The Jacobi Model of an Elliptic Curve and Side-Channel Analysis

Olivier Billet[1,2] and Marc Joye[1]

[1] Gemplus Card International, Card Security Group
Parc d'Activités de Gémenos, B.P. 100, 13881 Gémenos Cedex, France
marc.joye@gemplus.com – http://www.geocities.com/MarcJoye/
http://www.gemplus.com/smart/

[2] Télécom Paris (ENST)
46 rue Barrault
75634 Paris Cedex 13, France
http://www.enst.fr

UNSA, Laboratoire Dieudonné
Parc Valrose
06108 Nice Cedex 02, France
http://math.unice.fr

billet@eurecom.fr – http://studwww.eurecom.fr/~billet

Abstract. A way for preventing SPA-like attacks on elliptic curve systems is to use the same formula for the doubling and the general addition of points on the curve. Various proposals have been made in this direction with different results. This paper re-investigates the Jacobi form suggested by Liardet and Smart (CHES 2001). Rather than considering the Jacobi form as the intersection of two quadrics, the addition law is directly derived from the underlying quartic. As a result, this leads to substantial memory savings and produces the fastest unified addition formula for curves of order a multiple of 2.

Keywords. Elliptic curve cryptosystems, unified addition formula, side-channel analysis, SPA-like attacks, smart cards.

1 Introduction

In 1996, Kocher introduced the so-called *side-channel attacks*. By monitoring some side-channel information (e.g., timing [7] or power consumption [8]), an attacker tries to retrieve secret data involved in a cryptographic computation. For elliptic curve cryptosystems, a naïve implementation of the point multiplication is particularly susceptible to such attacks as the classical formulæ for doubling a point and for adding two (distinct) points are different. Hence, according to the implemented crypto-algorithm, a *simple power analysis* (SPA)[†] can yield the value of multiplier d used in the computation of $\boldsymbol{Q} = d\boldsymbol{P}$ on an elliptic curve.

A promising way for preventing SPA-like attacks consists in re-writing the addition formula so that the doubling and the general addition become indistinguishable from some side-channel information. In particular, an addition formula valid for both the doubling and the addition would be helpful.

[†] There is another class of side-channel attacks, the *differential attacks*, but we do not consider them as efficient protections are known (e.g., see [4]).

1.1 Related work

The use of a unified formula for the addition of points on an elliptic curve as a means for preventing SPA-like attacks has been independently suggested in [6] and [10]. In [6], the authors suggest the Hessian form while in [10], the intersection of two quadrics is considered. Unified addition formulæ for the general Weierstraß parameterization are given in [1].

1.2 Our results

Building on [10], we consider the Jacobi form not as the intersection of two quadrics but as a quartic. This allows points to be represented with triplets instead of quadruplets. Furthermore, this considerably reduces the number of required (field) multiplications. As a result, we obtain the most efficient (memory-wise and computation-wise) unified formula for adding points on an elliptic curve whose order is a multiple of 2. In particular, compared to [10], we get a 23% speed-up improvement with fewer memory requirements.

1.3 Organization of the paper

The rest of this paper is organized as follows. In the next section, we respectively review the Jacobi form of an elliptic curve as the intersection of two quadrics and as a quartic. Then, in Section 3, we show how the quartic model helps to prevent SPA-like attacks. Finally, we conclude in Section 4.

2 Jacobi Models

Throughout this paper, we assume that $\mathbb{K}$ represents a field of characteristic $\operatorname{Char}\mathbb{K} \neq 2$. Furthermore, since our ultimate goal is the study over large prime fields, we also assume that $\operatorname{Char}\mathbb{K} \neq 3$.

