Fast Point Multiplication on Elliptic Curves Through Isogenies

Éric Brier and Marc Joye

Gemplus Card International, Card Security Group
La Vigie, Avenue du Jujubier, ZI Athélia IV, 13705 La Ciotat Cedex, France
{eric.brier, marc.joye}@gemplus.com
http://www.gemplus.com/smart/ − http://www.geocities.com/MarcJoye/

Abstract. Elliptic curve cryptosystems are usually implemented over fields of characteristic two or over (large) prime fields. For large prime fields, projective coordinates are more suitable as they reduce the computational workload in a point multiplication. In this case, choosing for parameter a the value -3 further reduces the workload. Over $\mathbb{F}_p$, not all elliptic curves can be rescaled through isomorphisms to the case $a = -3$. This paper suggests the use of the more general notion of isogenies to rescale the curve. As a side result, this also illustrates that selecting elliptic curves with $a = -3$ (as those recommended in most standards) is not restrictive.

Keywords. Elliptic curves, scalar multiplication, isogenies, cryptography.

1 Introduction

Elliptic curves are plane curves defined by a polynomial equation having strong algebraic properties. In particular, it is possible to define an addition on points which yields a group structure. Furthermore, no sub-exponential algorithm is known to solve the Discrete Logarithm in the induced group.

From a practical viewpoint, fast addition formulæ are to be defined for efficient protocols using elliptic curve cryptography. As will be described in the next section, the case where elliptic curve parameter a is equal to -3 allows faster computation. Unfortunately, one cannot always obtain this value using the classical notion of isomorphism (though, according to the definition field, the probability is $1/2$ or $1/4$).

The aim of this paper is to show that it is possible to obtain the desired value $a = -3$ for an *isogenous* elliptic curve and to perform computations on this curve rather than on the original one. Being isogenous, both curves have the

same number of rational points and mappings between curves (called *isogenies*) allow to relate point multiplication in both groups.

The rest of this paper is organized as follows. The next section reviews the addition formulæ on elliptic curves. Section 3 explains how, in some cases, isomorphisms of curves may speed up the scalar multiplication. This idea is generalized and extended in Section 4 through the use of isogenies. A direct application to elliptic curve cryptography is given in Section 5. Finally, Section 6 concludes the paper. (A concrete example of our technique is given in Appendix A.)

2   Elliptic Curve Arithmetic

Let $\mathbb{K}$ be a field with $\operatorname{Char} \mathbb{K} \neq 2, 3$. An *elliptic curve E over* $\mathbb{K}$ is the set of points $(x, y) \in \mathbb{K} \times \mathbb{K}$ satisfying the Weierstraß equation

$$E_{/\mathbb{K}} : y^2 = x^3 + ax + b \tag{1}$$

along with the *point at infinity* $\mathcal{O}$. If this set is equipped with the so-called "chord-and-tangent" rule, it becomes an abelian group.

We use the additive notation. The point at infinity is the neutral element, $\boldsymbol{P} + \mathcal{O} = \mathcal{O} + \boldsymbol{P} = \boldsymbol{P}$. For two points $\boldsymbol{P} = (x_0, y_0)$ and $\boldsymbol{Q} = (x_1, y_1)$ with $\boldsymbol{P} \neq -\boldsymbol{Q}$, their sum $\boldsymbol{R} = \boldsymbol{P} + \boldsymbol{Q} = (x_2, y_2)$ is given by

$$x_2 = \lambda^2 - x_0 - x_1 \quad \text{and} \quad y_2 = (x_1 - x_2)\lambda - y_1$$

where $\lambda = (y_0 - y_1)/(x_0 - x_1)$ when $\boldsymbol{P} \neq \boldsymbol{Q}$ and $\lambda = (3x_1^2 + a)/(2y_1)$ otherwise.

