IEICE TRANS. FUNDAMENTALS, VOL.E88–A, NO.1 JANUARY 2005

PAPER *Special Section on Cryptography and Information Security*

On the Optimal Parameter Choice for Elliptic Curve Cryptosystems Using Isogeny*

Toru AKISHITA[†a)] ***and*** **Tsuyoshi TAKAGI**[††b)], ***Members***

SUMMARY Isogeny for elliptic curve cryptosystems was initially used for efficient improvement of order counting methods. Recently, Smart proposed a countermeasure using isogeny for resisting a refined differential power analysis by Goubin (Goubin's attack). In this paper, we examine a countermeasure using isogeny against zero-value point (ZVP) attack that is generalization of Goubin's attack. We show that some curves require higher order of isogeny to prevent ZVP attack. Moreover, we prove that the class of curves that satisfies $(-3/p) = 1$ and whose order is odd cannot be mapped by isogeny to curves with $a = -3$ and secure against ZVP attack. We point out that three SECG curves are in this class. In the addition, we compare some efficient algorithms that are secure against both Goubin's attack and ZVP attack, and present the most efficient method of computing a scalar multiplication for each curve from SECG. Finally, we discuss another improvement for an efficient scalar multiplication, namely the usage of a point $(0, y)$ for a base point of curve parameters. We are able to improve about 11% for double-and-add-always method, when the point $(0, y)$ exists in an underlying curve or its isogeny.

key words: *elliptic curve cryptosystems, isomorphism, isogeny, side channel attack, zero-value point attack*

1. Introduction

Elliptic curve cryptosystem (ECC) is an efficient public-key cryptosystem with a short key size. ECC is suitable for implementing on memory-constraint devices such as mobile devices. However, if an implementation is careless, side channel attacks (SCA) might reveal a secret key of ECC. We have to carefully investigate the implementation of ECC in order to achieve high security.

The standard method of defending SCA on ECC is randomizing curve parameters, for instance, randomizing a base point in projective coordinates [5] and randomizing curve parameters in its isomorphic class [11]. However, Goubin pointed out that a point $(0, y)$ cannot be randomized by these methods [7]. He proposed a refined differential power analysis using the point $(0, y)$. This attack has been extended to zero value of auxiliary registers, called the zero-value point (ZVP) attack [1]. Both Goubin's attack and the ZVP attack assume that a base point P can be chosen by an attacker and a secret scalar d is fixed, so that we need to care these attacks in ECIES and single-pass ECDH, but not in ECDSA and two-pass ECDH.

In order to resist Goubin's attack, Smart proposed to map an underlying curve to an isogenous curve that does not have the point $(0, y)$ [17]. This countermeasure with a small isogeny degree is faster than randomizing the secret scalar d with the order of the curve. However, the security of this countermeasure against the ZVP attack has not been discussed yet—it could be vulnerable to the ZVP attack.

In this paper, we examine a countermeasure using isogeny against the ZVP attack. The zero-value points *(ED1)* $3x^2 + a = 0$, *(MD1)* $x^2 - a = 0$, and *(MD2)* $x^2 + a = 0$ were examined. We show that some curves require higher order of isogeny to prevent the ZVP attack. For example, SECG secp112r1 [18] is secure against Goubin's attack, but insecure against the ZVP attack. Then, the 7-isogenous curve to secp112r1 is secure against both attacks. We require the isogeny of degree 7 to prevent the ZVP attack. For each SECG curve we search the minimal degree of isogeny to the curve that is secure against both Goubin's attack and the ZVP attack. Since the ZVP attack strongly depends on the structure of addition formulae, the minimal degree of isogeny depends on not only the curve itself but also addition formulae.

Interestingly, three SECG curves cannot be mapped to a curve with $a = -3$ that is secure against the ZVP attack. A curve with $a = -3$ is important for efficiency. We prove that this countermeasure cannot map a class of curves to a curve with $a = -3$ that is secure against the ZVP attack. In addition to $a = -3$, this class satisfies that the curve order is odd and $(-3/p) = -1$ for the base field p. We point out that these three curves belong to this class.

Moreover, we estimate the total cost of a scalar multiplication in the necessity of resistance against both Goubin's attack and the ZVP attack. We compare two efficient DPA-resistant methods, namely the window-based method and Montgomery-type method, with the countermeasure using isogeny, and present the most efficient method to compute the scalar multiplication for each SECG curve.

Finally we show another efficient method for computing a scalar multiplication, namely using a point $(0, y)$ for the base point of curve parameters. We prove that the discrete logarithm problem with the base point $(0, y)$ is as intractable as using a random one thanks to random self reducibility. Comparing with the previous method, we are

Manuscript received March 22, 2004.
Manuscript revised June 25, 2004.
Final manuscript received August 30, 2004.

[†]The author is with Information Technologies Laboratories, Sony Corporation, Tokyo, 141-0001 Japan.
[††]The author is with Fachbereich Informatik, Technische Universität Darmstadt, D-64283 Darmstadt, Germany.
a) E-mail: akishita@pal.arch.sony.co.jp
b) E-mail: takagi@informatik.tu-darmstadt.de

*This work was done while the first author stayed at Technische Universität Darmstadt, Germany. This paper was presented at the 7th International Workshop on Theory and Practice in Public Key Cryptography (PKC 2004), held in Singapore.

able to achieve about 11% faster scalar multiplication using the double-and-add-always method. This base point can also save 50% memory space without any compression trick. We propose a scenario to utilize the proposed method efficiently and show an example of a curve to achieve this scenario.