2.1 Intersection of two quadrics

It is well known that any elliptic curve over $\mathbb{K}$ can be embedded as the intersection of two quadrics in $\mathbb{P}^3$ [2, Chapter 7]. Indeed, a point (x, y) on a Weierstraß elliptic curve

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

corresponds to the point (X, Y, Z, T) on the intersection

$$\begin{cases} X^2 - TZ = 0 \\ Y^2 - aXZ - bZ^2 - TX = 0 \end{cases} \tag{1}$$

via the map $(x, y) \longmapsto (X, Y, Z, T) = (x, y, 1, x^2)$.

As for the Weierstraß parameterization, the group law on the intersection of two quadrics has a nice geometrical interpretation [11]. Let $\boldsymbol{P_1} = (X_1, Y_1, Z_1, T_1)$ and $\boldsymbol{P_2} = (X_2, Y_2, Z_2, T_2)$ be two points on the intersection given by Eq. (1). Then, the sum $\boldsymbol{P_3} = \boldsymbol{P_1} + \boldsymbol{P_2} = (X_3, Y_3, Z_3, T_3)$ is given by

$$\begin{aligned} X_3 &= \mathsf{F}(\boldsymbol{P_1}, \boldsymbol{P_2})\,\mathsf{H}(\boldsymbol{P_1}, \boldsymbol{P_2})\,, & Z_3 &= \mathsf{H}(\boldsymbol{P_1}, \boldsymbol{P_2})^2\,,\\ Y_3 &= Y_1\,\mathsf{G}(\boldsymbol{P_2}, \boldsymbol{P_1}) + Y_2\,\mathsf{G}(\boldsymbol{P_1}, \boldsymbol{P_2})\,, & T_3 &= \mathsf{F}(\boldsymbol{P_1}, \boldsymbol{P_2})^2\,, \end{aligned}$$

where

$$\begin{aligned} \mathsf{F}(\boldsymbol{P_1}, \boldsymbol{P_2}) &= T_1T_2 - 2aX_1X_2 - 4b(X_1Z_2 + Z_1X_2) + a^2Z_1Z_2\,,\\ \mathsf{G}(\boldsymbol{P_1}, \boldsymbol{P_2}) &= T_1^2T_2 + 2aX_1T_1X_2 + 4bX_1T_1Z_2 + 3aZ_1T_1T_2\\ &\quad + 12bZ_1T_1X_2 - 3a^2Z_1T_1Z_2 + 4bZ_1X_1T_2 - 2a^2X_1Z_1X_2\\ &\quad - 4abX_1Z_1Z_2 - a^3Z_1^2Z_2 - 8b^2Z_1^2Z_2\,,\\ \mathsf{H}(\boldsymbol{P_1}, \boldsymbol{P_2}) &= 2Y_1Y_2 + X_1T_2 + T_1X_2 + a(X_1Z_2 + Z_1X_2) + 2bZ_1Z_2\ . \end{aligned}$$

The above formulæ present the particularity of being valid for *both* the doubling and the general addition. This was therefore considered in [10] as a means for preventing side-channel attacks. However, as already noticed there, these addition formulæ are overly involved to be of any use in real-life implementations.

Following [3], attention was therefore restricted to the particular case given by

$$\begin{cases} X^2 + Y^2 - T^2 = 0\\ (1-\lambda)\,X^2 + Z^2 - T^2 = 0 \end{cases}. \tag{2}$$

As shown in [10], this corresponds to the Weiertraß equation

$$y^2 = x(x+1)(x+\lambda) \qquad (\cup\{\boldsymbol{O}\}) \tag{3}$$

via the inverse maps

$$(x, y) \longmapsto (-2y, x^2 - \lambda, x^2 + 2x\lambda + \lambda, x^2 + 2x + \lambda), \quad \boldsymbol{O} \longmapsto (0, 1, 1, 1)$$

and

$$(X, Y, Z, T) \longmapsto \begin{cases} \boldsymbol{O} & \text{if } X = 0 \text{ and } Y = Z = T,\\ \left(\frac{\lambda(Z-T)}{(1-\lambda)Y - Z + \lambda T}, \frac{\lambda(1-\lambda)X}{(1-\lambda)Y - Z + \lambda T}\right) & \text{otherwise}. \end{cases}$$

From the Weierstraß form (Eq. (3)), it clearly appears that this elliptic curve has three points of order 2. This implies that this elliptic curve contains a copy of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and so its group order is a multiple of 4.

