Zero-Value Point Attacks on Elliptic Curve Cryptosystem

Toru Akishita*[1] and Tsuyoshi Takagi[2]

[1] Sony Corporation, Ubiquitous Technology Laboratories,
6-7-35 Kitashinagawa Shinagawa-ku, Tokyo, 141-0001 Japan
akishita@pal.arch.sony.co.jp
[2] Technische Universität Darmstadt, Fachbereich Informatik,
Alexanderstr.10, D-64283 Darmstadt, Germany
ttakagi@cdc.informatik.tu-darmstadt.de

Abstract. The differential power analysis (DPA) might break the implementation of elliptic curve cryptosystem (ECC) on memory constraint devices. Goubin proposed a variant of DPA using the point $(0, y)$, which is not randomized in Jacobian coordinates or in the isomorphic class. This point often exists in the standard curves, and we have to care this attack. In this paper, we propose the zero-value point attack as an extension of Goubin's attack. Note that even if a point has no zero-value coordinate, the auxiliary registers might take zero-value. We investigate these zero-value registers that cannot be randomized by the above randomization. Indeed, we have found several points $P = (x, y)$ which cause the zero-value registers, e.g., (1)$3x^2 + a = 0$, (2)$5x^4 + 2ax^2 - 4bx + a^2 = 0$, (3)$P$ is y-coordinate self-collision point, etc. We demonstrate the standard curves that have these points. Interestingly, some conditions required for the zero-value attack depend on the explicit implementation of the addition formula — in order to resist this type of attacks, we have to care how to implement the addition formula. Finally, we note that Goubin's attack and the proposed attack assume that the base point P can be chosen by the attacker and the secret scalar d is fixed, so that they are not applicable to ECDSA signature generation.

Keywords: side channel attack, differential power analysis, elliptic curve cryptosystem, addition formula, zero-value register.

1 Introduction

Elliptic curve cryptosystem (ECC) is suitable for the implementation on memory constraint devices, because of its short key size. The differential power analysis (DPA) is a serious attack on such scare computational devices. If the implementation is careless, the attacker can successfully recover the secret key by observing the power consuming of the device. Several simulational or experimental results show that the DPA is effective on the ECC on these devices [5, 8].

* This work was done while the first author stayed at Technische Universität Darmstadt, Germany.

In order to resist the DPA we usually randomize the base point Q of the underlying curve E. There are two standard approaches. The first one is to transform the base point to the random equivalent class in Jacobian (or projective) coordinates [5]. The second one is to map the all parameters including the base point to the random isomorphic class [13]. However, Goubin pointed out that the two methods are not able to randomize the points with zero value, namely $(x, 0)$ and $(0, y)$ [7]. If we use the base point $P = (c^{-1} \bmod \#E)(0, y)$ for some integer c, the DPA can successfully detect the point cP is computed during the scalar multiplication. The attacker can know the secret key by recursively adapting this attack for different c. Several standard curves over prime field $\mathbb{F}_p$ contain point $(0, y)$, i.e., the curve coefficient b is quadratic residue modulo p. We have to care Goubin's attack on these curves.

In this paper we proposed a novel attack, called the *zero-value point attack*. On the contrary to Goubin's attack, the zero-value point attack uses the zero-value resister of the addition formula. Even if a point has no zero-value point coordinate, the auxiliary registers might take zero-value. We investigate all possible zero-value registers that are not randomized by the above randomization. Indeed we have found non-trivial points which take the zero-value registers in the addition formula of Jacobian coordinate implementation, e.g., $(1)3x^2 + a = 0$, $(2)3x^4 + 6ax^2 + 12bx - a^2 = 0$, $(3)P$ is y-coordinate self-collision point, etc. These points are different from Goubin's point $(x, 0)$ or $(0, y)$. We show that these points exist on some standard curves.

If we choose the curve that does not have these conditions, we can resist the zero-value point attack. Interestingly, the existence condition of these conditions depends how to explicitly implement the addition formula. For example, condition (2) appears if we implement $T = -2S + M^2$ in the doubling of the elliptic curve as $W = -S + M^2$ and then $T = U - S$, but it never appears if we implement it as $W = 2S$ and then $T = M^2 - U$. This observation suggests that the designer has to care how to securely assemble the multiplication and the addition in the addition formula. Moreover, we show zero-value points for Montgomery-type method and elliptic curves over binary fields. We have found that the security conditions for these classes are quite different from those of the standard addition formula of the curves over prime fields — the zero-value point attack strongly depends on the structure of the addition formula.

In order to perform Goubin's attack or our attack, we assume that the attacker is able to freely choose the base point P and the secret scalar d is fixed for the scalar multiplication. Hence, we need to care these attacks in only such protocols as ECIES and single-pass ECDH.

This paper is organized as follows: In section 2, we describe the basic properties of the elliptic curve cryptosystem. In section 3, we review the side channel attack and Goubin's attack using the non-randomized point. In section 4, we propose the zero-value point attack and investigate the zero-value points for implementation in Jacobian coordinates. In section 5, we investigate the zero-value points for Montgomery-type method and elliptic curves over binary fields. Finally we conclude in section 6.

2 Elliptic Curve Cryptosystems

Let $K = \mathbb{F}_p$ be a finite field, where $p > 3$ is a prime. The Weierstrass form of an elliptic curve over K is described as

$$E : y^2 = x^3 + ax + b \ \ (a, b \in K,\ 4a^3 + 27b^2 \neq 0).$$

The set of all points $P = (x, y)$ satisfying E, together with the point of infinity $\mathcal{O}$, is denoted by $E(K)$, which forms an Abelian group. We denote by $x(P)$ and $y(P)$ the x- and y- coordinate of the point P. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on $E(K)$ that don't equal to $\mathcal{O}$. The sum $P_3 = P_1 + P_2 = (x_3, y_3)$ can be computed as

$$x_3 = \lambda(P_1, P_2)^2 - x_1 - x_2, \quad y_3 = \lambda(P_1, P_2)(x_1 - x_3) - y_1,$$

where $\lambda(P_1, P_2) = (3{x_1}^2 + a)/(2y_1)$ for $P_1 = P_2$, and $\lambda(P_1, P_2) = (y_2 - y_1)/(x_2 - x_1)$ for $P_1 \neq \pm P_2$. We call the former, $P_1 + P_2$ ($P_1 = P_2$), the elliptic curve doubling (ECDBL) and the latter, $P_1 + P_2$ ($P_1 \neq \pm P_2$), the elliptic curve addition (ECADD) in affine coordinate (x, y). These two addition formulae respectively need one inversion over K, which is much more expensive than multiplication over K. Therefore, we transform affine coordinate (x, y) into other coordinates where inversion is not required. We give here the addition and doubling formulae in Jacobian coordinates, which are widely used [4]. In this paper we deal with Jacobian coordinates, but all discussions can be also applied to projective coordinates $(X : Y : Z)$ setting $x = X/Z$ and $y = Y/Z$.

In Jacobian coordinates, we set $x = X/Z^2$ and $y = Y/Z^3$, giving the equation $E_{\mathcal{J}} : Y^2 = X^3 + aXZ^4 + bZ^6$. Then, two points $(X : Y : Z)$ and $(r^2X : r^3Y : rZ)$ for some $r \in K^*$ are recognized as the same point. Let $P_1 = (X_1 : Y_1 : Z_1)$, $P_2 = (X_2 : Y_2 : Z_2)$, and $P_3 = P_1 + P_2 = (X_3 : Y_3 : Z_3)$. The doubling and addition formulae can be represented as follows.

ECDBL in Jacobian Coordinates (ECDBL$^{\mathcal{J}}$) :
$X_3 = T$, $Y_3 = -8{Y_1}^4 + M(S - T)$, $Z_3 = 2Y_1Z_1$,
$S = 4X_1{Y_1}^2$, $M = 3{X_1}^2 + a{Z_1}^4$, $T = -2S + M^2$.

ECADD in Jacobian Coordinates (ECADD$^{\mathcal{J}}$) :
$X_3 = -H^3 - 2U_1H^2 + R^2$, $Y_3 = -S_1H^3 + R(U_1H^2 - X_3)$, $Z_3 = Z_1Z_2H$,
$U_1 = X_1{Z_2}^2$, $U_2 = X_2{Z_1}^2$, $S_1 = Y_1{Z_2}^3$, $S_2 = Y_2{Z_1}^3$, $H = U_2 - U_1$, $R = S_2 - S_1$.

This addition formula is usually optimized in the sense of the number of multiplications in the base field. We require 11 and 16 multiplications for ECDBL and ECADD, respectively.

