the point $P$ is blinded by the random point $R$ which is changed at each scalar multiplication.

Therefore, this countermeasure can protect against various power analysis like DPA (RPA, ZPA, and doubling attacks) as well as classical DPA attacks.

Input : $d=(d_{n-1},\cdots,d_0)_2$, $P$
Output : $Q=dP$

1. $s=\varepsilon-d$
2. Update $R=(rx,ry,rz)$ by a random number $r$
3. $T[00]=O, T[01]=R, T[10]=P+R$, $T[11]=P+2R$
4. $Q=O$
5. for $i=n-1$ to 0
5.1 $Q=2Q$
5.2 $Q=Q+T[d_is_i]$
6. Return($Q$)

(Fig. 1) Proposed scalar multiplication for ECC

Moreover, the proposed countermeasure can be applied to RSA. Notice that it is not necessary to compute an inverse of the random number equivalent for $-R$. This design becomes very useful to speed up secure RSA implementation. From this point of view, the proposed countermeasure is a more efficient and general than Mamiya's countermeasure.

### 2.2 Low Cost Scalar Multiplication Algorithm

In order to protect against SPA, instructions performed during a cryptographic algorithm should not depend on the data being processed. However the proposed algorithm in Fig. 1 has an addition of infinity point in case of $d_is_i=00$. This computation might provide a weakness in SPA because it reveals whether $d_is_i$ is 00 or not. Fig. 2 shows that the proposed countermeasure can be applied to the side channel atomic doubling and addition multiplication procedure for ECC[14]. In this algorithm, we assume that the doubling is processed using the same algorithm as the addition as you see in Fig. 2. Although the Step 5.1 in Fig. 2 is either doubling or addition according to $d_i$ and $s_i$, these operations should be operated using same elliptic point operation to prevent from SPA. Therefore, the elliptic point operation for side channel atomic multiplication algorithm should be carefully implemented. An efficient algorithm for Step 5.1 in Fig. 2 is proposed by Mames *et al*[14].

We can reduce the number of loop iterations to

Input : $d=(d_{n-1},\cdots,d_0)_2$, $M$
Output : $Q=dP$

1. $s=t\cdot\varepsilon-d$, where $t>1$ is an integer.
2. Update $R=(rx,ry,rz)$ by a random number $r$
3. $T[00]=O, T[01]=R, T[10]=P+R,\ T[11]=P+2R$
4. $k=0,\ i=n-2,\ T[00]=T[d_{n-1}s_{n-1}]$
5. while($i\geq 0$)
5.1 $T[00]=T[00]+T[(d_is_i)\wedge(kk)]$
5.2 $k=k\oplus(d_i\vee s_i)$
5.3 $i=i-\neg k$
6. Return($Q=T[00]$)

[Fig. 2] The side channel atomic multiplication algorithm

$1.75n$ operations on average because of the properties of side channel atomic multiplication algorithm. So we can save 12.5% in computational load compared to Mamiya's one. Although the proposed countermeasure requires an extra register compared to BRIP, it can be solved by enhanced hardware technique nowadays.

## Ⅲ. Security Consideration

Let $E$ be an elliptic curve defined over a field $K$. $E[2]$ is defined as follows.

$$E[2]=\{G\in E(\overline{K})|2G=O\} \tag{2}$$

where $\overline{K}$ is an algebraic closure of $K$.

In new SPA (by exploiting specially chosen input messages), if 2-torsion point does not exit, then the attack is infeasible and useless. However, since almost elliptic curves $E$ defined over $K=F_{2^m}$ except $F_p$ and $F_{p^m}$ have an even cofactor, they have 2-torsion point[15]. So, new SPA should be considered to implement a secure scalar multiplication algorithm against power analysis attacks.

Contrary to BRIP, the proposed countermeasure is secure against new SPA because the basic concept of the proposed one is not $O=(1\bar{1}\bar{1}\cdots\bar{1}1)_2R-R$ but $O=\varepsilon R$, where $\bar{1}$ means -1. More clearly, as shown in Table 1 when $P$ is 2-torsion point, there are many possible values of $Q$ at the beginning of each iteration in Fig. 1.

In the case of BRIP, there are only two possible output values of $Q$ (either $R$ or $P+R$) depending on the value of $d_i$ no matter what the value of $Q$ was at the beginning of this iteration. While in the case of the proposed countermeasure, there are many possible output values of $Q$ depending on the value of $Q=\sum_{k=i}^{n-1}(d_k+s_k)\cdot 2^{k-i}R$. Moreover, the values of $Q$ differ from at each execution because the random point $R$ is randomly updated by a random number $r$. Therefore, the proposed countermeasure is resistant against not only various power analysis attacks like DPA but also the new SPA.

