A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems

Louis Goubin

CP8 Crypto Lab, SchlumbergerSema
36-38 rue de la Princesse, BP45, 78430 Louveciennes Cedex, France
lgoubin@slb.com

Abstract. As Elliptic Curve Cryptosystems are becoming more and more popular and are included in many standards, an increasing demand has appeared for secure implementations that are not vulnerable to side-channel attacks. To achieve this goal, several generic countermeasures against Power Analysis have been proposed in recent years.
In particular, to protect the basic scalar multiplication – on an elliptic curve – against Differential Power Analysis (DPA), it has often been recommended using "random projective coordinates", "random elliptic curve isomorphisms" or "random field isomorphisms". So far, these countermeasures have been considered by many authors as a cheap and secure way of avoiding the DPA attacks on the "scalar multiplication" primitive. However we show in the present paper that, for many elliptic curves, such a DPA-protection of the "scalar" multiplication is not sufficient. In a *chosen message* scenario, a Power Analysis attack is still possible even if one of the three aforementioned countermeasures is used. We expose a new Power Analysis strategy that can be successful for a large class of elliptic curves, including most of the sample curves recommended by standard bodies such as ANSI, IEEE, ISO, NIST, SECG or WTLS.
This result means that the problem of randomizing the basepoint may be more difficult than expected and that "standard" techniques have still to be improved, which may also have an impact on the performances of the implementations.

Keywords: Public-key cryptography, Side-channel attacks, Power Analysis, Differential Power Analysis (DPA), Elliptic curves, Smartcards.

1 Introduction

Since their introduction by V. Miller [21] and N. Koblitz [15], elliptic curve cryptosystems have been included in many international standards. One of their advantages is the small size of their keys, compared to those of RSA and ElGamal-type cryptosystems. Therefore, there has been a growing interest in implementing such cryptographic schemes in low-cost cryptographic devices such as smartcards.

Whereas the mathematical aspects of the security of such elliptic curve cryptosystems have been scrutinized for years now, a new threat appeared in 1998

Y.G. Desmedt (Ed.): PKC 2003, LNCS 2567, pp. 199–211, 2003.

when P. Kocher *et al.* [16, 17] introduced attacks based on power analysis. The idea of this new class of attacks is to monitor the power consumption of the electronic device while it is performing the cryptographic computation and then to use a statistical analysis of the measured consumption curves to deduce some information about the secret key stored in the device. The initial focus was on symmetric cryptosystems such as DES but public key cryptosystems were also shown vulnerable, including RSA [20] and elliptic curve cryptosystems [7].

The simple power analysis (SPA) only uses a single observed information. Two main stategies have been suggested to avoid this SPA attack.

The first strategy consists in hiding the fact that, during the computation of a scalar multiplication $d.P$ (d being an integer and P a point of the elliptic curve), the nature of the basic operations (*e.g.* addition or doubling) executed at each step depends on the value of the secret exponent d. Following this strategy, J.S. Coron proposed the "double-and-add-always" method [7]. The "Montgomery" method [23] also proved useful, giving a natural way of avoiding both timing and SPA attacks [25, 27]. For binary fields GF(2^m) a trick allows the computation of the scalar multiplication to be performed without using the y-coordinates [1, 19]. This property was extended to the case of prime fields GF(p) for elliptic curves which have "Montgomery-form" [28, 22] and then for any elliptic curve on GF(p) [12, 4, 8].

The second strategy consists in using indistinguishable addition and doubling in the scalar multiplication [5]. This has been shown feasible for some classes of curves over a prime field GF(p): Hesse-type [29, 13] and Jacobi-type [18] elliptic curves give a unified formula for computing both addition and doubling. A unified formula was recently proposed by E. Brier and M. Joye [4] to achieve the same indistinguishability for any elliptic curve on GF(2^m) or GF(p). For the binary field case, the insertion of dummy operations is also possible [3] to build an indistinguishable adding and doubling.

As pointed out in [7, 27, 14], these anti-SPA methods are not sufficient to prevent DPA attacks. However, many countermeasures have been proposed to transform an SPA-resistant scheme into a DPA-resistant scheme.

In [7], J.S. Coron suggested three anti-DPA methods: randomizing the secret exponent d, adding a random point R to P and using randomized projective homogeneous coordinates. The first two methods have been considered with skepticism in [27] and [12], but the third one is widely accepted: see [25], [27] or [18].