In elliptic curve cryptosystems, it is necessary to compute dP, where $P \in E(K)$ and d is an n bit integer. The standard method to compute dP is called as the binary method. $d = (d_{n-1} \cdots d_1 d_0)_2$ is the binary representation of d. The binary method is described as follows.

Algorithm 1: Binary method

Input: $d = (d_{n-1} \cdots d_1 d_0)_2,\ P \in E(K)\ \ (d_{n-1} = 1)$.
Output: dP.
1. $Q \leftarrow P$
2. For $i = (n-2)$ downto 0 do:
   $Q \leftarrow \mathrm{ECDBL}(Q)$,
   If $d_i = 1$ then
   $Q \leftarrow \mathrm{ECADD}(Q, P)$,
3. Return(Q).

When we compute the scalar multiplication using Jacobian coordinates, the point Q in step 2 is represented as $Q = (X : Y : Z)$. In step 3, the point Q must be recovered to affine coordinate by computing $x = X/Z^2$ and $y = Y/Z^3$.

Let $\#E$ be the order of $E(K)$. For the security of elliptic curve cryptography, we must choose $E(K)$ such that $\#E$ is the product of a large prime and a very small integer h, called the cofactor. To avoid the small subgroup attack, it is convenient that $h = 1$, i.e. $\#E$ is prime. In this paper, we are interested in the curves with prime order.

3 Side Channel Attacks on ECC

In this section we review the side channel attack on ECC. The simple power analysis (SPA), the differential power analysis (DPA), and the Goubin's attack are described. We explain the standard countermeasures that resist the SPA and the DPA. These known countermeasures cannot resist the Goubin's attack, if the point $(0, y)$ exist on the underlying curve.

3.1 SPA and Countermeasures

The SPA observes the power consumption of devices, and detects the difference of operations using the secret key. Algorithm 1 is vulnerable to the SPA. The scalar multiplication is computed by the addition formulae, namely ECDBL and ECADD, based on the bit of the secret scalar. The operation ECADD in Algorithm 1 is computed if and only if the underlying bit is 1, although the operation ECDBL is always computed. The addition formulae are assembled by the basic operations of the definition field (See Appendix A). There are differences between the basic operations of ECDBL and those of ECADD. Thus the SPA attacker can detect the secret bit. In order to resist the SPA, we have to eliminate the relations between the bit information and their addition formulae.

Coron proposed a simple countermeasure, which is called as the double-and-add-always method. The double-and-add-always method is described as follows:

Algorithm 2: Double-and-add-always method

Input: $d = (d_{n-1} \cdots d_1 d_0)_2,\ P \in E(K)\ \ (d_{n-1} = 1)$.
Output: dP.
1. $Q[0] \leftarrow P$
2. For $i = (n-2)$ downto 0 do:
   $Q[0] \leftarrow \mathrm{ECDBL}(Q[0])$,
   $Q[1-d_i] \leftarrow \mathrm{ECADD}(Q[0], P)$,
3. Return$(Q[0])$.

The double-and-add-always method always computes ECADD whether $d_i = 0$ or 1. Therefore, attackers cannot guess the bit information of d using SPA.

Three more different approaches that resist the SPA have been proposed. We show several schemes used for the Weierstrass form in the following. The first one is the Montgomery-type method, which always computes both ECADD and ECDBL for bit information d_i. It was originally proposed by Montgomery [19], and enhanced the Weierstrass form of elliptic curves over K [10, 12, 1, 6]. The second one is to use an indistinguishable addition formula, with which we can compute both ECDBL and ECADD [1, 2]. The third one is to use the addition chain with fixed pattern with pre-computed points [17, 18, 21].

3.2 DPA and Countermeasures

The differential power analysis (DPA) observes many power consumptions and analyzes this information together with statistic tools. Even if a method is secure against SPA, it might not secure against the DPA. The DPA attacker tries to guess that the computation cP for an integer c is performed during the scalar multiplication. He/She gathers many power consumptions cP_i for $i = 1, 2, 3, ...$, and detects the spike arisen from the correlation function based on the specific bit of cP_i. The DPA can break Algorithm 2, because the sequence of points generated by Algorithm 2 is deterministic and the DPA can find correlation for a specific bit.

Coron pointed out that it is necessary to insert random numbers during the computation of dP to prevent DPA [5]. The randomization eliminates the correlation between the secret bit and the sequence of points. The standard randomization methods for the base point P are Coron's 3rd [5] and Joye-Tymen countermeasures [13]. The main idea of these countermeasures is to randomize the base point before starting the scalar multiplication. If the base point is randomized, there is no correlation among the power consumptions of each scalar multiplication. The DPA cannot obtain the spike of the power consumption derived from the statistical tool. We describe the two standard randomization in the following. There are other DPA countermeasures (e.g. randomized window methods [25, 9], etc), but in this paper we aim at investigating the security of Coron's 3rd and Joye-Tymen countermeasures.

Coron's 3rd Countermeasure: Coron's 3rd countermeasure is based on randomization of Jacobian (or projective) coordinates. To prevent DPA we transform $P = (x, y)$ in affine coordinate to $P = (r^2 x : r^3 y : r)$ in Jacobian coordi-

nates for a random value $r \in K^*$. This randomization produces the randomization in each representation of point and the randomization of power consumption during scalar multiplication dP.

Joye-Tymen Countermeasure: Joye-Tymen countermeasure uses an isomorphism of an elliptic curve [13]. For a random value $r \in K^*$, an elliptic curve $E : y^2 = x^3 + ax + b$ and the point $P = (x, y)$ can be transformed to its isomorphic class like $E' : y'^2 = x'^3 + a'x' + b'$ for $a' = r^4a,\ b' = r^6b$ and $P' = (x', y') = (r^2x, r^3y)$. Instead of computing dP, we compute $Q' = dP' = (x_{Q'}, y_{Q'})$ on E' and then pull back $Q = (x_Q, y_Q)$ by computing $x_Q = r^{-2}x_{Q'}$ and $y_Q = r^{-3}y_{Q'}$. This countermeasure can hold the Z-coordinate equal to 1 during the computation of dP' and it enables good efficiency.

3.3 Goubin's Power-Analysis Attack

Goubin proposed a new power analysis using a point that can be randomized by neither Coron's 3rd nor Joye-Tymen countermeasure [7]. Goubin focused on the following two points: $(x, 0)$ and $(0, y)$. The points $(x, 0)$ and $(0, y)$ are represented by $(X : 0 : Z)$ and $(0 : Y : Z)$ in Jacobian coordinates. Even these points are randomized by Coron's 3rd countermeasure, one of the coordinate remains zero, namely $(r^2X : 0 : rZ)$ and $(0 : r^3Y : rZ)$ for some random integer $r \in K^*$. Similarly Joye-Tymen randomization cannot randomize these points. Therefore, the attacker can detect whether the point $(x, 0)$ or $(0, y)$ is used in the scalar multiplication using the DPA.

The attacker can break the secret scalar using these points as follows: For a given scalar c we can always generate a point P that satisfies $P = (c^{-1} \bmod \#E)(0, y)$, because the order of the curve $\#E$ is prime. If the attacker chooses P as the base point for the scalar multiplication, the DPA can detect whether cP is computed or not during the scalar multiplication. Then the attacker can obtain the whole secret scalar by recursively applying this process from the most significant bit. Unfortunately, Goubin has not discussed how effective his attack is. In Section 4.6, we discuss the multiplication with zero can be effectively detected for a standard implementation.

Goubin's attack is effective on the curves that have points $(x, 0)$ or $(0, y)$. The point $(x, 0)$ is not on the curves with prime order ($\neq 2$), because the order of the point $(x, 0)$ is 2. The point $(0, y)$ appears on the curve if b is quadratic residue modulo p, which is computed by solving $y^2 = b$.

4 Zero-Value Point Attack

In this section, we propose a novel attack, called the *zero-value point attack*. On the contrary to Goubin's attack, our attack utilizes the auxiliary register which takes the zero-value in the definition field. We investigate the zero-value registers that are randomized by neither Coron's 3rd nor Joye-Tymen countermeasure.

The addition formula is assembled by the operations of the base field, namely the multiplication and the addition. We have about 20 different operations of the auxiliary registers for both ECDBL and ECADD (See the addition formula in Appendix A). There are a lot of possibilities that the value of the auxiliary registers become zero. The zero-value registers of the ECDBL and those of the ECADD are quite different. We examine all possible operations that take zero in the auxiliary registers.

We show several criteria, with which the proposed attack is effective — the attack is strongly depending on the implementation of the addition formula. We list up all possible security conditions and we discuss their effectiveness. Moreover, we demonstrate the attack is effective on several standard curves.

4.1 Outline of Attack

We describe the outline of the zero-value point attack in the following.

