Weierstraß Elliptic Curves and Side-Channel Attacks

Éric Brier and Marc Joye

Gemplus Card International, Card Security Group
Parc d'Activités de Gémenos, B.P. 100, 13881 Gémenos, France
{eric.brier,marc.joye}@gemplus.com
http://www.gemplus.com/smart/
http://www.geocities.com/MarcJoye/

—*To Erik De Win.*

Abstract. Recent attacks show how an unskilled implementation of elliptic curve cryptosystems may reveal the involved secrets from a single execution of the algorithm. Most attacks exploit the property that addition and doubling on elliptic curves are different operations and so can be distinguished from side-channel analysis. Known countermeasures suggest to add dummy operations or to use specific parameterizations. This is at the expense of running time or interoperability.
This paper shows how to rewrite the addition on the general Weierstraß form of elliptic curves so that the same formulæ apply equally to add two different points or to double a point. It also shows how to generalize to the Weierstraß form a protection method previously applied to a specific form of elliptic curves due to Montgomery.
The two proposed methods offer generic solutions for preventing side-channel attacks. In particular, they apply to all the elliptic curves recommended by the standards.

1 Introduction

Elliptic curve cryptosystems become more and more popular. With much shorter key lengths they (presumably) offer the same level of security than older cryptosystems. This advantage is especially attractive for small cryptographic devices, like the smart cards.

In the last years, a new class of attacks was exploited to retrieve some secret information embedded in a cryptographic device: the so-called side-channel attacks [Koc96,KJJ99]. By monitoring some side-channel information (e.g., the power consumption) it is possible, in some cases, to deduce the inner workings of an (unprotected) crypto-algorithm and thereby to recover the secret keys. To counteract these attacks, a variety of countermeasures have been proposed (e.g., see [KJJ99,Cor99,LD99,OS00,JQ01,LS01,JT01,Möl01]).

This paper only deals with *simple* side-channel analysis (e.g., SPA), that is, side-channel analysis from a single execution of the crypto-algorithm. The more

D. Naccache and P. Paillier (Eds.): PKC 2002, LNCS 2274, pp. 335–345, 2002.

sophisticated differential side-analysis (e.g., DPA) plays the algorithm several times and handles the results thanks to statistical tools. This second type of attacks is not really a threat for elliptic curve cryptography since they are easily avoided by randomizing the inputs [Cor99,JT01].

Simple side-channel analysis is made easier for elliptic curve algorithms because the operations of doubling and addition of points are intrinsically different. Efficient countermeasures are known but they only apply to *specific* elliptic curves. Although one can always choose of an elliptic curve of the required form, it is very likely that people will select elliptic curves recommended in a standard. For example, over a large prime field, the National Institute of Standards and Technology (NIST) [NIST00] (see also [SECG00]) recommends to use elliptic curves of prime order whereas the order of the curves suggested in [OS00,JQ01,LS01] is always divisible by a small factor.

The rest of this paper is organized as follows. In the next section, we review SPA-like attacks. In Section 3 and 4, we present two different approaches to prevent these attacks for elliptic curve cryptosystems using the (fully general) Weierstraß parameterization. Finally, we conclude in Section 5. (An introduction to elliptic curves may be found in appendix.)

2 SPA-Like Attacks

The most commonly used algorithm for computing $\mathbf{Q} = k\mathbf{P}$ on an elliptic curve is the double-and-add algorithm, that is, the additively written *square-and-multiply algorithm* [Knu81, § 4.6.3].[1]

Input: $\mathbf{P}$, $k = (k_{l-1}, \ldots, k_0)_2$
Output: $\mathbf{Q} = k\mathbf{P}$

1. $\mathbf{R}_0 = \mathbf{P}$
2. for $i = l - 2$ downto 0 do
3. $\quad \mathbf{R}_0 \leftarrow 2\mathbf{R}_0$
4. $\quad$ if $(k_i \neq 0)$ then $\mathbf{R}_0 \leftarrow \mathbf{R}_0 + \mathbf{P}$

return $(\mathbf{Q} = \mathbf{R}_0)$

Fig. 1. Double-and-add algorithm for computing $\mathbf{Q} = k\mathbf{P}$.