In the same spirit, M. Joye and C. Tymen [14] proposed two other generic methods: performing the computations in another elliptic curve which is deduced from the usual one through a random isomorphism, and performing the basic field operations with another representation of the field which is deduced from the usual one though a random field isomorphism. Note that [14] also gives a specific method for ABC curves (see also [9]).

Hence [7, 14] propose three generic methods ("random projective coordinates", "random elliptic curve isomorphisms" and "random field isomorphisms"), which so far have been considered by many authors as a cheap and secure way of

thwarting the DPA attacks: see *e.g.* [26], [3], [12]. For example it is stated in [4] that DPA attacks are not really a threat for elliptic curve cryptography since they are easily avoided by randomizing the inputs.

However, in the present paper we prove that, for a large class of elliptic curves, a Power Analysis attack can still work, even if we apply one of the three countermeasures above (together with an SPA countermeasure, such as "Add-and-double always", the Montgomery method, or a unified add/double formula).

In our scenario, the attacker can choose the message, *i.e.* the input of the "scalar multiplication" primitive. The only way the sensitive data are blinded is by using random projective coordinates (for the input), random elliptic curve isomorphisms (for the curve itself) or random field isomorphism (for the algebraic structure).

The paper is organized as follows. In section 2, we give the mathematical background about elliptic curves and scalar multiplication. In section 3, we describe our new strategy of attack, for each of the three DPA-countermeasures of [7, 14]. In section 4, we study more precisely the necessary conditions on the elliptic curve for our attack to work, and show that most of the sample curves proposed by standardization bodies [2, 10, 11, 24, 30, 31] verify these conditions.

2 Mathematical Background

2.1 Parametrizations of Elliptic Curves

General (affine) Weierstraß Form We consider the elliptic curve defined over a field K by its Weierstraß equation:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We denote by $E(K)$ the set of points $(x, y) \in K^2$ satisfying this equation. If we introduce a formal "point at infinity" denoted by $\mathcal{O}$, the set $E(K) \bigcup \mathcal{O}$ can be equiped with an operation $+$ which makes it an abelian group whose identity element is $\mathcal{O}$.

Projective Coordinates To avoid costly inversions, it is convenient to use projective coordinates. Among many possibilities developed in [6], we describe *homogeneous* and *Jacobian* projective coordinates.

Homogeneous projective coordinates are obtained by setting $x = X/Z$ and $y = Y/Z$, so that the general Weierstraß equation becomes

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

The point at infinity $\mathcal{O}$ is then represented by $(0, \theta, 0)$ for some $\theta \in K^*$, the affine point (x, y) is represented by a projective point $(\theta x, \theta y, \theta)$ for some $\theta \in K^*$ and a projective point $(X, Y, Z) \neq \mathcal{O}$ corresponds to the affine point $(X/Z, Y/Z)$.

Jacobian projective coordinates are obtained by setting $x = X/Z^2$ and $y = Y/Z^3$, so that the general Weierstraß equation becomes

$$E : Y^2 + a_1XYZ + a_3YZ^3 = X^3 + a_2X^2Z^2 + a_4XZ^4 + a_6Z^6.$$

The point at infinity $\mathcal{O}$ is then represented by $(\theta^2, \theta^3, 0)$ for some $\theta \in K^*$, the affine point (x, y) is represented by a projective point $(\theta^2 x, \theta^3 y, \theta)$ for some $\theta \in K^*$ and a projective point $(X, Y, Z) \neq \mathcal{O}$ corresponds to the affine point $(X/Z^2, Y/Z^3)$.

Simplified (affine) Weierstraß Forms When $\mathrm{Char}(K) \neq 2, 3$, the general Weierstraß equation can be simplified to

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

and the addition formulas, giving $P + Q = (x_3, y_3)$ from $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, become

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases} \quad \text{with} \quad \lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & \text{if } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q \end{cases}$$

When $\mathrm{Char}(K) = 2$ and the curve is non-supersingular, the general Weierstraß equation can be simplified to

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

and the addition formulas to

$$\begin{cases} x_3 = \lambda^2 + \lambda + a + x_1 + x_2 \\ y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \end{cases} \quad \text{with} \quad \lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2} & \text{if } P \neq Q \\ x_1 + \frac{y_1}{x_1} & \text{if } P = Q \end{cases}$$

Montgomery Form In order to ease the additions, P.L. Montgomery considered in [23] the family of elliptic curves of the following form (on a field K of characteristic $\neq 2$):

$$E : By^2 = x^3 + Ax^2 + x \qquad \text{with } B(A^2 - 4) \neq 0.$$

As noticed in [27], on such elliptic curves, the point $(0, 0)$ is of order 2 and the cardinality of $E(K)$ is always divisible by 4.

