Hashing to elliptic curves over highly 2-adic fields $\mathbb{F}_q$ with $O(\log(q))$ operations in $\mathbb{F}_q$

Dmitrii Koshelev[0000−0002−4796−8989]

Parallel Computation Laboratory, École Normale Supérieure de Lyon, France
http://www.ens-lyon.fr/en/
dimitri.koshelev@gmail.com

Abstract. The current article provides a new deterministic hash function $\mathcal{H}$ to almost any elliptic curve E over a finite field $\mathbb{F}_q$, having an $\mathbb{F}_q$-isogeny of degree 3. Since $\mathcal{H}$ just has to compute a certain Lucas sequence element, its complexity always equals $O(\log(q))$ operations in $\mathbb{F}_q$ with a small constant hidden in O. In comparison, whenever $q \equiv 1 \pmod 3$, almost all previous hash functions need to extract at least one square root in $\mathbb{F}_q$. Over the field $\mathbb{F}_q$ of 2-adicity ν this amounts to $O(\log(q) + \nu^2)$ operations in $\mathbb{F}_q$ for the Tonelli–Shanks algorithm and $O(\log(q) + \nu^{3/2})$ ones for the recent Sarkar algorithm. A detailed analysis shows that $\mathcal{H}$ is several times faster than earlier state-of-the-art hash functions to the curve NIST P-224 (for which $\nu = 96$) from the American standard NIST SP 800-186.

Keywords: automorphism groups and twists · cubic polynomials · exceptional covers · genus 2 curves · hashing to elliptic curves · highly 2-adic fields · Lucas sequences

1 Introduction

Elliptic cryptography can be roughly divided into two types: discrete logarithm cryptography and isogeny-based one. At the moment, the main attention of the academic community is riveted to the second type, because it provides post-quantum protection. Nevertheless, the traditional cryptography is still actively used in the real world, for example in cryptocurrencies. In this regard, it is puzzling why the number of articles on elliptic cryptography in top journals and conferences is disproportionately less than twenty years ago. This is partly due to the fact that the pre-quantum cryptography has already been studied in detail, so it is probably difficult to make any significant scientific contribution.

In recent years, the author and some other researchers have made progress (see, e.g., [33, Tables 1, 2]) in constructing novel efficient hash functions to elliptic curves E over finite fields $\mathbb{F}_q$. Today, it can be undeniably said that the theory of such hash functions has become an independent, rapidly developing subarea of elliptic cryptography. This claim is particularly confirmed by the draft [16], being regularly updated, and by Chávez-Saab et al.'s article [13], which was recognized as one of the three best papers at Asiacrypt 2022. Thus, the given topic is one of the few that contribute to the development of the classical cryptography.

Chávez-Saab et al. obtain an indifferentiable hash function called *SwiftEC* to most elliptic curves used in practice. It requires to compute a square root in $\mathbb{F}_q$ and two Legendre symbols $\left(\frac{\cdot}{q}\right)$. Similarly to the inverse operation in $\mathbb{F}_q$ (see [6,40]), there are constant-time algorithms [20,41] of determining $\left(\frac{\cdot}{q}\right)$ whose performance does not exceed several field multiplications. Therefore, extracting $\sqrt{\cdot}$ is the only bottleneck of SwiftEC as well as of most hash functions to E.

Let $q - 1 = 2^\nu m$, where ν, $m \in \mathbb{N}$ and $2 \nmid m$. The value ν is said to be 2-*adicity* of the field $\mathbb{F}_q$. If ν is pretty small, then $\sqrt{\cdot}$ is either expressed via one-two exponentiations in $\mathbb{F}_q$ or found by the classical Tonelli–Shanks algorithm. Otherwise, Müller's refinement [38] of the old Cipolla–Lehmer method is more preferrable in a non-cryptographic context, because it is no more laborious than two exponentiations in $\mathbb{F}_q$. In particular, its running time is independent of ν. Unfortunately, the *Cipolla–Lehmer–Müller method* is not deterministic, hence it is vulnerable to timing attacks. As a result, most hash functions to elliptic curves (including SwiftEC) do not work in a constant linear time $O(\log(q))$ as $\nu \to +\infty$.

As we see, hashing to E for large ν is a much harder operation than a general scalar multiplication $[\cdot]$ on E, which earlier seemed the unique bottleneck in non-pairing-based protocols. At the same time, a lot of modern curves are actually defined over highly 2-adic fields (see, e.g., [1]). This allows to apply the fast Fourier transform (FFT) to speed up the arithmetic of polynomials over $\mathbb{F}_q$. The given acceleration has become in demand more and more due to the emergence of advanced protocols such as zero-knowledge proofs. On the one hand, the novel ECFFT (elliptic curve FFT) technique [2] is slower than the original FFT. On the other hand, the discrete logarithm problem (DLP) on elliptic curves over highly 2-adic fields is still recognized as intractable despite an attack attempt made in [39].

Whenever $q \equiv 2 \pmod 3$, we can utilize *Icart's encoding* [25], which extracts a (unique) cubic root in $\mathbb{F}_q$ instead of a square one. The solution of Icart is thereby optimal for the given case. Nevertheless, the opposite case $q \equiv 1 \pmod 3$ arises quite often in practice. For instance, this is known to be a necessary condition for the ordinariness of curves $E_b\colon y^2 = x^3 + b$ of j-invariant 0. Therefore, Icart's function is absolutely useless for them. Meanwhile, ordinary (a.k.a non-supersingular) curves E_b are very attractive, especially in pairing-based cryptography, because they (and only they) enjoy order 6 automorphisms and degree 6 twists. This positively influences on efficiency of diverse operations on E_b.

The work [30] succeeds in obtaining an indifferentiable hash function to E_b provided that $\sqrt{b} \in \mathbb{F}_q$ and hence $3 \mid \#E_b(\mathbb{F}_q)$. Surprisingly, it equally extracts $\sqrt[3]{\cdot}$, but in the desired case $q \equiv 1 \pmod 3$. Since highly 3-adic fields are not so popular in practice as their 2-adic counterparts, the new hash function costs one exponentiation in $\mathbb{F}_q$ at least for $q \not\equiv 1 \pmod{27}$. The order 3 automorphism $[\omega](x, y) := (\omega x, y)$ on E_b, where $\omega := \sqrt[3]{1} \neq 1$, underlies the established result. Unfortunately, the other elliptic curves do not possess a non-trivial automorphism of odd order. Consequently, the result cannot be generalized, staying within elliptic curves.

More concretely, Icart's idea consists in constructing (by elementary reasoning) a cyclic trigonal $\mathbb{F}_q$-curve $T: y^3 = f(x)$ and an $\mathbb{F}_q$-cover $\varphi: T \to E$. By the way, for the general E the curve T is of geometric genus 7 and the cover φ is of degree 4. Note that T has the automorphism $[\omega]$ as well as E_b. When $q \equiv 2 \pmod 3$, the projection $pr_x: T \to \mathbb{P}^1$ to the x-coordinate is an instance of a so-called *exceptional cover* in the sense of [17]. By definition, the restriction $pr_x: T(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ is bijective and hence $\#T(\mathbb{F}_q) = q + 1$. Eventually, Icart's encoding is nothing but the composition $\varphi \circ pr_x^{-1}: \mathbb{F}_q \to E(\mathbb{F}_q)$. It is useful to remember that $\mathbb{F}_q(\sqrt{-3}) = \mathbb{F}_q(\omega)$ and the discriminant of the cubic polynomial $y^3 - f(x)$ (in the variable y) equals $-3(12f(x))^2$.