Suppose that the doubling of a point and the addition of two different points are implemented with different formulæ, these two operations may then be distinguished by simple side-channel analysis, e.g., by simple power anal-

[1] Noting that the computation of the inverse of an point is virtually free, we can advantageously use a NAF representation for k —that is, $k = (k'_l, \ldots, k'_0)$ with $k'_i \in \{-1, 0, 1\}$ and $k'_i \cdot k'_{i+1} = 0$— and replace Step 4 in the double-and-add algorithm by $\mathbf{R}_0 \leftarrow \mathbf{R}_0 + k'_i\mathbf{P}$. The expected speedup factor is 11.11% [MO90].

ysis (SPA) [KJJ99]. When the power trace shows a doubling followed by an addition, the current bit, say k_i, is equal to 1; $k_i = 0$ otherwise.

The usual way to prevent simple side-channel attacks consists in always repeating the same pattern of instructions, whatever the processed data. This can be done by

- performing some dummy operations [Cor99];
- using an alternate parameterization for the elliptic curve [LS01,JQ01];
- using an algorithm already satisfying this property [LD99,OS00,Möl01].

In [Cor99], it is suggested to use the double-and-add-*always* variant of the double-and-add algorithm (Fig. 1): a dummy addition is performed when $k_i = 0$. The drawback in this variant is that it penalizes the running time.

There are other algorithms towards SPA-resistance (e.g., [CJ01]) but they require the elementary operations —in our case the doubling and the addition of points— to be indistinguishable. To this purpose, several authors suggested to use alternate parameterizations for the elliptic curves. In [LS01], Liardet and Smart represents points with the Jacobi form as the intersection of two quadrics in $\mathbb{P}^3$. In [JQ01], Joye and Quisquater suggest to use the Hessian form. Unfortunately, contrary to the Weierstraß form, these parameterizations are not fully general. The Jacobi form has always a point of order 4 and the Hessian form a point of order 3. This implies that the cardinality of the corresponding elliptic curve is a multiple of 4 and 3, respectively. On the other hand, standard bodies [NIST00] or companies [SECG00] recommend elliptic curves that do not all fit in these settings. For instance, they recommend to use several elliptic curves of prime cardinality over a large prime field. Rather than investigating specific forms for parameterizing an elliptic curve, we show in the next section how to perform —with the *same* formula— a doubling or an addition with the general Weierstraß parameterization.

The third approach for defeating SPA-like attacks is an application of Montgomery's binary technique [Mon87] (see also [Möl01] when memory constraints are not a concern). For elliptic curves over binary fields, the algorithm is described in [LD99]. Over large prime fields, the algorithm is described in [OS00]. This latter algorithm is unfortunately limited to the Montgomery parameterization (that is, elliptic curves with a point of order 2). We generalize it in Section 4 so that it works with the general Weierstraß parameterization.

3 Revisiting the Addition Formulæ

As given in textbooks (see also Appendices A.1 and A.3), the formulæ for adding or doubling points on a Weierstraß elliptic curve are different. The discrepancy comes from the geometrical interpretation of the addition law on elliptic curves, the so-called *chord-and-tangent rule* (see Fig. 2).

Let ℓ be the line passing through $\mathbf{P}$ and $\mathbf{Q}$ (tangent at the curve E if $\mathbf{P} = \mathbf{Q}$) and let $\mathbf{T}$ be the third point of intersection of ℓ with E. If ℓ' is the line connecting $\mathbf{P}$ and $\mathcal{O}$ then $\mathbf{P} + \mathbf{Q}$ is the point such that E intersects E at $\mathbf{T}$, $\mathcal{O}$ and $\mathbf{P} + \mathbf{Q}$.

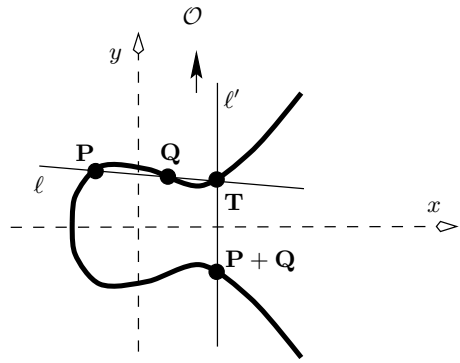

Fig. 2. Chord-and-tangent rule.