The above formulæ require an inversion (in $\mathbb{K}$), a usually costly operation, especially when $\mathbb{K}$ is a large prime field. For this reason, projective coordinates may be preferred. Within (Jacobian) projective coordinates [IEEE], the representation of a point is not unique, the triplets $(v^2 X : v^3 Y : v Z)$ for any $v \in \mathbb{K} \setminus \{0\}$ all represent the same point. The correspondence of $\boldsymbol{P} = (X_0 : Y_0 : Z_0)$ with its affine coordinates is given by $\boldsymbol{P} = (x_0, y_0)$ where $x_0 = X_0/Z_0^2$ and $y_0 = Y_0/Z_0^3$ if $Z_0 \neq 0$, and $\boldsymbol{P} = \mathcal{O}$ if $Z_0 = 0$. The addition formulæ of points $\boldsymbol{P} = (X_0 : Y_0 : Z_0)$ and $\boldsymbol{Q} = (X_1 : Y_1 : Z_1)$ (with $\boldsymbol{P} \neq -\boldsymbol{Q}$ and $Z_0, Z_1 \neq 0$) then become $\boldsymbol{R} = (X_2 : Y_2 : Z_2)$ where

$$\begin{cases} X_2 = R^2 - TW^2 \\ 2Y_2 = VR - MW^3 \quad \text{when } \boldsymbol{P} \neq \boldsymbol{Q} \\ Z_2 = Z_0 Z_1 W \end{cases} \tag{2}$$

with $U_0 = X_0 Z_1^2$, $U_1 = X_1 Z_0^2$, $S_0 = Y_0 Z_1^3$, $S_1 = Y_1 Z_0^3$, $W = U_0 - U_1$, $R = S_0 - S_1$, $T = U_0 + U_1$, $M = S_0 + S_1$, and $V = TW^2 - 2X_2$, and

$$\begin{cases} X_2 = M^2 - 2S \\ Y_2 = M(S - X_2) - T \quad \text{when } \boldsymbol{P} = \boldsymbol{Q} \\ Z_2 = 2Y_1 Z_1 \end{cases} \tag{3}$$

with $M = 3X_1{}^2 + aZ_1{}^4$, $S = 4X_1Y_1{}^2$, and $T = 8Y_1{}^4$.

We see that the addition of two (different) points requires 16 multiplications and only 11 when $Z_1 = 1$. The doubling of a point requires 10 multiplications, including the multiplication by the parameter a. When a is small, this latter multiplication can be neglected. The value $a = -3$ is particularly attractive since then $M = 3(X_1 - Z_1{}^2)(X_1 + Z_1{}^2)$ and so only 8 multiplications are required to double a point.

Another useful value for a is $a = 0$ since then the number of required multiplications decreases to 7. This case is not studied here because choosing $a = 0$ has too many implications on the endomorphism ring of the curve, which could decrease security (though no algorithm using this property is known today).

3   Isomorphisms

Two elliptic curves E and E', respectively given by the Weierstraß equations $E_{/\mathbb{K}} : y^2 = x^3 + ax + b$ and $E'_{/\mathbb{K}} : y^2 = x^3 + a'x + b'$, are *isomorphic over* $\mathbb{K}$ if and only if there exists a nonzero element $u \in \mathbb{K}$ such that $u^4 a' = a$ and $u^6 b' = b$. Moreover, the isomorphism is given by

$$\phi : E \xrightarrow{\sim} E', \begin{cases} (x, y) \longmapsto (u^{-2}x, u^{-3}y) \\ \mathcal{O} \longmapsto \mathcal{O} \end{cases} .$$

The elliptic curve $E_{/\mathbb{K}} : y^2 = x^3 + ax + b$ can thus be made isomorphic to the elliptic curve $E'_{/\mathbb{K}} : y^2 = x^3 - 3x + b'$ if and only if $a = -3u^4$ for some $u \in \mathbb{K} \setminus \{0\}$. When $\mathbb{K} = \mathbb{F}_p$, a (large) prime field, this occurs roughly with probability $1/2$ when $p \equiv 3 \pmod 4$ and with probability $1/4$ when $p \equiv 1 \pmod 4$. Consequently, there is a non-negligible probability that a *random* elliptic curve cannot be rescaled to the interesting[1] case $a = -3$. The next section investigates an alternative solution to overcome this limitation through the use of isogenies.

4   Isogenies

An *isogeny* between two elliptic curves E and E' defined over $\mathbb{K}$ is a non-constant[2] morphism $\phi : E \to E'$. The *degree of isogeny* ϕ is defined to be

$$\deg \phi = [\overline{\mathbb{K}}(E) : \phi^* \overline{\mathbb{K}}(E')]$$

where $\phi^* : \overline{\mathbb{K}}(E') \to \overline{\mathbb{K}}(E), f \mapsto \phi^*(f) = f \circ \phi$ denotes the map induced by ϕ. (Remark that an isogeny of degree 1 is an isomorphism.)