This paper is organized as follows: Section 2 briefly describes known results about elliptic curve cryptosystems. In Section 3 we review side channel attacks on elliptic curve cryptosystems. Section 4 describes the choices of a secure curve against the ZVP attack using isogeny. In Section 5 we show efficient implementations using isogeny. In Section 6 we state concluding remarks.

2. Elliptic Curve Cryptosystems

We shortly review some results on elliptic curve cryptosystems related to isogeny. Let $K = \mathbf{F}_p$ be a finite field, where $p > 3$. Elliptic curve over K is uniquely represented by the Weierstrass form $E : y^2 = x^3 + ax + b$ $(a, b \in K)$, where discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$. In this paper, we represent a point $P = (x, y)$ on the curve by Jacobian coordinates $(X : Y : Z)$ setting $x = X/Z^2$ and $y = Y/Z^3$. The result using other coordinates can be similarly obtained. Elliptic curve E has a group structure with neutral element $O = (0 : 1 : 0)$. The addition $P_3 = (X_3 : Y_3 : Z_3)$ of two points $P_1 = (X_1 : Y_1 : Z_1)$ and $P_2 = (X_2 : Y_2 : Z_2)$ is computed by the following formulae:

ECDBL in Jacobian Coordinates (ECDBL$^{\mathcal{J}}$) :

$X_3 = T$, $Y_3 = -8Y_1{}^4 + M(S - T)$, $Z_3 = 2Y_1Z_1$,
$S = 4X_1Y_1{}^2$, $M = 3X_1{}^2 + aZ_1{}^4$, $T = -2S + M^2$,
for $P_1 = P_2$.

ECADD in Jacobian Coordinates (ECADD$^{\mathcal{J}}$) :

$X_3 = -H^3 - 2U_1H^2 + R^2$,
$Y_3 = -S_1H^3 + R(U_1H^2 - X_3)$, $Z_3 = Z_1Z_2H$,
$U_1 = X_1Z_2{}^2$, $U_2 = X_2Z_1{}^2$, $S_1 = Y_1Z_2{}^3$,
$S_2 = Y_2Z_1{}^3$, $H = U_2 - U_1$, $R = S_2 - S_1$,
for $P_1 \neq \pm P_2$.

We call these formulae as the standard addition formulae. For ECADD$^{\mathcal{J}}$ we require 16 multiplications when $Z_1 \neq 1$ and 11 ones when $Z_1 = 1$. For ECDBL$^{\mathcal{J}}$ we require 10 multiplications in general, 9 ones when a is small, and only 8 ones when $a = -3$ by $M = 3(X_1+Z_1{}^2)(X_1-Z_1{}^2)$. All SECG random curves over $\mathbf{F}_p$ with prime order satisfy $a = -3$. In this paper, we are interested in the curves with prime order such as these curves.

2.1 Isomorphism and Isogeny

Two elliptic curves $E_1(a_1, b_1)$ and $E_2(a_2, b_2)$ are called isomorphic if and only if there exists $r \in K^*$ such that $a_1 = r^4a_2$ and $b_1 = r^6b_2$. Isomorphism is given by

$$\psi : \begin{cases} E_1 & \longrightarrow \quad E_2 \\ (x, y) & \longmapsto (r^{-2}x, r^{-3}y) \end{cases} .$$

There are $(p - 1)/2$ isomorphic classes.

Let $\Phi_l(X, Y)$ be a modular polynomial of degree l. Two elliptic curves $E_1(a_1, b_1)$ and $E_2(a_2, b_2)$ are called l-isogenous if and only if $\Phi_l(j_1, j_2) = 0$ satisfies, where j_i are j-invariant of curve E_i for $i = 1, 2$. Isogenous curves have the same order. Isogeny is given by

$$\psi : \begin{cases} E_1 & \longrightarrow \quad E_2 \\ (x, y) & \longmapsto (\frac{f_1(x)}{g(x)^2}, \frac{y \cdot f_2(x)}{g(x)^3}) \end{cases} ,$$

where f_1, f_2 and g are polynomials of degree l, $(3l - 1)/2$ and $(l - 1)/2$ respectively (see details in [2, Chapter VII]). By Horner's rule, the computational cost of this mapping is estimated as $(l+(3l-1)/2+(l-1)/2+5)M+I = (3l+4)M+I$.

The usage of isogeny for elliptic curve cryptosystem initially appeared for improving order counting methods (see, for example, [12]). Recently, some new applications of isogeny have been proposed, namely for improving the efficiency of a scalar multiplication [4], and for enhancing the security for a new attack [17].

Brier and Joye reported that isogeny could be used for improving the efficiency of ECDBL$^{\mathcal{J}}$ [4]. Recall that if a curve parameter a of an elliptic curve is equal to -3, the cost of ECDBL$^{\mathcal{J}}$ is reduced from 10 multiplications to 8 ones. If there is an integer r such that $-3 = r^4a$, then we can transform the original elliptic curve to its isomorphic curve with $a = -3$. However, its success probability is about 1/2 when $p \equiv 3 \pmod 4$ or about 1/4 when $p \equiv 1 \pmod 4$. They proposed that isogeny of the original curve could have a curve with $a = -3$.

