Improving the Arithmetic of Elliptic Curves in the Jacobi Model

Sylvain Duquesne

Improving the Arithmetic of Elliptic Curves in the Jacobi Model

Sylvain Duquesne

I3M, (UMR CNRS 5149) and Lirmm, (UMR CNRS 5506), Université Montpellier II.
CC 051, Place Eugène Bataillon, 34095 Montpellier Cedex 5, France.

Abstract

The use of elliptic curve cryptosystems on embedded systems has been becoming widespread for some years. Therefore the resistance of such cryptosystems to side-channel attacks is becoming crucial. Several techniques have recently been developed. One of these consists of finding a representation of the elliptic curve such that formulae for doubling and addition are the same. Until now, the best result has been obtained by using the Jacobi model. In this paper, we improve the arithmetic of elliptic curves in the Jacobi model and we relax some conditions required to work efficiently on this model. We thus obtained the fastest unified addition formulae for elliptic curve cryptography (assuming that the curve has a 2-torsion point).

Key words: Cryptography, elliptic curves, side-channel attacks, unified addition formulae

1. Introduction

Because of their short key length and their long-term strength, elliptic curve cryptosystems have become very popular. They have recently been recommended by NSA. This small key size is especially attractive for devices with limited capacities, like smart cards. However, such devices are sensitive to side-channel attacks. In the following, we focus on simple attacks since it is always possible to introduce countermeasures against differential attacks [5]. Such simple attacks are based on the difference of complexity between doubling and addition operations on an elliptic curve. They can be achieved by analysing information like timing [6], power consumption [7], electromagnetic radiation [9] or any other side-channel information.
Several methods have been developed to obtain an arithmetic which is resistant to side-channel attacks, and most of them can be found in [4]. Some

of these methods consist in rewriting the addition formulae so that it can be used for doubling a point. In this way, the doubling of a point and the addition of two distinct points become indistinguishable and simple side-channel attacks are staved off. Until now, the most efficient unified addition formulae have been obtained by using the Jacobi form of an elliptic curve with a 2-torsion point [2]. Based on curve representation, the authors present formulae requiring 14 field multiplications if some additional conditions are satisfied, and 16 unconditionally.
In this paper, we will improve these formulae. The result of this enhancement is that the unified addition requires only 12 field multiplications under conditions and 14 unconditionally. Moreover, we relax the conditions evoked above. Thus, we obtain the most efficient unified addition for an elliptic curve containing a 2-torsion point (which means that the order of the curve is even).

The paper is organized as follows. In Section 2 we review the Jacobi form of an elliptic curve and the unconditional unified addition formulae obtained

---

in [2]. In Section 3, we give our improved unconditional formulae and discuss the differences with the previous ones. Then, in Section 4, we explain how these formulae can again be improved under some conditions and how we are relaxing the conditions given in [2]. Finally, we conclude in Section 5.

2. Elliptic curves in Jacobi form

In this paper, the base field is a finite prime field $\mathbb{F}_p$ where p is a large prime number. In fact, it is easy to generalize the results to any finite field of characteristic greater than or equal to 5, but this is of no interest for cryptography in real life.

Let E be an elliptic curve defined over such a field. It is well known that E can be represented by the set of points (x, y) in $\mathbb{F}_p^2$ satisfying an equation of the form

$$E : y^2 = x^3 + a_4 x + a_6,$$

together with a point at infinity (denoted $\mathcal{O}$ in the following) [10]. Constants a_4 and a_6 are elements of $\mathbb{F}_p$ such that $4a_4^3 + 27a_6^2 \neq 0$. In [8], Liardet and Smart explain how the embedding of an elliptic curve as the intersection of two quadrics in $\mathbb{P}^3$ can be used to produce unified addition formulae. In [2], Brier and Joye are generalize and improve this idea by considering the (extended) Jacobi quartics given by equations of the form

$$Y^2 = \varepsilon X^4 - 2\delta X^2 Z^2 + Z^4. \tag{1}$$

With this equation, a point is represented by a triplet (X, Y, Z) satisfying equation (1). Let us note that two triplets (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) represent the same point if and only if there is an element k in $\mathbb{F}_p^*$ such that $X_1 = kX_2$, $Y_1 = k^2 Y_2$ and $Z_1 = kZ_2$.

