Hessian Elliptic Curves and Side-Channel Attacks

[Published in Ç.K. Koç, D. Naccache, and C. Paar, Eds., *Cryptographic Hardware and Embedded Systems – CHES 2001*, vol. 2162 of *Lecture Notes in Computer Science*, pp. 402–410, Springer-Verlag, 2001.]

Marc Joye[1] and Jean-Jacques Quisquater[2]

[1] Gemplus Card International, Card Security Group
Parc d'Activités de Gémenos, B.P. 100, 13881 Gémenos, France
marc.joye@gemplus.com
http://www.geocities.com/MarcJoye/
[2] UCL Crypto Group, Université catholique de Louvain
Place du Levant 3, 1348 Louvain-la-Neuve, Belgium
jjq@dice.ucl.ac.be

Abstract. Side-channel attacks are a recent class of attacks that have been revealed to be very powerful in practice. By measuring some side-channel information (running time, power consumption, ...), an attacker is able to recover some secret data from a carelessly implemented crypto-algorithm. This paper investigates the Hessian parameterization of an elliptic curve as a step towards resistance against such attacks in the context of elliptic curve cryptography. The idea is to use the same procedure to compute the addition, the doubling or the subtraction of points. As a result, this gives a 33% performance improvement as compared to the best reported methods and requires much less memory.

Keywords. Elliptic curves, cryptography, side-channel attacks, implementation, smart cards.

1 Introduction

Side-channel attacks are a recent class of attacks that have been revealed to be very powerful in practice. By measuring some side-channel information (running time, power consumption, ...), an attacker is able to recover some secret data from a carelessly implemented crypto-algorithm. This paper investigates the Hessian parameterization of an elliptic curve as a step towards resistance against such attacks in the context of elliptic curve cryptography. The idea is to use the same procedure to compute the addition, the doubling or the subtraction of points. As a result, this gives a 33% performance improvement as compared to the best reported methods and requires much less memory.

The rest of this paper is organized as follows. The next section introduces the theory of elliptic curves and reviews the related work for computing the multiple of a point on an elliptic curve. Section 3 presents the Hessian parameterization of an elliptic curve. It also proves some useful results on this special parameterization. The side-channel attacks are defined in Section 4 and some countermeasures are discussed. Finally, Section 5 shows how the Hessian parameterization helps to efficiently foil such attacks in the context of elliptic curve cryptography.

2 Elliptic Curve Multiplication

To ease the exposition we assume throughout this paper that $\mathbb{K}$ is a field of characteristic $p > 3$.

2.1 Basic facts

We start with a short introduction to elliptic curves.

Definition 1. *Up to a birational equivalence, an* elliptic curve *over a field* $\mathbb{K}$ *is a plane nonsingular cubic curve with a* $\mathbb{K}$*-rational point.*

Elliptic curves are often expressed in terms of Weierstraß equations:

$$E_{/\mathbb{K}} : y^2 = x^3 + ax + b \quad (\text{with } 4a^3 + 27b^2 \neq 0) \tag{1}$$

where a and $b \in \mathbb{K}$. The condition $4a^3 + 27b^2 \neq 0$ ensures that the *discriminant*

$$\Delta = -16(4a^3 + 27b^2) \tag{2}$$

is nonzero, or equivalently that the points (x, y) on the curve are nonsingular.

More importantly, together with the *point at infinity* $\boldsymbol{O}$, the points of an elliptic curve form an Abelian group (with identity element $\boldsymbol{O}$) under the *chord-and-tangent rule* defined as follows. If $\boldsymbol{P} = (x_1, y_1)$, then its inverse is given by $-\boldsymbol{P} = (x_1, -y_1)$. The sum of two points $\boldsymbol{P} = (x_1, y_1)$ and $\boldsymbol{Q} = (x_2, y_2)$ (with $\boldsymbol{Q} \neq -\boldsymbol{P}$) is equal to $\boldsymbol{R} = (x_3, y_3)$ where

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

$$\text{with } \lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} & \text{if } x_1 = x_2\,, \\ \dfrac{y_1 - y_2}{x_1 - x_2} & \text{otherwise}\ . \end{cases}$$

The previous formulæ require 2 or 3 multiplications and 1 inversion to add two points. Since this latter operation is costly (an inversion roughly takes the same amount of time as 23 multiplications [8]), *projective* representations of Weierstraß equations may be preferred.