3. Scalar Multiplication and Side Channel Attack

A scalar multiplication evaluates dP for a given integer d and a base point P of ECC. A standard algorithm of computing dP is the binary method, which repeatedly calls ECDBL and ECADD based on the secret bits. ECADD is computed if and only if the corresponding secret bit is 1. Note that the standard formulae are not same for computing ECADD and ECDBL. Therefore, a single observation of power consumption of computing the scalar multiplication might break the secret bit. This attack is called as a simple power analysis (SPA). The binary method is vulnerable to SPA.

Coron proposed a simple countermeasure against SPA, called as the double-and-add-always method [5]. The double-and-add-always method is as follows:

Algorithm 1: Double-and-add-always method

Input: $d = (d_{n-1} \cdots d_1d_0)_2$, $P \in E(K)$ $(d_{n-1} = 1)$.
Output: dP.
1. $Q[0] \leftarrow P$.
2. For $i = (n - 2)$ downto 0 do:
   2.1. $Q[0] \leftarrow$ ECDBL($Q[0]$).
   2.2. $Q[1 - d_i] \leftarrow$ ECADD($Q[0], P$).
3. Return($Q[0]$).

An attacker cannot guess the bit information because this method always computes ECADD whether $d_i = 0$ or 1. Two more efficient SPA-resistant methods have been proposed. The first is window-based method [13], [14], [16] and the second is Montgomery-type method [3], [6], [8]–[10].

However, the SPA-resistant scheme is not generally secure against a differential power analysis (DPA), which uses many observations of power consumption together with statistical tools. In order to enhance SPA security to DPA security, we must insert random numbers during computation of dP. The standard randomization methods for the base point P are Coron's 3rd countermeasure [5] and Joye-Tymen countermeasure [11]. Coron's 3rd countermeasure randomizes point $P = (X : Y : Z)$ in Jacobian coordinates, namely $P = (Xr^2 : Yr^3 : Zr)$ with randomly chosen $r \in K^*$. Joye-Tymen countermeasure maps an underlying curve to a random isomorphic curve.

3.1 Efficient Methods Secure against SCA

3.1.1 Window-Based Method

The window-based method secure against SPA was first proposed by Möller [13], [14], and optimized by Okeya and Takagi [16]. This method uses the standard addition formulae the same as the double-and-add-always method. It makes the fixed pattern $|0 \cdots 0x|0 \cdots 0x| \cdots |0 \cdots 0x|$ for some x. Though a SPA attacker distinguishes ECDBL and ECADD in the scalar multiplication by measuring power consumption, he obtains only the identical sequence $|D \cdots DA|D \cdots DA| \cdots |D \cdots DA|$, where D and A denote ECDBL and ECADD, respectively. Therefore, he cannot guess the bit information. This method reduces ECADD as compared with the double-and-add-always method and thus enables efficiency. In order to enhance this method to be DPA-resistant, we have to insert a random value using Coron's 3rd countermeasure or Joye-Tymen countermeasure. Moreover, we have to randomize the value of table to protect 2nd order DPA. We estimate the computational cost of a scalar multiplication dP according to [16]. Denote the computational cost of multiplication and inversion in the definition field by M and I, respectively. The total cost is estimated as $(16 \cdot 2^w + (9w + 21)k - 18)M + I$ when a is small and $(16 \cdot 2^w + (8w + 21)k - 18)M + I$ when $a = -3$, where n is the bit length of d, w is the window size, and $k = \lceil n/w \rceil$.

3.1.2 Montgomery-Type Method

Montgomery-type method was originally proposed by Montgomery [15] and enhanced to the Weierstrass form of elliptic curves over K [3], [6], [8]–[10]. This method always computes ECADD and ECDBL whether $d_i = 0$ or 1 as the double-and-add-always method, and thus satisfies SPA-resistance. In this method, we don't need to use y-coordinate (Y-coordinate in projective coordinates) to compute a scalar multiplication dP. This leads the efficiency of Montgomery-type method. In the original method ECADD and ECDBL are computed separately. However, Izu and Takagi encapsulated these formulae into one formula mECADDDBL to share intermediate variables and cut two multiplications [10]. 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 encapsulated formula mECADDDBL$^{\mathcal{P}}$, which compute $P_3 = (X_3 : Z_3) = P_1 + P_2$ and $P_4 = (X_4 : Z_4) = 2P_1$, where $P_1 \neq \pm P_2$, $P_3{}' = (X_3{}' : Z_3{}') = P_1 - P_2$ and $(X_3', Z_3' \neq 0)$.