A useful result is that for every isogeny $\phi : E \to E'$, there exists a unique isogeny $\hat{\phi} : E' \to E$, called the *dual isogeny* [Sil86, III.4], such that

$$\hat{\phi} \circ \phi = [m] \quad \text{and} \quad \phi \circ \hat{\phi} = [m]'$$

---

[1] i.e., suitable for fast implementations; see Section 2.
[2] We do not consider the zero isogeny $\phi = [0]$.

where $m = \deg \phi$ and $[m]$ (resp. $[m]'$) is the multiplication-by-m isogeny on E (resp. E'). Interestingly, this leads to a different way for computing $\boldsymbol{Q} = [rm]\boldsymbol{P}$ as $\boldsymbol{Q} = \hat{\phi}\big([r]'\phi(\boldsymbol{P})\big)$.

$$
\begin{array}{ccc}
\boldsymbol{P} \in E(\mathbb{K}) & \xrightarrow{\;[rm]\;} & \boldsymbol{Q} = [rm]\boldsymbol{P} \in E(\mathbb{K}) \\
\phi \downarrow & & \uparrow \hat{\phi} \\
\boldsymbol{P}' \in E'(\mathbb{K}) & \xrightarrow{\;[r]'\;} & \boldsymbol{Q}' = [r]'\boldsymbol{P}' \in E'(\mathbb{K})
\end{array}
$$

Fig. 1. Computing $\boldsymbol{Q} = [rm]\boldsymbol{P}$ through isogenies.

Isogenies have been intensively studied in order to improve point counting algorithms. What we are interested in is to build an isogeny of small degree. We know that we can find an isogeny ϕ of degree m from E to a curve E' if and only if the equation

$$\Phi_m(j, X) = 0$$

where Φ_m is the m-th modular polynomial and j is the j-invariant of the curve, has a rational solution. If so, we can follow the method described in [BSS99, pp. 126–130] to find the isogenous curve equation. We check that the new curve is isomorphic to a curve with parameter $a = -3$. It then remains to compute the isogeny itself. An algorithm for producing the isogeny is presented in [CM94].

5   Application to Cryptography

The basic operation of elliptic curve cryptosystems is the point multiplication: given a point $\boldsymbol{P} = (x_1, y_1) \in E(\mathbb{K})$, one has to compute $\boldsymbol{Q} = [k]\boldsymbol{P} = (x_k, y_k)$ for some $1 \le k < \mathrm{ord}_E \boldsymbol{P}$. Assume that the definition field is $\mathbb{F}_p$ where p is a large prime. We have seen in Section 2 that in this case an elliptic curve with parameter $a = -3$ yields a point multiplication substantially faster when working within projective coordinates. We compute $\boldsymbol{Q} = [k]\boldsymbol{P}$ as $(X_k : Y_k : Z_k) = [k](x_1 : y_1 : 1)$ and then $(x_k, y_k) = (X_k/Z_k{}^2, Y_k/Z_k{}^3)$ with only 8 multiplications (in $\mathbb{F}_p$) per doubling. When E has not parameter $a = -3$ (or cannot be reduced to this case through isomorphism) then we can apply the following methodology.

Let ϕ denote an isogeny of degree m between the elliptic curves $E_{/\mathbb{F}_p} : y^2 = x^3 + ax + b$ and $E'_{/\mathbb{F}_p} : y^2 = x^3 - 3x + b'$. Since, for security reasons, point $\boldsymbol{P}$ has large prime order, we may assume w.l.o.g. that $\gcd(m, \mathrm{ord}_E \boldsymbol{P}) = 1$ and so m is invertible modulo $\mathrm{ord}_E \boldsymbol{P}$. We define $k_m \equiv k/m \pmod{\mathrm{ord}_E \boldsymbol{P}}$. Hence, we can obtain $\boldsymbol{Q} = [k]\boldsymbol{P}$ according to

$$\boldsymbol{Q} = \hat{\phi}\big([k_m]'\phi(\boldsymbol{P})\big) \ . \tag{4}$$

Example 1. We give a "toy" example to illustrate the technique. A concrete example (i.e., with cryptographic size) can be found in appendix.