Kammerer et al. demonstrate in [28, Section 3.1] that for the role of T and φ it is sufficient to take a genus 2 curve (of the same shape $y^3 = f(x)$) and a degree 2 cover if E is a Hessian curve. Since their article was written after Icart and has the same restriction $q \equiv 2 \pmod 3$, it is not of great interest in the author's opinion. According to the famous classification (see, e.g., [24, Sections 1.82.1-2]), a general member of Kammerer et al.'s family has the geometric automorphism group $\mathrm{Aut}(\overline{T}) \simeq \mathrm{D}_{12}$, i.e., the dihedral group of order 12. Moreover, $[\omega]$ does not belong to the $\mathbb{F}_q$-automorphism group $\mathrm{Aut}(T)$ or, equivalently, $3 \nmid \#\mathrm{Aut}(T)$.

In [46] encodings to E obtained from exceptional covers to $\mathbb{P}^1$ are called *Icart-like*. As shown in that article, for ordinary curves E such encodings cannot be surjective. At the same time, the DLP on supersingular curves is known to be weaker. To the author's knowledge, all previous Icart-like encodings are based on the exceptional projection $pr_x: S \to \mathbb{P}^1$ (of degree d) from a superelliptic curve $S: y^d = f(x)$. By assumption, $q \not\equiv 0, 1 \pmod d$. Surprisingly, beyond $d = 3$ the only known example (with $d = 7$) is represented in [33, Section 2.2]. However, it is available exclusively for the curve of j-invariant $-3^3 5^3$, that is, with the complex multiplication (CM) discriminant -7.

There is also in [31] a cute encoding for $d = 2$, where $h: \mathbb{P}^1(\mathbb{F}_q) \to S(\mathbb{F}_q)$ is a bijective map whose inverse map coincides with pr_x "by half". From the formal point of view, the given encoding is not Icart-like, because pr_x is obviously not bijective for all odd q. Anyway, since h needs to compute a square root in $\mathbb{F}_q$, it is not suitable for highly 2-adic fields.

The associated function field extension $\mathbb{F}_q(S)/\mathbb{F}_q(x)$, generated by $y = \sqrt[d]{f(x)}$, is clearly not Galois (i.e., not normal) whenever $q \not\equiv 0, 1 \pmod d$. The current article proposes to use an exceptional cover $\psi: H \to \mathbb{P}^1$ of another type. More precisely, $\mathbb{F}_q(H) \simeq \mathbb{F}_q(t)[x]/\widehat{\rho}$, where $\widehat{\rho}(x) = x^3 + \widehat{\rho}_1 x + \widehat{\rho}_0$ is a certain cubic (irreducible) polynomial. Its discriminant $\Delta(t) = vD(t)^2$ for some quadratic non-residue $v \in \mathbb{F}_q^*$ and function $D(t) \in \mathbb{F}_q(t)$. The situation resembles the case $d = 3$ and $q \equiv 2 \pmod 3$. We conclude (see, e.g., [26, Section 2]) that the Galois group of $\widehat{\rho}$ is the symmetric one S_3 and hence $\mathbb{F}_q(H)/\mathbb{F}_q(t)$ is equally not Galois even for $q \equiv 1 \pmod 3$. Consequently, the given extension is not Kummer, that is, it cannot be generated by a cubic root.

We will generalize *Kammerer et al.'s encoding* to the case $q \equiv 1 \pmod 3$. For this purpose, it is suggested to take a quadratic twist H of T with the property $3 \nmid \#\mathrm{Aut}(H)$. As a result, there is on H an order 3 automorphism σ whose Frobenius conjugate coincides with $\sigma^2 = \sigma^{-1}$. Meanwhile, the quotient map $\psi\colon H \to C := H/\langle\sigma\rangle$ is still defined over $\mathbb{F}_q$, because the group $\langle\sigma\rangle$ is Frobenius invariant. Besides, C obviously remains a rational curve parametrizable over $\mathbb{F}_q$. Finally, since the identity map is the only $\mathbb{F}_q$-map in $\langle\sigma\rangle$, the cover ψ is an exceptional one to $\mathbb{P}^1$ (up to an $\mathbb{F}_q$-isomorphism).

In order to be relevant to elliptic cryptography the Jacobian of H has to be $\mathbb{F}_q$-split. By virtue of [19, Lemma 3], this is in particular true when the Klein four-group $(\mathbb{Z}/2)^2 \hookrightarrow \mathrm{Aut}(H)$. Indeed, if so, then there are on H two non-hyperelliptic $\mathbb{F}_q$-involutions $\tau_\pm$ whose composition $\tau_+ \circ \tau_- = \tau_- \circ \tau_+$ is the hyperelliptic one. Therefore, we have the two complementary quadratic $\mathbb{F}_q$-covers $\varphi_\pm\colon H \to E_\pm$ to the elliptic curves $E_\pm := H/\tau_\pm$. It turns out that the curve $E_\pm$ is 3-isogenous over $\mathbb{F}_q$ to the quadratic twist $E_\mp^T$ of $E_\mp$.

Furthermore, we will prove that for almost any elliptic $\mathbb{F}_q$-curve E, having an $\mathbb{F}_q$-isogeny of degree 3, there is a genus 2 curve H such that $\mathrm{Aut}(\overline{H}) \simeq \mathrm{D}_{12}$ and $\mathrm{Aut}(H) \simeq (\mathbb{Z}/2)^2$ and E is $\mathbb{F}_q$-isomorphic to E_+ or E_+^T (alternatively, E_- or E_-^T). For instance, most twisted Hessian curves [5] are appropriate, since they have an $\mathbb{F}_q$-point of order 3. Eventually, we will obtain an Icart-like function to E based on $\varphi_\pm \circ \psi^{-1}$. It is worth noting that generalizing similarly Icart's original encoding to the case $q \equiv 1 \pmod 3$ is more difficult, because twists of genus 7 curves are much less studied. However, this may help to cover remaining elliptic curves E.

Hashing to (elliptic) curves can be realized as a simplified version of hashing to isogeny graphs of (elliptic) curves. Unfortunately, at this stage in the development of mathematics, the latter problem is intractable (even for supersingular isogenies) as confirmed by the recent works [7,37].

As is known (see, e.g., [18, Sections 10.7-8]), a smooth projective $\mathbb{F}_q$-curve C of genus g is supersingular whenever all its first g Frobenius traces t_i are zero, that is, $\#C(\mathbb{F}_{q^i}) = q^i + 1$, where $1 \leqslant i \leqslant g$. Also, recall that any two supersingular curves of the same genus are isogenous at least geometrically. Therefore, one of the ways to construct a hash function to the isogeny graph of supersingular curves consists in parametrizing explicitly a certain family of them. In contrast to the case $g = 1$, there are a lot of rational curves in the moduli space of supersingular curves of $g = 2$ according to [29]. However, it is not clear how to parametrize them in large characteristics. Maybe in the future, breakthroughs in computational algebraic geometry will allow to find a desired parametrization.

Kammerer et al. and the author solve a similar simpler problem by providing one-parameter families of genus 2 curves with $t_1 = 0$ and diverse t_2. So, these curves are *"semi-supersingular"*, although in general they are not isogenous even geometrically. With this paper, the author wants to inspire isogenists to focus on hashing to elliptic curves in the hope that this will sooner or later help in hashing to isogeny graphs.