The goal of the zero-value point attack is to break the secret scalar by adaptively choosing the base point Q. We assume that the scalar multiplication is computed by Algorithm 2. But, we can apply our zero-value point attack to the SPA countermeasures using the deterministic addition chain described in section 3.1. The attacker breaks the secret key from the most significant bit. The second most significant bit d_{n-2} can be broken by checking whether one of addition formulae ECDBL($2Q$), ECADD($2Q, Q$), ECDBL($3Q$), and ECADD($3Q, Q$) is computed. If we can generate the zero-value register for these addition formulae, we can detect the second most bit — $d_{n-2} = 0$ holds if ECDBL($2Q$) or ECADD($2Q, Q$) has the zero-value register, and $d_{n-2} = 1$ holds if ECDBL($3Q$) or ECADD($3Q, Q$) has the zero-value register.

Next, we assume that $(n-i-1)$ most significant bits $(d_{n-1}, \cdots, d_{i+1})_2$ of d are known. We can break the i-th bit d_i by checking whether one of ECDBL($2kQ$), ECADD($2kQ, Q$), ECDBL($(2k+1)Q$), and ECADD($(2k+1)Q, Q$) is computed, where $k = \sum_{j=i+1}^{n-1} d_j 2^{j-i-1}$. We know that $d_i = 0$ holds if ECDBL($2kQ$) or ECADD($2kQ, Q$) has the zero-value register, and $d_i = 1$ holds if ECDBL($(2k+1)Q$) or ECADD($(2k+1)Q, Q$) has the zero-value register. Therefore if we find a point P that takes the zero-value register at ECDBL, we can use the base point $Q = (c^{-1} \bmod \#E)P$ for some integer c for this attack. On the other hand, in order to use the zero-value register at ECADD, the base point Q that causes the zero-value register at ECADD(cQ, Q) must be found.

Thus the attacker has to find the points Q which cause the zero-value register at ECDBL(cQ) or ECADD(cQ, Q) for a given integer c. The ECDBL causes the zero-value register for a given one point Q, but the zero-value register for the ECADD depends on the two points Q and cQ. In this paper we call these points *zero-value point (ZVP)*.

4.2 Possible Zero-Value Points from ECDBL

We investigate the ZVP for addition formulae in Jacobian coordinates, but the same arguments apply to addition formulae in projective coordinates. We search

the zero-value points in the following. We examine all auxiliary registers of the ECDBL in Jacobian coordinates. There are 21 intermediate values for $\mathrm{ECDBL}^{\mathcal{J}}$, as described in Appendix A. We prove the following theorem.

Theorem 1. *Let E be an elliptic curve over a prime field $\mathbb{F}_p$ defined by $y^2 = x^3+ax+b$. The elliptic curve E has the zero-value point $P = (x, y)$ of $\mathrm{ECDBL}^{\mathcal{J}}(P)$ if and only if one of the following five conditions is satisfied: (ED1) $3x^2 + a = 0$, (ED2) $5x^4 + 2ax^2 - 4bx + a^2 = 0$, (ED3) the order of P is equal to 3, (ED4) $x(P) = 0$ or $x(2P) = 0$, and (ED5) $y(P) = 0$ or $y(2P) = 0$. Moreover, the zero-value points are not randomized by either Coron's 3rd or Joye-Tymen randomization.*

Conditions *(ED4)* and *(ED5)* are exactly those of Goubin's attack.

We will prove this theorem in the following. Let $P_1 = (X_1 : Y_1 : Z_1)$, and $P_3 = (X_3 : Y_3 : Z_3) = \mathrm{ECDBL}^{\mathcal{J}}(P_1)$. The intermediate values of ECDBL can be zero if and only if one of the following values is zero.

$$X_1, Y_1, Z_1, X_3, Y_3, M, -S + M^2, S - T$$

Here $Z_1 = 0$ implies $P = \mathcal{O}$, which never appears for input of $\mathrm{ECDBL}^{\mathcal{J}}(P)$. The conditions $X_1 = 0$, $Y_1 = 0$, $X_3 = 0$, and $Y_3 = 0$ are equivalent to $x(P) = 0$, $y(P) = 0$, $x(2P) = 0$, and $y(2P) = 0$ which are exactly the points discussed by Goubin. Next $M = 3X_1^2+aZ_1^4 = 0$ implies the condition $3x^2+a = 0$, which is the condition *(ED1)*. Note that neither Coron's 3rd nor Joye-Tymen randomization can randomize this point. Indeed the randomized point $(X_1' : Z_1') = (r^2X_1 : rZ_1)$ by Coron's 3rd randomization satisfies $3X_1'^2 + aZ_1'^4 = r^4(3X_1^2 + aZ_1^4) = 0$, where $r \in K^*$. The randomized point $(X_1'' : Z_1'') = (s^2X_1 : Z_1)$ and curve parameter $a'' = s^4a$ by Joye-Tymen randomization satisfies $3X_1''^2 + a''Z_1''^4 = s^4(3X_1^2+aZ_1^4) = 0$, where $s \in K^*$. The condition $-S+M^2 = 0$ implies $-4X_1Y_1^2+(3X_1^2 + aZ_1^4)^2 = 0$, which is equivalent to $-4xy^2 + (3x^2 + a)^2 = 0$, namely condition *(ED2)*. The condition $S - T = 0$ implies $x_1 = x_3$. This occurs only if $2P = \pm P$, which means $P = \mathcal{O}$ or the order of P equals to 3, namely condition *(ED3)*.

Remark 1. There are two orders of the additions to obtain $T = -2S + M^2$. $-S + M^2$ appears if we compute with the following ordered additions $W = -S + M^2$ and then $T = W - S$ as in Appendix A. If we compute $W = 2S$ and then $T = M^2 - W$, condition *(ED2)* does not appear in the ECDBL. Thus we should avoid the former order of the two additions for the implementation of ECDBL.

4.3 Possible Zero-Value Points from ECADD

We investigate the possible zero-value points from ECADD, namely all possible zero-value points P which satisfies $\mathrm{ECADD}(cP, P)$ for some integer c. We examine the addition formula in Jacobian coordinates. There are 23 auxiliary values in the ECADD, as described in Appendix A. We prove the following theorem.

Theorem 2. *Let E be an elliptic curve over prime field $\mathbb{F}_p$ defined by $y^2 = x^3 + ax + b$. The elliptic curve E has the zero-value point $P = (x, y)$ of* $\mathrm{ECADD}^{\mathcal{J}}(cP, P)$ *for some $c \in \mathbb{Z}$ if and only if one of the following seven conditions is satisfied: (EA1) P is a y-coordinate self-collision point, (EA2) $x(cP) + x(P) = 0$, (EA3) $x(P) - x(cP) = \lambda(P, cP)^2$, (EA4) $2x(cP) = \lambda(P, cP)^2$, $x(cP) = \lambda(P, cP)^2$, or $x(P) = \lambda(P, cP)^2$, (EA5) the order of P is $2c+1$, (EA6) $x(cP) = 0$, $x(P) = 0$, or $x((c+1)P) = 0$, and (EA7) $y(cP) = 0$, $y(P) = 0$, or $y((c+1)P) = 0$. Moreover, the zero-value points are not randomized by either Coron's 3rd or Joye-Tymen randomization.*

A point $P = (x, y)$ is called the y-coordinate self-collision point if there is a positive integer c such that the y-coordinate of the point cP is equal to y. Conditions *(EA6)* and *(EA7)* are those of Goubin's attack.

Let $P_1 = (X_1 : Y_1 : Z_1)$, $P_2 = (X_2 : Y_2 : Z_2)$, and $\mathrm{ECADD}^{\mathcal{J}}(P_1, P_2) = (X_3 : Y_3 : Z_3)$. Here we can set $P_1 = cP_2$ for some integer c. If one of the following values is zero, at least one of the intermediate values must be zero.

$$X_1, Y_1, Z_1, X_2, Y_2, Z_2, X_3, Y_3, H, R, U_1H^2 - X_3.$$

Here if one of $X_1, Y_1, X_2, Y_2, X_3, Y_3$ is zero, this provides conditions *(EA6)* and *(EA7)*. $Z_1 = 0$, $Z_2 = 0$ and $H = 0$ imply $P_1 = \mathcal{O}$, $P_2 = \mathcal{O}$, and $P_1 = \pm P_2$, respectively, which never appear for input of $\mathrm{ECADD}^{\mathcal{J}}(P_1, P_2)$. Next, $R = Y_1Z_2^3 - Y_2Z_1^3 = 0$ implies $y_1 = y_2$, where $y_1 = Y_1/Z_1^3$ and $y_2 = Y_2/Z_2^3$, namely condition *(EA1)*. This is equal to the y-coordinate collision point. Note that neither Coron's 3rd nor Joye-Tymen randomization can randomize this point. Indeed the randomized point $(Y_1' : Z_1') = (r^3Y_1 : rZ_1), (Y_2' : Z_2') = (s^3Y_2 : sZ_2)$ by Coron's 3rd randomization satisfies $Y_1'Z_2'^3 - Y_2'Z_1'^3 = r^3s^3(Y_1Z_2^3 - Y_2Z_1^3) = 0$, where $r, s \in K^*$. The randomized point $(Y_1'' : Z_1'') = (t^3Y_1 : Z_1), (Y_2'' : Z_2'') = (t^3Y_2 : Z_2)$ by Joye-Tymen randomization satisfies $Y_1''Z_2''^3 - Y_2''Z_1''^3 = t^3(Y_1Z_2^3 - Y_2Z_1^3) = 0$, where $t \in K^*$. Finally $U_1H^2 - X_3 = 0$ implies $3U_1H^2 + H^3 - R^2 = 0$, which is $x_1 - x_3 = 0$. This occurs only if $(c+1)P = \pm cP$, which means $P = \mathcal{O}$ or the order of P equals to $2c + 1$, namely condition *(EA5)*.