It is however possible to write the slope of line ℓ, λ, so that its expression remains valid for the addition or the doubling of points, which consequently unify the addition formulæ. This is explicited in the next proposition.

Proposition 1. *Let E be the elliptic curve over a field $\mathbb{K}$, given by the equation $E_{/\mathbb{K}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Let also $\mathbf{P} = (x_1, y_1)$ and $\mathbf{Q} = (x_2, y_2) \in E(\mathbb{K}) \setminus \{\mathcal{O}\}$ with $\mathrm{y}(\mathbf{P}) \neq \mathrm{y}(-\mathbf{Q})$. Then $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ where $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$, $y_3 = -(\lambda + a_1)x_3 - \mu - a_3$ with*

$$\lambda = \frac{x_1^2 + x_1x_2 + x_2^2 + a_2x_1 + a_2x_2 + a_4 - a_1y_1}{y_1 + y_2 + a_1x_2 + a_3}$$

and $\mu = y_1 - \lambda x_1$.

Proof. The condition $\mathrm{y}(\mathbf{P}) \neq \mathrm{y}(-\mathbf{Q})$ is equivalent to $y_1 \neq -y_2 - a_1x_2 - a_3$. Starting from the definition of λ when $\mathbf{P} \neq \mathbf{Q}$ (see Eq. (13) in Appendix A.1), we obtain

$$\begin{aligned}
\lambda &= \tfrac{y_1-y_2}{x_1-x_2} = \tfrac{y_1-y_2}{x_1-x_2} \cdot \tfrac{y_1-(-y_2-a_1x_2-a_3)}{y_1-(-y_2-a_1x_2-a_3)} \\
&= \tfrac{y_1^2+a_1x_2y_1+a_3y_1-y_2^2-a_1x_2y_2-a_3y_2}{(x_1-x_2)(y_1+y_2+a_1x_2+a_3)} \\
&= \tfrac{(y_1^2+a_1x_1y_1+a_3y_1)-(y_2^2+a_1x_2y_2+a_3y_2)+a_1x_2y_1-a_1x_1y_1}{(x_1-x_2)(y_1+y_2+a_1x_2+a_3)} \\
&= \tfrac{(x_1^3+a_2x_1^2+a_4x_1+a_6)-(x_2^3+a_2x_2^2+a_4x_2+a_6)-a_1y_1(x_1-x_2)}{(x_1-x_2)(y_1+y_2+a_1x_2+a_3)} \\
&= \tfrac{x_1^2+x_1x_2+x_2^2+a_2x_1+a_2x_2+a_4-a_1y_1}{y_1+y_2+a_1x_2+a_3} \quad .
\end{aligned}$$

We see that if we replace x_2 by x_1 and y_2 by y_1 (i.e., if we assume $\mathbf{P} = \mathbf{Q}$), the above formula for λ yields $\lambda = \frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}$, that is, the λ for the doubling (again see Eq. (13) in Appendix A.1). □

The above proposition can be particularized to the simplified Weierstraß equations (see Appendix A.3), depending on the field of definition.

Corollary 1. *Let* $\mathbb{K}$ *be a field of characteristic* $\mathrm{Char}\,\mathbb{K} \neq 2, 3$*, and let* E *be the elliptic curve given by the equation* $E_{/\mathbb{K}} : y^2 = x^3 + ax + b$*. Then for any* $\mathbf{P} = (x_1, y_1)$ *and* $\mathbf{Q} = (x_2, y_2) \in E(\mathbb{K}) \setminus \{\mathcal{O}\}$ *with* $y_1 \neq -y_2$*, we have* $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ *where*

$$x_3 = \left(\frac{x_1^2 + x_1x_2 + x_2^2 + a}{y_1 + y_2}\right)^2 - x_1 - x_2 \tag{1}$$

and

$$y_3 = \left(\frac{x_1^2 + x_1x_2 + x_2^2 + a}{y_1 + y_2}\right)(x_1 - x_3) - y_1 \ . \tag{2}$$