Hessian Form The Hessian-type elliptic curves were considered because they provide a unified formula for adding and doubling. Defined as the intersection of two quadrics, they can be given in the following form (on a field $K = \mathrm{GF}(q)$ with $q \equiv 2 \bmod 3$)

$$E : x^3 + y^3 + 1 = 3Dxy \qquad \text{with } D \in K, D^3 \neq 1.$$

As mentioned in [29, 13], point $(-1, 0)$ has order 3, that implies that the cardinality of $E(K)$ is always divisible by 3.

2.2 Usual SPA Countermeasures

To compute the scalar multiplication $d.P$, where $d = d_{n-1}2^{n-1} + d_{n-2}2^{n-2} + ... + d_1 2 + d_0$, with $d_{n-1} = 1$ and $P \in E(K)$, the following generic schemes have been proposed.

Classical Binary Method This method (see Algorithm 1) is analogous to the "square-and-multiply" principle used in RSA. Note that an analogous method exists, which is from the least significant bit. As noticed in [7], both are vulnerable to SPA attacks. That is why two other methods were introduced: the "Double-and-add-always" and the "Montgomery" methods.

Algorithm 1 Binary method (from the most significant bit)

Require: d, P
Ensure: $Q = d.P$
  $Q := P$
  for $i = n - 2$ down to 0 **do**
    $Q := 2.Q$
    if $d_i = 1$ **then**
      $Q := Q + P$
    end if
  end for
  Return Q

Double-and-Add-Always This method (Algorithm 2) was proposed in [7]. Note that an analogous method also exists, which is from the least significant bit [7, 12]. Both are SPA-resistant.

Algorithm 2 Double-and-add-always (from the most significant bit)

Require: d, P
Ensure: $Q_0 = d.P$
  $Q_0 := P$
  for $i = n - 2$ down to 0 **do**
    $Q_0 := 2.Q_0$
    $Q_1 := Q_0 + P$
    $Q_0 := Q_{d_i}$
  end for
  Return Q_0

Montgomery Method This method (Algorithm 3) was originally proposed in [23] and then elaborated in [1, 19, 25, 27, 28, 28, 22, 12, 4, 8]. It is SPA-resistant.

Algorithm 3 Montgomery's method

Require: d, P
Ensure: $Q_0 = d.P$
  $Q_0 := P$
  $Q_1 := 2.P$
  for $i = n - 2$ down to 0 **do**
    $Q_{1-d_i} := Q_0 + Q_1$
    $Q_{d_i} := 2.Q_{d_i}$
  end for
  Return Q_0

3 Our New Power Analysis Attack

We present here a Power Analysis attack that can work on many elliptic curves, even if an SPA-countermeasure (such as *Double-and-add-always* or the *Montgomery* method) is used, together with one of three aforementioned DPA-countermeasures (*Random projective coordinates*, *Random elliptic curve isomorphisms* or *Random field isomorphisms*).

3.1 The Strategy of the Attack

In this section, we describe the generic attack on an elliptic curve scalar multiplication, SPA-protected with *Double-and-add-always* or the *Montgomery* method. Note however that the attack is not limited to the case of binary methods (such as Algorithm 2 or Algorithm 3) and can be extended to the case of other addition chains.

Suppose the attacker already knows the highest bits d_{n-1}, ..., d_{i+1} of the secret multiplier d. We illustrate below how he can find the next bit d_i.

Let us suppose that the elliptic curve $E(K)$ contains a "special" point $P_0 \neq \mathcal{O}$, *i.e.* a point $P_0 \neq \mathcal{O}$ such that one of the (affine or projective) coordinates equals 0 in K.

Note that, for each of the three aforementioned DPA-countermeasures, the randomization does not affect the "special" property of the point P_0 (see section 3.2).