The other possible intermediate values appear only at the computation of $X_3 = -H^3 - 2U_1H^2 + R^2$. For $\mathrm{ECADD}^{\mathcal{J}}$ in Appendix A, we compute $-H^3 + R^2$, but we can differently implement it. We have 6 possible conditions:

$$\begin{aligned}
&(a1) - H^3 - 2U_1H^2 = 0, \quad (a2) - 2U_1H^2 + R^2 = 0,\\
&(a3) - H^3 + R^2, = 0 \quad (a4) - H^3 - U_1H^2 = 0,\\
&(a5) - U_1H^2 + R^2 = 0, \quad (a6)(-H^3 - U_1H^2) + R^2 = 0.
\end{aligned}$$

We examine these conditions in the following. These above points are randomized by neither Coron 3rd nor Joye-Tymen randomization. Condition *(a1)* implies $H(X_2Z_1^2 + X_1Z_2^2) = 0$, namely $H = 0$ or $x_1 + x_2 = 0$ in affine coordinate. The condition $H = 0$ has already appeared. $x_1 + x_2 = 0$ implies $x(cP) + x(P) = 0$, which is equal to condition *(EA2)*. Condition *(a2)* implies $-2X_1Z_2^2(X_2Z_1^2 - X_1Z_2^2)^2 + (Y_2Z_1^3 - Y_1Z_2^3)^2 = 0$, which is $2x_1 = \lambda^2$ in affine coordinate. It is

condition *(EA4)*. Condition *(a3)* implies $-(X_2Z_1^2-X_1Z_2^2)^3+(Y_2Z_1^3-Y_1Z_2^3)^2=0$, which is $x_2-x_1=\lambda(P_2,P_1)^2$, namely condition *(EA3)*. Condition *(a4)* implies $H=0$ or $U_2=0$, which has already discussed. Condition *(a5)* is converted to $-X_1Z_2^2(X_2Z_1^2-X_1Z_2^2)^2+(Y_2Z_1^3-Y_1Z_2^3)^2=0$, which is $x_1=\lambda^2$ in affine coordinate. It is equal to condition *(EA4)*. Condition *(a6)* implies $-(X_2Z_1^2-X_1Z_2^2)^3-X_1Z_2^2(X_2Z_1^2-X_1Z_2^2)^2+(Y_2Z_1^3-Y_1Z_2^3)^2=0$, which is $x_2=\lambda(P_2,P_1)^2$ in affine coordinate. It is equal to condition *(EA4)*.

Remark 2. If we implement the addition $-H^3-2U_1H^2+R^2$ with either condition *(a1)*, *(a2)*, or *(a3)*, then conditions *(a4)*, *(a5)*, and *(a6)* never appear in ECADD. Condition *(a1)*, *(a2)*, and *(a3)* are never simultaneously satisfied — only one of them can be occurred. For example, the implementation of ECADD in Appendix A uses *(a3)*, and thus the other conditions will never appear. The security of ECADD against the zero-value point attack strongly depends on its implementation, and we should care how to implement it.

4.4 How to Find the ZVP

We discuss how to find the ZVP described in the previous sections. A zero-value point is called as trivial, if the order of the point is smaller than that of the curve. The standard curves over prime fields have prime order, i.e., the orders of these elliptic curves are always prime and there is no trivial ZVP on them. Goubin's point $(0,y)$ is a non-trivial point. In the following we discuss the non-trivial ZVP that is different from Goubin's point.

First we discuss the non-trivial ZVP from ECDBL. There are two non-trivial points (x,y) such that *(ED1)* $3x^2+a=0$, *(ED2)* $5x^4+2ax^2-4bx+a^2=0$. The solution of these polynomials over finite fields can be easily computed using the Cantor-Zassenhaus algorithm [3].

Next we discuss the non-trivial ZVP from ECADD. The existence conditions of these points are determined by not only one base point P but also the scalar c. In order to find these ZVP we have to know how to represent the relation between P and cP, for example, $x(cP)+x(P)=0$. Izu and Takagi discussed a similar self-collision for Brier-Joye addition formula [11]. Here we can similarly apply their approach to finding the ZVP. We explain it in the following. Let $P=(x,y)$ be the point on the elliptic curve. The division polynomial $\psi(P)$, $\phi(P)$, $\omega(P)$ is a useful tool for representing these relationships as the polynomials over the definition field K. The point cP can be represented as follows:

$$cP=\left(\frac{\phi_c(P)}{\psi_c^2(P)},\frac{\omega_c(P)}{\psi_c^3(P)}\right)$$

where c is a scalar value (see for example, [22]). For small c, we know $\psi_1(P)=1,\psi_2(P)=2y$, and $\psi_3(P)=3x^4+6ax^2+12bx-a^2$, where $P=(x,y)$. We define $\phi_c=x\psi_c^2-\psi_{c-1}\psi_{c+1}$ and $4y\omega_c=\psi_{c+2}\psi_{c-1}^2-\psi_{c-2}\psi_{c+1}^2$.

For example, the points $P=(x,y)$ which satisfy $x(cP)+x(P)=0$ are the solutions of $\phi_c(P)+x(P)\psi_c^2(P)=0$. The points $P=(x,y)$ with $x(P)-$

$x(cP) = \lambda(P, cP)^2$ are the solutions of polynomial $(x(P)\psi_c^2(P) - \phi_c(P))^3 = (y(P)\psi_c^3(P) - \omega_c(P))^2$. Similarly we can construct the equations whose solutions imply the ZVP. The polynomials $\psi_c(P), \omega_c(P), \phi_c(P)$ have degree with order $\mathcal{O}(c^2)$, which increases exponentially in $\log c$. Therefore, it is a hard problem to fin the solutions of these equations for a large c — we can find the ZVP only for a small c using the division polynomials. It is an open problem to find a more efficient algorithm of computing the ZVP.

4.5 ZVP on Standard Curves

We have examined the existence of several ZVP over the SECG [23] random curves over prime fields. Especially we discuss the non-trivial conditions from ECDBL$^{\mathcal{J}}$, namely *(ED1)* $3x^2 + a = 0$, *(ED2)* $5x^4 + 2ax^2 - 4bx + a^2 = 0$. These conditions are most effectively used for the proposed zero-value point attack. We have found enough curves which have the points with condition *(ED1)* or *(ED2)*. In Table 1 we summarize the existence of these points. Notation 'o' means that the curve has the point with one of the aforementioned conditions. For comparison we also show point $(0, y)$ used in Goubin's attack in Table 1. Some curves, e.g., secp112r1, secp224r1, are secure against Goubin's attack, but not against ours. SECG secp224r1 is insecure only against condition *(ED2)*.

	$(0, y)$	*(ED1)*	*(ED2)*
SECG secp112r1	-	o	o
SECG secp128r1	o	-	-
SECG secp160r1	o	-	-
SECG secp160r2	o	-	o
SECG secp192r1	o	o	o
SECG secp224r1	-	-	o
SECG secp256r1	o	-	o
SECG secp384r1	o	o	-
SECG secp521r1	o	o	-

Table 1. The existence of non-trivial ZVP of ECDBL$^{\mathcal{J}}$

4.6 Detecting the Zero-Value Registers

We discuss how the DPA can detect the multiplication or the addition with the zero-value register on memory constrained devices such as smart cards.

The embedded CPU on a smart card, typically an 8 bit CPU, has only so poor computing power that we usually equip a coprocessor for implementing ECC. In the coprocessor, a multiplication circuit and an addition circuit are generally embedded for computing the modular multiplication and the modular addition of the base field $\mathbb{F}_p$, respectively. These circuits compute the outputs by inputting two k-bit values, where we usually choose $k = 32$. The power consumption of

the multiplication circuit might be dominant for the whole power consumption of the device.