The addition law, $\boldsymbol{P_3} = \boldsymbol{P_1} + \boldsymbol{P_2}$, on the specialized intersection given by Eq. (2) becomes

$$\begin{aligned} X_3 &= T_1Y_2 \cdot X_1Z_2 + Z_1X_2 \cdot Y_1T_2, & Z_3 &= T_1Z_1T_2Z_2 - k^2X_1Y_1X_2Y_2,\\ Y_3 &= T_1Y_2 \cdot Y_1T_2 - Z_1X_2 \cdot X_1Z_2, & T_3 &= (T_1Y_2)^2 + (Z_1X_2)^2, \end{aligned} \tag{4}$$

so that 16 (field) multiplications (plus 1 multiplication by constant k^2) are required. The inverse of a point $\boldsymbol{P_1} = (X_1, Y_1, Z_1, T_1)$ is $-\boldsymbol{P_1} = (-X_1, Y_1, Z_1, T_1)$. Again, we see that (excluding the neutral element $(0, 1, 1, 1)$) there are three points of order 2, namely, $(0, -1, 1, 1)$, $(0, 1, -1, 1)$ and $(0, 1, 1, -1)$.

2.2 Jacobi quartic

Jacobi also studied quartics of the form

$$y^2 = (1 - x^2)(1 - k^2\,x^2) \tag{5}$$

with $k \neq 0, \pm 1$. This type of elliptic curve can be parameterized with Jacobi's elliptic functions, namely the "*sinus amplitudinus*" and its derivative. So, a point $\boldsymbol{P} = (x, y)$ on the Jacobi quartic given by Eq. (5) is represented as $(\mathrm{sn}(u), \mathrm{cn}(u)\,\mathrm{dn}(u))$. From the rich body of addition formulæ for elliptic functions (see [13] for instance), we directly derive the addition law on the quartic. We have

$$\begin{aligned}
\mathrm{sn}(u_1+u_2) &= \frac{\mathrm{sn}(u_1)\,\mathrm{cn}(u_2)\,\mathrm{dn}(u_2) + \mathrm{sn}(u_2)\,\mathrm{cn}(u_1)\,\mathrm{dn}(u_1)}{1 - k^2\,\mathrm{sn}(u_1)^2\,\mathrm{sn}(u_2)^2}\;,\\
\mathrm{cn}(u_1+u_2) &= \frac{\mathrm{cn}(u_1)\,\mathrm{cn}(u_2) - \mathrm{sn}(u_1)\,\mathrm{sn}(u_2)\,\mathrm{dn}(u_1)\,\mathrm{dn}(u_2)}{1 - k^2\,\mathrm{sn}(u_1)^2\,\mathrm{sn}(u_2)^2}\;,\\
\mathrm{dn}(u_1+u_2) &= \frac{\mathrm{dn}(u_1)\,\mathrm{dn}(u_2) - k^2\,\mathrm{sn}(u_1)\,\mathrm{sn}(u_2)\,\mathrm{cn}(u_1)\,\mathrm{cn}(u_2)}{1 - k^2\,\mathrm{sn}(u_1)^2\,\mathrm{sn}(u_2)^2}\;.
\end{aligned} \tag{6}$$

Hence, if $(x_i, y_i) = (\mathrm{sn}(u_i), \mathrm{cn}(u_i)\,\mathrm{dn}(u_i))$ for $i = 1, 2$ are two generic points on the Jacobi quartic, the sum $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ is given by

$$(x_3, y_3) = (\mathrm{sn}(u_1+u_2), \mathrm{cn}(u_1+u_2)\,\mathrm{dn}(u_1+u_2))\;.$$

Here again, the formulæ present the tremendous advantage of remaining valid for the doubling (i.e., when $u_1 = u_2$).

