Efficient constant-time hashing to some elliptic curves of j-invariant 0

Dmitrii Koshelev [1]

Versailles Laboratory of Mathematics, Versailles Saint-Quentin-en-Yvelines University
Center for Research and Advanced Development, Infotecs
Algebra and Number Theory Laboratory, Institute for Information Transmission Problems

Abstract. Let $\mathbb{F}_p$ be a prime finite field ($p > 5$) and $E_b\colon y_0^2 = x_0^3 + b$ be an elliptic $\mathbb{F}_p$-curve of j-invariant 0. In this article we produce the simplified SWU hashing to curves E_b having an $\mathbb{F}_{p^2}$-isogeny of degree 5. This condition is fulfilled for some Barreto–Naehrig curves, including BN512 from the standard ISO/IEC 15946-5. Moreover, we show how to implement the simplified SWU hashing in constant time (for any j-invariant), namely without quadratic residuosity tests and inversions in $\mathbb{F}_p$. Thus in addition to the protection against timing attacks, the new hashing $h\colon \mathbb{F}_p \to E_b(\mathbb{F}_p)$ turns out to be much more efficient than the (universal) SWU hashing, which generally requires to perform 2 quadratic residuosity tests.

Key words: constant-time implementation, hashing to elliptic curves, Kummer surfaces, pairing-based cryptography, rational curves and their parametrization, vertical isogenies.

Contents

Introduction

For definiteness, we will suppose that E_b is an ordinary curve. According to [1, Example V.4.4] this condition means that $p \equiv 1 \pmod 3$, i.e., $\omega := \sqrt[3]{1} \in \mathbb{F}_p$, where $\omega \neq 1$. Many protocols of *pairing-based cryptography* [2] use a mapping $h\colon \mathbb{F}_p \to E_b(\mathbb{F}_p)$ called *hashing* [2, §8] such that the cardinality of its image equals $\Theta(p) = \Theta\big(|E_b(\mathbb{F}_p)|\big)$. In this type of cryptography the priority is given to the curves E_b, because the pairing computation on them is the most efficient (see [2, §4]).

[1] web page: https://www.researchgate.net/profile/Dimitri_Koshelev
email: dishport@yandex.ru
This work was supported in part by the RFBR under grant no. 19-31-90029\19.

For $c \in \mathbb{F}_p^*$ (such that $\sqrt{c} \notin \mathbb{F}_p$) let $E'_b\colon y_1^2 = c(x_1^3 + b)$ be the (unique) quadratic $\mathbb{F}_p$-twist of E_b and

$$K'_b := (E_b \times E'_b)/[-1] \qquad K'_b\colon y^2 = c(x_0^3 + b)(x_1^3 + b) \quad \subset \quad \mathbb{A}^3_{(x_0,x_1,y)},$$

where $y := y_0 y_1$, be the *Kummer surface* (see, e.g., [3, §2]) of the direct product $E_b \times E'_b$.

Let us give a strict mathematical definition so that the article is equally interesting to algebraic geometers, and not just to cryptographers. *Simplified SWU hashing* is any non-constant rational $\mathbb{F}_p$-map $h_{SWU}\colon \mathbb{A}^1 \dashrightarrow K'_b$, that is an $\mathbb{F}_p$-parametrization of any *rational* (possibly singular) $\mathbb{F}_p$-*curve* [4] on K'_b. It is known that h_{SWU} induces a (usual) hashing h (a constant-time implementation is represented in §2). We know from [5] that finding h_{SWU} is generally considered a difficult task only if $\sqrt[3]{b} \notin \mathbb{F}_p$, that is $2 \nmid |E_b(\mathbb{F}_p)|$. Therefore for definiteness, it is further assumed that this condition is met.

The quotient by the point $(0, \sqrt{b}) \in E_b(\mathbb{F}_{p^2})$ always gives the (unique) $\mathbb{F}_p$-endomorphism of degree 3 on E_b. If $\sqrt[3]{4b} \in \mathbb{F}_p$, then the curve E_b also has a *vertical* $\mathbb{F}_p$-*isogeny* (see its definition in [6, Proposition 36]) of degree 3 onto the curve of $j = -2^{15}5^33$ [7, Table 1], since the 3-division polynomial of E_b equals $\psi_3(x) = 3x(x^3 + 4b)$. In this case, the problem of constructing h_{SWU} is obviously reduced to the analogous problem already solved for $j \neq 0$ (see, e.g, [8]). In particular, this reduction applies to the curve BN256 from [9] early very popular in the industry. Thus we will assume that $\sqrt[3]{4b} \notin \mathbb{F}_p$.