The modular multiplication algorithm suitable for the multiplication circuit is the Montgomery multiplication [16]. Algorithm 3 describes the Montgomery multiplication using a k bit multiplication circuit. The computations of $x_j y_i$, $a_0 m'$, and $m_j u_i$ at Step 2 use the k multiplication circuit.

Algorithm 3: Montgomery multiplication

Input: $M = (m_{n-1} \cdots m_0)_b,\ X = (x_{n-1} \cdots x_0)_b,\ Y = (y_{n-1} \cdots y_0)_b,\ b = 2^k,$
$R = b^n,\ \gcd(m, b) = 1,\ m' = m^{-1} \bmod b.$
Output: $XYR^{-1} \bmod M$.
1. $A \leftarrow 0$ $(A = (a_n \cdots a_0)_b)$.
2. For i from 0 to $(n-1)$ do:
  $temp \leftarrow 0$,
  For j from 0 to $(n-1)$ do:
    $\{temp, a_j\} \leftarrow x_j y_i + a_j + temp$,
  $a_n \leftarrow temp,\ temp \leftarrow 0,\ u_i \leftarrow a_0 m' \bmod b$,
  For j from 0 to n do:
    $\{temp, a_j\} \leftarrow m_j u_i + a_j + temp$,
  $A \leftarrow A/b$.
3. If $A \geq M$, $A \leftarrow A - M$.
4. Return(A).

Suppose that one of the input X, Y in the Montgomery multiplication equals to 0. If the input X (or Y) is 0, then values x_j (or y_j), a_0, and u_i at Step 2 always take 0, respectively. Therefore, one of the inputs of the multiplication circuit is always 0 during the computation of the Montgomery multiplication.

We explain the implication of this zero input for the multiplication circuit in the following. A 32-bit multiplication circuit comprises three parts (see [24] for example): (1) AND gates for partial products, (2) carry-save adder trees such as Wallace trees, and (3) fast carry propagate adder. The gate counts of these three parts are roughly estimated to about 2K ,7K, and 1K gates, respectively. If one of the inputs to the multiplication circuit is 0, then it behaves as follows: The output of the AND gate (1) always takes 0 though the other input varies. The inputs and outputs of both the carry save adder (2) and fast carry propagate adder (3) are always 0. This means that the power consumption of first part considerably decreases, and those of the latter two parts are almost nothing during the computation of Montgomery multiplication. Thus the power consumption of the zero-value multiplication dramatically decreases, namely more than 80%. We guess that the attacker can distinguish it only by the single observation of the power consumption.

On the other hand, modular addition ($X + Y \bmod M$) and subtraction ($X - Y \bmod M$) is implemented by using k bit addition circuit. If one of the input X, Y in modular addition or subtraction equals to zero, one of the inputs of addition circuit is always 0 during the computation of $X + Y$ or $X - Y$. Thus, the power consumption of the addition circuit considerably decreases. However, because the gate counts of the addition circuit are much smaller than those of

the multiplication circuit, it does not reflect the whole power consumption as the case of modular multiplication. Thus, the attacker makes much more efforts in order to detect the modular addition and subtraction with the zero value comparing with the modular multiplication with the zero value.

In the standard curves such as SECG [23] random curves over prime fields, the prime p is chosen to be a Mersenne-like prime because of efficient modular reduction. In this case, the multiplication circuit is used only for the multiplication $X \cdot Y$. Therefore, the modular multiplication with the zero value can be also detected efficiently.

5 Application to Other Classes

In this section we discuss how the zero-value point attack is effective on other classes of ECC. The Montgomery-type methods and the curves over $\mathbb{F}_{2^n}$ are investigated. The analyses of the zero-value points for these classes are quite similar that of Jacobian coordinates over prime fields. We examine all possible zero-value register randomized by neither Coron's 3rd nor Joye-Tymen countermeasure.

5.1 Montgomery-Type Method

We investigate the ZVP over the Montgomery-type method. It was originally proposed by Montgomery [19], and enhanced the Weierstrass form of elliptic curves over K [10, 12, 1, 6]. The scalar multiplication is computed as follows:

Algorithm 4: Montgomery-type method

Input: $d = (d_{n-1} \cdots d_1 d_0)_2,\ P \in E(K)\ \ (d_{n-1} = 1)$.
Output: dP.
1. $Q[0] \leftarrow P,\ Q[1] \leftarrow \mathrm{mECDBL}(P)$
2. For $i = (n-2)$ downto 0 do:
   $Q[1-d_i] \leftarrow \mathrm{mECADD}(Q[0], Q[1])$,
   $Q[d_i] \leftarrow \mathrm{mECDBL}(Q[d_i])$.
3. Return$(Q[0])$.

mECADD and mECDBL are the special elliptic curve addition and doubling for the Montgomery-type method. In this method, we don't need to use y-coordinate (Y-coordinate in projective coordinates) to compute the scalar multiplication dP. This leads the efficiency of the Montgomery-type method. Let $P_1 = (X_1 : Z_1)$ and $P_2 = (X_2 : Z_2)$ in projective coordinates, which don't equal to $\mathcal{O}$, by setting $x = X/Z$. In the following we describe the doubling formula $P_3 = (X_3 : Z_3) = 2P_1$ and the addition formula $P_3 = (X_3 : Z_3) = P_1 + P_2$, where $P_1 \neq \pm P_2$ and ${P_3}' = ({X_3}' : {Z_3}') = P_2 - P_1$ where $(X_3', Z_3' \neq 0)$. There are also several variations of these formulae [10, 12, 1, 6].

ECDBL in Montgomery-Type Method ($\mathrm{mECDBL}^{\mathcal{P}}$) :
$X_3 = ({X_1}^2 - a{Z_1}^2)^2 - 8bX_1{Z_1}^3$, $Z_3 = 4(X_1Z_1({X_1}^2 + a{Z_1}^2) + b{Z_1}^4)$.

ECADD in Montgomery-Type Method ($\mathrm{mECADD}^{\mathcal{P}}$) :
$X_3 = Z_3'((X_1X_2 - aZ_1Z_2)^2 - 4bZ_1Z_2(X_1Z_2 + X_2Z_1))$, $Z_3 = X_3'(X_1Z_2 - X_2Z_1)^2$.

If the base point is chosen as $P = (0, y)$, this addition formula $\mathrm{mECADD}^{\mathcal{P}}$ causes error at the end of scalar multiplication due to the zero Z-coordinate. This point should not be used for the base point.

The Montgomery-type method always computes mECADD and mECDBL whether $d_i = 0$ or 1. Therefore, attackers cannot guess the bit information of d using SPA (see [10, 12, 1, 6] for further discussions). We can enhance SPA-resistance to DPA-resistance by applying either Coron's 3rd or Joye-Tymen countermeasure to the Montgomery-type method.

Here we investigate the zero-value points for $\mathrm{mECDBL}^{\mathcal{P}}$ and $\mathrm{mECADD}^{\mathcal{P}}$ in the following. We assume that $(n-i-1)$ most significant bits $(d_{n-1}, \cdots, d_{i+1})_2$ of d are known, and let $k = \sum_{j=i+1}^{n-1} d_j 2^{j-i-1}$. If $d_i = 0$, $\mathrm{mECDBL}^{\mathcal{P}}(kP)$ at i-th loop and $\mathrm{mECADD}^{\mathcal{P}}(2kP, (2k+1)P)$ at $(i-1)$-th loop will be computed. On the contrary, if $d_i = 1$, $\mathrm{mECDBL}^{\mathcal{P}}((k+1)P)$ at i-th loop and $\mathrm{mECADD}^{\mathcal{P}}((2k+1)P, (2k+2)P)$ at $(i-1)$-th loop will be computed. Thus the attacker can detect the i-th bit d_i by checking whether one of $\mathrm{mECDBL}^{\mathcal{P}}(kP)$, $\mathrm{mECDBL}^{\mathcal{P}}((k+1)P)$, $\mathrm{mECADD}^{\mathcal{P}}(2kP, (2k+1)P)$, $\mathrm{mECADD}^{\mathcal{P}}((2k+1)P, (2k+2)P)$ is computed. We investigate the ZVP at $\mathrm{mECDBL}^{\mathcal{P}}(P)$ and $\mathrm{mECADD}^{\mathcal{P}}(cP, (c+1)P)$ for given integer c in following two theorems. We prove these two theorems in Appendix B.