ECADDDBL in Montgomery-Type Method
(mECADDDBL$^{\mathcal{P}}$):

$$X_3 = Z_3{}'(2(X_1Z_2 + X_2Z_1)(X_1X_2 + aZ_1Z_2) + 4bZ_1{}^2Z_2{}^2) - X_3{}'(X_1Z_2 - X_2Z_1)^2,$$
$$Z_3 = Z_3{}'(X_1Z_2 - X_2Z_1)^2,$$
$$X_4 = (X_1{}^2Z_2{}^2 - aZ_1{}^2Z_2{}^2)^2 - 8bX_1Z_1{}^3Z_2{}^4,$$
$$Z_4 = 4Z_1Z_2(X_1Z_2(X_1{}^2Z_2{}^2 + aZ_1{}^2Z_2{}^2) + bZ_1{}^3Z_2{}^3).$$

We call this formula as Montgomery addition formula. mECADDDBL requires 17 multiplications in general and 15 ones when a is small. By using this formula, the scalar multiplication is computed as follows:

Algorithm 2: Montgomery-type method
Input: $d = (d_{n-1} \cdots d_1d_0)_2,\ P \in E(K)\ \ (d_{n-1} = 1)$.
Output: dP.
1. $Q[0] \leftarrow P,\ Q[1] \leftarrow$ mECDBL(P).
2. For $i = (n-2)$ downto 0 do:
   $(Q[1-d_i], Q[d_i]) \leftarrow$ mECADDDBL$(Q[d_i], Q[1-d_i])$.
3. Return$(Q[0])$.

In order to enhance this method to DPA-resistant, we have to use Coron's 3rd countermeasure or Joye-Tymen countermeasure. The total cost of scalar multiplication dP is estimated as $(17n+8)M+I$ in general and $(15n+10)M+I$ when a is small, where n is the bit length of the scalar d (see [8]).

3.2 Goubin's Attack and Isogeny Defense

Goubin proposed a new power analysis on ECC [7]. This attack utilizes points $(x, 0)$ and $(0, y)$ that cannot be randomized by the above two standard randomization techniques. Goubin's attack is effective on a curve that has a point $(x, 0)$ or $(0, y)$ in such protocols as ECIES and single-pass ECDH. The point $(x, 0)$ is not on a curve with odd order because the order of $(x, 0)$ is 2. The point $(0, y)$ appears on a curve if b is quadratic residue modulo p, which is computed by solving $y^2 = b$.

As a countermeasure to Goubin's attack, Smart utilized isogeny [17]. He proposed that if an original curve E has the point $(0, y)$, an isogenous curve E' to E could have no point $(0, y)$. If we can find E' which has no point $(0, y)$, we transfer a base point $P \in E$ to $P' \in E'$ using the isogeny $\psi : E \to E'$. Instead of computing the scalar multiplication $Q = dP$, we compute $Q' = dP'$ on E' and then pull back $Q \in E$ from $Q' \in E'$ by the mapping $\psi^{-1} : E' \to E$. The mappings ψ, ψ^{-1} require $(3l + 4)M + I$ respectively, so that the additional cost for this countermeasure is $(6l+8)M+2I$.

3.3 Zero-Value Point Attack

At ISC'03, we proposed the zero-value point (ZVP) attack which is an extension of Goubin's attack [1]. We pointed out that if a point has no zero-value coordinate, auxiliary registers might take zero value. We found several points (x, y) which cause zero-value registers and called these points as the zero-value points (ZVP). ZVP strongly depend on the structure of addition formula, and namely ZVP for the standard addition formulae are different from those for Montgomery addition formula. The points with the following conditions from ECDBL are effectively used for the ZVP attack.

– *(ED1)* $3x^2 + a = 0$ for the standard addition formulae
– *(MD1)* $x^2-a = 0$ and *(MD2)* $x^2+a = 0$ for Montgomery addition formula

An attacker can utilize the points that cause zero-value registers in ECADD, however finding ZVP in ECADD is much more difficult than in ECDBL. In this paper we consider only the above points *(ED1)*, *(MD1)*, and *(MD2)*.

4. Isogeny Countermeasure against ZVP Attack

In this section we examine a countermeasure using isogeny against the ZVP attack. In order to prevent the ZVP attack, we have to choose a curve which has neither the point $(0, y)$ nor *(ED1)* for the methods using the standard addition formulae, and neither $(0, y)$, *(MD1)* nor *(MD2)* for Montgomery-type method. The degree of isogeny depends on not only a curve itself but also addition formulae. We examine the standard curves from SECG [18].

4.1 Example from SECG Curve

For example, we mention a curve secp112r1 from SECG curves [18]. secp112r1 $E : y^2 = x^3 + ax + b$ over $\mathbf{F}_p$ is defined by

$$\begin{cases} p = 4451685225093714772084598273548427, \\ a = 4451685225093714772084598273548424 = -3, \\ b = 2061118396808653202902996166388514. \end{cases}$$

This curve does not have $(0, y)$, but has *(ED1)* $3x^2 + a = 0$ as

$$(x, y) = (1, 1170244908728626138608688645279825).$$

Therefore secp112r1 is secure against Goubin's attack, but vulnerable against the ZVP attack for the methods using the standard addition formulae. However, the 7-isogenous curve $E' : y^2 = x^3 + a'x + b'$ over $\mathbf{F}_p$ defined by

$$\begin{cases} a' = 1, \\ b' = 811581442038490117125351766938682, \end{cases}$$

has neither $(0, y)$ nor *(ED1)* $3x^2 + a' = 0$. Thus E' is secure against both Goubin's attack and the ZVP attack for the methods using the standard addition formulae. We don't require isogeny defense to prevent Goubin's attack, but require the isogeny of degree 7 to prevent the ZVP attack.