3 Hessian Curves

In this section, we formally define the Hessian elliptic curves [10] (see also [2, p. 36] and [15]) and give some results on this special parameterization.

Definition 2. *An* Hessian elliptic curve *over* $\mathbb{K}$ *is a plane cubic curve given by an equation of the form*

$$E_{/\mathbb{K}} : u^3 + v^3 + 1 = 3Duv\,, \tag{3}$$

or in projective coordinates,

$$E_{/\mathbb{K}} : U^3 + V^3 + W^3 = 3DUVW \tag{4}$$

where $D \in \mathbb{K}$ *and* $D^3 \neq 1$.

As shown in the next lemma, the condition $D^3 \neq 1$ imposes that the curve is nonsingular, that is, elliptic.

Lemma 1. *An Hessian cubic curve* $E_D(\mathbb{K})$ *is singular if and only if* $D^3 = 1$.

Proof. Let $\boldsymbol{P} = (U_1 : V_1 : W_1)$ be a singular point. Then $U_1^2 - DV_1W_1 = V_1^2 - DU_1W_1 = W_1^2 - DV_1W_1 = 0$, hence $U_1^3 = V_1^3 = W_1^3$ $(\neq 0)$. Therefore there exist $k \in \mathbb{K}^*$ and $r, s, t \in \mathbb{Z}_3$ such that $U_1 = k\omega^r$, $V_1 = k\omega^s$ and $W_1 = k\omega^t$ where ω is a non-trivial cubic root of unity. Together with Eq. (4), this yields $3k^3 = 3Dk^3\omega^{r+s+t}$, or equivalently, $D^3 = 1$. □

Proposition 1. *The Hessian curve given by Eq. (3) is birationnally equivalent to the Weierstraß equation*

$$y^2 = x^3 - 27D(D^3 + 8)x + 54(D^6 - 20D^3 - 8)\,, \tag{5}$$

under the transformations

$$(u, v) = \big(\eta(x + 9D^2), -1 + \eta(3D^3 - Dx - 12)\big) \tag{6}$$

and

$$(x, y) = \big(-9D^2 + \xi u, 3\xi(v - 1)\big) \tag{7}$$

where $\eta = \frac{6(D^3-1)(y+9D^3-3Dx-36)}{(x+9D^2)^3+(3D^3-Dx-12)^3}$ *and* $\xi = \frac{12(D^3-1)}{Du+v+1}$.

Proof. Sending the point $\boldsymbol{P_0} = (0, -1)$ to the origin via the map $v \mapsto v - 1$, Eq. (3) becomes

$$\sum_{i=1}^{3} c_i(u, v) = 0 \tag{*}$$

where $c_3(u, v) = u^3 + v^3$, $c_2(u, v) = -3v(Du + v)$ and $c_1(u, v) = 3(Du + v)$. The slope λ of the tangent at $\boldsymbol{P_0}$ is equal to $-D$. Letting $d(u, v) = c_2(u, v)^2 - 4c_1(u, v)c_3(u, v)$, we have $d(u, \lambda u+1) = 12(D^3-1)u^3-27D^2u^2+18Du-3$. Hence, by Nagell reduction (see Theorem 7.4.9 in [5, p. 393]) and letting $B = 12(D^3-1)$,