Double-and-Add-Always In Algorithm 2, for any given input point P, the value Q_0 obtained at the end of the i-th step of the loop is

$$Q_0 = \Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i} + d_i \Big).P.$$

We then have two cases:

- If $d_i = 0$, the values that appear during the $(i+1)$-st step of the loop are $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} \Big).P$ and $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 1 \Big).P$.
- If $d_i = 1$, the values that appear during the $(i+1)$-st step of the loop are $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 2 \Big).P$ and $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 3 \Big).P$.

We consider the point P_1 given by

$$P_1 = \Big[\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 1 \Big)^{-1} \bmod |E(K)| \Big].P_0$$

if $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 1 \Big)$ is coprime to $|E(K)|$ (this corresponds to the guess $d_i = 0$), or

$$P_1 = \Big[\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 3 \Big)^{-1} \bmod |E(K)| \Big].P_0$$

if $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 3 \Big)$ is coprime to $|E(K)|$ (this corresponds to the guess $d_i = 1$). In many cases, both possibilities can be chosen.

Let us now denote by C_r, for $1 \leq r \leq R$, the power consumption curves associated to r distinct computations of $d.P_1$. Because of the randomization performed before each computation, two curves corresponding to the same input value can be different.

We then consider the mean curve

$$\mathcal{M}_{P_1} = \frac{1}{R} \sum_{r=1}^{R} C_r.$$

If the guess for d_i (*i.e.* the choice for the point P_1) is incorrect, then $\mathcal{M}_{P_1} \simeq 0$, since the values appearing in the $(i+1)$-st step of the loop in Algorithm 2, are correctly randomized.

On the contrary, if the guess for d_i is correct, the mean curve $\mathcal{M}_{P_1}$ shows appreciable consumption "peaks" (compared to the mean power consumption of random points), corresponding to the treatment of the zero value in the $(i+1)$-st step of the loop.

Once d_i is known, the remaining bits d_{i-1}, ..., d_0 are recovered recursively, in the same way.

The Montgomery Method In Algorithm 3, for any given input point P, the values Q_0 and Q_1 obtained at the end of the i-th step of the loop are

$$Q_0 = \Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i} + d_i \Big).P$$

$$Q_1 = \Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i} + d_i + 1 \Big).P$$

We then have two cases:

- If $d_i = 0$, the values that appear during the $(i+1)$-st step of the loop are $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 1 \Big).P$ on the one hand, and $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} \Big).P$ or $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 2 \Big).P$ on the other hand.
- If $d_i = 1$, the values that appear during the $(i+1)$-st step of the loop are $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 3 \Big).P$ on the one hand, and $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 2 \Big).P$ or $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 4 \Big).P$ on the other hand.

We then consider then point P_1 given by

$$P_1 = \Big[\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 1 \Big)^{-1} \bmod |E(K)| \Big].P_0$$

if $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 1 \Big)$ is coprime to $|E(K)|$ (the guess is $d_i = 0$), or

$$P_1 = \Big[\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 3 \Big)^{-1} \bmod |E(K)| \Big].P_0$$

if $\Big(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 3 \Big)$ is coprime to $|E(K)|$ (the guess is $d_i = 1$).

The rest of the attack is then exactly the same as for the "Double-and-add-always" method: the bit d_i is found by power analysis, and the remaining bits d_{i-1}, ..., d_0 in the same way.

3.2 Application to Three Usual DPA-Countermeasures

Random Projective Coordinates The basic idea of this method is the following. The computation $Q = d.P$ is performed in projective coordinates. The basepoint $P = (x, y)$ can be represented by $(\theta x, \theta y, \theta)$ (*homogeneous* projective coordinates) or $(\theta^2 x, \theta^3 y, \theta)$ (*Jacobian* projective coordinates) for some $\theta \in K^*$.

Thus the computation is performed in 3 steps:

1. Choose a random $\theta \in K^*$ and let $P' = (\theta x, \theta y, \theta)$ (*homogeneous* projective coordinates) or $P' = (\theta^2 x, \theta^3 y, \theta)$ (*Jacobian* projective coordinates).
2. Compute $Q' = (X', Y', Z') = d.P'$.
3. Compute $Q = (X'/Z', Y'/Z')$ (*homogeneous* projective coordinates) or $Q = (X'/Z'^2, Y'/Z'^3)$ (*Jacobian* projective coordinates).

It is easy to see that the "special" point mentioned in section 3.1 remains of the form $(X, 0, Z)$ or $(0, Y, Z)$, whatever the random value θ may be. This shows that the above strategy applies.