3 Preventing SPA-like Attacks

We consider slightly more general quartics than those originally considered by Jacobi. Namely, we investigate quartics given by

$$y^2 = \epsilon\,x^4 - 2\delta\,x^2 + 1\;. \tag{7}$$

(Jacobi quartics correspond to the case $\epsilon = k^2$ and $\delta = (1 + k^2)/2$.)

Remarkably, all elliptic curves with a point of order 2 can be expressed by a quartic equation of the form of Eq. (7). Let E denote an elliptic curve (over $\mathbb{K}$)[‡] given by a Weierstraß equation

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

with its point 'at infinity' $\boldsymbol{O}$. Suppose that E has a point of order 2, say, $(\theta, 0) \in E(\mathbb{K})$. Then, the above Weierstraß elliptic curve is birationnally equivalent to the (extended) Jacobi quartic

$$Y^2 = \epsilon\,X^4 - 2\delta\,X^2Z^2 + Z^4 \tag{8}$$

[‡] Remember that we assume $\mathrm{Char}\,\mathbb{K} \neq 2, 3$.

with $\epsilon = -(3\theta^2 + 4a)/16$ and $\delta = 3\theta/4$, under the transformations

$$\begin{cases} (\theta, 0) \longmapsto (0 : -1 : 1)\,, \\ (x, y) \longmapsto \big(2(x-\theta) : (2x+\theta)(x-\theta)^2 - y^2 : y\big)\ , \\ \quad \boldsymbol{O} \quad \longmapsto (0 : 1 : 1)\,, \end{cases} \tag{9}$$

and

$$\begin{cases} \ (0 : 1 : 1) \ \ \longmapsto \boldsymbol{O}\,, \\ (0 : -1 : 1) \longmapsto (\theta, 0)\,, \\ (X : Y : Z) \longmapsto \left(2\dfrac{(Y+Z^2)}{X^2} - \dfrac{\theta}{2},\ Z\dfrac{4(Y+Z^2) - 3\theta\, X^2}{X^3}\right) \ . \end{cases} \tag{10}$$

In Equations (9) and (10), the notation $(X : Y : Z)$ stands for equivalence classes. Two triplets $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ represent the same point if and only if there exists $t \in \mathbb{K} \setminus \{0\}$ such that $X_1 = tX_2$, $Y_1 = t^2 Y_2$ and $Z_1 = tZ_2$.

We now give the group law on the elliptic curve given by Eq. (8). From [9] (see also [5]), the sum of two points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ is given by $(X_3 : Y_3 : Z_3)$ where

$$\begin{aligned} X_3 &= X_1 Z_1 Y_2 + Y_1 X_2 Z_2\,, \\ Y_3 &= \left[(Z_1 Z_2)^2 + \epsilon(X_1 X_2)^2\right]\left[Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2\right] \\ &\quad + 2\epsilon X_1 X_2 Z_1 Z_2 (X_1^2 Z_2^2 + Z_1^2 X_2^2)\,, \\ Z_3 &= (Z_1 Z_2)^2 - \epsilon(X_1 X_2)^2 \ . \end{aligned} \tag{11}$$

The negation of a point $(X : Y : Z)$ on the (extended) Jacobi quartic (Eq. (8)) is given by $(-X : Y : Z)$.

To sum up, our unified method for adding points on an elliptic curve with a point of order 2 goes as follows. We first represent the given Weierstraß curve as a quartic given by Eq. (8) and transform points $\boldsymbol{P_1}$ and $\boldsymbol{P_2}$ according to Eq. (9). Next, given the two points on the corresponding quartic, $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$, we apply the addition formula given by Eq. (11) and obtain $(X_3 : Y_3 : Z_3) = (X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)$. Finally, we recover the sum as a point on the initial Weierstraß curve, $\boldsymbol{P_3} = \boldsymbol{P_1} + \boldsymbol{P_2}$, by the transformation given by Eq. (10).