□

Corollary 2. *Let* $\mathbb{K}$ *be a field of characteristic* $\mathrm{Char}\,\mathbb{K} = 2$*, and let* E *be the non-supersingular elliptic curve given by the equation* $E_{/\mathbb{K}} : y^2 + xy = x^3 + ax^2 + b$*. Then for any* $\mathbf{P} = (x_1, y_1)$ *and* $\mathbf{Q} = (x_2, y_2) \in E(\mathbb{K}) \setminus \{\mathcal{O}\}$ *with* $y_1 \neq y_2 + x_2$*, we have* $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ *where*

$$\begin{aligned} x_3 = &\left(\frac{x_1^2 + x_1x_2 + x_2^2 + ax_1 + ax_2 + y_1}{y_1 + y_2 + x_2}\right)^2 + \\ &\left(\frac{x_1^2 + x_1x_2 + x_2^2 + ax_1 + ax_2 + y_1}{y_1 + y_2 + x_2}\right) + a + x_1 + x_2 \end{aligned} \tag{3}$$

and

$$y_3 = \left(\frac{x_1^2 + x_1x_2 + x_2^2 + ax_1 + ax_2 + y_1}{y_1 + y_2 + x_2}\right)(x_1 + x_3) + x_3 + y_1 \ . \tag{4}$$

□

Over a field $\mathbb{K}$ of characteristic $\mathrm{Char}\,\mathbb{K} \neq 2, 3$, remarking that $x_1^2 + x_1x_2 + x_2^2 = (x_1 + x_2)^2 - x_1x_2$, our formulæ (Eqs. (1) and (2)) require 1 inversion and 5 multiplications for adding two points. Over a field $\mathbb{K}$ of characteristic $\mathrm{Char}\,\mathbb{K} = 2$, our formulæ (Eqs. (3) and (4)) require 1 inversion and 3 multiplications plus 1 multiplication by a constant for adding two points (we neglect the cost of a squaring).

When $\mathrm{Char}\,\mathbb{K} \neq 2, 3$, projective coordinates are preferred [DMPW98]. (See Appendix A.2 for a short introduction to projective coordinates.)

We now give the projective (homogeneous) version of Eqs. (1) and (2). Write $\lambda = \frac{x_1^2 + x_1x_2 + x_2^2 + a}{y_1 + y_2} = \frac{(x_1 + x_2)^2 - x_1x_2 + a}{y_1 + y_2}$. Owing to the symmetry of λ, we may write from Eq. (2), $y_3 = \lambda(x_2 - x_3) - y_2$, since $\mathbf{P} + \mathbf{Q} = \mathbf{Q} + \mathbf{P}$, and consequently we have $2y_3 = \lambda(x_1 + x_2 - 2x_3) - (y_1 + y_2)$. Setting $x_i = \frac{X_i}{Z_i}$ and $y_i = \frac{Y_i}{Z_i}$, we so obtain after a few algebra

$$\begin{cases} X_3 = 2FW \\ Y_3 = R(G - 2W) - L^2 \\ Z_3 = 2F^3 \end{cases} \tag{5}$$

where $U_1 = X_1Z_2$, $U_2 = X_2Z_1$, $S_1 = Y_1Z_2$, $S_2 = Y_2Z_1$, $Z = Z_1Z_2$, $T = U_1 + U_2$, $M = S_1 + S_2$, $R = T^2 - U_1U_2 + aZ^2$, $F = ZM$, $L = MF$, $G = TL$, and

$W = R^2 - G$. Therefore, adding two points with our unified formulæ require 17 multiplications plus 1 multiplication by constant. When $a = -1$ then we may write $R = (T - Z)(T + Z) - U_1U_2$ and the number of multiplications decreases to 16.

4 Generalizing Montgomery's Technique

In [Mon87], Montgomery developed an original technique to compute multiples of points on an elliptic curve. His technique is based on the fact that the sum of two points whose difference is a known point can be computed without the y-coordinate of the two points.