In fact, in order to construct h_{SWU}, it is sufficient that the curve E_b has a vertical $\mathbb{F}_{p^2}$-isogeny. Moreover, if its degree is lower, then the computation of h_{SWU} (and hence h) is more efficient in practice. This fact was realized in [3], where we use a vertical $\mathbb{F}_{p^2}$-isogeny of degree 2, which exists for any curve of j-invariant 1728. This article is devoted to the case of degree 5 (and $j = 0$).

Let t_1 be the $\mathbb{F}_p$-trace and $D_1 = t_1^2 - 4p$ be the $\mathbb{F}_p$-discriminant of E_b. Since the $\mathbb{F}_{p^2}$-trace $t_2 = t_1^2 - 2p$, then the $\mathbb{F}_{p^2}$-discriminant $D_2 = t_2^2 - 4p^2 = t_1^2 D_1$. According to [6, Proposition 37] the curve E_b has a vertical $\mathbb{F}_{p^2}$-isogeny of degree 5, undefined over $\mathbb{F}_p$, (we denote it by $\phi_+\colon E_+ \to E_b$) if and only if $5 \mid t_1$. Moreover, in this case E_b does not have $\mathbb{F}_p$-isogenies of degree 5, because 5 cannot simultaneously divide t_1 and D_1. By the way, E_b never has horizontal isogenies (or, equivalently for $j = 0$, endomorphisms) of degree 5. Finally, it is easy to check that quite popular *Barreto–Naehrig (BN) curves* [2, Example 4.2] cannot have $\mathbb{F}_p$-isogenies of degree 5 at all.

In particular, the desired condition is fulfilled for the $\mathbb{F}_p$-curves BN512 and BN638 from [10, §4.1] (the first is also from [11, Part 5]), where the numbers in the notation are equal to $\lceil \log_2(p) \rceil$. Such bit lengths will become actual for pairing-based cryptography in the future, hence these curves are potentially useful. Factorizing D_1, we see that the smallest degree of a vertical $\mathbb{F}_p$-isogeny for BN512 (resp. BN638) is 1291 (resp. 1523). Therefore the idea of [8, §4.3] does not work here.

1 Main result

The 5-division polynomial of the curve E_b equals

$$\psi_5(x) = f_5(x^3), \qquad \text{where} \qquad f_5(z) := 5z^4 + 380bz^3 - 240b^2z^2 - 1600b^3z - 256b^4.$$

$$\begin{array}{ccccc} E_+ \times E_- & \stackrel{\varphi}{\to} & E_b \times E_b & \stackrel{\psi}{\to} & E_b \times E'_b \\ \rho \downarrow & & \rho \downarrow & & \downarrow \rho \\ K_\pm & \stackrel{\overline{\varphi}}{\to} & K_b & \stackrel{\overline{\psi}}{\to} & K'_b \end{array}$$

Figure 1

We get that any point of order 5 on E_b has the form $P = \big(\sqrt[3]{z_i}, \sqrt{z_i + b}\big)$, where $z_i \in \mathbb{F}_{p^4}^*$ $(0 \leqslant i \leqslant 3)$ are roots of the polynomial f_5. If P generates an $\mathbb{F}_{p^2}$-invariant subgroup (of the form $G = \{\mathcal{O}, \pm P, \pm 2P\}$), then obviously $\sqrt[3]{z_i} \in \mathbb{F}_{p^4}^*$ and $P \in E_b(\mathbb{F}_{p^8})$. Using Ferrari's method for expressing the roots z_i in radicals, it is easy to show that under the condition $\sqrt{5} \notin \mathbb{F}_p$ (in particular, if $5 \mid t_1$, this is true for all BN curves) we have $z_i \notin \mathbb{F}_{p^2}$. Therefore G is not $\mathbb{F}_p$-invariant and the norm of z_i equals $\mathrm{N}_{\mathbb{F}_{p^4}/\mathbb{F}_p}(z_i) = -2^8 b^4/5$. As a consequence, $\sqrt[3]{4b/5} \in \mathbb{F}_p$ and hence $\sqrt[3]{5} \notin \mathbb{F}_p$. The case $\sqrt{5} \in \mathbb{F}_p$ is expected to be simpler, hence we omit it.