Eq. (*) is birationnally equivalent to $y^2 = x^3 - 27D^2x^2 + 18DBx - 3B^2$ under the transformations

$$\begin{aligned}(u,v) &= \left(\tfrac{x(By-c_2(x,\lambda x+B))}{2c_3(x,\lambda x+B)}, \tfrac{(\lambda x+B)(By-c_2(x,\lambda x+B))}{2c_3(x,\lambda x+B)}\right)\\ &= \left(\tfrac{Bx(y+3B-3Dx)}{2(x^3+(B-Dx)^3)}, \tfrac{B(B-Dx)(y+3B-3Dx)}{2(x^3+(B-Dx)^3)}\right)\end{aligned}$$

and, noting from Eq. (*) that $2c_3(u,v) + c_2(u,v) = -2c_1(u,v) - c_2(u,v)$,

$$(x,y) = \left(\tfrac{Bu}{v-\lambda u}, \tfrac{B(2c_3(u,v)+c_2(u,v))}{(v-\lambda u)^2}\right) = \left(\tfrac{12(D^3-1)u}{Du+v}, \tfrac{36(D^3-1)(v-2)}{Du+v}\right) .$$

Replacing now x by $x+9D^2$, we finally obtain the required equation and the corresponding transformations. □

A 'straight-forward' application of the chord-and-tangent rule yields rather cumbersome formulæ for the doubling and the addition on an Hessian curve. The correct way is to use the Cauchy-Desboves' s formulæ (see Appendix A), which exploit the symmetry of Eq. (4). Plugging $W = 0$ into Eq. (4), we get the point at infinity $\boldsymbol{O} = (1 : -1 : 0)$. The inverse of $\boldsymbol{O}$ is $\boldsymbol{O}$. For $\boldsymbol{P} \neq \boldsymbol{O}$ we can work in affine coordinates. Let $\boldsymbol{P} = (u_1, v_1)$ be a point on the curve. The line $v = -u + (u_1 + v_1)$ contains the point $\boldsymbol{P}$ and, considering its projective version $V = -U + (u_1 + v_1)Z$, it also contains the point at infinity $\boldsymbol{O}$. Therefore, $-\boldsymbol{P}$ is the third point of intersection of this line connecting $\boldsymbol{P}$ and $\boldsymbol{O}$ with the curve. Substituting $v = -u + (u_1 + v_1)$ into Eq. (3), we obtain

$$\begin{aligned}& u^3 + (-u + (u_1 + v_1))^3 + 1 = 3Du(-u + (u_1 + v_1))\\ \iff\ & 3(u_1 + v_1 + D)u^2 - 3(u_1 + v_1)(u_1 + v_1 + D)u + (u_1 + v_1)^3 + 1 = 0\\ \iff\ & u^2 - (u_1 + v_1)u + u_1v_1 = 0 .\end{aligned}$$

(Note that $u_1 + v_1 + D \neq 0$ because $D^3 \neq 1$.) So, the u-coordinate of $-\boldsymbol{P}$ is v_1, and hence its v-coordinate is u_1, i.e., $-\boldsymbol{P} = (v_1, u_1)$ or, in projective coordinates,

$$-\boldsymbol{P} = (V_1 : U_1 : W_1) . \tag{8}$$

We use the same notations as in Appendix A. The tangent at $\boldsymbol{P} = (U_1 : V_1 : W_1)$ intersects the curve at the third point $-2\boldsymbol{P}$ whose coordinates are given by Eq. (15), with $F(U,V,W) = U^3 + V^3 + W^3 - 3DUVW$. We have $\varphi = 3({U_1}^2 - DV_1W_1)$, $\chi = 3({V_1}^2 - DU_1W_1)$ and $\psi = 3({W_1}^2 - DU_1V_1)$ and so, $-2\boldsymbol{P} = ((\psi^3 - \chi^3)/{U_1}^2 : (-\psi^3 + \varphi^3)/{V_1}^2 : (\chi^3 - \varphi^3)/{W_1}^2)$. A short calculation gives