2 Explicit formulas

Throughout this section, facts and notions from [11] will be freely used unless otherwise indicated. As usual, $\mathbb{F}_q$ stands for a finite field of characteristic $p > 3$ and $\overline{\mathbb{F}_q}$ does for its algebraic closure. Given $u \in \mathbb{F}_q \setminus \{0, 4^{-1}\}$, consider the smooth genus 2 curve

$$H_u \colon y^2 = x^6 + x^3 + u.$$

In the case $u = -50^{-1}$, the curve is still smooth, namely a twist of the *Bolza curve* $B\colon y^2 = x^5 - x$. By the way, the twists of B are completely studied in [10]. For this curve (and only for it) $\mathrm{Aut}(\overline{B}) \simeq \widetilde{\mathrm{S}}_4 \simeq \mathrm{GL}_2(\mathbb{F}_3)$, the maximum possible automorphism group of genus 2 curves. Since the given case requires separate consideration, hereafter, $u \neq -50^{-1}$ to be definite.

Over $\overline{\mathbb{F}_q}$ the curve H_u has the dihedral automorphism group $\mathrm{Aut}(\overline{H_u}) \simeq \mathrm{D}_{12}$ of order 12. And conversely, every smooth genus 2 curve $H\colon y^2 = f(x)$ over $\mathbb{F}_q$ such that $\mathrm{Aut}(\overline{H}) \simeq \mathrm{D}_{12}$ is a twist of some unique $H_u/\mathbb{F}_q$. In other words, u is an absolute invariant of the given curve family. Recall that

$$\mathrm{D}_{12} = \langle U, V \mid U^2 = V^6 = 1, VU = UV^5 \rangle$$

as an abstract group. In particular, the hyperelliptic involution $(x, y) \mapsto (x, -y)$ on H corresponds to V^3. Denote by $\tau_\pm$ the non-hyperelliptic involutions on H corresponding to U, UV^3. As always, they give the quadratic covers $\varphi_\pm\colon H \to E_\pm$ to the elliptic curves $E_\pm := H/\tau_\pm$.

Up to an $\mathbb{F}_q$-isomorphism, H possesses the form $H_{u,v}\colon y^2 = f(x) := \sum_{i=0}^{6} f_i x^i$ with the coefficients

$$f_6 := 27(u + 2z), \qquad f_5 := -324sv, \qquad f_4 := 27(u - 10z)v, \qquad f_3 := 360sv^2,$$

$$f_2 := 9(u + 10z)v^2, \qquad f_1 := -36sv^3, \qquad f_0 := (u - 2z)v^3$$

for some s, $z \in \mathbb{F}_q$, and $v \in \mathbb{F}_q^*$ such that $3s^2v = u^3 - z^2$.

By virtue of [9, Section 2], the j-invariants of $E_\pm$ are equal to

$$j_\pm := j(E_\pm) = \frac{\pm 2^8 3^3 \alpha (2 \mp 5\alpha)^3}{(1 \mp 2\alpha)(1 \pm 2\alpha)^3}, \tag{1}$$

where $\alpha := \sqrt{u}$. Note that $j_\pm$ do not depend on the parameters s, z, and v. It is suggested to put $s = 0$ for the sake of simplicity. In particular, $\alpha = z/u \in \mathbb{F}_q$ up to a sign. In this case, H_u (or, equivalently, $H_{u,v}$) has exactly 6 twists according to [8, Proposition 13]. We will see that vanishing s will not lead to the loss of generality, because our final destination is the twists of $E_\pm$ and not those of H_u. From now on, $f_5 = f_3 = f_1 = 0$ and

$$f_6 = 27(1+2\alpha), \qquad f_4 = 27(1-10\alpha)v, \qquad f_2 = 9(1+10\alpha)v^2, \qquad f_0 = (1-2\alpha)v^3$$

up to the multiplication by u.

As is known, each ($\mathbb{F}_q$-)automorphism on an arbitrary genus 2 curve $H/\mathbb{F}_q$ (given by a hyperelliptic model) can be represented by the unique ($\mathbb{F}_q$-)matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{as follows:} \qquad (x,y) \mapsto \left(\frac{ax+b}{cx+d}, \frac{ad-bc}{(cx+d)^3} \cdot y \right).$$

In other words, there is a natural embedding $\mathrm{Aut}(\overline{H}) \hookrightarrow \mathrm{GL}_2(\overline{\mathbb{F}_q})$ of $\mathbb{F}_q$-modules.

In this notation, the order 3 automorphisms on $H_{u,v}$ are associated with the matrices

$$\sigma := \frac{1}{2} \begin{pmatrix} -1 & \sqrt{v} \\ \dfrac{-3}{\sqrt{v}} & -1 \end{pmatrix}, \qquad \sigma^2 = \sigma^{-1} = \frac{1}{2} \begin{pmatrix} -1 & -\sqrt{v} \\ \dfrac{3}{\sqrt{v}} & -1 \end{pmatrix}.$$

Among other things, σ (or, equivalently, σ^2) is not defined over $\mathbb{F}_q$ if and only if $\sqrt{v} \not\in \mathbb{F}_q$ as assumed henceforth. In this case, $H_{u,v}$ is a non-trivial quadratic twist of H_u and, at the same time, $H_{u,v}$ is the unique non-trivial hyperelliptic twist of $H_{u,1}$.

By abuse of notation, $H_{u,v}$ will be denoted just by H. Below, the author sometimes uses the computer algebra system Magma [32] to derive or verify the formulas. First, the quotient curve $C := H/\langle\sigma\rangle$ and map are represented in the following way:

$$C\colon y^2 = f_6x^2 + \frac{f_0}{v^2}, \qquad \psi\colon H \to C \qquad (x,y) \mapsto \left(\frac{x(x^2-v)}{9x^2-v}, \frac{y}{9x^2-v} \right).$$

The conic C does not seem to possess a visible point rationally expressed through α, v (and even ω). As a result, we need to introduce additional variables x_0, y_0 being the coordinates of a general point P_0 on C. Whenever the field $\mathbb{F}_q$ and the parameters α, v are fixed, we can readily find $P_0 \in C(\mathbb{F}_q)$ once and for all.

As usual, the projection from P_0 has the form

$$pr_{P_0}\colon C \to \mathbb{A}^1_t \qquad (x,y) \mapsto \frac{x-x_0}{y-y_0}.$$

Therefore, the composition

$$pr_{P_0} \circ \psi\colon H \to \mathbb{A}^1_t \qquad (x,y) \mapsto T(x,y) := \frac{x(x^2-v) - x_0(9x^2-v)}{y - y_0(9x^2-v)}$$

is of degree 3. Besides, $y = Y(x, T(x,y))$, where

$$Y(x,t) := \frac{x(x^2-v) + (ty_0 - x_0)(9x^2-v)}{t}.$$

Substituting $Y(x,t)$ instead of y in the equation of H, we obtain an reducible curve on $\mathbb{A}^2_{(x,t)}$. One of the irreducible components K (depending on t) has the defining polynomial $\rho(x) := \sum_{i=0}^{3} \rho_i x^i$ with the $\mathbb{F}_q[t]$-coefficients

$$\rho_3 := f_6t^2 - 1, \qquad \rho_2 := 9(f_6x_0t^2 - 2y_0t + x_0), \qquad \rho_1 := -v\rho_3, \qquad \rho_0 := -\frac{v\rho_2}{9}.$$

Also, there are the birational isomorphisms

$$\begin{aligned} \chi\colon H \to K \qquad & (x,y) \mapsto (x, T(x,y)),\\ \chi^{-1}\colon K \to H \qquad & (x,t) \mapsto (x, Y(x,t)). \end{aligned}$$

For the sake of convenience, put $d_i := \rho_i/\rho_3$. Let's get rid of x^2 in ρ by means of the map

$$\begin{aligned} \eta\colon K \to \widehat{K} \qquad & (x,t) \mapsto \Big(x + \frac{d_2}{3}, t\Big),\\ \eta^{-1}\colon \widehat{K} \to K \qquad & (x,t) \mapsto \Big(x - \frac{d_2}{3}, t\Big). \end{aligned} \tag{2}$$

Here, the curve $\widehat{K} \subset \mathbb{A}^2_{(x,t)}$ is defined by the polynomial $\widehat{\rho}(x) := x^3 + \widehat{\rho}_1 x + \widehat{\rho}_0$ with the $\mathbb{F}_q(t)$-coefficients

$$\widehat{\rho}_1 := d_1 - \frac{d_2^2}{3}, \qquad \widehat{\rho}_0 := d_0 - \frac{d_1 d_2}{3} + \frac{2d_2^3}{27}. \tag{3}$$

For compactness, the argument t is omitted in the notation of the rational functions ρ_i, d_i, and $\widehat{\rho}_i$. Trivially, the latter have poles exactly at the roots of the polynomial ρ_3, i.e., at $\pm 1/\sqrt{f_6}$.