Input: $\mathbf{P}$, $k = (k_{l-1}, \ldots, k_0)_2$
Output: $\mathrm{x}(k\mathbf{P})$

1. $\mathbf{R}_0 = \mathbf{P}$; $\mathbf{R}_1 = 2\mathbf{P}$
2. for $i = l - 2$ downto 0 do
3. if $(k_i = 0)$ then
4. $\mathrm{x}(\mathbf{R}_1) \leftarrow \mathrm{x}(\mathbf{R}_0 + \mathbf{R}_1)$; $\mathrm{x}(\mathbf{R}_0) \leftarrow \mathrm{x}(2\mathbf{R}_0)$
5. else [if $(k_i = 1)$]
6. $\mathrm{x}(\mathbf{R}_0) \leftarrow \mathrm{x}(\mathbf{R}_0 + \mathbf{R}_1)$; $\mathrm{x}(\mathbf{R}_1) \leftarrow \mathrm{x}(2\mathbf{R}_1)$

return $(\mathrm{x}(\mathbf{R}_0))$

Fig. 3. Montgomery's technique for computing $\mathrm{x}(k\mathbf{P})$.

(Observe that the difference $\mathbf{R}_1 - \mathbf{R}_0$ remains invariant throughout the algorithm: $\mathbf{R}_1 - \mathbf{R}_0 = \mathbf{P}$.)

For sake of efficiency, Montgomery restricted his study to elliptic curves of the form $by^2 = x^3 + ax^2 + x$ over a field $\mathbb{K}$ of characteristic $\neq 2, 3$. The next proposition gives the corresponding formulæ in the general case. The formulæ over a field of characteristic 2 are given in [LD99, Lemmas 2 and 3].

Proposition 2. *Let $\mathbb{K}$ be a field of characteristic* $\mathrm{Char}\,\mathbb{K} \neq 2, 3$*, and let E be the elliptic curve given by the equation $E_{/\mathbb{K}} : y^2 = x^3 + ax + b$. Let also $\mathbf{P} = (x_1, y_1)$ and $\mathbf{Q} = (x_2, y_2) \in E(\mathbb{K}) \setminus \{\mathcal{O}\}$ with $\mathbf{P} \neq \pm\mathbf{Q}$. Given the point $\mathbf{P} - \mathbf{Q} = (x, y)$, the x-coordinate of $\mathbf{P} + \mathbf{Q}$ satisfies*

$$\mathrm{x}(\mathbf{P} + \mathbf{Q}) = \frac{-4b(x_1 + x_2) + (x_1x_2 - a)^2}{x(x_1 - x_2)^2} \quad . \tag{6}$$

Furthermore, if $y_1 \neq 0$ then the x-coordinate of $2\mathbf{P}$ satisfies

$$\mathrm{x}(2\mathbf{P}) = \frac{({x_1}^2 - a)^2 - 8bx_1}{4({x_1}^3 + ax_1 + b)} \quad . \tag{7}$$

Proof. From Eq. (16) (in Appendix A.3), letting x_3 the x-coordinate of $\mathbf{P}+\mathbf{Q}$, we have

$$\begin{aligned} x_3(x_1-x_2)^2 &= (y_1-y_2)^2-(x_1+x_2)(x_1-x_2)^2 \\ &= ({y_1}^2+{y_2}^2-2y_1y_2)-({x_1}^3+{x_2}^3-{x_1}^2x_2-x_1{x_2}^2) \\ &= -2y_1y_2+2b+(a+x_1x_2)(x_1+x_2)\ . \end{aligned}$$

Similarly, the x-coordinate of $\mathbf{P}-\mathbf{Q}$ satisfies $x(x_1-x_2)^2 = 2y_1y_2+2b+(a+x_1x_2)(x_1+x_2)$. Now by multiplying the two equations, we obtain

$$\begin{aligned} x_3\cdot x(x_1-x_2)^4 &= -4{y_1}^2{y_2}^2+[2b+(a+x_1x_2)(x_1+x_2)]^2 \\ &= -4({x_1}^3+ax_1+b)({x_2}^3+ax_2+b)+ \\ &\qquad [2b+(a+x_1x_2)(x_1+x_2)]^2 \\ &= [-4b(x_1+x_2)+(x_1x_2-a)^2](x_1-x_2)^2 \end{aligned}$$

which, dividing through by $(x_1-x_2)^2$, yields the desired result.