$$\begin{aligned}\psi^3 - \chi^3 &= 27({W_1}^2 - DU_1V_1)^3 - 27({V_1}^2 - DU_1W_1)^3\\ &= 27[({W_1}^6 - {V_1}^6) + D^3{U_1}^3({W_1}^3 - {V_1}^3) - 3DU_1V_1W_1({W_1}^3 - {V_1}^3)]\\ &= 27({W_1}^3 - {V_1}^3)(D^3 - 1){U_1}^3 ,\end{aligned}$$

and, by symmetry, $-\psi^3 + \varphi^3 = 27({U_1}^3 - {W_1}^3)(D^3 - 1){V_1}^3$ and $\chi^3 - \varphi^3 = 27({V_1}^3 - {U_1}^3)(D^3 - 1){W_1}^3$. Hence, with Eq. (8), we finally obtain

$$2\boldsymbol{P} = \big(V_1({U_1}^3 - {W_1}^3) : U_1({W_1}^3 - {V_1}^3) : W_1({V_1}^3 - {U_1}^3)\big) . \tag{9}$$

From Eq. (16) (in Appendix A), the line connecting the points $\boldsymbol{P} = (U_1 : V_1 : W_1)$ and $\boldsymbol{Q} = (U_2 : V_2 : W_2)$ intersects the curve at the third point $-(\boldsymbol{P}+\boldsymbol{Q}) = (U_1\Theta - U_2\Upsilon : V_1\Theta - V_2\Upsilon : W_1\Theta - W_2\Upsilon)$, where $\Theta = 3U_1({U_2}^2 - DV_2W_2) + 3V_1({V_2}^2 - DU_2W_2) + 3W_1({W_2}^2 - DU_2V_2)$ and $\Upsilon = 3U_2({U_1}^2 - DV_1W_1) + 3V_2({V_1}^2 - DU_1W_1) + 3W_2({W_1}^2 - DU_1V_1)$. We have

$$\begin{aligned}
U_1\Theta - U_2\Upsilon &= 3V_1V_2(U_1V_2 - U_2V_1) \\
&\quad + 3W_1W_2(U_1W_2 - U_2W_1) - 3D({U_1}^2V_2W_2 - {U_2}^2V_1W_1)\,, \\
V_1\Theta - V_2\Upsilon &= 3U_1U_2(U_2V_1 - U_1V_2) \\
&\quad + 3W_1W_2(V_1W_2 - V_2W_1) - 3D({V_1}^2U_2W_2 - {V_2}^2U_1W_1)\,, \\
W_1\Theta - W_2\Upsilon &= 3U_1U_2(U_2W_1 - U_1W_2) \\
&\quad + 3V_1V_2(V_2W_1 - V_1W_2) - 3D({W_1}^2U_2V_2 - {W_2}^2U_1V_1)\,,
\end{aligned}$$

and thus, exploiting the fact that $\boldsymbol{P}$ and $\boldsymbol{Q}$ belong to the curve [9, no. 12], we obtain

$$\begin{aligned}
\frac{U_1\Theta - U_2\Upsilon}{W_1\Theta - W_2\Upsilon} &= \frac{{U_1}^2V_2W_2 - {U_2}^2V_1W_1}{{W_1}^2U_2V_2 - {W_2}^2U_1V_1}\,, \\
\frac{V_1\Theta - V_2\Upsilon}{W_1\Theta - W_2\Upsilon} &= \frac{{V_1}^2U_2W_2 - {V_2}^2U_1W_1}{{W_1}^2U_2V_2 - {W_2}^2U_1V_1}\,.
\end{aligned}$$

Therefore, with Eq. (8), the sum $\boldsymbol{R} = \boldsymbol{P} + \boldsymbol{Q}$ is given by

$$\boldsymbol{R} = \left({V_1}^2U_2W_2 - {V_2}^2U_1W_1 : {U_1}^2V_2W_2 - {U_2}^2V_1W_1 : {W_1}^2U_2V_2 - {W_2}^2U_1V_1\right)\,. \quad (10)$$