Magma says that the discriminant of $\widehat{\rho}$ equals

$$\varDelta(t) = -16\big(4\widehat{\rho_1}^3 + 27\widehat{\rho_0}^2\big) = vD(t)^2,$$

where $D(t) := 8 \cdot num(t)/(v\rho_3)^2$ and

$$\begin{aligned} num(t) := {} & v^2 f_6^2(27x_0^2 + v)\cdot t^4 - 108v^2 f_6 x_0 y_0 \cdot t^3 + 2(81 f_6 v^2 x_0^2 + 54 f_0 - f_6 v^3)\cdot t^2 \\ & -108 v^2 x_0 y_0 \cdot t + v^2(27x_0^2 + v). \end{aligned}$$

As a result, $\sqrt{\varDelta(t)} \notin \mathbb{F}_q$ for each $t \in \mathbb{F}_q$ such that $num(t)$, $\rho_3(t) \neq 0$. As is well known, this means that $\widehat{\rho}$ has the unique $\mathbb{F}_q$-root $X(t)$ for such elements t.

Moreover, $X(t)$ is expressed through the n-th element of the *(full) Lucas sequence*

$$V_i(a,b) = V_i := aV_{i-1} - bV_{i-2}, \qquad V_0 := 2, \qquad V_1 := a$$

given a, $b \in \mathbb{F}_q$. Indeed, as said in [14, Theorem 2] (be careful, a, b are swapped),

$$X(t) = -c_1 V_n\big(-27\widehat{\rho_0}, -27\widehat{\rho_1}^3\big),$$

where

$$(n, c_1) := \begin{cases} \Big(\dfrac{q+2}{3},\ \dfrac{1}{9\widehat{\rho_1}}\Big) & \text{if} \quad q \equiv 1 \pmod 3,\\ \Big(\dfrac{q-2}{3},\ \widehat{\rho_1}\Big) & \text{if} \quad q \equiv 2 \pmod 3. \end{cases}$$

Thus, the projection $pr_t\colon \widehat{K} \to \mathbb{A}^1_t$ is an exceptional cover, because on $\mathbb{F}_q$-points it enjoys the inverse map

$$pr_t^{-1}\colon \mathbb{F}_q \to \widehat{K}(\mathbb{F}_q) \qquad t \mapsto \big(X(t), t\big).$$

Now, we come back to the involutions $\tau_\pm$. For $s = 0$ they take the elementary form

$$\tau_\pm\colon H \to H \qquad (x, y) \mapsto (-x, \pm y).$$

The corresponding quadratic covers

$$\begin{aligned} \varphi_+\colon H \to E_+ &\qquad (x, y) \mapsto (x^2, y), \\ \varphi_-\colon H \to E_- &\qquad (x, y) \mapsto \Big(\frac{1}{x^2}, \frac{y}{x^3}\Big) \end{aligned}$$

often occur in the literature. Here, the elliptic curves have the equations

$$E_\pm\colon y^2 = g_\pm(x) := \sum_{i=0}^{3} g_{\pm,i}\cdot x^i$$

with the coefficients $g_{+,i} := f_{2i}$ and $g_{-,i} := f_{6-2i}$.

As is customary, the leading coefficients can be eliminated as follows:

$$\zeta_\pm\colon E_\pm \to \widehat{E}_\pm \qquad (x, y) \mapsto (g_{\pm,3}\cdot x,\ g_{\pm,3}\cdot y),$$

thereby leading to the equations

$$\widehat{E}_\pm\colon y^2 = \widehat{g}_\pm(x) := x^3 + \sum_{i=0}^{2} \widehat{g}_{\pm,i}\cdot x^i$$

having the coefficients $\widehat{g}_{\pm,i} := g_{\pm,i}\cdot g_{\pm,3}^{2-i}$.

By analogy with the transformation (2), there are ones $\phi_\pm\colon \widehat{E}_\pm \to W_\pm$ to short Weierstrass forms

$$W_\pm\colon y^2 = h_\pm(x) := x^3 + h_{\pm,1}\cdot x + h_{\pm,0}$$

with the coefficients computable by the formulas (3). Let's shorten these coefficients by means of the auxiliary maps

$$\begin{aligned} \theta_+\colon W_+ \to \widehat{W}_+ &\qquad (x, y) \mapsto \Big(\frac{x}{6^2 v}, \frac{y}{6^3 v^2}\Big), \\ \theta_-\colon W_- \to \widehat{W}_- &\qquad (x, y) \mapsto \Big(\frac{x}{(2v)^2}, \frac{y}{(2v)^3}\Big). \end{aligned}$$

The resulting models

$$\widehat{W}_+\colon vy^2 = \widehat{h}_+(x) := x^3 + \widehat{h}_{+,1}x + \widehat{h}_{+,0}, \qquad \widehat{W}_-\colon y^2 = \widehat{h}_-(x) := x^3 + \widehat{h}_{-,1}x + \widehat{h}_{-,0}$$

possess the quite simple coefficients

$$\widehat{h}_{+,1} := 3(2-5\alpha)\alpha, \qquad \widehat{h}_{+,0} := -(1-14\alpha+22\alpha^2)\alpha,$$
$$\widehat{h}_{-,1} := -27(2+5\alpha)\alpha, \qquad \widehat{h}_{-,0} := 27(1+14\alpha+22\alpha^2)\alpha.$$

The discriminants of $\widehat{h}_\pm$ are equal to

$$\varDelta_+ = 2^4 3^3 (2\alpha-1)(2\alpha+1)^3\alpha^2, \qquad \varDelta_- = 2^4 3^9 (2\alpha-1)^3(2\alpha+1)\alpha^2,$$

respectively. Note that $\varDelta_\pm = 0$ if and only if $\alpha \in \{0, \pm 2^{-1}\}$. This is impossible by our assumption on u. Also, do not forget that $\alpha \neq \pm 1/(5\sqrt{-2})$ to bypass the Bolza curve.