As a special case, if the random point $R$ in step 2 of Fig. 1 is updated using not a random projective co-

[Table 1] Possible values of $Q$ at the beginning of each iteration in Fig. 1

| | CASE 1 | CASE 2 |
|---|---|---|
| Step 5.1 | $Q=2\sum_{k=i+1}^{n-1}(d_k+s_k)\cdot 2^{k-i-1}R$ $=\sum_{k=i+1}^{n-1}(d_k+s_k)\cdot 2^{k-i}R$ | $Q=2(P+\sum_{k=i+1}^{n-1}(d_k+s_k)\cdot 2^{k-i-1}R)$ $=\sum_{k=i+1}^{n-1}(d_k+s_k)\cdot 2^{k-i}R$ |
| Step 5.2 | $Q=\sum_{k=i}^{n-1}(d_k+s_k)\cdot 2^{k-i}R$ (if $d_i=0$) $Q=P+\sum_{k=i}^{n-1}(d_k+s_k)\cdot 2^{k-i}R$ (if $d_i=1$) | $Q=\sum_{k=i}^{n-1}(d_k+s_k)\cdot 2^{k-i}R$ (if $d_i=0$) $Q=P+\sum_{k=i}^{n-1}(d_k+s_k)\cdot 2^{k-i}R$ (if $d_i=1$) |

where $\sum_{k=0}^{n-1}(d_k+s_k)\cdot 2^k=\varepsilon$.

ordinate but the multiplication by 2 maps, this countermeasure is susceptible to doubling attack. Therefore, the random point $R$ should be carefully and randomly updated.

## Ⅳ. Conclusion

This letter presents a countermeasure against the several types of DPA as well as new SPA-based 2-torsion point attack. The computational cost of the proposed countermeasure is very low when compared to the previous methods which rely on Coron's simple SPA countermeasure. Notice especially that the proposed countermeasure is a more general countermeasure which can be applied to ECC as well as RSA systems without inverse operation.

## Reference

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

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

[3] K. Okeya and K. Sakurai, "Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack," INDOCRYPT'00, LNCS 1977, pp.178-190, Springer-Verlag, 2000.

[4] P. Liardet and N. Smart, "Preventing SPA/DPA in ECC Systems using the Jacobi Form," CHES'01, LNCS 2162, pp. 391-401, Springer-Verlag, 2001.

[5] M. Joye and J. Quisquater, "Hessian Elliptic Curves and Side-Channel Attacks," CHES'01, LNCS 2162, pp. 402-410, Springer-Verlag, 2001.

[6] L. Goubin, "A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems," PKC'03, LNCS 2567, pp. 199-210, Springer-Verlag, 2003.

[7] T. Akishita and T. Takagi, "Zero-Value Point Attacks on Elliptic Curve Cryptosystem," ISC'03, LNCS 2851, pp. 218-233, Springer-Verlag, 2003.

[8] P. A. Fouque and F. Valette, "The Doubling Attack - Why Upwards Is Better than Downwards," CHES'03, LNCS 2779, pp. 269-280, Springer-Verlag, 2003.

[9] N. P. Smart, "An Analysis Goubin's Refined Power Analysis Attack," CHES'03, LNCS 2779, pp. 281-290, Springer-Verlag, 2003.

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

[11] S. Yen, W. Lien, S. Moon, and J. Ha, "Power Analysis by Exploiting Chosen Message and Internal Collisions - Vulnerability of Checking Mechanism for RSA-Decryption," MYCRYPT'05, LNCS 3715, pp. 183-195, Springer-Verlag, 2005.

[12] C. K. Kim, J. C. Ha, S. H. Kim, S. K. Kim, S. M. Yen, and S. J. Moon, "A Secure and Practical CRT-based RSA to Resist Side Channel Attacks," ICCSA'04, LNCS 3043, pp. 150-158, Springer-Verlag, 2004.

[13] C. Clavier and M. Joye, "Universal Exponentiation Algorithm," CHES'01, LNCS 2162, pp.300-308, Springer-Verlag, 2001.

[14] B. C. Mames, M. Ciet, and M. Joye, "Low-Cost Solutions for Preventing Simple Side-Channel Analysis: Side-Channel Atomicity," IEEE Transactions on Computers, vol. 53, No. 6, June 2004.

[15] National Institute of Standards and Technology, Digital Signature Standard, FIPS 186-2, Feb. 2000.

## 〈著者紹介〉

**김 창 균 (ChangKyun Kim) 정회원**
2001년 2월: 경북대학교 전자전기공학부 졸업
2003년 2월: 경북대학교 전자공학과 석사
2003년 3월~현재: 경북대학교 전자공학과 박사과정
2004년 11월~현재: 국가보안기술연구소
<관심분야> 정보보호기술

**하 재 철 (JaeCheol Ha) 종신회원**
1989년 2월: 경북대학교 전자공학과 졸업
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2006년 1월: 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2006년 7월~2006년 12월: QUT in Australia 연구 교수
2007년 3월~현재: 호서대학교 정보보호학과 부교수
2002년 3월~현재: 한국정보보호학회 이사
<관심분야> 정보보호, 네트워크 보안, 스마트카드 보안

**문 상 재 (SangJae Moon) 종신회원**
1972년 2월: 서울대학교 공업교육(전자)과 졸업
1974년 2월: 서울대학교 전자공학과 석사
1984년 6월: 미국 UCLA 전자공학과 박사
1984년 7월~1985년 6월: UCLA Postdoctoral 근무
1984년 7월~1985년 6월: 미국 OMNET 컨설턴트
1974년 12월~현재: 경북대학교 공과대학 전자전기컴퓨터공학부 교수
2000년 8월~현재: 경북대학교 이동네트워크 정보보호기술 연구센터 소장
2002년 2월~현재: 한국정보보호학회 명예회장
<관심분야> 정보보호, 디지털 통신, 이동 네트워크