We now study the points of order 2 and 3. We work in affine coordinates since we are looking at points $\boldsymbol{P} \neq \boldsymbol{O}$ such that $2\boldsymbol{P} = \boldsymbol{O}$ or $3\boldsymbol{P} = \boldsymbol{O}$. Let $\boldsymbol{P} = (u_1, v_1)$. The condition $2\boldsymbol{P} = \boldsymbol{O}$ is equivalent to $\boldsymbol{P} = -\boldsymbol{P}$. Therefore, since $-\boldsymbol{P} = (v_1, u_1)$, the points $\boldsymbol{P} = (u_1, v_1)$ of order 2 are those for which $u_1 = v_1$.

Suppose $\boldsymbol{P} = (u_1, v_1)$ with $u_1 \neq v_1$, that is, $\boldsymbol{P}, 2\boldsymbol{P} \neq \boldsymbol{O}$. To find the points $\boldsymbol{P}$ of order 3, we use the doubling formula: $3\boldsymbol{P} = \boldsymbol{O} \iff 2\boldsymbol{P} = -\boldsymbol{P}$. So, a few algebra shows that the points of order 3 are exactly those with $u_1 = 0$ or $v_1 = 0$. In particular, the points $(0, -1)$ and $(-1, 0)$ have order 3.

Finally, it is interesting to note that a generic point $\boldsymbol{P} = (U : V : W)$ on the Hessian curve (4) satisfies

$$(D^2+D+1)(U+V+W)^3 = 3(DU+V+W)(U+DV+W)(U+V+DW)\,, \quad (11)$$

since $(D^2+D+1)(U+V+W)^3 - 3(DU+V+W)(U+DV+W)(U+V+DW) = (D-1)^2(U^3+V^3+W^3-3DUVW) = 0$. Moreover, since $(DU+V+W)+(U+DV+W)+(U+V+DW) = (D+2)(U+V+W)$, it follows that

$$(\tilde{U} + \tilde{V} + \tilde{W})^3 = 3\tilde{D}\tilde{U}\tilde{V}\tilde{W}\,, \quad (12)$$

where $\begin{cases} \tilde{U} = DU + V + W \\ \tilde{V} = U + DV + W \\ \tilde{W} = U + V + DW \end{cases}$ and $\tilde{D} = \frac{(D+2)^3}{D^2+D+1}$.

4 Side-Channel Attacks

At CRYPTO '96 and subsequently at CRYPTO '99, Kocher *et al.* introduced a new class of attacks, the so-called *side-channel attacks*. By measuring some side-channel information (e.g., timing [11], power consumption [12]), they were able to find the secret keys from tamper-resistant devices.

When only a single measurement is performed the attack is referred to as *simple side-channel attack*, and when there are several correlated measurements sometimes it is referred to as a *differential side-channel attack*. The main concern at the moment for public-key cryptography are the simple side-channel attacks [12]. Efficient countermeasures are known for exponentiation-based cryptosystems (e.g., [4]), but they require the atomic operations to be indistinguishable. For elliptic curve cryptography, the atomic operations are addition, subtraction and doubling of points. Within the Weierstraß model, as suggested in [1], these operations appear to be different and some secret information may therefore leak through side-channel analysis.

The next section shows that the Hessian parameterization allows one to implement the same algorithm for the addition (or subtraction) of two points or for the doubling of a point.

5 Implementing the Hessian Curves

Figure 1 gives a detailed implementation to add two (different) points on an Hessian curve. The algorithm requires 12 multiplications (or 10 multiplications if one point has its last coordinate equal to 1) and 7 temporary variables.