The formulas of the compositions $\varphi'_\pm := \theta_\pm \circ \phi_\pm \circ \zeta_\pm \circ \varphi_\pm$ are fairly compact to be exhibited:

$$\varphi'_+ \colon H \to \widehat{W}_+ \qquad (x,y) \mapsto \left(\frac{3(1+2\alpha)x^2 + (1-10\alpha)v}{4v}, \frac{1+2\alpha}{8v^2}\cdot y \right),$$
$$\varphi'_- \colon H \to \widehat{W}_- \qquad (x,y) \mapsto \left(\frac{3(1+10\alpha)x^2 + (1-2\alpha)v}{4x^2}, \frac{1-2\alpha}{8x^3}\cdot y \right).$$

To sum up, we obtain the rational $\mathbb{F}_q$-maps

$$e_\pm := \varphi'_\pm \circ \chi^{-1} \circ \eta^{-1} \colon \ \widehat{K} \to \widehat{W}_\pm$$

and the associated encodings

$$e'_\pm := e_\pm \circ pr_t^{-1} \colon \ \mathbb{F}_q \to \widehat{W}_\pm(\mathbb{F}_q).$$

For readability, it is better to change the notation:

$$A := \widehat{h}_{+,1}, \qquad B := \widehat{h}_{+,0}, \qquad h(x) := \widehat{h}_+(x), \qquad W := \widehat{W}_+, \qquad W' := \widehat{W}_-,$$

because the further reasoning will be asymmetric. Denote by $W^T \colon y^2 = h(x)$ the unique non-trivial quadratic twist of W. The corresponding $\mathbb{F}_{q^2}$-isomorphism is obviously

$$\iota \colon W \to W^T \qquad (x,y) \mapsto (x, \sqrt{v}\cdot y).$$

The 3-division polynomial $\psi_3(x)$ of the curve W' has the root 9α. Consequently, there is the 3-isogeny

$$\delta \colon W' \to W^T \qquad (x,y) \mapsto \left(\frac{num_x(x)}{9(x-9\alpha)^2}, \frac{num_y(x)}{27(x-9\alpha)^3}\cdot y \right)$$

with the numerators

$$num_x(x) := x^3 - 18\alpha x^2 - 27(4-11\alpha)\alpha x + 108(1+5\alpha-14\alpha^2)\alpha,$$
$$num_y(x) := x^3 - 27\alpha x^2 + 27(4+\alpha)\alpha x - 27(8+4\alpha-13\alpha^2)\alpha.$$

It is notable that for $u \in \mathbb{F}_p$ and $q = p^2$ the curve W' (up to an $\mathbb{F}_q$-isomorphism) is the reduction to $\mathbb{F}_q$ of a so-called $\mathbb{Q}$-*curve of degree* 3 over the field $\mathbb{Q}(\sqrt{u'})$, where u' is a lift of u to $\mathbb{Q}$. Incidentally, $\mathbb{Q}$-curves also appear in [44] in the context of efficient scalar multiplication.

3 New hash function and its complexity

We will stick to the notation of the previous section. In addition, let $E\colon y^2 = g(x) := x^3 + ax + b$ be an ordinary elliptic $\mathbb{F}_q$-curve with the j-invariant j. Assume that E enjoys an $\mathbb{F}_q$-isogeny of degree 3 to some elliptic $\mathbb{F}_q$-curve E' of j-invariant j'. This is equivalent to the fact that the 3-division polynomial $\psi_3(x) = 3x^4 + 6ax^2 + 12bx - a^2$ of the curve E admits an $\mathbb{F}_q$-root x_1. If so, then the kernel of the isogeny is generated by the order 3 point (x_1, y_1), where $y_1 := \sqrt{g(x_1)} \in \mathbb{F}_{q^2}^*$. As usual, j' can be found by means of Vélu's formulas [18, Section 25.1.1].

As is known (see, e.g., [18, Section 25.2]), pairs of 3-isogenous (over $\overline{\mathbb{F}_q}$) j-invariants constitute a plane affine singular $\mathbb{F}_q$-curve M_3 given by the classical modular polynomial $\Phi_3(x,y)$. We do not use the traditional notation $Y_0(3)$, because it usually stands for the non-singular model of M_3, parametrizing 3-isogenies rather than just the pairs (j, j'). It is easy to check that the roots of $\Phi_3(y,y)$ are exactly

$$0, \qquad j_8 := 8000 = 2^6 5^3, \qquad j_{11} := -32768 = -2^{15}, \qquad j_{12} := 54000 = 2^4 3^3 5^3.$$

These j-invariants correspond to the CM discriminants $D_{\mathrm{CM}} = -3, -8, -11$, and -12, respectively. Moreover, 0, j_{12} are simple roots and j_8, j_{11} are of multiplicity 2.

The formulas (1) provide the rational $\mathbb{F}_q$-parametrization $par\colon \alpha \mapsto (j_+, j_-)$ of the curve M_3. By the way, in [36, Tables 4, 5] one can find a slightly simpler parametrization, but we are forced to work with par. The inverse map $\pi : M_3 \dashrightarrow \mathbb{A}^1_\alpha$ to par (as a birational map) is readily determined by Magma [32]. Furthermore, $\pi = par^{-1}$ (as a biregular map) outside the subsets $S_1 \subset \mathbb{A}^1_\alpha$ and $S_2 \subset M_3$ of the form

$$S_1 := par^{-1}(Sing) \cup \left\{\pm\frac{1}{2}\right\}, \qquad S_2 := Sing \cup \big\{(j_{12}, j_{12})\big\},$$

where $Sing$ is the set of all singular $\overline{\mathbb{F}_q}$-points on M_3. To be more concrete, $\#S_1 = 18$ and $\#S_2 = 9$. Among other things,

$$\frac{\pm 1}{5\sqrt{-2}} \in par^{-1}(Sing), \qquad (j_8, j_8), (j_{11}, j_{11}) \in Sing.$$

The CM discriminants of the remaining j-invariants from the set $pr_x(Sing)$ are precisely -20, -32, and -35.

Henceforth, it is supposed everywhere that $(j, j') \not\in S_2$ and so we deal with the $\mathbb{F}_q$-curve $W^T : y^2 = x^3 + Ax + B$ (with $j(W^T) = j_+ = j$) whose coefficients are instantiated by the value $\alpha = \pi(j, j') \in \mathbb{F}_q$. In particular, $j_+ = 0$ (i.e., $D_{\mathrm{CM}} = -3$) if and only if $\alpha \in \{0, 2/5\}$. In the present case, $\psi_3(x) = 3x(x^3 + 4b)$. Unlike $-\sqrt[3]{4b}$, the root $x_1 = 0$ (for which $y_1 = \pm\sqrt{b}$) generates an endomorphism on E or, equivalently, $j' = 0$. Thereby, it is easy to memorize that $\alpha = 0 \Leftrightarrow j = j' = 0 \Leftrightarrow x_1 = 0$. However, the zero α is not allowable in the previous section, hence it is more correct to reassign $S_1 := S_1 \cup \{0\}$ and $S_2 := S_2 \cup \{(0,0)\}$. In turn, the value $\alpha = 2/5$ does not contradict anything. It is also worth adding that $\Phi_3(0, y) = y(y + 2^{15}3{\cdot}5^3)^3$.

Besides, $j_+ = 1728$ (i.e., $D_{\mathrm{CM}} = -4$) if and only if $22\alpha^2 - 14\alpha + 1 = 0$, that is, $\alpha = (7 \pm 3\sqrt{3})/22$. Recall that $q \equiv 1 \pmod 4$ (i.e., $\sqrt{-1} \in \mathbb{F}_q$) is a necessary condition for 1728 to be an ordinary j-invariant. At the same time, the results of this article are relevant only for $q \equiv 1 \pmod 3$ (i.e., $\sqrt{-3} \in \mathbb{F}_q$). So, the mentioned values α always lie in $\mathbb{F}_q$ in our cryptographic context, although the curves $y^2 = x^3 + ax$ do not occur in real-world cryptography (especially over highly 2-adic fields). The polynomial $\Phi_3(1728, y) = Q(y)^2$, where $Q(y)$ is a certain quadratic $\mathbb{F}_q$-polynomial. Its discriminant is a quadratic residue in $\mathbb{F}_q$ if and only if so is 3, which is consistent with the fact that $\alpha \in \mathbb{F}_q$.