It is proved in [2] that any elliptic curve defined over $\mathbb{F}_p$ having a 2-torsion point is birationally equivalent to such a quartic.

Let $(\theta, 0)$ be such a 2-torsion point, then constants ε and δ are defined by

$$\varepsilon = -\frac{3\theta^2 + 4a_4}{16},$$
$$\delta = \frac{3}{4}\theta,$$

and the birational transformations are given by

$$\psi : \begin{cases} (\theta, 0) \rightarrow (0, -1, 1), \\ \mathcal{O} \rightarrow (0, 1, 1), \\ (x, y) \rightarrow \left(2(x - \theta), (2x + \theta)(x - \theta)^2 - y^2, y\right), \end{cases}$$

and

$$\psi^{-1} : \begin{cases} (0, 1, 0) \rightarrow \mathcal{O}, \\ (0, -1, 0) \rightarrow (\theta, 0), \\ (X, Y, Z) \rightarrow \left(\frac{2(Y + Z^2)}{X^2} - \frac{\theta}{2}, Z\frac{4(Y + Z^2) - 3\theta^2}{X^3}\right). \end{cases}$$

Of course, this means that all the curves cannot be transformed into an extended Jacobi quartic. In particular, the cardinality of a curve transformable into such a form is even. However, this is more general than the intersection of two quadrics [8] or the Montgomery form [4] whose cardinality can be divided by 4.

Let us now give the formulae for the addition

$$(X_1, Y_1, Z_1) + (X_2, Y_2, Z_2) = (X_3, Y_3, Z_3).$$

We have

$$\begin{cases} X_3 = X_1 Z_1 Y_2 + Y_1 X_2 Z_2, \\ Y_3 = (Z_1^2 Z_2^2 + \varepsilon X_1^2 X_2^2)(Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2) \\ \qquad + 2\varepsilon X_1 X_2 Z_1 Z_2(X_1^2 Z_2^2 + Z_1^2 X_2^2), \\ Z_3 = Z_1^2 Z_2^2 - \varepsilon X_1^2 X_2^2 \end{cases} \tag{2}$$

The main interest of these formulae is that they remain valid if $(X_1, Y_1, Z_1) = (X_2, Y_2, Z_2)$. They are also valid if one of the points is the neutral element. According to [2], these formulae require **13 multiplications** and **3 multiplications by constants**, which has provided the best unified formulae until now. They also require **14 modular reductions** and **8 temporary variables**. Note that we give both the number of multiplications (which is standard) and the number of modular reductions because the latter is the most important operation in RNS representation, which can be used for performing a safe arithmetic on elliptic curves, as explained in [1]. This complexity can be reduced by eliminating 2 multiplications by constants if ε is small, which is possible under some conditions. Before explaining these conditions and relaxing them in comparison with [2], let us explain how to reduce the number of multiplications and modular reductions.

2

3. Improved addition formulae

Let φ be the map

$$\varphi: \quad \mathbb{F}_p^3 \quad \longrightarrow \quad \mathbb{F}_p^4$$
$$(X, Y, Z) \mapsto (X^2, XZ, Z^2, Y)$$

Let (X, Y, Z) be a point on the extended Jacobi quartic. To reduce the number of field multiplications, we will use $\varphi(X, Y, Z)$ instead of (X, Y, Z). Of course this increases the memory required compared to [2]. This is a drawback for small devices, but we will see that in practice only 9 temporary variables are necessary instead of 8 in [2], so the memory extra cost is not very high.

We thus use the formulae (2) and give, in Table 1, the operations necessary to add two points (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) represented by $\varphi(X_1, Y_1, Z_1) = (U_1, V_1, W_1, Y_1)$ and $\varphi(X_2, Y_2, Z_2) = (U_2, V_2, W_2, Y_2)$. If the sum of these points is (X_3, Y_3, Z_3), the operations described can either return (X_3, Y_3, Z_3) or return $\varphi(X_3, Y_3, Z_3) = (U_3, V_3, W_3, Y_3)$.