Figure 1 details the procedure for adding points $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$. It appears that only **13** (field) **multiplications** (plus 3 multiplications by constants) are required. We insist that the same procedure equally applies for doubling a point. We further note that the neutral element is $(0 : 1 : 1)$ and that the procedure remains valid for it too.

When constant δ (resp. ϵ) is small, the cost of a multiplication by δ (resp. ϵ) can be neglected. A good choice consists in imposing a small value for ϵ since this removes two multiplications by constants —as shown in Fig. 1, there are 2 multiplications by ϵ and 1 multiplication by δ. In particular, most elliptic curves over the prime field $\mathbb{K} = \mathbb{F}_p$, with three points of order 2, can be rescaled

```
$T_1 \leftarrow X_1; T_2 \leftarrow Y_1; T_3 \leftarrow Z_1; T_4 \leftarrow X_2; T_5 \leftarrow Y_2; T_6 \leftarrow Z_2$
$T_7 \leftarrow T_1 \cdot T_3$          $(= X_1Z_1)$
$T_7 \leftarrow T_2 + T_7$          $(= X_1Z_1 + Y_1)$
$T_8 \leftarrow T_4 \cdot T_6$          $(= X_2Z_2)$
$T_8 \leftarrow T_5 + T_8$          $(= X_2Z_2 + Y_2)$
$T_2 \leftarrow T_2 \cdot T_5$          $(= Y_1Y_2)$
$T_7 \leftarrow T_7 \cdot T_8$          $(= X_3 + Y_1Y_2 + X_1X_2Z_1Z_2)$
$T_7 \leftarrow T_7 - T_2$          $(= X_3 + X_1X_2Z_1Z_2)$
$T_5 \leftarrow T_1 \cdot T_4$          $(= X_1X_2)$
$T_1 \leftarrow T_1 + T_3$          $(= X_1 + Z_1)$
$T_8 \leftarrow T_3 \cdot T_6$          $(= Z_1Z_2)$
$T_4 \leftarrow T_4 + T_6$          $(= X_2 + Z_2)$
$T_6 \leftarrow T_5 \cdot T_8$          $(= X_1X_2Z_1Z_2)$
$T_7 \leftarrow T_7 - T_6$          $(= X_3)$
$T_1 \leftarrow T_1 \cdot T_4$          $(= X_1Z_2 + X_2Z_1 + X_1X_2 + Z_1Z_2)$
$T_1 \leftarrow T_1 - T_5$          $(= X_1Z_2 + X_2Z_1 + Z_1Z_2)$
$T_1 \leftarrow T_1 - T_8$          $(= X_1Z_2 + X_2Z_1)$
$T_3 \leftarrow T_1 \cdot T_1$          $(= X_1^2Z_2^2 + X_2^2Z_1^2 + 2X_1X_2Z_1Z_2)$
$T_6 \leftarrow T_6 + T_6$          $(= 2X_1X_2Z_1Z_2)$
$T_3 \leftarrow T_3 - T_6$          $(= X_1^2Z_2^2 + X_2^2Z_1^2)$
$T_4 \leftarrow \epsilon \cdot T_6$          $(= 2\epsilon\, X_1X_2Z_1Z_2)$
$T_3 \leftarrow T_3 \cdot T_4$          $(= 2\epsilon\, X_1X_2Z_1Z_2(X_1^2Z_2^2 + X_2^2Z_1^2))$
$T_4 \leftarrow \delta \cdot T_6$          $(= 2\delta\, X_1X_2Z_1Z_2)$
$T_2 \leftarrow T_2 - T_4$          $(= Y_1Y_2 - 2\delta\, X_1X_2Z_1Z_2)$
$T_4 \leftarrow T_8 \cdot T_8$          $(= Z_1^2Z_2^2)$
$T_8 \leftarrow T_5 \cdot T_5$          $(= X_1^2X_2^2)$
$T_8 \leftarrow \epsilon \cdot T_8$          $(= \epsilon\, X_1^2X_2^2)$
$T_5 \leftarrow T_4 + T_8$          $(= Z_1^2Z_2^2 + \epsilon\, X_1^2X_2^2)$
$T_2 \leftarrow T_2 \cdot T_5$          $(= (Z_1^2Z_2^2 + \epsilon\, X_1^2X_2^2)(Y_1Y_2 - 2\delta\, X_1X_2Z_1Z_2))$
$T_2 \leftarrow T_2 + T_3$          $(= Y_3)$
$T_5 \leftarrow T_4 - T_8$          $(= Z_3)$
$X_3 \leftarrow T_7; Y_3 \leftarrow T_2; Z_3 \leftarrow T_5$
```