We need the additional value

$$\mathfrak{f} := \begin{cases} \dfrac{AB}{ab} & \text{if} \qquad ab \neq 0, \ \text{i.e.,} \ j \notin \{0, 1728\}, \\ \dfrac{A}{a} & \text{if} \qquad b = 0, \ \text{i.e.,} \ j = 1728, \\ \dfrac{B}{b} & \text{if} \qquad a = 0, \ \text{i.e.,} \ j = 0. \end{cases}$$

Let $d \in \{2, 4, 6\}$ be the order of the (cyclic) group $\mathrm{Aut}(E)$. From the general theory we know that the curves E, W^T are isomorphic precisely over the extension $\mathbb{F}_q(\sqrt[d]{\mathfrak{f}})/\mathbb{F}_q$ of degree $\leqslant d$. The corresponding isomorphism has the form

$$\gamma_-\colon W^T \to E \qquad (x, y) \mapsto \Big(\frac{x}{z^2}, \frac{y}{z^3}\Big),$$

where

$$z := \begin{cases} \dfrac{a\sqrt{\mathfrak{f}}}{A} = \dfrac{B}{b\sqrt{\mathfrak{f}}} & \text{if} \qquad j \notin \{0, 1728\}, \ \text{i.e.,} \ d = 2, \\ \sqrt[d]{\mathfrak{f}} & \text{otherwise.} \end{cases}$$

The next lemma seems folklore, but we prove it for lack of a reference.

Lemma 1. *Assume as above that $(j, j') \notin S_2$ or, alternatively, $\alpha \notin S_1$. It turns out that $\mathfrak{g} := \sqrt[d/2]{\mathfrak{f}} \in \mathbb{F}_q$. In other words, $W^T \simeq_{\mathbb{F}_q} E$ or $W \simeq_{\mathbb{F}_q} E$, depending on whether the condition $\sqrt{\mathfrak{g}} \in \mathbb{F}_q$ (i.e., $\sqrt[d]{\mathfrak{f}} \in \mathbb{F}_q$) is met or not, respectively. In the latter case, the composition $\gamma_+ := \gamma_- \circ \iota\colon W \to E$ is defined over $\mathbb{F}_q$.*

Proof. The lemma is trivial whenever $j \notin \{0, 1728\}$.

Consider the case $j = 0$. We need to show that W (equivalently, W^T) cannot be a higher degree twist of E. As well as E, the curve W has an $\mathbb{F}_q$-isogeny of degree 3 to a curve of non-zero j-invariant $j' = -2^{15}3{\cdot}5^3$. Unlike E and W, the curve E' has no higher degree twists. Therefore, W has to be $\mathbb{F}_q$-isogenous to E' (and so to E) or to its quadratic twist (and so to E^T). At the same time, the twists of E are pairwise non-isogenous over $\mathbb{F}_q$, since it is an ordinary curve. Thereby, if W was not $\mathbb{F}_{q^2}$-isomorphic to E, then we would come to a contradiction.

For the case $j = 1728$ the given argumentation does seem to work, because there are two possibilities for j'. Fortunately, there is another simple reasoning. Denote by t the $\mathbb{F}_q$-trace of E. As is well known, the Frobenius discriminant $t^2 - 4q = -4f^2$ for some $f \in \mathbb{N}$. Owing to [21, Proposition 8], the $\mathbb{F}_q$-trace of W equals $\pm 2f$ under the assumption that W is a higher degree twist of E (namely of degree 4). Meanwhile, according to [18, Theorem 25.4.6], the 3-isogenies from the curves E, W are necessarily vertical. This means that $3 \mid f$ (that is, $3 \mid t^2 - 4q$) and $3 \mid 4(f^2 - q)$ for the same reason. As a result, $3 \mid q$, which is prohibited in this article. □

From the previous section we have the encodings $e'_\pm : \mathbb{F}_q \to \widehat{W}_\pm(\mathbb{F}_q)$. Based on them, we come to the new one

$$e\colon \mathbb{F}_q \to E(\mathbb{F}_q) \qquad e := \begin{cases} \gamma_- \circ \delta \circ e'_- & \text{if} \quad \sqrt{\mathfrak{g}} \in \mathbb{F}_q, \\ \gamma_+ \circ e'_+ & \text{if} \quad \sqrt{\mathfrak{g}} \notin \mathbb{F}_q. \end{cases}$$

It is important to realize that e is not correctly defined at a few $t \in \mathbb{F}_q$. This happens when at least one of the denominators within the components of e is zero. Nonetheless, for a random element t the probability of the given event is negligible. And if desired, such degenerate cases can be easily processed.

Denote by $G \subset E(\mathbb{F}_q)$ a subgroup in which we consider the DLP. Let r be the (large prime) order of G and $h := \#E(\mathbb{F}_q)/r$ be the cofactor of G. The scalar multiplication $[h]\colon E(\mathbb{F}_q) \to G$ is said to be *clearing cofactor*. Let's also introduce the *tensor square*

$$e^{\otimes 2}\colon \mathbb{F}_q^2 \to E(\mathbb{F}_q) \qquad (t, t') \mapsto e(t) + e(t').$$

Below are some statistical notions, which are common in the current research area. They can be found, e.g., in [13,15], so all the details on this matter are omitted.

By analogy with [31, Corollary 1], the maps $e'_\pm$ are 2-*well-distributed*. Consequently, their tensor squares are *regular*. If $\sqrt{\mathfrak{g}} \in \mathbb{F}_q$ and $\ker(\delta) \subset W'(\mathbb{F}_q)$ (and so $3 \mid h$), then the 3-isogeny δ is far from surjective on the level of $\mathbb{F}_q$-points. In the present case, $e^{\otimes 2}$ is obviously not regular. However, we are in fact interested in the composition

$$[h] \circ e^{\otimes 2} = ([h] \circ e)^{\otimes 2}\colon\ \mathbb{F}_q^2 \to G,$$

which is in contrast regular. Besides, $[h] \circ e^{\otimes 2}$ is clearly *samplable* and hence it is *admissible*. Eventually, given an indifferentiable hash function $\mathcal{H}\colon \{0,1\}^* \to \mathbb{F}_q^2$, the composition $[h] \circ e^{\otimes 2} \circ \mathcal{H}\colon \{0,1\}^* \to G$ is also indifferentiable. In practice, one prefers to take for the role of $\mathcal{H}$ standard hash functions (e.g., SHA) rather than provable ones. Since the former manipulate bits instead of finite field elements, we can neglect their complexity.

Let $\ell := \lceil \log_2(q) \rceil$ and let $q - 1 = 2^\nu m$, where ν, $m \in \mathbb{N}$ and $2 \nmid m$. To be definite, we focus on the case $q \equiv 1 \pmod 3$ more interesting for us. We will also need the natural numbers

$$n := \frac{q+2}{3}, \qquad n - 1 = \frac{q-1}{3} = 2^\nu \frac{m}{3}, \qquad m' := \frac{m-1}{2}.$$

Below, $\omega(k)$ stands for the Hamming weight of a number $k \in \mathbb{N}$ in its binary representation. As should be clear,

$$\log_2(n) \approx \log_2(n-1) \approx \ell, \qquad \log_2(m) \approx \log_2(m') \approx \ell - \nu$$

as well as

$$\omega(n) \approx \omega(n-1), \qquad \omega(m) \approx \omega(m') \approx \omega(q).$$

For simplicity, we will not distinguish squarings and general multiplications in $\mathbb{F}_q$. Evaluating each component in the definition of e costs at most several multiplications. So, the bottleneck of the new encoding is computing the n-th member of the Lucas sequence V_i. There is the (deterministic) *Joye–Quisquater algorithm* [27] slightly improved by Koval [34]. In addition to V_n, the given algorithm determines the n-th member of the sister (full) Lucas sequence

$$U_i(a,b) = U_i := aU_{i-1} - bU_{i-2}, \qquad U_0 := 0, \qquad U_1 := 1.$$

Since it is not very famous, it is reasonable to write out Algorithm 1 and to check it in Magma [32].