Assuming that the input and output are represented using φ, executing operations of Table 1 requires only **11 multiplications** and **3 multiplications by constants**. They also require **12 modular reductions** and **9 temporary variables**. Compared to [2], this is a gain of 14% and even 17% if ε is assumed to be small (as discussed in the next section). Thus, this provides the best unified addition for an elliptic curve with a 2-torsion point. Let us now describe in detail how this new system of coordinates can be used to perform a scalar multiplication which is resistant to side-channel attacks.

Let E be an elliptic curve defined over $\mathbb{F}_p$ containing a 2-torsion point and let P be a point in $E(\mathbb{F}_p)$ and n an integer. The computation of nP is crucial in elliptic curve cryptography since this operation is used in almost all cryptosystems and is the most time-consuming operation. We can proceed as follows:

(1) Compute constants ε and θ to obtain the equation of the (extended) Jacobi quartic (of the form (1)).
(2) Send the point P to the (extended) Jacobi quartic model using the rational transformation ψ.
(3) Compute the new coordinates (U, V, W, Y) of $\psi(P)$ using the map φ.

Table 1
Unified addition on a Jacobi quartic using φ

Operation	Value of the variable
$T_1 \leftarrow U_1$	X_1^2
$T_2 \leftarrow U_2$	X_2^2
$T_3 \leftarrow V_1$	$X_1 Z_1$
$T_4 \leftarrow V_2$	$X_2 Z_2$
$T_5 \leftarrow W_1$	Z_1^2
$T_6 \leftarrow W_2$	Z_2^2
$T_7 \leftarrow Y_1$	Y_1
$T_8 \leftarrow Y_2$	Y_2
$T_9 \leftarrow T_7 T_8$	$Y_1 Y_2$
$T_7 \leftarrow T_7 + T_3$	$X_1 Z_1 + Y_1$
$T_8 \leftarrow T_8 + T_4$	$X_2 Z_2 + Y_2$
$T_3 \leftarrow T_3 T_4$	$X_1 X_2 Z_1 Z_2$
$T_7 \leftarrow T_7 T_8$	$(X_1 Z_1 + Y_1)(X_2 Z_2 + Y_2)$
$T_7 \leftarrow T_7 - T_9$	$X_1 Z_1 Y_2 + X_2 Z_2 Y_1 + X_1 Z_1 X_2 Z_2$
$T_7 \leftarrow T_7 - T_3$	$\mathbf{X_3}$
$T_4 \leftarrow T_1 T_2$	$X_1^2 X_2^2$
$T_8 \leftarrow T_5 T_6$	$Z_1^2 Z_2^2$
$T_1 \leftarrow T_1 + T_5$	$X_1^2 + Z_1^2$
$T_2 \leftarrow T_2 + T_6$	$X_2^2 + Z_2^2$
$T_5 \leftarrow T_1 T_2$	$\left(X_1^2 + Z_1^2\right)\left(X_2^2 + Z_2^2\right)$
$T_5 \leftarrow T_5 - T_4$	$X_1^2 Z_2^2 + X_2^2 Z_1^2 + Z_1^2 Z_2^2$
$T_5 \leftarrow T_5 - T_8$	$X_1^2 Z_2^2 + X_2^2 Z_1^2$
$T_4 \leftarrow \varepsilon T_4$	$\varepsilon X_1^2 X_2^2$
$T_1 \leftarrow T_8 - T_4$	$\mathbf{Z_3}$
$T_2 \leftarrow T_8 + T_4$	$Z_1^2 Z_2^2 + \varepsilon X_1^2 X_2^2$
$T_6 \leftarrow 2\delta T_3$	$2\delta X_1 X_2 Z_1 Z_2$
$T_6 \leftarrow T_9 - T_6$	$Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2$
$T_6 \leftarrow T_6 T_2$	$(Z_1^2 Z_2^2 + \varepsilon X_1^2 X_2^2)(Y_1 Y_2 - 2\delta X_1 X_2 Z_1 Z_2)$
$T_3 \leftarrow 2\varepsilon T_3$	$2\varepsilon X_1 X_2 Z_1 Z_2$
$T_3 \leftarrow T_5 T_3$	$2\varepsilon X_1 X_2 Z_1 Z_2 \left(X_1^2 Z_2^2 + X_2^2 Z_1^2\right)$
$T_8 \leftarrow T_6 + T_3$	$\mathbf{Y_3}$
$T_2 \leftarrow T_7^2$	$\mathbf{U_3}\left(= X_3^2\right)$
$T_4 \leftarrow T_1 T_7$	$\mathbf{V_3}\ (= X_3 Z_3)$
$T_6 \leftarrow T_1^2$	$\mathbf{W_3}\left(= Z_3^2\right)$