Fig. 1. Unified Addition on an (extended) Jacobi quartic.

to the case $\epsilon = 1$ as follows. Let $(\theta_1, 0)$, $(\theta_2, 0)$ and $(\theta_3, 0)$ denote the three points of order 2 on the Weierstraß curve, i.e., $y^2 = x^3 + ax + b = (x - \theta_1)(x - \theta_2)(x - \theta_3)$. Then, an application of map given by Eq. (9) with $\theta = \theta_1$ transforms the Weierstraß curve into the (extended) Jacobi curve

$$Y^2 = \epsilon\, X^4 - 2\delta\, X^2Z^2 + Z^4 \tag{12}$$

with $\delta = 3\theta_1/4$ and $\epsilon = -(3\theta_1^2 + 4a)/16 = (\theta_2 - \theta_3)^2/16$. If $p \equiv 3 \pmod 4$ then -1 is not a square modulo p and consequently either $(\theta_2 - \theta_3)$ or $-(\theta_2 - \theta_3)$ is a square modulo p. Letting ξ a square-root of the corresponding square $\pm(\theta_2 - \theta_3)$, it follows that $\epsilon = \xi^4/16 = (\xi/2)^4$. If $p \equiv 1 \pmod 4$ then there is a 1/8 chance that we cannot find a pair of indices such that $(\theta_i - \theta_j)$ is a square modulo p. If such a pair exists, we let ξ denote the corresponding square-root and again, after a possible re-arrangement, we get $\epsilon = (\xi/2)^4$. The change of variable $X \leftarrow 2X/\xi$ then transforms the previous quartic into

$$Y^2 = X^4 - 2\rho\, X^2 Z^2 + Z^4 \tag{13}$$

where $\rho = 4\delta/\xi^2$.

This latter case corresponds exactly to the curves considered by Liardet and Smart ([10]). The first advantage of using the quartic representation is that only 13 multiplications (in $\mathbb{F}_p$) plus 1 multiplication by constant ρ are required —the representation as the intersection of two quadrics requires 16 multiplications (in $\mathbb{F}_p$) plus 1 multiplication by constant k^2 (cf. § 2.1)— resulting in a $(\frac{16}{13}-1) \simeq 23\%$ speed improvement. The second advantage is that fewer memory resources are required since points are represented with triplets instead of quadruplets.

4 Conclusion

This paper revisited the Jacobi model initially suggested in [10] as a means for preventing side-channel attacks. Using an (extended) form of the Jacobi quartic, we derived a unified addition formula for adding or doubling points with only 13 field multiplications. This is the fastest known unified addition law for elliptic curves whose order is a multiple of 2.

References

1. Éric Brier and Marc Joye. Weierstraß elliptic curves and side-channel attacks. In D. Naccache, editor, *Public Key Cryptography*, volume 2274 of *Lecture Notes in Computer Science*, pages 335–345. Springer-Verlag, 2002.
2. J.W.S. Cassels and E.V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2.* Number 230 in London Mathematical Society, Lecture Notes Series. Cambridge Univ. Press, 2000.
3. D.V. Chudnovsky and G.V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. Appl. Math.*, 7:385–434, 1986/87.
4. 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.
5. Jun-ichi Igusa. On the transformation theory of elliptic functions. *Amer. J. Math.*, 81:436–452, 1959.
6. 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 402–410. Springer-Verlag, 2001.
7. 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.