When $y_1\neq 0$ (i.e., when $2\mathbf{P}\neq\mathcal{O}$), we have from Eq. (16) (in appendix) that $\mathrm{x}(2\mathbf{P}) = \frac{({3x_1}^2+a)^2}{4{y_1}^2}-2x_1 = \frac{({x_1}^2-a)^2-8bx_1}{4({x_1}^3+ax_1+b)}$. □

Another useful feature of Montgomery's technique is that the y-coordinate of a point $\mathbf{P}$ can be deduced from its x-coordinate, the x-coordinate of another point $\mathbf{Q}$ and the coordinates of the point $\mathbf{P}-\mathbf{Q}$. This is explicited in the next proposition.

Proposition 3. *Let $\mathbb{K}$ be a field of characteristic* $\mathrm{Char}\,\mathbb{K}\neq 2,3$*, and let E be the elliptic curve given by the equation $E_{/\mathbb{K}}: y^2=x^3+ax+b$. Let also $\mathbf{P}=(x_1,y_1)$ and $\mathbf{Q}=(x_2,y_2)\in E(\mathbb{K})\setminus\{\mathcal{O}\}$ with $\mathbf{P}\neq\mathbf{Q}$. Given the point $\mathbf{P}-\mathbf{Q}=(x,y)$, if $y\neq 0$ then the y-coordinate of $\mathbf{P}$ satisfies*

$$\mathrm{y}(\mathbf{P}) = y_1 = \frac{2b+(a+xx_1)(x+x_1)-x_2(x-x_1)^2}{2y}\ . \tag{8}$$

Proof. Define $\mathbf{D}=\mathbf{P}-\mathbf{Q}=(x,y)$. Since $\mathbf{Q}=\mathbf{P}+\mathbf{D}=(x_2,y_2)$, we obtain from Eq. (16) (in appendix) $x_2 = \left(\frac{y_1-y}{x_1-x}\right)^2-x_1-x = \frac{-2yy_1+2b+(a+xx_1)(x+x_1)}{(x_1-x)^2}$, which concludes the proof, multiplying through by $(x_1-x)^2$. □

Assume we are working on an elliptic curve over a field $\mathbb{K}$ of characteristic different from 2 or 3. We refer the reader to [LD99] for a field of characteristic 2. Within projective (homogeneous) coordinates, Equation (6) becomes

$$\begin{cases} \mathrm{X}(\mathbf{P}+\mathbf{Q}) = -4bZ_1Z_2(X_1Z_2+X_2Z_1)+(X_1X_2-aZ_1Z_2)^2\,, \\ \mathrm{Z}(\mathbf{P}+\mathbf{Q}) = x\cdot(X_1Z_2-X_2Z_1)^2\,. \end{cases} \tag{9}$$

Hence, the addition of two points requires 7 multiplications plus 3 multiplications by a constant.

The formulæ to double a point within homogeneous projective coordinates are obtained similarly from Eq. (7). We get

$$\begin{cases} \mathrm{X}(2\mathbf{P}) = ({X_1}^2 - a{Z_1}^2)^2 - 8bX_1{Z_1}^3, \\ \mathrm{Z}(2\mathbf{P}) = 4Z_1({X_1}^3 + aX_1{Z_1}^2 + b{Z_1}^3). \end{cases} \tag{10}$$

This can be evaluated with 7 multiplications plus 2 multiplications by a constant.

Consequently, the whole protected algorithm of Fig. 3 requires roughly $14l$ multiplications, $5l$ multiplications by a constant and 1 inversion for computing $\mathrm{x}(k\mathbf{P})$, where l is the bit-length of k. This is more than in [OS00] but our method does not require specific curves. Note also that, by Proposition 3, the y-coordinate of $\mathbf{Q} = k\mathbf{P}$ can be recovered from $\mathrm{x}(\mathbf{R}_0) = \mathrm{x}(\mathbf{Q})$, $\mathrm{x}(\mathbf{R}_1)$ and $\mathbf{P}$.

5 Conclusion

This paper described two alternative approaches in the development of countermeasures against simple side-channel attacks. The main merits of the proposed methods is that they are not specific to a particular class of elliptic curves. In particular, they apply to all the elliptic curves recommended in the standards.

References

CJ01. Christophe Clavier and Marc Joye. Universal exponentiation algorithm: A first step towards provable SPA-resistance. In Ç.K. Koç, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 305–314. Springer-Verlag, 2001.