In fact, it is enough to put $b = 10$. Indeed, since $\sqrt[3]{b/10} \in \mathbb{F}_p$, the curves E_b, E_{10} are isomorphic at most over $\mathbb{F}_{p^2}$. Therefore the surfaces K'_b, K'_{10} are isomorphic over $\mathbb{F}_p$.

Let E_- be the curve $\mathbb{F}_p$-conjugate to E_+, that is $j(E_-) = j(E_+)^p$. Similarly, $\varphi_- \colon E_- \to E_b$ is the isogeny $\mathbb{F}_p$-conjugate to φ_+, that is $\varphi_- = \mathrm{Fr} \circ \varphi_+ \circ \mathrm{Fr}^{-1}$, where Fr is the Frobenius endomorphism. An explicit form of the dual isogenies $\widehat{\varphi_\pm} \colon E_b \to E_\pm$ and then isogenies $\varphi_\pm$ can be easily found, using *Velu's formulas* [6, Proposition 38]. Besides, let us clarify Figure 1. We denote by $K_\pm$ (resp. K_b) the Kummer surface of the direct product $E_+ \times E_-$ (resp. $E_b \times E_b$). In addition, $\varphi := (\varphi_+, \varphi_-)$, the isogeny ψ is defined in §[3, §1], and ρ is the natural quotient map. Finally, $\overline{\varphi}$ (resp. $\overline{\psi}$) is the restriction of φ (resp. ψ) to the Kummer surfaces.

Due to [7, Table 2], by substituting 0 in the *modular polynomial* [12, Exercise 2.18] of level 5, we obtain

$$\Phi_5(0, j) = H_D(j)^3, \qquad \text{where} \qquad H_D(j) = j^2 + 654403829760 \cdot j + 5209253090426880$$

is the *Hilbert class polynomial* [12, §II.6] of discriminant $D = -5^2 3$. Its roots equal

$$j_\pm := j(E_\pm) = \pm 146329141248 \cdot \sqrt{5} - 327201914880.$$

Since the ideal class group [6, Proposition 51] of the field $\mathbb{Q}(\sqrt{5})$ is trivial, the curves $E_\pm$, considered over $\mathbb{Q}(\sqrt{5})$, have a *global minimal model* [13], which, as it turns out, is a short Weierstrass form, for instance

$$E_\pm \colon y^2 = x^3 + 60(\pm 9\sqrt{5} - 25)x - 50(\pm 252\sqrt{5} - 521).$$

Using the computer algebra system Magma, we obtain in [14] a non-trivial map $\chi \colon \mathbb{A}^1 \dashrightarrow K_\pm$ invariant under the "twisted" Frobenius endomorphism from [3, §1]. The arguments given when finding it are almost the same as those of [3, §3.1]. Thus we have the map

$$h_{SWU} := \overline{\psi} \circ \overline{\varphi} \circ \chi = \big(x_0(t), x_1(t), y(t)\big),$$

which is also explicitly written out in [14]. Here $x_0(t), x_1(t)$ are rational $\mathbb{F}_p$-functions of the variable t of degree 20 and $y(t)$ is that of degree 60. An explanation of why h_{SWU} is defined

over $\mathbb{F}_p$ is given in [3, §1]. Finally, using [3, Theorem 1.1] and [4, §6.1.2], one can easily check that it is birational with its own image.

Let's summarize the main result of the article.

Theorem 1. *If an ordinary elliptic $\mathbb{F}_p$-curve E_b has an $\mathbb{F}_{p^2}$-isogeny of degree 5, then (except for a finite number of p) there is a simplified SWU hashing $h_{SWU}\colon \mathbb{A}^1 \dashrightarrow K'_b$. Moreover, the latter can be found explicitly.*

According to [7, Tables 1, 2] there are exactly 5 non-maximal (i.e., $\subsetneq \mathbb{Z}[\omega]$) orders of the quadratic field $\mathbb{Q}(\sqrt{-3})$, having class number 1 or 2. Their conductors are 2, 3 and 4, 5, 7 respectively. Thus there remains only the case of a vertical $\mathbb{F}_{p^2}$-isogeny of degree 7 to (from) E_b, for which, apparently, it is possible to construct h_{SWU} in a similar way, carrying out reasoning regardless of p, that is over a number field.

Finally, we emphasize that all the above arguments remain valid for an elliptic curve E_b over any finite field $\mathbb{F}_q$ of characteristic p such that $2, 3 \nmid \log_p(q)$ and $p \equiv 1 \pmod 3$. In turn, we do not expect significant obstacles to extend Theorem 1 if at least one of the last restrictions does not hold.