We note that there are variants for this implementation. For instance, we are able to describe similar implementations with only 4 auxiliary variables and 18 multiplications, 5 auxiliary variables and 16 multiplications, and 6 auxiliary variables and 14 multiplications.

More remarkably, owing to the high symmetry of the Hessian parameterization, the *same* algorithm can be used for doubling a point. We have:

Proposition 2. *Let* $\boldsymbol{P} = (U_1 : V_1 : W_1)$ *be a point on an Hessian elliptic curve* $E_D(\mathbb{K})$*. Then*

$$2(U_1 : V_1 : W_1) = (W_1 : U_1 : V_1) + (V_1 : W_1 : U_1) \ . \tag{13}$$

Furthermore, we have $(W_1 : U_1 : V_1) \neq (V_1 : W_1 : U_1)$.

Proof. Addition formula (10) yields $(W_1 : U_1 : V_1)+(V_1 : W_1 : U_1) = ({U_1}^2V_1U_1 - {W_1}^2W_1V_1 : {W_1}^2W_1U_1 - {V_1}^2U_1V_1 : {V_1}^2V_1W_1 - {U_1}^2W_1U_1) = (V_1({U_1}^3 - {W_1}^3) : U_1({W_1}^3 - {V_1}^3) : W_1({V_1}^3 - {U_1}^3)) = 2(U_1 : V_1 : W_1)$ by Eq. (9).

Input: $\boldsymbol{P} = (U_1 : V_1 : W_1)$ and $\boldsymbol{Q} = (U_2 : V_2 : W_2)$ with $\boldsymbol{P} \neq \boldsymbol{Q}$
Output: $\boldsymbol{P} + \boldsymbol{Q} = (U_3 : V_3 : W_3)$

$T_1 \leftarrow U_1$; $T_2 \leftarrow V_1$; $T_3 \leftarrow W_1$ $T_4 \leftarrow U_2$; $T_5 \leftarrow V_2$; $T_6 \leftarrow W_2$
$T_7 \leftarrow T_1 \cdot T_6$ $(= U_1W_2)$
$T_1 \leftarrow T_1 \cdot T_5$ $(= U_1V_2)$
$T_5 \leftarrow T_3 \cdot T_5$ $(= W_1V_2)$
$T_3 \leftarrow T_3 \cdot T_4$ $(= W_1U_2)$
$T_4 \leftarrow T_2 \cdot T_4$ $(= V_1U_2)$
$T_2 \leftarrow T_2 \cdot T_6$ $(= V_1W_2)$
$T_6 \leftarrow T_2 \cdot T_7$ $(= U_1V_1W_2^2)$
$T_2 \leftarrow T_2 \cdot T_4$ $(= V_1^2U_2W_2)$
$T_4 \leftarrow T_3 \cdot T_4$ $(= V_1W_1U_2^2)$
$T_3 \leftarrow T_3 \cdot T_5$ $(= W_1^2U_2V_2)$
$T_5 \leftarrow T_1 \cdot T_5$ $(= U_1W_1V_2^2)$
$T_1 \leftarrow T_1 \cdot T_7$ $(= U_1^2V_2W_2)$
$T_1 \leftarrow T_1 - T_4$; $T_2 \leftarrow T_2 - T_5$; $T_3 \leftarrow T_3 - T_6$
$U_3 \leftarrow T_2$; $V_3 \leftarrow T_1$; $W_3 \leftarrow T_3$

Fig. 1. AddHesse($\boldsymbol{P}$, $\boldsymbol{Q}$): Addition algorithm on an Hessian curve.