4.2 Experimental Results from SECG Curves

For each SECG curve we search the minimal degree of isogeny to a curve which has neither $(0, y)$ nor ZVP as described above. If the original curve has neither $(0, y)$ nor ZVP, we specify this degree as 1. For the standard addition formulae, we also search the minimal isogeny degree to a curve which we prefer for particularly efficient implementation, namely $a = -3$ as described in section 2. We call the former as the minimal isogeny degree and the latter as the preferred isogeny degree, and define l_{std}, l_{prf}, and l_{mnt} as follows:

– l_{std} : the minimal isogeny degree for the standard addition formulae,
– l_{prf} : the preferred isogeny degree for the standard addition formulae,
– l_{mnt} : the minimal isogeny degree for Montgomery addition formula.

Here we show the searching method of these degrees for the standard addition formulae.

Algorithm 3: Searching method for the standard addition formulae

Input: $E : y^2 = x^3 + ax + b$ over $GF(p)$,
$j = j$-invariant of E
Output: minimal isogeny degree l_{std} and preferred isogeny degree l_{prf}

1. Set $l \leftarrow 3$.
2. Solve the equation $\Phi_l(j', j) = 0$.
3. If the equation has no solution then go to Step 4, else then
   3.1. Construct $E' : y^2 = x^3 + a'x + b'$ where $j' = j$-invariant of E'.
   3.2. Check E' has the point $(0, y)$ or *(ED1)*.
   3.3. If E' has then go to Step 4, else then
      3.3.1. If l_{std} is null, set $l_{\text{std}} \leftarrow l$.
      3.3.2. Check $r \in GF(p)^*$ exists where $r^4 a' = -3 \bmod p$.
      3.3.3. If exists then set $l_{\text{prf}} \leftarrow l$ and stop, else then go to Step 4.
4. If $l > 107$ then stop, else then $l \leftarrow \text{nextprime}(l)$ and go to Step 2.

In this algorithm nextprime(l) is a function which returns the smallest prime number larger than l. For l_{mnt}, we check *(MD1)* and *(MD2)* instead of *(ED1)* in Step 3.2.

Table 1 shows isogeny degrees l_{std}, l_{prf}, and l_{mnt} for SECG curves. The number in $(\cdot)$ is the minimal isogeny degree listed in [17], which considers only Goubin's point $(0, y)$ (not the ZVP). In order to prevent the ZVP attack, some curves require higher degree of isogeny, e.g., secp112r1 for l_{std}. These isogeny degrees depend on not only a curve itself but also addition formulae, namely some curves require different isogeny degrees for the standard addition formulae and Montgomery addition formula. Interestingly, we have not found preferred isogeny degree up to 107 for secp112r1, secp192r1, and secp384r1.

Table 1 Minimal and preferred isogeny degree for SECG curves.

	l_{std}	l_{prf}	l_{mnt}
secp112r1	7 (1)	> 107 (1)	1 (1)
secp128r1	7 (7)	7 (7)	7 (7)
secp160r1	13 (13)	13 (13)	19 (13)
secp160r2	19 (19)	41 (41)	19 (19)
secp192r1	23 (23)	> 107 (73)	23 (23)
secp224r1	1 (1)	1 (1)	1 (1)
secp256r1	3 (3)	23 (11)	3 (3)
secp384r1	31 (19)	> 107 (19)	19 (19)
secp521r1	5 (5)	5 (5)	7 (5)

4.3 Some Properties of ZVP Attack

Here we show some properties of the zero-value point attack.

Theorem 1: Let E be an elliptic curve over prime field $\mathbf{F}_p$ defined by $y^2 = x^3 + ax + b$. The elliptic curve E has point $(0, y)$, if E satisfies *(MD2)* $x^2 + a = 0$ (i.e., there exists a point (x, y) on the curve E with $x^2 + a = 0$).

Proof: If $a = 0$ or $b = 0$ holds, then the assertion is trivial. We assume that $a \neq 0$ and $b \neq 0$. Note that $(0, y)$ exists on the curve E if b is a quadratic residue in $\mathbf{F}_p^*$. Let $s \in \mathbf{F}_p^*$ be the solution of equation $x^2+a = 0$. Condition *(MD2)* implies that there is a solution $y = t$ of equation $y^2 = s^3+as+b$. Thus E has a point $(0, t)$ due to $t^2 = s^3+as+b = (s^2+a)s+b = b$.

All curves which satisfy condition *(MD2)* have Goubin's point $(0, y)$. These curves are insecure against both Goubin's attack and the ZVP attack.

Theorem 2: Let E be an elliptic curve over prime field $\mathbf{F}_p$ defined by $y^2 = x^3 + ax + b$. The elliptic curve E satisfies condition *(ED1)* $3x^2 + a = 0$ (i.e., there exists a point (x, y) on the curve E with $3x^2 + a = 0$), if E satisfies the following three conditions: (1) $a = -3$, (2) $\#E$ is odd, and (3) p satisfies $(-3/p) = -1$, where $(\cdot/\cdot)$ is Legendre symbol.