2 Simplified SWU hashing in constant time

We would like to explain how a simplified SWU hashing $h_{SWU}\colon \mathbb{A}^1 \dashrightarrow K'_b$ gives a (usual) hashing $h\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$, where $b \in \mathbb{F}_q^*$. In fact, any elliptic $\mathbb{F}_q$-curve of $j \neq 1728$ can be next considered instead of E_b. In practice, one almost always takes $q \equiv 3 \pmod 4$ (i.e., $\sqrt{-1} \notin \mathbb{F}_q$). Let $f_i := x_i^3 + b$ and $y := y_0 y_1$. Then the Kummer surface can be taken in the form $K'_b\colon y^2 = -f_0 f_1 \subset \mathbb{A}^3_{(x_0,x_1,y)}$. We denote by U and V respectively the domain of definition and the image for h_{SWU}. Also, let $\theta := f_0^{(q+1)/4}$. Consider the auxiliary map

$$h'\colon V(\mathbb{F}_q) \to E_b(\mathbb{F}_q), \qquad (x_0, x_1, y) \mapsto \begin{cases} (x_0, \theta) & \text{if} \quad \theta^2 = f_0, \\ (x_1, y/\theta) & \text{otherwise, i.e.,} \quad \theta^2 = -f_0. \end{cases}$$

Since

$$\theta^2 = f_0^{(q+1)/2} = f_0^{(q-1)/2} \cdot f_0 = \pm f_0,$$

this map is well defined everywhere on $V(\mathbb{F}_q)$. We can thus put

$$h := h' \circ h_{SWU}\colon U(\mathbb{F}_q) \to E_b(\mathbb{F}_q).$$

The set $\mathbb{F}_q \setminus U(\mathbb{F}_q)$ containing only $\mathbb{F}_q$-roots of the denominators of the functions $x_0(t)$, $x_1(t)$, $y(t)$ has insignificant cardinality ($\leqslant \deg(x_0) + \deg(x_1) + \deg(y) = 100$). Therefore, if necessary, the value of h on its elements can be specified manually.

We emphasize that in the definition of h' the Legendre symbol $\left(\frac{\cdot}{q}\right)$ (in other words, a quadratic residuosity test) in the field $\mathbb{F}_q$ does not appear. In turn, the element θ can be calculated without the inversion operation in $\mathbb{F}_q$ even if the function $x_0(t)$ is not polynomial (see [8, §4.2]). Therefore, by returning the value of h in (weighted) projective coordinates, we entirely avoid inversions. Thus the hashing h is *constant-time*, that is the computation time of its value is independent of an input argument.

The latter circumstance is considered a great advantage over the (universal) *SWU-hashing* [2, §8.3.4, §8.4.2], which, on the contrary, generally requires the computation of two Legendre symbols. The point is that time-constant implementations protect cryptographic protocols against timing attacks [2, §8.2.2, §12.1.1]. And the operations $\left(\frac{\gamma}{q}\right)$, γ^{-1} (for $\gamma \in \mathbb{F}_q^*$) are possible sources of such attacks.

Note that computing the Legendre symbol in $\mathbb{F}_q$ is reduced to the same task in $\mathbb{F}_p$, using the obvious equality $\left(\frac{\gamma}{q}\right) = \left(\frac{\mathrm{N}(\gamma)}{p}\right)$, where $\mathrm{N}(\gamma)$ is the norm of γ with respect to the extension $\mathbb{F}_q/\mathbb{F}_p$. There are two common methods for computing the Legendre symbol in $\mathbb{F}_p$. One uses Euler's criterion $\left(\frac{\gamma}{p}\right) = \gamma^{(p-1)/2}$ (for $\gamma \in \mathbb{F}_p^*$), but requires the very inefficient exponentiation operation in $\mathbb{F}_p$. The second is based on Gauss's quadratic reciprocity law $\left(\frac{\gamma}{\delta}\right)\left(\frac{\delta}{\gamma}\right) = (-1)^{(\gamma-1)(\delta-1)/4}$ for the Jacobi symbol (with odd $\gamma, \delta \in \mathbb{Z}$). This method is much more efficient, but difficult to implement in constant time. Identical conclusions are also made in [2, §2.2.9, §8.4.2].