Cor99. Jean-Sébastien Coron. Resistance against differential power analysis for elliptic curve cryptosystems. In Ç.K. Koç and C. Paar, editors, *Cryptographic Hardware and Embedded Systems (CHES '99)*, volume 1717 of *Lecture Notes in Computer Science*, pages 292–302. Springer-Verlag, 1999.

DMPW98. Erik De Win, Serge Mister, Bart Preneel, and Michael Wiener. On the performance of signature schemes based on elliptic curves. In J.-P. Buhler, editor, *Algorithmic Number Theory Symposium*, volume 1423 of *Lecture Notes in Computer Science*, pages 252–266. Springer-Verlag, 1998.

JQ01. Marc Joye and Jean-Jacques Quisquater. Hessian elliptic curves and side-channel attacks. In Ç.K. Koç, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 412–420. Springer-Verlag, 2001.

JT01. Marc Joye and Christophe Tymen. Protections against differential analysis for elliptic curve cryptography: an algebraic approach. In Ç.K. Koç, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 386–400. Springer-Verlag, 2001.

KJJ99. Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In M. Wiener, editor, *Advances in Cryptology – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer-Verlag, 1999.

Knu81. Donald E. Knuth. *The art of computer programming, v. 2. Seminumerical algorithms*. Addison-Welsley, 2nd edition, 1981.

Koc96. Paul Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In N. Koblitz, editor, *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer-Verlag, 1996.

LD99. Julio López and Ricardo Dahab. Fast multiplication on elliptic curves over $GF(2^m)$ without precomputation. In Ç.K. Koç and C. Paar, editors, *Cryptographic Hardware and Embedded Systems*, volume 1717 of *Lecture Notes in Computer Science*, pages 316–327. Springer-Verlag, 1999.

LS01. Pierre-Yvan Liardet and Nigel P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In Ç.K. Koç, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 401–411. Springer-Verlag, 2001.

MO90. François Morain and Jorge Olivos. Speeding up the computations on an elliptic curve using addition-subtraction chains. *Theoretical Informatics and Applications*, 24:531–543, 1990.

Möl01. Bodo Möller. Securing elliptic curve point multiplication against side-channel attacks. In G.I. Davida and Y. Frankel, editors, *Information Security*, volume 2200 of *Lecture Notes in Computer Science*, pages 324–334. Springer-Verlag, 2001.

Mon87. Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, January 1987.

NIST00. National Institute of Standards and Technology (NIST). Digital signature standard (DSS). FIPS PUB 186-2, 2000.

OS00. Katsuyuki Okeya and Kouichi Sakurai. Power analysis breaks elliptic curve cryptosystems even secure against the timing attack. In B. Roy and E. Okamoto, editors, *Progress in Cryptology – INDOCRYPT 2000*, volume 1977 of *Lecture Notes in Computer Science*, pages 178–190. Springer-Verlag, 2000.

SECG00. Certicom Research. Standards for efficient cryptography. Version 1.0, 2000. Available at url `http://www.secg.org/`.

Sil86. Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.

A Mathematical Background

A.1 Elliptic Curves

Consider the elliptic curve defined over a field $\mathbb{K}$ given by the Weierstraß equation:

$$E_{/\mathbb{K}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ . \tag{11}$$

It is well-known that formally adding the point $\mathcal{O}$ makes the set of points $(x, y) \in \mathbb{K} \times \mathbb{K}$ satisfying Eq. (11) into an Abelian group [Sil86, Chapter III]. We denote this group $E(\mathbb{K})$. We have:

(i) $\mathcal{O}$ is the identity element: $\forall \mathbf{P} \in E(\mathbb{K})$, $\mathbf{P} + \mathcal{O} = \mathbf{P}$.

(ii) The inverse of $\mathbf{P} = (x_1, y_1)$ is $-\mathbf{P} = (x_1, -y_1 - a_1 x_1 - a_3)$.
(iii) If $\mathbf{Q} = -\mathbf{P}$ then $\mathbf{P} + \mathbf{Q} = \mathcal{O}$.
(iv) Let $\mathbf{P} = (x_1, y_1)$ and $\mathbf{Q} = (x_2, y_2) \in E(\mathbb{K})$ with $\mathbf{Q} \neq -\mathbf{P}$. Then $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ where

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad \text{and} \quad y_3 = -(\lambda + a_1)x_3 - \mu - a_3 \tag{12}$$

with

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } \mathbf{P} \neq \mathbf{Q} \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } \mathbf{P} = \mathbf{Q} \end{cases} \tag{13}$$

and $\mu = y_1 - \lambda x_1$.