(4) Use the full Table 1 and your favorite exponentiation algorithm to compute $n(U, V, W, Y)$.
(5) Remember to use only the first part of Table 1 for the last operation of the exponentiation, so that the result of the exponentiation is a point

3

on the (extended) Jacobi quartic with standard coordinates (X, Y, Z).

(6) Send this point back to the original elliptic curve via the reverse rational transformation ψ^{-1}.

Of course, steps (1), (2) and (6) are not necessary if the curve is originally given in (extended) Jacobi quartic form. Moreover, note that, since addition and doubling are indistinguishable, any of the many exponentiation algorithms (double-and-add, w-NAF, addition chains, fixed base point methods) can be used without jeopardizing the security against simple side-channel attacks.

4. The case of small coefficients

In formulae (2), there are two multiplications by ε, so it is very interesting to assume that ε is small. In [2], the authors explained that this is possible for most elliptic curves with **three** points of order 2. More precisely they prove that ε can always be rescaled to 1 if $p \equiv 3 \bmod 4$ and with a probability 7/8 if $p \equiv 1 \bmod 4$. In this part, we explain how to relax the condition on the number of 2-torsion points. Indeed, it is not necessary to make additional assumptions to obtain this result and it is even possible to conclude in more cases.

Thus, we only assume in the following that the elliptic curve E has **one** 2-torsion point (which is a necessary condition to transform the curve into a Jacobi quartic). Let $(\theta, 0)$ be this 2-torsion point on E, and recall that

$$\varepsilon = -\frac{3\theta^2 + 4a_4}{16}.$$

Let $\alpha \in \mathbb{F}_p$. We will consider the change of variables

$$x = \frac{X}{\alpha^2}, \quad y = \frac{Y}{\alpha^3}$$

which makes the elliptic curve E isomorphic to the elliptic curve

$$E' : Y^2 = X^3 + a_4'X + a_6',$$

with $a_4' = a_4\alpha^4$ and $a_6' = b\alpha^6$. This curve has, of course, a 2-torsion point $(\theta', 0)$ with $\theta' = \theta\alpha^2$, so if one wants to transforms E' into a Jacobi quartic, the new value of ε is

$$\varepsilon' = \varepsilon\alpha^4.$$

We therefore have to find an α such that $\varepsilon\alpha^4$ is a small number. For this, let μ denote the smallest integer (greater than or equal to -1) which is not a square modulo p. Using the multiplicativity of the Legendre symbol, one can prove that four cases can occur (with the same probability):

(i) ε is a fourth power in $\mathbb{F}_p$ and we can choose α such that $\varepsilon' = 1$.

(ii) ε is not a square in $\mathbb{F}_p$ and $\sqrt{\frac{\varepsilon}{\mu}}$ is a square. In this case, $\frac{\varepsilon}{\mu}$ is a fourth power and we can choose α such that $\varepsilon' = \mu$.

(iii) ε is a square in $\mathbb{F}_p$ but not $\sqrt{\varepsilon}$. In this case, $\frac{\varepsilon}{\mu^2}$ is a fourth power and we can choose α such that $\varepsilon' = \mu^2$.

(iv) Neither ε nor $\sqrt{\frac{\varepsilon}{\mu}}$ are squares in $\mathbb{F}_p$. In this case, $\frac{\varepsilon}{\mu^3}$ is a fourth power and we can choose α such that $\varepsilon' = \mu^3$.