Random Elliptic Curve Isomorphisms This method applies for an elliptic curve $E : y^2 = x^3 + ax + b$ on a field K of characteristic $\neq 2, 3$. For $P = (x, y)$, the computation of $Q = d.P$ is performed as follows:

1. Choose a random $\theta \in K^*$ and let $P' = (\theta^2 x, \theta^3 y, 1)$, $a' = \theta^{-4} a$ and $b' = \theta^{-6} b$.
2. Compute $Q' = (X', Y', Z') = d.P'$ in $E' : Y^2 Z = X^3 + a' X Z^2 + b' Z^3$ (homogeneous projective coordinates).
3. Compute $Q = (\theta^2 X'/Z', \theta^3 Y'/Z')$.

A variant consists in computing $Q' = d.P'$ in $E' : Y^3 = X^3 + a' X Z^4 + b' Z^6$ (Jacobian projective coordinates). It is easy to see that the "special" point mentioned in section 3.1 remains of the form $(X, 0, Z)$ or $(0, Y, Z)$, whatever the random value θ may be. This shows that the strategy of section 3.1 applies again.

Random Field Isomorphisms This method applies for an elliptic curve over a field $K = \mathrm{GF}(2^m) = \mathrm{GF}(2)[X]/\Pi(X)$, where Π is an irreducible polynomial of degree m over GF(2). The idea is that there are many such irreducible polynomials, so that K can be replaced (randomly) by an isomorphic field K'. The computation of $Q = d.P$ is performed as follows:

1. Choose a random irreducible polynomial Π' of degree m over GF(2) and let $K' = \mathrm{GF}(2)[X]/\Pi'(X)$.
2. Let φ be the field isomorphism between K and K' and $P' = \varphi(P)$.
3. Compute $Q' = d.P' \in K'^2$ in $E_{/K'}$.
4. Compute $Q = \varphi^{-1}(Q') \in K^2$.

Again, the "special" point mentioned in section 3.1 remains of the form $(x, 0)$ or $(0, y)$ (with the usual representation of the zero value), whatever the random polynomial Π' may be, so that the strategy of section 3.1 also applies.

4 Practical Applications

4.1 Computation of the "Special" Point

Special Points $(0, y)$ For a non-singular binary elliptic curve, whose reduced Weierstraß form is $E : y^2 + xy = x^3 + ax^2 + b$ over $K = \mathrm{GF}(2^m)$, we can choose $P_0 = (0, b^{2^{m-1}})$ as the "special" point.

For an elliptic curve $E : y^2 = x^3 + ax + b$ over a prime field $K = \mathrm{GF}(p)$ ($p > 3$), a special point of the form $(0, y)$ exists if and only if b is a quadratic residue modulo p, *i.e.* $\left(\frac{b}{p}\right) = 1$, where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol.

Among the standardized curves over a prime field satisfying the condition are: four curves proposed in FIPS 186-2 [24], the basic curve (curve number 7) proposed in WTLS [31], the seven curves proposed in ANSI X9.62 [2] (Annex J5), and two curves proposed in the working draft ISO/IEC 15946-4 [11] (Annexes A2.1 and A3.1). Only one curve of FIPS 186-2 (P224) and four curves of ISO/IEC 15946-4 (Annexes A1.1[1], A4.1, A5.1 and A6.1) have no special point $(0, y)$.

Special Points $(x, 0)$ For an elliptic curve $E : y^2 = x^3 + ax + b$ over a prime field $K = \mathrm{GF}(p)$ ($p > 3$), a special point of the form $(x, 0)$ exists if and only if the equation $x^3 + ax + b = 0$ has at least one root α in K.

Note that $P_0 = (\alpha, 0)$ is then a point of order 2 in $E(K)$. At first glance, it may seem that the strategy of section 3.1 fails, because P_1 does not depend on the guess made on d_i (P_1 is always equal to P_0). However, the successive values of Q that appear during Algorithm 2, for $i = n-2, ..., 0$ are either $\mathcal{O}$ (if $d_i = 0$) or P (if $d_i = 1$). Therefore the mean curve $\mathcal{M}_{P_1}$ shows in fact many peaks: for instance if Algorithm 2 is applied, with random homogeneous projective coordinates, the chip instructions manipulating $\mathcal{O} = (0, \theta, 0)$ are likely to create 2 such peaks (one for each 0), whereas the instructions manipulating $(\theta x, 0, \theta)$ are likely to create only 1 peak. This allows the attacker to recover all the bits d_i of the secret exponent d with only one application of the strategy of 3.1.