Over the field $\mathbb{F}_{149}$, we define the elliptic curves

$$E_{/\mathbb{F}_{149}} : y^2 = x^3 + x + 133$$

and

$$E'_{/\mathbb{F}_{149}} : y^2 = x^3 - 3x - 14$$

which are isogenous via the maps

$$\varphi : \quad E \quad \longrightarrow E'$$
$$(x, y) \longmapsto \left(\frac{x^5 + 4x^4 + 99x^3 + 42x^2 + 99x + 49}{(17x^2 + 34x + 50)^2}, \frac{x^6 + 6x^5 + 107x^4 + 126x^3 + 112x^2 + 116x + 139}{(17x^2 + 34x + 50)^3} \right)$$

$$\hat{\varphi} : \quad E' \quad \longrightarrow E$$
$$(x, y) \longmapsto \left(\frac{x^5 + 85x^4 + 60x^3 + 137x^2 + 26x + 95}{(123x^2 + 87x + 86)^2}, \frac{x^6 + 53x^5 + 134x^4 + 74x^3 + 106x^2 + 50x + 34}{(123x^2 + 87x + 86)^3} \right)$$

Choosing a *random* point $\boldsymbol{P} = (107, 6)$ on the curve E, we have

$$\varphi(\boldsymbol{P}) \quad = (56, 106) \in E'$$
$$\hat{\varphi}(\varphi(\boldsymbol{P})) = (70, 143) \in E$$

whereby it is easily checked that

$$\hat{\varphi}(\varphi(\boldsymbol{P})) = [5]\boldsymbol{P} \ .$$

6   Concluding Remarks

The first consequence of our work on isogenies is that computing a point multiplication can in most of cases be made using a curve with $a = -3$ even when such a value cannot be rescaled directly through isomorphism. This leads to a faster point multiplication.

The second consequence is that when choosing a random curve, one can restrict oneself to curves with parameter $a = -3$ and a random value for parameter b. This follows from the observation that most curves are mapped to a curve with $a = -3$ by an isogeny of small degree. The Discrete Logarithm Problem on the isogenous curve is then as hard as on the original curve.

This paper can be seen as a justification to the fact that most curves recommended in cryptographic standards use for parameter a the value -3.

References

[BSS99] Ian Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1999.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, 1993.

[IEEE]   IEEE Computer Society. IEEE standard specifications for public-key cryptography. IEEE Std 1363-2000, 2000.

[NIST] National Institute of Standards and Technology (NIST). Digital signature standard (DSS). FIPS PUB 186-2, 2000.
[SECG] 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.
[CM94] Jean-Marc Couveignes and François Morain *Schoof's algorithm and isogeny cycles*, Proc. ANTS-I, vol 877 of *Lecture Notes in Computer Science*, pp. 43–58, Springer-Verlag, 1994.

A   A Concrete Example

The following example is taken from [BSS99]. The curve equation is

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

with
$$\begin{cases} p = 2^{160} + 7 \\ a = 1 \\ b = 1010685925500572430206879608558642904226772615919 \\ \#E(\mathbb{F}_p) = 1461501637330902918203683038630093524408650319587 \end{cases}.$$

[It should be noted that this curve is not isomorphic to a curve with parameter $a = -3$.]

This curve is isogenous to

$$E'_{/\mathbb{F}_p} : y^2 = x^3 - 3x + b'$$

with $b' = 632739926637917759594186681013274896520567575517$. The isogeny, whose degree is $m = 11$, is given by

$$\phi(x,y) = \left(\frac{u(x)}{w(x)^2}, y \cdot \frac{v(x)}{w(x)^3} \right)$$

where

$$\begin{aligned}
u(x) = \ & 370690178134646041774135216324801714060106373562\ + \\
& 861256312888039375439296090988112886597456503254\ x\ - \\
& 710816068955948441247024728782103926686793729401\ x^2\ - \\
& 660949999632736745607557761155749317154796231190\ x^3\ + \\
& 104899805475825460399317568666533147309646767733\ x^4\ - \\
& 682987121612996351004314311578456905260387427374\ x^5\ - \\
& 540119027692075395022771129540214285068704207535\ x^6\ + \\
& 796617542631289284086426144833751968835133978328\ x^7\ + \\
& 563704518387054717437229862610850421868057177503\ x^8\ - \\
& 424589103609629859400080142081400291591066256566\ x^9\ + \\
& 876425480231036355075555366979717142934963067430\ x^{10} + x^{11}
\end{aligned}$$