The simplest case to treat is $p \equiv 3 \bmod 4$. Indeed, we can choose $\mu = -1$ so that we can always rescale ε to 1 or -1. Note that this is the most current case in cryptographic applications (pseudo-Mersenne primes or generalized Mersenne primes). If $p \equiv 1 \bmod 4$, we have to check that μ is sufficiently small. It is easy to prove (again using the properties of the Legendre symbol) that the proportion of prime fields such that the n first prime numbers are squares is only $\frac{1}{2^n}$. Thus, in most cases it is possible to rescale ε to a small number.

Anyway, if μ is too large to assume that the multiplication by ε' can be neglected (for instance, if we are in cases (iii) or (iv)), there is another way to rescale ε to a small value. This method is explained in [3]. The principle is to find an isogeny of small degree between the elliptic curve E and a new elliptic curve, say E'', having the same cardinality. One can then hope that the method explained above (i.e. via isomorphisms) will give a better result on E'' than on E (for instance, if we are in cases (i) or (ii)). Basically, this is the same idea as the previous isomorphism between E and E' (an isomorphism is an isogeny of degree 1), but the composition of the isogeny and its dual is not the identity on E, so the scalar multiplication must be modified to give a good result. This operation is of negligeable cost compared to full scalar multiplication, as explained in detail in [3].

4

5. Conclusion

In this paper, we provide better unified addition formulae for elliptic curves having a 2-torsion point by introducing a new system of coordinates on the (extended) Jacobi quartic model. Moreover, we prove that, in most cases, it is not necessary to assume that the elliptic curve has three 2-torsion points to be able to rescale ε to a small value. In particular, we prove that, if $p \equiv 3 \bmod 4$, ε can be rescaled to 1 or -1 without any additional assumption on the curve.

Finally, we obtain unified addition formulae (on elliptic curves with a 2-torsion point) requiring only 12 multiplications on the base field in most cases, which represents a gain of 17% compared to the best known formulae until now ([2]). This formulae will allow more efficient scalar multiplication, which is resistant to side-channel attacks, on elliptic curves whose order is even.

References

[1] J. C. Bajard, S. Duquesne, M. Ercegovac, N. Meloni, Residue systems efficiency for modular products summation: application to elliptic curves cryptography, Proc. SPIE Vol. 6313, 631304 (Aug. 25, 2006).

[2] O. Billet, M. Joye, The Jacobi Model of an Elliptic Curve and Side-Channel Analysis, Applied Algebra, Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Sci., vol.2643, Springer, Berlin, 2003, pp. 34–42.

[3] E. Brier, M. Joye, Fast Point Multiplication on Elliptic Curves Trough Isogenies, Applied Algebra, Algorithms and Error-Correcting Codes, Lecture Notes in Comput. Sci., vol.2643, Springer, Berlin, 2003, pp. 43–50.

[4] Cohen, H., Frey, G., Handbook of elliptic and hyperelliptic curve cryptography, Discrete Math. Appl., Chapman & Hall/CRC, 2006.

[5] Coron, J.S., Resistance against differential power analysis for elliptic curve cryptosystems, CHES'99, Lecture Notes in Comput. Sci. vol. 1717, Springer, Berlin, 1999, pp. 292–302.

[6] Kocher, P.C., Timing attacks on implementations of DH, RSA, DSS and other systems, CRYPTO'96, Lecture Notes in Comput. Sci. vol. 1109, Springer, Berlin, 1996, pp. 104–113.

[7] Kocher, P.C., Jaffe, J., Jun, B., Differential power analysis, CRYPTO'99, Lecture Notes in Comput. Sci. vol. 1666, Springer, Berlin, 1999, pp. 388–397.

[8] P. Y. Liardet, N. Smart, Preventing SPA/DPA in ECC systems using the Jacobi form, CHESS 2001, Lecture Notes in Comput. Sci. vol. 2162, Springer, Berlin, 2001, pp. 391–401.

[9] Quisquater, J.J., Samyde, D., ElectroMagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards, e-smart 2001, Lecture Notes in Comput. Sci. vol. 2140, Springer, Berlin, 2001, pp. 200–210.

[10] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathemtics, vol. 106, Springer, Berlin, 1986.