Theorem 3. *Let E be an elliptic curve over a prime field $\mathbb{F}_p$ defined by $y^2 = x^3+ax+b$. The elliptic curve E has the zero-value point $P = (x, y)$ of* $\mathrm{mECDBL}^{\mathcal{P}}$ *(P) if and only if one of the following four conditions is satisfied: (MD1) $x^2 - a = 0$, (MD2) $x^2 + a = 0$, (MD3) $x(P) = 0$ or $x(2P) = 0$, and (MD4) $y(P) = 0$. Moreover, the zero-value points are not randomized by either Coron's 3rd or Joye-Tymen randomization.*

Theorem 4. *Let E be an elliptic curve over a prime field $\mathbb{F}_p$ defined by $y^2 = x^3+ax+b$. The elliptic curve E has the zero-value point $P = (x, y)$ of* $\mathrm{mECADD}^{\mathcal{P}}$ *$(cP, (c+1)P)$ for $c \in \mathbb{Z}$ if and only if one of the following three conditions is satisfied: (MA1) $x(cP)x((c+1)P) = a$, (MA2) $x(cP) + x((c+1)P) = 0$, and (MA3) $x(cP) = 0$, $x((c+1)P) = 0$, or $x((2c+1)P) = 0$. Moreover, the zero-value points are not randomized by either Coron's 3rd or Joye-Tymen randomization.*

The conditions in Theorem 3 and Theorem 4 are different from those of the standard addition formula. The zero-value point attack strongly depends on the structure of the addition formula.

5.2 Curves over $\mathbb{F}_{2^n}$

We investigate the ZVP over ECC over binary fields $\mathbb{F}_{2^n}$.

An elliptic curve over $\mathbb{F}_{2^n}$ is defined as $E : y^2 + xy = x^3 + ax^2 + b$, where $a, b \in \mathbb{F}_{2^n}$ and $b \neq 0$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E

that don't equal to $\mathcal{O}$. The sum $P_3 = P_1 + P_2 = (x_3, y_3)$ can be computed as $x_3 = \lambda(P_1, P_2)^2 + \lambda(P_1, P_2) + x_1 + x_2 + a$, $y_3 = \lambda(P_1, P_2)(x_1 + x_3) + x_3 + y_1$, where $\lambda(P_1, P_2) = y_1/x_1 + x_1$ for $P_1 = P_2$ and $\lambda(P_1, P_2) = (y_1 + y_2)/(x_1 + x_2)$ for $P_1 \neq \pm P_2$. In ECC over $\mathbb{F}_{2^n}$, most efficient addition and doubling formulae for the double-and-add-always method was proposed by López and Dahab [14]. In this paper, affine coordinate (x, y) is transformed into projective coordinates $(X : Y : Z)$ by setting $x = X/Z$ and $y = Y/Z^2$. Let $P_1 = (X_1 : Y_1 : Z_1)$, $P_2 = (X_2 : Y_2 : Z_2)$, and $P_3 = P_1 + P_2 = (X_3 : Y_3 : Z_3)$. The doubling and addition formulae can be presented as follows.

ECDBL in Projective Coordinates ($\mathrm{ECDBL}_{2^n}^{\mathcal{P}}$) :
$X_3 = {X_1}^4 + b{Z_1}^4$, $Y_3 = b{Z_1}^4 Z_3 + X_3(aZ_3 + {Y_1}^2 + b{Z_1}^4)$, $Z_3 = {X_1}^2{Z_1}^2$.

ECADD in Projective Coordinates ($\mathrm{ECADD}_{2^n}^{\mathcal{P}}$) :
$X_3 = C^2 + H + G$, $Y_3 = HI + Z_3 J$, $Z_3 = F^2$,
$A_1 = Y_1{Z_2}^2$, $A_2 = Y_2{Z_1}^2$, $B_1 = X_1 Z_2$, $B_2 = X_2 Z_1$, $C = A_1 + A_2$, $D = B_1 + B_2$,
$E = Z_1 Z_2$, $F = DE$, $G = D^2(F + aE^2)$, $H = CF$, $I = D^2 B_1 E + X_3$,
$J = D^2 A_1 + X_3$

The combination of the double-and-add-always method and Coron's 3rd countermeasure was considered to achieve DPA resistance. However, Goubin's attack can break this DPA resistance. Moreover, we investigate the ZVP in following two theorems. We prove these two theorems in Appendix B.

Theorem 5. *Let E be an elliptic curve over a binary field $\mathbb{F}_{2^n}$ defined by $y^2 + xy = x^3 + ax^2 + b$. The elliptic curve E has the zero-value point $P = (x, y)$ of $\mathrm{ECDBL}_{2^n}^{\mathcal{P}}(P)$ if and only if one of the following four conditions is satisfied: (BD1) $x^2 + y = 0$, (BD2) $ax^2 + y^2 = 0$, $ax^2 + b = 0$ or $y^2 + b = 0$ (BD3) $x(P) = 0$ or $x(2P) = 0$, and (BD4) $y(P) = 0$ or $y(2P) = 0$. Moreover, the zero-value points are not randomized by Coron's 3rd randomization.*

Theorem 6. *Let E be an elliptic curve over a binary field $\mathbb{F}_{2^n}$ defined by $y^2 + xy = x^3 + ax^2 + b$. The elliptic curve E has the zero-value point $P = (x, y)$ of $\mathrm{ECADD}_{2^n}^{\mathcal{P}}(cP, P)$ if and only if one of the following seven conditions is satisfied: (BA1) P is a y-coordinate self-collision point, (BA2) $x(cP) + x(P) + a = 0$, (BA3) $\lambda(cP, P) = 1$, $\lambda(cP, P)^2 = x(cP) + x(P) + a$ or $\lambda(cP, P) = x(cP) + x(P) + a$, (BA4) the order of P is $2c+1$, (BA5) $y(cP) + x((c+1)P) = 0$, (BA6) $x(cP) = 0$, $x(P) = 0$, or $x((c+1)P) = 0$, and (BA7) $y(cP) = 0$, $y(P) = 0$, or $y((c+1)P) = 0$. Moreover, the zero-value points are not randomized by Coron's 3rd randomization.*

The conditions in Theorem 5 and Theorem 6 are also different from those of the standard addition formula or the Montgomery-type Method of the curves over prime fields. A different implementation of addition formula might cause the different zero-value point attack. Finally we point out that there is no ZVP other than Goubin's point $(0, y)$ for the Montgomery-type method over $\mathbb{F}_{2^m}$ proposed by López and Dahab [15].

6 Conclusion

We presented the zero-value point attack on elliptic curve cryptosystem, which detect the zero-value auxiliary registers of the addition formulae. These points can be randomized by neither Coron's 3rd nor Joye-Tymen countermeasure, and we can detect these operations using the DPA. We have found the several non-trivial points P, which take the zero-value, namely $(1)3x^2 + a = 0$, $(2)5x^4 + 2ax^2 - 4bx + a^2 = 0$, $(3)P$ is a y-coordinate self-collision point, etc. These points exist on several standard curves from SECG. Moreover, we showed the zero-value points for the other classes, e.g., the Mongomery-type method and ECC over finite field $\mathbb{F}_{2^m}$. These conditions provide us new security criteria for the secure implementation of ECC.

We should care the zero-value point attack under the computation environment allowed to perform the DPA. The zero-value point attack could be resisted if we randomized the scalar. We should randomize not only the base point but also the secret scalar.

References

1. É. Brier and M. Joye, "Weierstrass Elliptic Curve and Side-Channel Attacks", *Public Key Cryptography - PKC 2002*, LNCS 2274, pp. 335-345, Springer-Verlag, 2002.
2. C. Clavier and M. Joye, "Universal exponentiation algorithm", *Cryptographic Hardware and Embedded Systems - CHES 2001*, LNCS 2162, pp.300-308, Springer-Verlag, 2001.
3. H. Cohen, *Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Vol. 138, Springer-Verlag, 1994.
4. H. Cohen, A. Miyaji, and T. Ono, "Efficient Elliptic Curve Exponentiation Using Mixed Coordinates", *Advances in Cryptography - ASIACRYPT '98*, LNCS 1514, pp. 51-65, Springer-Verlag, 1998.
5. J.-S. Coron, "Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems", *Cryptographic Hardware and Embedded Systems - CHES '99*, LNCS 1717, pp. 292-302, Springer-Verlag, 2002.
6. W. Fischer, C. Giraud, E. W. Knundsen, and J. -P. Seifert, "Parallel Scalar Multiplication on General Elliptic Curves over $\mathbb{F}_p$ Hedged against Non-Differential Side-Channel Attacks", IACR Cryptology ePrint Archive 2002/007. http://eprint.iacr.org/2002/007/
7. L. Goubin, "A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems", *Public Key Cryptography - PKC 2003*, LNCS 2567, pp. 199-211, Springer-Verlag, 2003.
8. K. Itoh, T. Izu, and M. Takenaka, "Address-bit Differential Power Analysis on Cryptographic Schemes OK-ECDH and OK-ECDSA", to appear in *Workshop on Cryptographic Hardware and Embedded Systems 2002 - CHES 2002*, 2002.
9. K. Itoh, J. Yajima, M. Takenaka, and N. Torii, "DPA Countermeasures by improving the window method", to appear in *Workshop on Cryptographic Hardware and Embedded Systems 2002 - CHES 2002*, 2002.
10. T. Izu and T. Takagi, "A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks", *Public Key Cryptography - PKC 2002*, LNCS 2274, pp. 280-296, Springer-Verlag, 2002.