The value U_n is unnecessary for us and computing V_n does not depend on U_i in the algorithm. Thereby, we could exclude from it all the lines containing U_i. After doing that, the complexity of the algorithm becomes $\approx 4\ell + \omega(n)$ field multiplications. The number n is odd, hence the second (simplified) loop **for** is not executed. Alternatively, the 2-adic valuation of $n-1$ is equal to ν. At the same time,

$$V_n = \frac{aV_{n-1} + (a^2 - 4b)U_{n-1}}{2}$$

as follows from [45, Equality (3.8)]. So, it is suggested to first compute U_{n-1}, V_{n-1} and then V_n. This approach costs $\approx \mathrm{JQK} := 4\ell + \omega(n) - \nu$ multiplications in $\mathbb{F}_q$ and hence it is a little quicker than the previous one.

It is worth emphasizing that the non-full Lucas sequence $V_i(a,1)$ (for some $a \in \mathbb{F}_q$) underlies Müller's square root method. There is faster *Postl's algorithm* [42] of finding its members in comparison with $V_i(a,b)$ for an arbitrary $b \in \mathbb{F}_q$. That is why the given paper would be meaningless if Müller's method was deterministic.

As said in the introduction, the bottleneck of SwiftEC is one square root in $\mathbb{F}_q$. The constant-time Tonelli–Shanks algorithm of extracting $\sqrt{\cdot}$ is represented in [16, Appendix I.4]. In two words, the algorithm consists of the exponentiation to m' and a double loop. It is readily checked that the overall complexity equals $\approx \mathrm{TS} := \ell + \omega(q) + \nu(\nu+1)/2$ multiplications in $\mathbb{F}_q$. Eventually, putting $c := \omega(q) - \omega(n) - 3\ell$, we conclude that

$$\mathrm{TS} - \mathrm{JQK} \;=\; \frac{\nu(\nu+3)}{2} + c > 0 \qquad \Leftrightarrow \qquad \nu > \frac{-3 + \sqrt{9 - 8c}}{2}. \tag{4}$$

Table 1 exhibits some real-world elliptic curves for which the new encoding e (and hence $e^{\otimes 2}$) is relevant. By coincidence, all of them are of prime order r (i.e.,

Algorithm 1: The Joye–Quisquater–Koval algorithm of computing simultaneously the n-th members of the sister Lucas sequences

```
Data: $n = 2^{\nu} \cdot \sum_{i=\nu}^{\ell-1} n_i 2^{i-\nu} \in \mathbb{N}$, where $n_{\nu} = 1$, as well as $a$, $b \in \mathbb{F}_q$.
Result: $U_n(a,b)$, $V_n(a,b)$.
begin
    $V_l := 2$;
    $V_h := a$;
    $Q_l := 1$;
    $Q_h := 1$;
    for $i := \ell - 1$ downto $\nu$ do
        $Q_l := Q_l * Q_h$;
        if $n_i = 1$ then
            $Q_h := b * Q_l$;
            $V_l := V_h * V_l - a * Q_l$;
            $V_h := V_h^{\wedge}2 - 2 * Q_h$
        else
            $Q_h := Q_l$;
            $V_h := V_h * V_l - a * Q_l$;
            $V_l := V_l^{\wedge}2 - 2 * Q_l$
        end
    end
    $Q_l := Q_l * Q_h$;
    $D := a^{\wedge}2 - 4 * b$;
    $U_h := (2 * V_h - a * V_l)/D$;
    for $i := 1$ to $\nu$ do
        $U_h := U_h * V_l$;
        $V_l := V_l^{\wedge}2 - 2 * Q_l$;
        $Q_l := Q_l^{\wedge}2$
    end
    return $U_h$, $V_l$.
end
```

$h = 1$), but this property was non-essential in the choice of the curves. More importantly, they are defined over finite fields $\mathbb{F}_q$ of various 2-adicity, respecting the principal condition $q \equiv 1 \pmod 3$. In fact, as is customary in cryptography, the fields are also prime, that is, q is equal to the characteristic p.

SwiftEC is not applicable to the curve NIST P-224 from the standard NIST SP 800-186, namely from [12, Section 4.2.1.2]. Indeed, it is easily checked that the condition 3 of [13, Theorem 3] is not met. As a result, before this article, the state-of-the-art admissible map to the given curve was the tensor square $e_{sSWU}^{\otimes 2}$ of the so-called *simplified SWU encoding* e_{sSWU} (see, e.g., [47, Section 2.4]). Recall that e_{sSWU} (resp., $e_{sSWU}^{\otimes 2}$) needs to extract one (resp., two) square roots in $\mathbb{F}_q$. Meanwhile, $\nu = 96$ for the base field of NIST P-224 and, as far as the author knows, this is the largest 2-adicity occurring anywhere in practice today.

The remaining four curves from the table are of j-invariant 0. They are divided into two *cycles* of length 2. Put another way, we deal with two pairs of curves $E_1/\mathbb{F}_q$ and $E_2/\mathbb{F}_r$ such that $r := \#E_1(\mathbb{F}_q)$ and $q = \#E_2(\mathbb{F}_r)$. As the name indicates, the hybrid cycle of *BN382-Plain curves* [1, Section 5.4] consists of a Barreto–Naehrig curve and a non-pairing-friendly one. In turn, the second cycle is composed of two non-pairing-friendly curves called *Pasta (Pallas-Vesta) curves.*

The latter curves were generated, taking into account the indirect hashing approach of Wahby–Boneh [47]. On the Internet page [22] it is written: *"both Pallas and Vesta have low-degree isogenies* (*both of degree* 3) *from curves with a nonzero j-invariant. This is useful when hashing to the curve using the "simplified SWU" algorithm, and perhaps for other not-yet-known purposes".* The same motivation exists for the hybrid *cycle Pluto-Eris* [23]. SwiftEC is applied to all curves of j-invariant 0, hence the composition of e_{sSWU} (or $e_{sSWU}^{\otimes 2}$) with isogenies is now an obsolete solution. Nonetheless, the result of this article qualifies for "other not-yet-known purpose".

As seen from the last line of the table, e (resp., $e^{\otimes 2}$) performs approximately 4144 (resp., 8288) fewer multiplications than e_{sSWU} (resp., $e_{sSWU}^{\otimes 2}$). Without doubt, this is a substantial acceleration, especially for NIST P-224. The point is that this curve has the 112-bit security level, which is smaller than the standard 128-bit one. So, the given curve is chosen for cryptographic environments in which a part of the security is sacrificed for the sake of performance. In other words, the last indicator is the most significant in such environments. At one time, Bernstein [4] (cf. [35]) made a low-level implementation of NIST P-224, benefiting (among other things) from the large 2-adicity of $\mathbb{F}_q$.

In turn, for BN382-Plain curves, unlike $e^{\otimes 2}$, the encoding e itself is more efficient with respect to SwiftEC. To be more precise, e performs ≈ 1212 fewer multiplications. In some applications the behavior of a hash function to E as a random oracle is unnecessary, hence the function e is sufficient. Finally, in the case of Pasta curves, SwiftEC is even better than e, not to mention $e^{\otimes 2}$.