8. 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.
9. Peter S. Landweber. Supersingular elliptic curves and congruences for Legendre polynomials. In P.S. Landweber, editor, *Elliptic Curves and Modular Forms in Algebraic Topology*, volume 1326 of *Lecture Notes in Mathematics*, Springer-Verlag, 1988.
10. 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 391–401. Springer-Verlag, 2001.
11. J.R. Merriman, S. Siksek, and N.P. Smart. Explicit 4-descents on an elliptic curve. *Acta Arith.*, 77(4):385–404, 1996.
12. Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1986.
13. E.T. Whittaker and G.N. Watson. *A course of modern analysis*. Cambridge University Press, 4th edition, 1927.

A Illustration

Here is an example of a cryptographic elliptic curve (i.e., the group order has a cofactor ≤ 4) over $\mathbb{F}_p$. This example is adapted from [10].

Let $p = 2^{192} - 2^{64} - 1$. Over $\mathbb{F}_p$, consider the Weierstraß elliptic curve E given by

$$E_{/\mathbb{F}_p} : y^2 = x^3 - 3x + b \quad (\cup\{\boldsymbol{O}\}) \tag{14}$$

where $b = 5785156510951660859948362664535565676137370865272662811849$. The order of E is four times a prime:

$$\#E = 4 \cdot 1569275433846670190958947355830249374250393459078477724241 \ .$$

The three points of order 2 on the Weierstraß curve are $(\theta_i, 0)$ with

$$\begin{cases} \theta_1 = 3931134103214925937592361744683965239873651308020133387956 \\ \theta_2 = 3722240065524459449962883383651126589463273788373166826730 \\ \theta_3 = 2161748259540728720113669865088143302633269781215144746593 \end{cases} .$$

An application of transformation given by Eq. (9) shows that the Weierstraß curve E is equivalent to the Jacobi curve

$$Y^2 = \epsilon\, X^4 - 2\delta\, X^2 Z^2 + Z^4$$

with $\epsilon = 4392384375834284450995086699732976092557230326145055776 52$ and $\delta = 2948350577411194453194271308512973929905238481015100409 67$. Further, since there are three points of order 2, ϵ can be rescaled to the case $\epsilon = 1$ via the additional transformation $X \leftarrow 2X/\xi$ with

$$\begin{aligned} \xi &= \sqrt{\theta_2 - \theta_3} \\ &= 2362324240509570404961221823945617479743113384215829517748\,. \end{aligned}$$

Consequently, the Weierstraß curve E (Eq. (14)) is also equivalent to the Jacobi curve

$$Y^2 = X^4 - 2\rho\, X^2 Z^2 + Z^4 \tag{15}$$

with $\rho = 4513535057349470453996210490020750613469858160756852710254$ via the map

$$\begin{cases} (\theta_1, 0) \longmapsto (0 : -1 : 1) \\ (x, y) \longmapsto \big(\xi(x-\theta_1) : (2x+\theta_1)(x-\theta_1)^2 - y^2 : y\big) \\ \boldsymbol{O} \longmapsto (0 : 1 : 1) \end{cases}$$

and conversely, the Jacobi curve (Eq. (15)) is equivalent to the initial Weierstraß curve (Eq. (14)) via the map

$$\begin{cases} (0 : 1 : 1) \longmapsto \boldsymbol{O} \\ (0 : -1 : 1) \longmapsto (\theta_1, 0) \\ (X : Y : Z) \longmapsto \left(\dfrac{\xi^2(Y+Z^2)}{2X^2} - \dfrac{\theta_1}{2}, Z\xi\,\dfrac{\xi^2(Y+Z^2) - 3\theta_1\, X^2}{2X^3}\right) \end{cases} .$$