$$
\begin{aligned}
v(x) = \ & 452495052944959116984585216749653914270910889527\ + \\
& 106938056042105603920415432157075009245555960036\ x+ \\
& 49633669527287210061590288590396941307155703319 1\ x^2+ \\
& 71879179729824148515446616026183765047313280591 8\ x^3+ \\
& 89347021676196991929966264352461222669954368759 4\ x^4+ \\
& 95360109982590787180111885348013732359702675720 5\ x^5+ \\
& 18886633622622298256790036603277695633740632445 0\ x^6+ \\
& 43273774401193542010990857967967390374744414016 5\ x^7+ \\
& 71042908863420436180409854193276857166599029914 8\ x^8+ \\
& 125413744485636798818070606529284113687990997420 0\ x^9+ \\
& 136193167152384738320497876605520992065543883410 6\ x^{10}+ \\
& 224174838124749514144448341849636056852679202105\ x^{11}+ \\
& 822580180065442824400025136323882213536827521732\ x^{12}+ \\
& 868139349472303188526373742085334684040049294310\ x^{13}+ \\
& 131463822034655453261333305046957571440244460114 5\ x^{14} + x^{15}
\end{aligned}
$$

$$
\begin{aligned}
w(x) = \ & 32501987297990211502240187587861871049872879448\ + \\
& 136393708764515461796279036305611379991137239531 7\ x+ \\
& 141192101827026132779724561821435058427949423805 1\ x^2+ \\
& 70237665636693548622727735807424896198713030751\ x^3+ \\
& 54041111397077468645890073148187670715073826739 0\ x^4+ \\
& 185696743461557439053221819709786835990283193274\ x^5
\end{aligned}
$$

and the dual isogeny is given by

$$
\hat{\phi}(x,y) = \left(\frac{\hat{u}(x)}{\hat{w}(x)^2}, y \cdot \frac{\hat{v}(x)}{\hat{w}(x)^3} \right)
$$

where

$$
\begin{aligned}
\hat{u}(x) = \ & 75311255693795382396930090686297414097787191914 3\ + \\
& 65809795177082413448982034865179786648563343729 4\ x- \\
& 35183501384647667442846092389667749196892404625 7\ x^2+ \\
& 25545246903672634894298841107332021021490857074 6\ x^3- \\
& 18334420650014871229322739744326227560447380518 3\ x^4+ \\
& 12575220850464771436402576110126009544585842516 34\ x^5- \\
& 69024973193875784615274350969816794845898829972 4\ x^6- \\
& 25965441700829881061329929468284859568810501028\ x^7- \\
& 18567603955952416315987761166471180706572838123 6\ x^8- \\
& 71626255671962842060388116547325332721478308415 8\ x^9+ \\
& 106034814417423153262246032820624542697129316890 0\ x^{10} + x^{11}
\end{aligned}
$$

$$\hat{v}(x) = 106706502733340491737102103276366850697246963 0529 +$$
$$8833614797969153026207984898706625663232722096 34 \; x+$$
$$1473543133280135405561737630087260277601867771 84 \; x^2+$$
$$3680780365097882540415410677062419567005571449 7 \; x^3+$$
$$1165987233874930893186423892075380266512707088 792 \; x^4+$$
$$1310036537737376847950424064579599212263547248 75 \; x^5+$$
$$1261920559979225427898222520995078688704637834 874 \; x^6+$$
$$1757290499903509181865286512582556015946533961 76 \; x^7+$$
$$8974057283078431908061484250040246497450136475 6 \; x^8+$$
$$1399715860686557861571172231451517092102243078 837 \; x^9+$$
$$1246192589478925975703839359801414492925549285 355 \; x^{10}+$$
$$6160267099924948800624474674093262102741528758 56 \; x^{11}+$$
$$4288149345648354861094144101244508062555564181 00 \; x^{12}+$$
$$2412971662261056882297674507252325391446035097 070 \; x^{13}+$$
$$1290205789304443807300056595930851208010072103 67 \; x^{14} + x^{15}$$

$$\hat{w}(x) = \quad 135333262963423915607144923995277271284729908 723 +$$
$$8597353468613275816570571658629794863365967762 58 \; x+$$
$$1293953775189763869954229560164157649159824538 936 \; x^2+$$
$$8795488307557375542072275955903363094922415500 00 \; x^3+$$
$$8401874862354523614288420851342251939740035412 59 \; x^4+$$
$$7845702924381311560519225078811093846232241174 2 \; x^5$$