Proof: From Cardano's formula, equation $x^3 + ax + b = 0$ has a solution, if $(-3\Delta/p) = 1$ holds and all elements over $\mathbf{F}_p$ are cubic residue. Note that $(-3/p) = -1$ implies $p \bmod 3 = 2$ and all elements over $\mathbf{F}_p$ are cubic residue. Since E has odd order, E does not have a point $(x, 0)$, and thus the equation $x^3 + ax + b = 0$ has no root. Therefore, we obtain $(\Delta/p) = 1$ due to $(-3/p) = -1$. Equation $\Delta = -16(4(-3)^3 + 27b^2) = -3(12)^2(b + 2)(b - 2)$ implies either $((b + 2)/p) = 1$ or $((b - 2)/p) = 1$. In other words, an equation $y^2 = b + 2$ or $y^2 = b - 2$ is solvable, namely curve E has a point (x, y) with $a = -3$ and either $x = 1$ or $x = -1$. Consequently, the elliptic curve E with the above three conditions satisfies *(ED1)* $3x^2 + a = 0$.

The definition fields $\mathbf{F}_p$ that satisfy $(-3/p) = -1$ in Table 1 are secp112r1, secp192r1, and secp384r1. These curves also have odd order and satisfy $a = -3$. Therefore, these curves satisfy *(ED1)* and are vulnerable to the ZVP attack.

Since an isogenous curve has same order as E, any isogenous curve with $a = -3$ always satisfies $(ED1)$ and thus is insecure against the ZVP attack. We have the following corollary.

Corollary 1: Let E be an elliptic curve over prime field $\mathbf{F}_p$. We assume that $\#E$ is odd and $(-3/p) = -1$. Any isogeny cannot map E to a curve with $a = -3$ that is secure against the ZVP attack.

Corollary 1 shows that it is impossible to find an isogenous curve with $a = -3$ which does not satisfy *(ED1)*, namely l_{prf}-isogenous curve, for these three curves.

5. Efficient Implementation Using Isogeny

5.1 Most Efficient Method for Each SECG Curve

We estimate the total cost of a scalar multiplication in the necessity of resistance against both Goubin's attack and the ZVP attack. This situation corresponds to a scalar multiplication in ECIES and single-pass ECDH.

Here we notice two efficient DPA-resistant methods, namely the window-based method and Montgomery-type method. We have to use the window-based method on l_{std}-isogenous curve because this method uses the standard addition formulae. Isomorphism enables efficient implementation with small a. Moreover, more efficient implementation with $a = -3$ can be achieved on l_{prf}-isogenous curve. On the other hand, we have to use Montgomery-type method on l_{mnt}-isogenous curve. Isomorphism also enables efficient implementation with small a.

Therefore, we mention the following three methods:

Method 1 Window-based method with small a on l_{std}-isogenous curve,
Method 2 Window-based method with $a = -3$ on l_{prf}-isogenous curve,
Method 3 Montgomery-type method with small a on l_{mnt}-isogenous curve.

From section 2 and 3 we estimate the total cost of each method as follows:

Method 1 $T_1 = (16 \cdot 2^w + (9w + 21)k + 6l_{\mathrm{std}} - 10)M + 3I$.
Method 2 $T_2 = (16 \cdot 2^w + (8w + 21)k + 6l_{\mathrm{prf}} - 10)M + 3I$,
Method 3 $T_3 = (15n + 6l_{\mathrm{mnt}} + 18)M + 3I$.

If the degree of isogeny equals to 1, the cost of isogeny $14M + 2I$ is cut.

Table 2 shows the estimated cost for each SECG curve. A number in $(\cdot)$ is window size for Method 1 and 2. Method 2 cannot be used for some curves because there is no preferred isogeny degree l_{prf} (notation '—' indicates these curves). We emphasize the most efficient method for each curve with bold letters. The most efficient method differs on each curve because the degree of isogeny depends on the curve and implementation method.

Table 2 Total cost of scalar multiplication to resist Goubin's attack and the ZVP attack.

	Method 1	Method 2	Method 3
secp112r1	$1884M + 3I$ (4)	—	$\mathbf{1690M + I}$
secp128r1	$2112M + 3I$ (4)	$1984M + 3I$ (4)	$\mathbf{1980M + 3I}$
secp160r1	$2604M + 3I$ (4)	$\mathbf{2444M + 3I}$ **(4)**	$2532M + 3I$
secp160r2	$2640M + 3I$ (4)	$2612M + 3I$ (4)	$\mathbf{2532M + 3I}$
secp192r1	$3120M + 3I$ (4)	—	$\mathbf{3036M + 3I}$
secp224r1	$3430M + I$ (4)	$\mathbf{3206M + I}$ **(4)**	$3370M + I$
secp256r1	$3912M + 3I$ (4)	$\mathbf{3776M + 3I}$ **(4)**	$3876M + 3I$
secp384r1	$\mathbf{5770M + 3I}$ **(5)**	—	$5892M + 3I$
secp521r1	$7462M + 3I$ (5)	$\mathbf{6937M + 3I}$ **(5)**	$7875M + 3I$

5.2 Efficient Scalar Multiplication Using $(0, y)$

In this section we propose another improvement for computing an efficient scalar multiplication.