11. T. Izu and T. Takagi, "Exceptional Procedure Attack on Elliptic Curve Cryptosystems", *Public Key Cryptography - PKC 2003*, LNCS 2567, pp. 224-239, Springer-Verlag, 2003.
12. T. Izu, B, Möller, and T. Takagi, "Improved Elliptic Curve Multiplication Methods Resistant against Side Channel Attacks", *Progress in Cryptology - INDOCRYPT 2002*, LNCS 2551, pp. 296-313, Springer-Verlag, 2002.
13. M. Joye and C. Tymen, "Protection against Differential Analysis for Elliptic Curve Cryptography", *Cryptographic Hardware and Embedded Systems - CHES 2001*, LNCS 2162, pp. 377-390, 2001.
14. J. López and R. Dahab, "Improved Algorithms for Elliptic Curve Arithmetic in $GF(2^n)$", *Selected Areas in Cryptography - SAC '98*, LNCS 1556, pp. 201-212, Springer-Verlag, 1999.
15. J. López and R. Dahab, "Fast Multiplication on Elliptic Curves over $GF(2^m)$ without Precomputation", *Cryptographic Hardware and Embedded Systems - CHES '99*, LNCS 1717, pp. 316-327, 1999.
16. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
17. B. Möller, "Securing Elliptic Curve Point Multiplication against Side-Channel Attacks", *Information Security - ISC 2001*, LNCS 2200, pp.324-334, 2001.
18. B. Möller, "Parallelizable Elliptic Curve Point Multiplication Method with Resistance against Side-Channel Attacks", *Information Security - ISC 2002*, LNCS 2433, pp.402-413, 2002.
19. P. L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization", *Mathematics of Computation*, vol. 48, pp. 243-264, 1987.
20. K. Okeya and K. Sakurai, "Power Analysis Breaks Elliptic Curve Cryptosystems even Secure against the Timing Attack", *Progress in Cryptology - INDOCRYPT 2000*, LNCS 1977, pp. 178-190, Springer-Verlag, 2000.
21. K. Okeya and T. Takagi, "The Width-w NAF Method Provides Small Memory and Fast Elliptic Scalar Multiplications Secure against Side Channel Attacks", to appear in *Cryptographer's Track RSA Conference - CT-RSA 2003*, 2003.
22. J. Silverman, *The Arithmetic of Elliptic Curves*, GMT 106, Springer-Verlag, 1986.
23. Standard for Efficient Cryptography (SECG), *SEC2: Recommended Elliptic Curve Domain Parameters*, Version 1.0, 2000. http://www.secg.org/
24. C. S. Wallace, "A Suggestion for a Fast Multiplier", *IEEE Trans. Electron. Comput.*, pp. 14-17, 1964.
25. C. Walter, "MIST: An Efficient, Randomized Exponentiation Algorithm for Resisting Power Analysis", *Cryptographer's Track RSA Conference - CT-RSA 2002*, LNCS 2271, pp.53-66, 2002.

Appendix A

In this appendix we describe an implementation of ECDBL and ECADD in the Jacobian coordinate. The addition formulae are assembled by the basic arithmetic of the definition field, namely the addition $+$, the subtraction $-$, and the multiplication $\times$.

ECDBL$^{\mathcal{J}}$	
Input (X_1, Y_1, Z_1, a)	
Output (X_3, Y_3, Z_3)	
$T_4 \leftarrow X_1, T_5 \leftarrow Y_1, T_6 \leftarrow Z_1$	
$T_1 \leftarrow T_4 \times T_4;$	$(= X_1^2)$
$T_2 \leftarrow T_5 \times T_5;$	$(= Y_1^2)$
$T_2 \leftarrow T_2 + T_2;$	$(= 2Y_1^2)$
$T_4 \leftarrow T_4 \times T_2;$	$(= 2X_1Y_1^2)$
$T_4 \leftarrow T_4 + T_4;$	$(= 4X_1Y_1^2 = S)$
$T_2 \leftarrow T_2 \times T_2;$	$(= 4Y_1^4)$
$T_2 \leftarrow T_2 + T_2;$	$(= 8Y_1^4)$
$T_3 \leftarrow T_6 \times T_6;$	$(= Z_1^2)$
$T_3 \leftarrow T_3 \times T_3;$	$(= Z_1^4)$
$T_6 \leftarrow T_5 \times T_6;$	$(= Y_1Z_1)$
$T_6 \leftarrow T_6 + T_6;$	$(= 2Y_1Z_1)$
$T_5 \leftarrow T_1 + T_1;$	$(= 2X_1^2)$
$T_1 \leftarrow T_1 + T_5;$	$(= 3X_1^2)$
$T_3 \leftarrow a \times T_3;$	$(= aZ_1^4)$
$T_1 \leftarrow T_1 + T_3;$	$(= 3X_1^2 + aZ_1^4 = M)$
$T_3 \leftarrow T_1 \times T_1;$	$(= M^2)$
$T_3 \leftarrow T_3 - T_4;$	$(= -S + M^2)$
$T_3 \leftarrow T_3 - T_4;$	$(= -2S + M^2 = T)$
$T_4 \leftarrow T_4 - T_3;$	$(= S - T)$
$T_1 \leftarrow T_1 \times T_4;$	$(= M(S - T))$
$T_4 \leftarrow T_1 - T_2;$	$(= 8Y_1^4 - M(S - T))$
$X_2 \leftarrow T_3, Y_2 \leftarrow T_4, Z_2 \leftarrow T_6$	

ECADD$^{\mathcal{J}}$	
Input $(X_1, Y_1, Z_1, X_2, Y_2, Z_2)$	
Output (X_3, Y_3, Z_3)	
$T_2 \leftarrow X_1, T_3 \leftarrow Y_1, T_4 \leftarrow Z_1, T_5 \leftarrow X_2, T_6 \leftarrow Y_2, T_7 \leftarrow Z_2$	
$T_1 \leftarrow T_7 \times T_7;$	$(= Z_2^2)$
$T_2 \leftarrow T_2 \times T_1;$	$(= X_1Z_2^2 = U_1)$
$T_3 \leftarrow T_3 \times T_7;$	$(= Y_1Z_2)$
$T_3 \leftarrow T_3 \times T_1;$	$(= Y_1Z_2^3 = S_1)$
$T_1 \leftarrow T_4 \times T_4;$	$(= Z_1^2)$
$T_5 \leftarrow T_5 \times T_1;$	$(= X_2Z_1^2 = U_2)$
$T_6 \leftarrow T_6 \times T_4;$	$(= Y_2Z_1)$
$T_6 \leftarrow T_6 \times T_1;$	$(= Y_2Z_1^3 = S_2)$
$T_5 \leftarrow T_5 - T_2;$	$(= U_2 - U_1 = H)$
$T_7 \leftarrow T_4 \times T_7;$	$(= Z_1Z_2)$
$T_7 \leftarrow T_5 \times T_7;$	$(= Z_1Z_2H = Z_3)$
$T_6 \leftarrow T_6 - T_3;$	$(= S_2 - S_1 = R)$
$T_1 \leftarrow T_5 \times T_5;$	$(= H^2)$
$T_4 \leftarrow T_6 \times T_6;$	$(= R^2)$
$T_2 \leftarrow T_2 \times T_1;$	$(= U_1H^2)$
$T_5 \leftarrow T_1 \times T_5;$	$(= H^3)$
$T_4 \leftarrow T_4 - T_5;$	$(= -H^3 + R^2)$
$T_1 \leftarrow T_2 + T_2;$	$(= 2U_1H^2)$
$T_4 \leftarrow T_4 - T_1;$	$(= -H^3 - 2U_1H^2 + R^2 = X_3)$
$T_2 \leftarrow T_2 - T_4;$	$(= U_1H^2 - X_3)$
$T_6 \leftarrow T_6 \times T_2;$	$(= R(U_1H^2 - X_3))$
$T_1 \leftarrow T_3 \times T_5;$	$(= S_1H^3)$
$T_1 \leftarrow T_6 - T_1;$	$(= -S_1H^3 + R(U_1H^2 - X_3))$
$X_3 \leftarrow T_4, Y_3 \leftarrow T_1, Z_3 \leftarrow T_7$	

Appendix B

Proof of Theorem 3

The intermediate values can be zero if and only if one of the following value are zero.

$$X_1, Z_1, X_3, Z_3, {X_1}^2 - a{Z_1}^2, {X_1}^2 + a{Z_1}^2$$

Here $Z_1 = 0$ implies $P = \mathcal{O}$, which can be discarded. $X_1 = 0$ and $X_3 = 0$ are equivalent to $x(P) = 0$ and $x(2P) = 0$, namely conditions *(MD3)*. $Z_3 = 0$ implies $X_1 Z_1({X_1}^2 + a{Z_1}^2) + b{Z_1}^4 = 0$, namely ${x_1}^3 + ax_1 + b = 0$. This is equivalent to $y_1 = 0$, namely *(MD4)*.