Some particular classes of curves automatically have such points of order 2. As mentioned in section 2.1, for all Montgomery-form elliptic curves, $(0, 0)$ is of order 2: its double is $\mathcal{O} = (0, 1, 0)$. For the Hessian form, all (x, x) are of order 2: their double is $\mathcal{O} = (-1, 1, 0)$.

4.2 Cardinality of the Elliptic Curve

Another condition for our strategy of attack to work is the fact that at least one of the values $\left(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 1\right)$ and $\left(\sum_{j=i+1}^{n-1} d_j 2^{j-i+1} + 3\right)$ is coprime to $|E(K)|$.

Over a prime field, FIPS 186-2 [24] or SECG [30] recommend to use elliptic curves of prime cardinality, and binary curves of cardinality $2q$ or $4q$ (q prime). All the curves proposed by WTLS [31] and ISO/IEC 15946-4 [11] have cardinality q, $2q$, $4q$, $6q$ (q prime). It is also true for most of the curves of ANSI X9.62 [2].

This shows that the condition above is true for most standardized elliptic curves.

[1] This curve however has a point of order 2, hence a special point $(x, 0)$.

5 Conclusion

This attack we present here shows that the problem of randomizing the base-point may be more difficult than expected and that "standard" techniques for securing the "scalar multiplication" primitive still have to be improved. Evaluating the performances of secure implementations of elliptic curve cryptosystems will require to take those improvements into account. The results of this paper also highlight the necessity to choose a message blinding method (before entering the "scalar multiplication" primitive) that prevents an attacker from choosing the messages.

References

[1] G. B. Agnew, R. C. Mullin, S. A. Vanstone, *An Implementation of Elliptic Curve Cryptosystems over* $\mathbf{F}_{2^{155}}$. IEEE Journal on Selected Areas in Communications, vol. 11, n. 5, pp 804-813, 1993. 200, 204

[2] ANSI X9.62, Public Key Cryptography for the Financial Services Industry, *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 1999. 201, 208

[3] A. Bellezza, *Countermeasures against Side-Channel Attacks for Elliptic Curve Cryptosystems*. IACR, Cryptology ePrint Archive, 2001/103, 2001. Available from `http://eprint.iacr.org/2001/103/` 200, 201

[4] E. Brier, M. Joye, *Weierstraß Elliptic Curves and Side-Channel Attacks*. In Proceedings of PKC'2002, LNCS 2274, pp. 335-345, Springer-Verlag, 2002. 200, 201, 204

[5] C. Clavier, M. Joye, *Universal Exponentiation Algorithm – A First Step towards Provable SPA-Resistance*. In Proceedings of CHES'2001, LNCS 2162, pp. 300-308, Springer-Verlag, 2001. 200

[6] H. Cohen, A. Miyaji, T. Ono, *Efficient Elliptic Curve Exponentiation Using Mixed Coordinates*. In Proceedings of ASIACRYPT'98, LNCS 1514, pp. 51-65, Springer-Verlag, 1998. 201

[7] J.-S. Coron, *Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems*. In Proceedings of CHES'99, LNCS 1717, pp. 292-302, Springer-Verlag, 1999. 200, 201, 203

[8] W. Fischer, C. Giraud, E. W. Knudsen, 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, 2002. Available from `http://eprint.iacr.org/2002/007/` 200, 204

[9] M. A. Hasan, *Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems*. In Proceedings of CHES'2000, LNCS 1965, pp. 93-108, Springer-Verlag, 2000. 200

[10] IEEE P1363, *Standard Specifications for Public-Key Cryptography*, 2000. Available from `http://groupe.ieee.org/groups/1363/` 201

[11] ISO/IEC 15946-4, *Information technology - Security techniques – Cryptographic techniques based on elliptic curves - Part 4: Digital signatures giving message recovery*. Working Draft, JTC 1/SC 27, December 28th, 2001. 201, 208

[12] T. Izu, T. Takagi, *A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks*. In Proceedings of PKC'2002, LNCS 2274, pp. 280-296, Springer-Verlag, 2002. 200, 201, 203, 204