The second part of the proposition follows by contradiction. Suppose that $(W_1 : U_1 : V_1) = (V_1 : W_1 : U_1)$, i.e., that there exists some $t \in \mathbb{K}^*$ s.t. $W_1 = tV_1$, $U_1 = tW_1$ and $V_1 = tU_1$. This implies $W_1 \neq 0$ and $t^3 = 1$. Moreover, since $(U_1 : V_1 : W_1) \in E_D(\mathbb{K})$, ${U_1}^3 + {V_1}^3 + {W_1}^3 = 3DU_1V_1W_1$, which in turn implies $(t^3 + t^6 + 1){W_1}^3 = 3Dt^3{W_1}^3$ and thus $D = 1$, a contradiction by Lemma 1. □

In [13], Liardet and Smart suggest to represent elliptic curves as the intersection of two quadrics in $\mathbb{P}^3$ as a means to protect against side-channel attacks. Considering the special case of an elliptic curve whose order is divisible by 4 (i.e., the Jacobi form), they observe that the same algorithm can be used for adding and doubling points with **16 multiplications** (see also [3] for the formulæ). Using the proposed Hessian parameterization, only **12 multiplications** are necessary for adding or doubling points. The Hessian parameterization gives thus a **33% improvement** over the Jacobi parameterization. Another advantage of the Hessian parameterization is that points are represented with fewer coordinates, which results in substantial memory savings.

Finally, contrary to other parameterizations, there is no (field) subtraction to compute the inverse of a point (see Eq. (8)). Hence, our addition algorithm can be used *as is* for subtracting two points $\boldsymbol{P} = (U_1 : V_1 : W_1)$ and $\boldsymbol{Q} = (U_2 : V_2 : W_2)$ on an Hessian elliptic curve:

$$(U_1 : V_1 : W_1) - (U_2 : V_2 : W_2) = (U_1 : V_1 : W_1) + (V_2 : U_2 : W_2) \ . \qquad (14)$$

To sum up, by adapting the order of the inputs accordingly to Eq. (13) or (14), the addition algorithm presented in Fig. 1 can be used *indifferently* for

– adding two (different) points;

– doubling a point;
– subtracting two points;

with only 12 multiplications and 7 auxiliary variables including the 3 result variables. This results in the *fastest* known method for implementing the elliptic curve scalar multiplication towards resistance against side-channel attacks.

Acknowledgements. The first author would like to acknowledge Prof. Laih and the members of his lab for their generous hospitality while part of this work was performed. Thanks also to the anonymous referees.

References

1. IEEE Std 1363-2000, *IEEE standard specifications for public-key cryptography*, IEEE Computer Society, August 29, 2000.
2. J. W. S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, 1991.
3. D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Advances in Applied Math. **7** (1986/7), 385–434.
4. Christophe Clavier and Marc Joye, *Universal exponentiation algorithm: A first step towards provable SPA-resistance*, these proceedings.
5. Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, 1993.
6. Henri Cohen, Atsuko Miyaji, and Takatoshi Ono, *Efficient elliptic curve exponentiation using mixed coordinates*, Advances in Cryptology – ASIACRYPT '98 (K. Ohta and D. Pei, eds.), Lecture Notes in Computer Science, vol. 1514, Springer-Verlag, 1998, pp. 51–65.
7. Jean-Sébastien Coron, *Resistance against differential power analysis for elliptic curve cryptosystems*, Cryptographic Hardware and Embedded Systems (CHES '99) (Ç.K. Koç and C. Paar, eds.), Lecture Notes in Computer Science, vol. 1717, Springer-Verlag, 1999, pp. 292–302.
8. Erik De Win, Serge Mister, Bart Preneel, and Michael Wiener, *On the performance of signature schemes based on elliptic curves*, Algorithmic Number Theory Symposium (J.-P. Buhler, ed.), Lecture Notes in Computer Science, vol. 1423, Springer-Verlag, 1998, pp. 252–266.
9. M. Desboves, *Résolution, en nombres entiers et sous sa forme la plus générale, de l'équation cubique, homogène, à trois inconnues*, Ann. de Mathémat. **45** (1886), 545–579.
10. Otto Hesse, *Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln*, Journal für die reine und angewandte Mathematik **10** (1844), 68–96.
11. Paul C. Kocher, *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems*, Advances in Cryptology – CRYPTO '96 (N. Koblitz, ed.), Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, 1996, pp. 104–113.
12. Paul Kocher, Joshua Jaffe, and Benjamin Jun, *Differential power analysis*, Advances in Cryptology – CRYPTO '99 (M. Wiener, ed.), Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, 1999, pp. 388–397.