In order to clearly describe our method, we categorize improvements of efficiency into five classes, namely, (1) curve parameter (e.g. $a = -3$, $Z = 1$, etc), (2) addition chain (e.g. binary method, NAF, etc), (3) base field (e.g. optimal normal base, OEF, etc), (4) coordinate (e.g. projective coordinates, Jacobian coordinates, etc). (5) curve form (e.g. Montgomery form, Hessian form, etc). The proposed method belongs to class (1), but its improvement is related to classes (2), (4), and (5). Our improvement can be simultaneously used with other methods in class one. For sake of convenience, we discuss the improvement for the double-and-add-always method in section 3 on a curve with parameters $a = -3$, $Z = 1$, Jacobian coordinates, and the Weierstrass form.

The main idea of the improvement is to use a point $(0, y)$ for the base point of an underlying curve, namely the point with zero x-coordinate. The double-and-add-always method in section 3 is a left-to-right method, and thus the base point P is fixed during the scalar multiplication dP. The addition formula with the point $X = 0$ is represent as follows:

ECADD in Jacobian Coordinates with $X = 0$ ($\mathrm{ECADD}^{\mathcal{J}}_{X=0}$) :

$$X_3 = -H^3 + R^2,\ Y_3 = -S_1H^3 - RX_3,\ Z_3 = Z_1Z_2H,$$
$$H = X_2Z_1{}^2,\ S_1 = Y_1Z_2{}^3,\ S_2 = Y_2Z_1{}^3,\ R = S_2 - S_1.$$

We denote by $\mathrm{ECADD}^{\mathcal{J}}_{X=0}$ the addition formula for ECADD in Jacobian Coordinates with $X = 0$. Formula $\mathrm{ECADD}^{\mathcal{J}}_{X=0}$ requires only 14 multiplications when $Z_1 \neq 1$ and 9 multiplications when $Z_1 = 1$.

Table 3 shows estimations of cost for n-bit scalar multiplication with $a = -3$, $Z = 1$ using Jacobian coordinates and the double-and-add-always method in section 3. The proposed scheme can achieve about 11% improvement over the scheme $X \neq 0$.

Here we have a question about the security of choosing a base point $(0, y)$. The following theorem can be easily proven thanks to random self reducibility.

Theorem 3: Let E be an elliptic curve over $\mathbf{F}_p$. We assume that $\#E$ is prime. Breaking the discrete logarithm problem with the base point $(0, y)$ is as intractable as doing with a random base point.

Table 3 Comparison of efficiency with $X \neq 0$ and $X = 0$.

	n-bit ECC	160-bit ECC
Scheme $X \neq 0$	$19nM$	$3040M$
Scheme $X = 0$	$17nM$	$2720M$

Proof: ($\Leftarrow$) Let $\log_{G_0} P_0$ be the discrete logarithm problem for the base point $G_0 = (0, y)$ and a point P_0. We can randomize these points by multiplying random exponents $r, s \in [1, \#E]$, namely let $G = rG_0, P = sP_0$ be randomized points. From the assumption, we can solve the discrete logarithm problem $\log_G P$, and thus the discrete logarithm $\log_{G_0} P_0 = (\log_G P)r/s \bmod \#E$.
($\Rightarrow$) Let A_0 be an oracle which solves the discrete logarithm problem for the base point $G_0 = (0, y)$, namely A_0 answers $\log_{G_0} P_0$ for a random point P_0. We try to construct algorithm A that solves the discrete logarithm problem with a random base. Algorithm A is going to compute $\log_G P$ for random inputs G, P. Algorithm A randomizes G with a random exponent $t \in [1, \#E]$ and obtains discrete logarithm $\log_{G_0} G$ by asking tG, G_0 to oracle A_0. Similarly, algorithm A obtains $\log_{G_0} P$. Then algorithm A returns the discrete logarithm $\log_G P = (\log_{G_0} P)/(\log_{G_0} G) \bmod \#E$.

From this theorem, there is no security disadvantage of using the based point $(0, y)$. Another advantage of using the base point $(0, y)$ is that memory required for base point is reduced to half.

In order to utilize the proposed method efficiently, we propose the following scenario. If we need to resist against both Goubin's attack and the ZVP attack as ECIES and single-pass ECDH, we compute the scalar multiplication on the original curve which has neither Goubin's point $(0, y)$ nor ZVP. Otherwise as ECDSA and two-pass ECDH, we compute on the isogenous curve of a small degree which has a point $G = (0, y)$, and map the result point to the original curve using isogeny.

We show the example of a curve to achieve this scenario. The curve $E : y^2 = x^3 + ax + b$ over $\mathbf{F}_p$ defined by

$$\begin{cases} p = 1461501637330902918203684832716283019653785059327, \\ a = 1461501637330902918203684832716283019653785059324 = -3, \\ b = 650811658836496945486322213172932667970910739301, \\ \#E = 1461501637330902918203686418909428858432566759883, \end{cases}$$

has neither $(0, y)$ nor *(ED1)* $3x^2 + a = 0$. Therefore this curve is secure against both Goubin's attack and the ZVP attack for the methods using the standard addition formulae. Then, the 3-isogenous curve $E' : y^2 = x^3 + a'x + b'$ over $\mathbf{F}_p$ defined by

$$\begin{cases} a' = 1461501637330902918203684832716283019653785059324 = -3, \\ b' = 457481734813551707109011364830625202028249398260, \end{cases}$$

has the point $G' = (0, y)$ such as

$$G' = (0, 914154799534049515652763431190255872227303582054).$$

The isogeny $\psi : E \to E'$ and $\psi^{-1} : E' \to E$ cost only $13M + I$ respectively. This cost is much smaller than improvement of the proposed method. The details of finding such a map are described in [2, Chapter VII].