[13] M. Joye, J.-J. Quisquater, *Hessian Elliptic Curves and Side-Channel Attacks*. In Proceedings of CHES'2001, LNCS 2162, pp. 412-420, Springer-Verlag, 2001. 200, 202

[14] M. Joye, C. Tymen, *Protections against Differential Analysis for Elliptic Curve Cryptography – An Algebraic Approach*. In Proceedings of CHES'2001, LNCS 2162, pp. 377-390, Springer-Verlag, 2001. 200, 201

[15] N. Koblitz, *Elliptic curve cryptosystems*. Mathematics of Computation, Vol. 48, pp. 203-209, 1987. 199

[16] P. Kocher, J. Jaffe, B. Jun, *Introduction to Differential Power Analysis and Related Attacks*. Technical Report, Cryptography Research Inc., 1998. Available from `http://www.cryptography.com/dpa/technical/index.html` 200

[17] P. Kocher, J. Jaffe, B. Jun, *Differential Power Analysis*. In Proceedings of CRYPTO'99, LNCS 1666, pp. 388-397, Springer-Verlag, 1999. 200

[18] P.-Y. Liardet, N. P. Smart, *Preventing SPA/DPA in ECC system using the Jacobi Form*. In Proceedings of CHES'2001, LNCS 2162, pp. 401-411, Springer-Verlag, 2001. 200

[19] J. López, R. Dahab, *Fast Multiplication on Elliptic Curves over GF*(2^m) *without Precomputation*. In Proceedings of CHES'99, LNCS 1717, pp. 316-327, Springer-Verlag, 1999. 200, 204

[20] T. S. Messerges, E. A. Dabbish, R. H. Sloan, *Power Analysis Attacks of Modular Exponentiation in Smartcards*. In Proceedings of CHES'99, pp. 144-157, Springer-Verlag, 1999. 200

[21] V. Miller, *Uses of elliptic curves in cryptography*. In Proceedings of CRYPTO'85, LNCS 218, pp. 417-426, Springer-Verlag, 1986. 199

[22] B. Möller, *Securing Elliptic Curve Point Multiplication against Side-Channel Attacks*. In Proceedings of ISC'2001, LNCS 2200, pp. 324-334, Springer-Verlag, 2001. 200, 204

[23] P. L. Montgomery, *Speeding the Pollard and Elliptic Curve Methods for Factorizations*. Mathematics of Computation, vol. 48, pp. 243-264, 1987. 200, 202, 204

[24] National Institute of Standards and Technology (NIST), *Recommended Elliptic Curves for Federal Government Use*. In the appendix of FIPS 186-2, available from `http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf` 201, 208

[25] K. Okeya, H. Kurumatani, K. Sakurai, *Elliptic Curve with the Montgomery Form and their cryptographic Applications*. In Proceedings of PKC'2000, LNCS 1751, pp. 238-257, Springer-Verlag, 2000. 200, 204

[26] K. Okeya, K. Miyazaki, K. Sakurai, *A Fast Scalar Multiplication Method with Randomized Projective Coordinates on a Montgomery-form Elliptic Curve Secure against Side Channel Attacks*. In Pre-proceedings of ICICS'2001, pp. 475-486, 2001. 201

[27] K. Okeya, K. Sakurai, *Power Analysis Breaks Elliptic Curve Cryptosystem even Secure against the Timing Attack*. In Proceedings of INDOCRYPT'2000, LNCS 1977, pp. 178-190, Springer-Verlag, 2000. 200, 202, 204

[28] K. Okeya, K. Sakurai, *Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the y-coordinate on a Montgomery-form Elliptic Curve*. In Proceedings of CHES'2001, LNCS 2162, pp. 126-141, Springer-Verlag, 2001. 200, 204

[29] N. P. Smart, *The Hessian Form of an Elliptic Curve*. In Proceedings of CHES'2001, LNCS 2162, pp. 118-125, Springer-Verlag, 2001. 200, 202

[30] Standards for Efficient Cryptography Group (SECG), *Specification of Standards for Efficient Cryptography*, Ver. 1.0, 2000. Available from `http://www.secg.org/secg_docs.htm` 201, 208

[31] Wireless Application Protocol (WAP) Forum, *Wireless Transport Layer Security (WTLS) Specification*. Available from `http://www.wapforum.org` 201, 208