13. Pierre-Yvan Liardet and Nigel P. Smart, *Preventing SPA/DPA in ECC systems using the Jacobi form*, these proceedings.
14. Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan, *Power analysis attacks of modular exponentiation in smartcards*, Cryptographic Hardware and Embedded Systems (CHES '99) (Ç.K. Koç and C. Paar, eds.), Lecture Notes in Computer Science, vol. 1717, Springer-Verlag, 1999, pp. 144–157.
15. Nigel P. Smart, *The Hessian form of an elliptic curve*, these proceedings.

A Cauchy-Desboves' s Formulæ

Let $F(U,V,W)=0$ be the (homogeneous) equation of a general cubic curve and let $\boldsymbol{P_1}=(U_1:V_1:W_1)$ and $\boldsymbol{P_2}=(U_2:V_2:W_2)$ be two points on the curve.

We let denote $\varphi=\frac{\partial F(\boldsymbol{P_1})}{\partial U}$, $\chi=\frac{\partial F(\boldsymbol{P_1})}{\partial V}$ and $\psi=\frac{\partial F(\boldsymbol{P_1})}{\partial W}$. Then the tangent at $\boldsymbol{P_1}$ intersects the curve at the third point [9, Eq. (16)] given by

$$\left(\frac{F(0,\psi,-\chi)}{{U_1}^2}:\frac{F(-\psi,0,\varphi)}{{V_1}^2}:\frac{F(\chi,-\varphi,0)}{{W_1}^2}\right)\ . \tag{15}$$

Moreover, the secant joining $\boldsymbol{P_1}$ and $\boldsymbol{P_2}$ intersects the curve at the third point [9, Eq. (16)] given by

$$(U_1\Theta-U_2\Upsilon:V_1\Theta-V_2\Upsilon:W_1\Theta-W_2\Upsilon)\ , \tag{16}$$

where $\Theta=U_1\frac{\partial F(\boldsymbol{P_2})}{\partial U}+V_1\frac{\partial F(\boldsymbol{P_2})}{\partial V}+W_1\frac{\partial F(\boldsymbol{P_2})}{\partial W}$ and $\Upsilon=U_2\frac{\partial F(\boldsymbol{P_1})}{\partial U}+V_2\frac{\partial F(\boldsymbol{P_1})}{\partial V}+W_2\frac{\partial F(\boldsymbol{P_1})}{\partial W}$.

B Samples

Here are two examples of cryptographic Hessian elliptic curves $E_D(\mathbb{F}_p)$ defined over the prime field $\mathbb{F}_p$ with $p=2^{160}-2933$ and $p=2^{224}-2^{10}-1$, respectively. Both curves are adapted from [6] using Proposition 1. Note that since $(0,-1)$ is on the curve whatever the values of D and p and that this point has order 3, the order of an Hessian curve, $\#E_D(\mathbb{F}_p)$, is always a multiple of 3. Note also that this specialized representation does not impact the security of the resulting cryptographic applications.

B.1 160-bit prime

$p=2^{160}-2933$
$D=945639186043697550302587435415597619883075636292$
$\#E_D(\mathbb{F}_p)=3\cdot 5\cdot 157\cdot 620595175087432237029165529381611169224913337$

B.2 224-bit prime

$p=2^{224}-2^{10}-1$
$D=25840187014857916932759133078916563544400020237401312879815735566345$
$\#E_D(\mathbb{F}_p)=3\cdot 23\cdot 39072386474131362021256543604376277771282351667\backslash$
3432244734573782061