In fact, the hashing $h\colon \mathbb{F}_q \to E_a(\mathbb{F}_q)$, proposed in [3, §4], to an elliptic $\mathbb{F}_q$-curve $E_a\colon y^2 = x^3 - ax$ (where $\sqrt{a} \notin \mathbb{F}_q$) of j-invariant 1728 can also be made constant-time. Let $q \equiv 1 \pmod 4$ (or, equivalently, $i := \sqrt{-1} \in \mathbb{F}_q$) and $q \not\equiv 1 \pmod 8$. In other words, $q \equiv 5 \pmod 8$. The first condition is necessary for the curve E_a to be ordinary. And second is sufficient to implement the square root extraction in $\mathbb{F}_q$ by means of one exponentiation in $\mathbb{F}_q$. As it is easy to see, under the given conditions we have $\sqrt{i} \notin \mathbb{F}_q$.

Let $h_{SWU}\colon \mathbb{A}^1 \dashrightarrow K'_a$ be the simplified SWU hashing built in [3, §3.1]. We will assume that the Kummer surface is given in the form $K'_a\colon y^2 = if_0f_1 \subset \mathbb{A}^3_{(x_0,x_1,y)}$, where $f_i = x_i^3 - ax_i$. As above, U and V are respectively the domain of definition and the image for h_{SWU}. Also, let $\theta := f_0^{(q+3)/8}$. Consider the auxiliary map

$$h'\colon V(\mathbb{F}_q) \to E_a(\mathbb{F}_q), \qquad (x_0, x_1, y) \mapsto \begin{cases} \big(x_0, \theta\big) & \text{if} & \theta^2 = f_0, \\ \big(x_0, i\theta\big) & \text{if} & \theta^2 = -f_0, \\ \big(x_1, y/\theta\big) & \text{if} & \theta^2 = if_0, \\ \big(x_1, y/(i\theta)\big) & \text{otherwise, i.e.,} & \theta^2 = -if_0. \end{cases}$$

Since

$$\theta^2 = f_0^{(q+3)/4} = f_0^{(q-1)/4} \cdot f_0 \ \in \ \{\pm f_0, \pm if_0\},$$

this map is well defined everywhere on $V(\mathbb{F}_q)$. Thus

$$h = h' \circ h_{SWU}\colon U(\mathbb{F}_q) \to E_a(\mathbb{F}_q).$$

As before, the set $\mathbb{F}_q \setminus U(\mathbb{F}_q)$ can be processed separately.

Acknowledgements. The author expresses his deep gratitude to his scientific advisor M. Tsfasman.

References

[1] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, **106**, Springer, New York, 2009.

[2] N. El Mrabet, M. Joye, *Guide to Pairing-Based Cryptography*, Cryptography and Network Security Series, Chapman and Hall/CRC, New York, 2016.

[3] D. Koshelev, *Hashing to elliptic curves of j-invariant* 1728, eprint IACR 2019/1294, 2019.

[4] J. Sendra, F. Winkler, S. Pérez-Díaz, *Rational Algebraic Curves: A Computer Algebra Approach*, Algorithms and Computation in Mathematics, **22**, Springer, Berlin, 2008.

[5] D. Koshelev, *Hashing to elliptic curves of $j = 0$ and Mordell–Weil groups*, arXiv:2005.08336, 2020.

[6] L. De Feo, *Mathematics of isogeny based cryptography*, arXiv:1711.04062, 2017.

[7] Y. Bilu, F. Luca, A. Pizarro-Madariaga, "Rational products of singular moduli", *Journal of Number Theory*, **158** (2016), 397–410.

[8] R. Wahby, D. Boneh, "Fast and simple constant-time hashing to the BLS12-381 elliptic curve", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, **2019(4)**, 154–179.

[9] M. Naehrig, R. Niederhagen, P. Schwabe, "New software speed records for cryptographic pairings", Latincrypt 2010, Security and Cryptology, **6212**, ed. M. Abdalla, P. Barreto, Springer, Puebla, Mexico, 2010, 109–123.

[10] FIDO Alliance, *FIDO ECDAA Algorithm*, 2018.

[11] ISO/IEC, *Cryptographic techniques based on elliptic curves (ISO/IEC 15946)*, 2017.

[12] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, **151**, Springer, New York, 1994.

[13] J. Jones, J. Cremona, *Global minimal model*, https://www.lmfdb.org/knowledge/show/ec.global_minimal_model, 2018.

[14] D. Koshelev, *Magma code*, https://github.com/dishport/Efficient-constant-time-hashing-to-some-elliptic-curves-of-j-invariant-0, 2020.