Next ${X_1}^2 - a{Z_1}^2 = 0$ implies ${x_1}^2 - a = 0$, where $x_1 = X_1/Z_1$, namely *(MD1)*. Note that neither the Coron's 3rd nor the Joye-Tymen countermeasure can randomize the points. Indeed the randomized point $(X_1' : Z_1') = (rX_1 : rZ_1)$ by the Coron's 3rd countermeasure satisfies ${X_1'}^2 - a{Z_1'}^2 = r^2({X_1}^2 - a{Z_1}^2) = 0$, where $r \in K^*$. The randomized point $(X_1'' : Z_1'') = (s^2 X_1 : Z_1)$ and curve parameter $a'' = s^4 a$ by the Joye-Tymen countermeasure satisfies ${X_1''}^2 - a{Z_1''}^2 = s^4({X_1}^2 - a{Z_1}^2) = 0$, where $s \in K^*$.

Finally ${X_1}^2 + a{Z_1}^2 = 0$ implies ${x_1}^2 + a = 0$, namely *(MD2)*. This condition is influenced by neither the Coron's 3rd countermeasure nor the Joye-Tymen countermeasure, the same as *(MD1)*.

Proof of Theorem 4

The intermediate values can be zero if and only if one of the following value are zero.

$$X_1, Z_1, X_2, Z_2, X_3, X_1Z_2 - X_2Z_1, X_1X_2 - aZ_1Z_2, X_1Z_2 + X_2Z_1$$

Here $Z_1 = 0$, $Z_2 = 0$, and $X_1Z_2 - X_2Z_1 = 0$ imply $P_1 = \mathcal{O}$, $P_2 = \mathcal{O}$, and $P_1 = \pm P_2$, respectively, which can be discarded. If one of X_1, X_2, X_3 is zero, this provides conditions *(MA3)*.

Next $X_1X_2 - aZ_1Z_2 = 0$ implies $x_1x_2 - a = 0$, where $x_1 = X_1/Z_1$ and $x_2 = X_2/Z_2$, namely condition *(MA1)*. Note that neither Coron's 3rd nor Joye-Tymen countermeasure can randomize the points. Indeed the randomized points $(X_1' : Z_1') = (rX_1 : rZ_1)$, $(X_2' : Z_2') = (sX_2 : sZ_2)$ by Coron's 3rd countermeasure satisfies $X_1'X_2' - aZ_1'Z_2' = rs(X_1X_2 - aZ_1Z_2) = 0$, where $r, s \in K^*$. The randomized point $(X_1'' : Z_1'') = (t^2X_1 : Z_1)$, $(X_2'' : Z_2'') = (t^2X_2 : Z_2)$ and curve parameter $a'' = t^4a$ by Joye-Tymen countermeasure satisfies $X_1''X_2'' - aZ_1''Z_2'' = t^4(X_1X_2 - aZ_1Z_2) = 0$, where $t \in K^*$.

Finally $X_1Z_2 + X_2Z_1 = 0$ implies $x_1 + x_2 = 0$, namely *(MA2)*. This condition is influenced by neither Coron's 3rd nor Joye-Tymen countermeasure, the same as *(MA1)*.

Proof of Theorem 5

If one of the following values is zero, at least one of the intermediate values must be zero.

$$X_1, Y_1, Z_1, X_3, Y_3, aZ_3 + {Y_1}^2 + b{Z_1}^4.$$

Here $Z_1 = 0$ implies $P = \mathcal{O}$, which never appears for input of $\mathrm{ECDBL}^{\mathcal{P}}_{2^n}(P)$. The condition $X_1 = 0$, $X_3 = 0$, $Y_1 = 0$, and $Y_3 = 0$ are equivalent to $x(P) = 0$, $x(2P) = 0$, $y(P) = 0$, and $y(2P) = 0$, namely conditions *(BD3)*, *(BD4)*. Next, $aZ_3 + {Y_1}^2 + b{Z_1}^4 = a{X_1}^2{Z_1}^2 + {Y_1}^2 + b{Z_1}^4 = 0$ implies $a{x_1}^2 + {y_1}^2 + b = 0$, where $x_1 = X_1/Z_1$ and $y_1 = Y_1/{Z_1}^2$, namely $x_1({x_1}^2 + y_1) = 0$. This indicates $x_1 = 0$, which is condition *(BD3)*, or ${x_1}^2 + y_1 = 0$, which is condition *(BD1)*. Note that Coron's 3rd countermeasure cannot randomize the point. Indeed the randomized point $(X_1' : Y_1' : Z_1') = (rX_1 : r^2Y_1 : rZ_1)$ by Coron's 3rd countermeasure satisfies $a{X_1'}^2{Z_1'}^2 + {Y_1'}^2 + b{Z_1'}^4 = r^4(a{X_1}^2{Z_1}^2 + {Y_1}^2 + b{Z_1}^4) = 0$, where $r \in \mathbb{F}^*_{2^n}$.

The other possible intermediate values appear only at the computation of $aZ_3 + {Y_1}^2 + b{Z_1}^4$. we have three possible intermediate values:

$$aZ_3 + {Y_1}^2, aZ_3 + b{Z_1}^4, {Y_1}^2 + b{Z_1}^4.$$

$aZ_3 + {Y_1}^2 = 0$, $aZ_3 + b{Z_1}^4 = 0$, and ${Y_1}^2 + b{Z_1}^4 = 0$ imply $a{x_1}^2 + {y_1}^2 = 0$, $a{x_1}^2 + b = 0$, and ${y_1}^2 + b = 0$, respectively. These three conditions are never simultaneously satisfied, which indicates condition *(BD2)*.

Proof of Theorem 6

If one of the following values is zero, at least one of the intermediate values must be zero.

$$X_1, Y_1, Z_1, X_2, Y_2, Z_2, X_3, Z_3, C, D, F + aE^2, I, J.$$

Here if one of $X_1, Y_1, X_2, Y_2, X_3, Y_3$ is zero, this provides conditions *(BA6)* or *(BA7)*. $Z_1 = 0$, $Z_2 = 0$ and $D = 0$ imply $P_1 = \mathcal{O}$, $P_2 = \mathcal{O}$, and $P_1 = \pm P_2$, respectively, which never appear for input of $\mathrm{ECADD}^{\mathcal{P}}_{2^n}(P_1, P_2)$. Next, $C = 0$ implies $y_1 = y_2$, where $y_1 = Y_1/{Z_1}^2$ and $y_2 = Y_2/{Z_2}^2$, namely condition *(BA1)*. This point never appears for input of $\mathrm{ECADD}^{\mathcal{P}}_{2^n}$. Next $F + aE^2 = 0$ implies $x_1 + x_2 + a = 0$, namely condition *(BA2)*. $I = 0$ implies $x_1 + x_3 = 0$, which is condition *(BA4)*. Finally $J = 0$ implies $y_2 + x_3 = 0$, namely condition *(BA5)*. These conditions aren't randomized by Coron's 3rd countermeasure.

The other possible intermediate values appear only at the computation of $X_3 = C^2 + H + G$. We have three possible intermediate values:

$$C^2 + H, C^2 + G, H + G.$$

$C^2 + H = 0$ implies $y_1 + y_2 + x_1 + x_2 = 0$, namely $\lambda(P_1, P_2) = 1$. Next $C^2 + G = 0$ implies $(y_1 + y_2)^2 + (x_1 + x_2)^2(x_1 + x_2 + a) = 0$, namely $\lambda(P_1, P_2)^2 = x_1 + x_2 + a$. Finally $H + G = 0$ implies $y_1 + y_2 + (x_1 + x_2)(x_1 + x_2 + a) = 0$, namely $\lambda(P_1, P_2) = x_1 + x_2 + a$. These three conditions are never simultaneously satisfied, which indicates condition *(BA3)*.