6. Conclusion

We examined a countermeasure using isogeny against the ZVP attack. We showed that a class of curves (including some SECG curves) is still insecure against the ZVP attack despite the countermeasure—it can be never mapped to an efficient curve that is secure against the ZVP attack. This class satisfies the following three conditions: $a = -3$, E has odd order, and $(-3/p) = -1$. The condition $a = -3$ and E has prime order are important for security or efficiency. Thus the base field $\mathbf{F}_p$ with $(-3/p) = 1$ may be recommended.

In the addition, we compare some efficient methods of computing a scalar multiplication for each curve from SECG in consideration of the resistance against the ZVP attack. Finally we proposed a positive use of Goubin's point. If Goubin's point is used for a base point of scalar multiplication, we can improve about 11% for the double-and-add-always method.

References

[1] T. Akishita and T. Takagi, "Zero-value point attacks on elliptic curve cryptosystem," Information Security Conference—ISC2003, LNCS 2851, pp.218–233, Springer-Verlag, 2003.

[2] I. Blake, G. Seroussi, and N. Smart, Elliptic Curve in Cryptography, Cambridge University Press, 1999.

[3] E. Brier and M. Joye, "Weierstrass elliptic curve and side-channel attacks," Public Key Cryptography—PKC2002, LNCS 2274, pp.335–345, Springer-Verlag, 2002.

[4] E. Brier and M. Joye, "Fast point multiplication on elliptic curves through isogenies," Applied Algebra, Algebraic Algorithms and Error-Correcting Codes—AAECC2003, LNCS 2643, pp.43–50, Springer-Verlag, 2003.

[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, 1999.

[6] W. Fischer, C. Giraud, E.W. Knundsen, and J.-P. Seifert, "Parallel scalar multiplication on general elliptic curves over $\mathbf{F}_p$ 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—PKC2003, LNCS 2567, pp.199–211, Springer-Verlag, 2003.

[8] T. Izu, B. Möller, and T. Takagi, "Improved elliptic curve multiplication methods resistant against side channel attacks," Progress in Cryptology—INDOCRYPT2002, LNCS 2551, pp.296–313, Springer-Verlag, 2002.

[9] T. Izu and T. Takagi, "A fast parallel elliptic curve multiplication resistant against side channel attacks," Public Key Cryptography—PKC2002, LNCS 2274, pp.280–296, Springer-Verlag, 2002.

[10] T. Izu and T. Takagi, "A fast parallel elliptic curve multiplication resistant against side channel attacks," Technical Report CORR 2002-03. http://www.cacr.math.uwaterloo.ca/techreports/2002/corr2002-03.ps

[11] M. Joye and C. Tymen, "Protection against differential analysis for elliptic curve cryptography," Cryptographic Hardware and Embedded Systems—CHES2001, LNCS 2162, pp.377–390, Springer-Verlag, 2001.

[12] R. Lercier and F. Morain, "Counting the number of points of on elliptic curves over finite fields: Strategies and performances," Advances in Cryptology—Eurocrypt'95, LNCS 921, pp.79–94, Springer-Verlag, 1995.

[13] B. Möller, "Securing elliptic curve point multiplication against side-channel attacks," Information Security—ISC2001, LNCS 2200, pp.324–334, Springer-Verlag, 2001.

[14] B. Möller, "Parallelizable elliptic curve point multiplication method with resistance against side-channel attacks," Information Security—ISC2002, LNCS 2433, pp.402–413, Springer-Verlag, 2002.

[15] P.L. Montgomery, "Speeding the pollard and elliptic curve methods of factorization," Math. Comput., vol.48, pp.243–264, 1987.

[16] K. Okeya and T. Takagi, "The width-w NAF method provides small memory and fast elliptic scalar multiplications secure against side channel attacks," Cryptographer's Track RSA Conference—CT-RSA2003, LNCS 2612, pp.328–343, Springer-Verlag, 2003.

[17] N. Smart, "An analysis of Goubin's refined power analysis attack," Cryptographic Hardware and Embedded Systems—CHES2003, LNCS 2779, pp.281–290, Springer-Verlag, 2003.

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

Toru Akishita received the B.E. and M.E. degrees from University of Tokyo in 1996 and 1998, respectively. He has been working for Sony Corporation since 1998. He was a visiting researcher of the Department of Computer Science at Technische Universität Darmstadt from 2002 to 2003. His current research interests include cryptography and information security.

Tsuyoshi Takagi received the B.Sc. and M.Sc. degrees in mathematics from Nagoya University in 1993 and 1995, respectively. He had engaged in the research on network security at NTT Laboratories from 1995 to 2001. He received the Dr.rer.nat degree from Technische Universität Darmstadt, Germany in 2001. He is currently an assistant professor in the Department of Computer Science at Technische Universität Darmstadt. His current research interests are information security and cryptography. Dr. Takagi is a member of International Association for Cryptologic Research (IACR) and Darmstädter Zentrum für IT-Sicherheit (DZI).