A.2 Projective Representations

The formula for λ involves an inversion and this may be a rather costly operation. For this reason, one usually prefer *projective coordinates*.

Within *projective Jacobian coordinates*, we put $x = X/Z^2$ and $y = Y/Z^3$ and the Weierstraß equation of the elliptic curve becomes

$$E_{/\mathbb{K}} : Y^2 + a_1XYZ + a_3YZ^3 = X^3 + a_2X^2Z^2 + a_4XZ^4 + a_6Z^6 \tag{14}$$

where the point at infinity is represented as $\mathcal{O} = (\theta^2, \theta^3, 0)$ for some $\theta \in \mathbb{K} \setminus \{0\}$. The affine point (x_1, y_1) is represented by a projective point $(\theta^2 x_1, \theta^3 y_1, \theta)$ for some $\theta \in \mathbb{K} \setminus \{0\}$ and conversely a projective point $(X_1, Y_1, Z_1) \neq \mathcal{O}$ corresponds to the affine point $(X_1/Z_1^2, Y_1/Z_1^3)$.

Within *projective homogeneous coordinates*, we put $x = X/Z$ and $y = Y/Z$ and the Weierstraß equation of the elliptic curve is

$$E_{/\mathbb{K}} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \ . \tag{15}$$

The point at infinity is represented as $(0, \theta, 0)$ for some $\theta \in \mathbb{K} \setminus \{0\}$. The affine point (x_1, y_1) is represented by a projective point $(\theta x_1, \theta y_1, \theta)$ for some $\theta \in \mathbb{K} \setminus \{0\}$ and a projective point $(X_1, Y_1, Z_1) \neq \mathcal{O}$ corresponds to the affine point $(X_1/Z_1, Y_1/Z_1)$.

Note that in projective coordinates (Jacobian or homogeneous), only the point at infinity has its Z-coordinate equal to 0. The addition formulæ in projective coordinates are derived from the affine formulæ by replacing each affine point (x_i, y_i) by a projective equivalent (X_i, Y_i, Z_i).

A.3 Simplified Equations

Two main families of elliptic curves are used in cryptography, according to the base field $\mathbb{K}$ over which the curve is defined. In this appendix, we give the corresponding simplified formulæ for each family.

Char $\mathbb{K} \neq 2, 3$

In this case, the general Weierstraß equation (Eq. (11)) may be simplified to

$$E_{/\mathbb{K}} : y^2 = x^3 + ax + b \ .$$

Taking $a_1 = a_2 = a_3 = 0$, $a_4 = a$ and $a_6 = b$ in Eqs. (12) and (13), the sum of $\mathbf{P} = (x_1, y_2)$ and $\mathbf{Q} = (x_2, y_2)$ (with $\mathbf{P} \neq -\mathbf{Q}$) is given by $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda(x_1 - x_3) - y_1 \tag{16}$$

with $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$ if $\mathbf{P} \neq \mathbf{Q}$, and $\lambda = \frac{3{x_1}^2 + a}{2y_1}$ if $\mathbf{P} = \mathbf{Q}$.

Char $\mathbb{K} = 2$ (Non-supersingular Curves)

Supersingular elliptic curves are cryptographically weaker, we therefore consider only non-supersingular elliptic curves. The simplified Weierstraß equation then becomes

$$E_{/\mathbb{K}} : y^2 + xy = x^3 + ax^2 + b \ .$$

Again, from Eqs. (12) and (13), the sum of $\mathbf{P} = (x_1, y_2)$ and $\mathbf{Q} = (x_2, y_2)$ (with $\mathbf{P} \neq -\mathbf{Q}$) is given by $\mathbf{P} + \mathbf{Q} = (x_3, y_3)$ where

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 \quad \text{and} \quad y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \tag{17}$$

with $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$ if $\mathbf{P} \neq \mathbf{Q}$, and $\lambda = x_1 + \frac{y_1}{x_1}$ if $\mathbf{P} = \mathbf{Q}$.