Curve	Reference	D_{CM}	ℓ	ν	$\omega(q)$	$\omega(n)$	TS	2·TS	JQK	2·JQK
Pallas	[22]	-3	254	32	47	107	829	1658	1091	2182
Vesta					44	113	826	1652	1097	2194
BN382	[1, Section 5.4]		382	67	107	92	2767	5534	1553	3106
Plain					109	99	2769	5538	1560	3120
NIST P-224	[12, Section 4.2.1.2]	$\approx -2^{222.5}$	224	96	129	65	5009	10018	865	1730

Table 1. Some popular elliptic curves (suitable for the new hash function) over highly 2-adic (prime) fields $\mathbb{F}_q$ such that $q \equiv 1 \pmod 3$ as well as the approximate number of multiplications in $\mathbb{F}_q$ of the constant-time Tonelli–Shanks algorithm and of the Joye et al. algorithm 1. The entries are verified in Magma [32].

4 Conclusion

A constant-time version of the recent *Sarkar algorithm* [43] probably improves upon that of the Tonelli–Shanks algorithm. Given this circumstance, further research is needed to establish the exact lower bound on ν like (4). This is problematic to do in this article, because the scientific community has not yet sufficiently explored the actual running time of the new square-root algorithm or of its potential modifications.

The same can be said about computing the full Lucas sequence $V_i(a, b)$, because the attention of researchers has been focused much more on extracting roots $\sqrt[d]{\cdot}$ (especially on $\sqrt{\cdot}$). It is likely that in the near future a new method will be proposed with a smaller constant in $O(\log(q))$. The given article can serve as an additional motivation for this.

In any case, the Sarkar algorithm has a worse asymptotic behaviour as $\nu \to +\infty$ than the Joye et al. algorithm 1. Perhaps, elliptic curves of the next generation will be soon generated over fields of 2-adicity $\nu > 96$. As said in [1, Section 1], larger values of ν allow *"to prove deeper arithmetic circuits*".

Finally, it is worth mentioning Bernstein [3] and Sarkar's table look-up based variants of the square-root algorithms. They have smaller complexity at the price of an exponentiational growth of required memory. In the context of hashing to elliptic curves this is an essential obstacle, because elliptic cryptography is often implemented on tiny devices with limited amount of memory.

Acknowledgements. The author expresses his gratitude to Damien Stehlé for hiring him as a postdoc at École Normale Supérieure de Lyon.

References

1. Aranha, D.F., El Housni, Y., Guillevic, A.: A survey of elliptic curves for proof systems. Designs, Codes and Cryptography (2022), `https://link.springer.com/article/10.1007/s10623-022-01135-y`

2. Ben-Sasson, E., Carmon, D., Kopparty, S., Levit, D.: Elliptic curve fast Fourier transform (ECFFT) Part I: Low-degree extension in time $O(n \log n)$ over all finite fields. In: Bansal, N., Nagarajan, V. (eds.) ACM-SIAM Symposium on Discrete Algorithms (SODA 2023). pp. 700–737. Society for Industrial and Applied Mathematics, Philadelphia, Pennsylvania (2023)
3. Bernstein, D.J.: Faster square roots in annoying finite fields (2001), `https://cr.yp.to/papers.html#sqroot`
4. Bernstein, D.J.: nistp224 (2001), `https://cr.yp.to/nistp224.html`
5. Bernstein, D.J., Chuengsatiansup, C., Kohel, D., Lange, T.: Twisted Hessian curves. In: Lauter, K., Rodríguez-Henríquez, F. (eds.) Progress in Cryptology – LATINCRYPT 2015. Lecture Notes in Computer Science, vol. 9230, pp. 269–294. Springer, Cham (2015)
6. Bernstein, D.J., Yang, B.Y.: Fast constant-time GCD computation and modular inversion. IACR Transactions on Cryptographic Hardware and Embedded Systems **2019**(3), 340–398 (2019)
7. Booher, J., Bowden, R., Doliskani, J., Fouotsa, T.B., Galbraith, S.D., et al.: Failing to hash into supersingular isogeny graphs (2022), `https://eprint.iacr.org/2022/518`
8. Cardona, G.: On the number of curves of genus 2 over a finite field. Finite Fields and Their Applications **9**(4), 505–526 (2003)
9. Cardona, G.: $\mathbb{Q}$-curves and abelian varieties of GL_2-type from dihedral genus 2 curves. In: Cremona, J.E., Lario, J.C., Quer, J., Ribet, K.A. (eds.) Modular Curves and Abelian Varieties. Progress in Mathematics, vol. 224, pp. 45–52. Birkhäuser, Basel (2004)
10. Cardona, G.: Representations of G_k-groups and twists of the genus two curve $y^2 = x^5 - x$. Journal of Algebra **303**(2), 707–721 (2006)
11. Cardona, G., Quer, J.: Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12}. Transactions of the American Mathematical Society **359**(6), 2831–2849 (2007)
12. Chen, L., Moody, D., Regenscheid, A., Randall, K.: Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters (Draft NIST Special Publication 800-186) (2019), `https://csrc.nist.gov/publications/detail/sp/800-186/draft`
13. Chávez-Saab, J., Rodríguez-Henríquez, F., Tibouchi, M.: SWIFTEC: Shallue-van de Woestijne indifferentiable function to elliptic curves. In: Agrawal, S., Lin, D. (eds.) Advances in Cryptology – ASIACRYPT 2022. Lecture Notes in Computer Science, vol. 13791, pp. 63–92. Springer, Cham (2022)
14. Dudeanu, A., Oancea, G.R., Iftene, S.: An x-coordinate point compression method for elliptic curves over $\mathbb{F}_p$. In: 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. pp. 65–71. Institute of Electrical and Electronics Engineers, New York (2010)
15. Farashahi, R.R., Fouque, P.A., Shparlinski, I.E., Tibouchi, M., Voloch, J.F.: Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. Mathematics of Computation **82**(281), 491–512 (2013)
16. Faz-Hernandez, A., Scott, S., Sullivan, N., Wahby, R.S., Wood, C.A.: Hashing to elliptic curves (2022), `https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve`
17. Fried, M.D.: Global construction of general exceptional covers, with motivation for applications to encoding. In: Mullen, G.L., Shiue, P.J. (eds.) Finite Fields: Theory, Applications, and Algorithms. Contemporary Mathematics, vol. 168, pp. 69–100. American Mathematical Society, Providence (1994)

18. Galbraith, S.D.: Mathematics of public key cryptography. Cambridge University Press, New York (2012)
19. Gaudry, P., Schost, E.: On the invariants of the quotients of the Jacobian of a curve of genus 2. In: Boztas, S., Shparlinski, I.E. (eds.) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 2001. Lecture Notes in Computer Science, vol. 2227, pp. 373–386. Springer, Berlin, Heidelberg (2001)
20. Hamburg, M.: Computing the Jacobi symbol using Bernstein–Yang (2021), `https://eprint.iacr.org/2021/1271`
21. Hess, F., Smart, N.P., Vercauteren, F.: The eta pairing revisited. IEEE Transactions on Information Theory **52**(10), 4595–4602 (2006)
22. Hopwood, D.: The Pasta curves for Halo 2 and beyond (2020), `https://electriccoin.co/blog/the-pasta-curves-for-halo-2-and-beyond`
23. Hopwood, D.: Pluto/Eris supporting evidence (2021), `https://github.com/daira/pluto-eris`
24. Hurt, N.E.: Many rational points: Coding theory and algebraic geometry, Mathematics and Its Applications, vol. 564. Springer, Dordrecht (2003)
25. Icart, T.: How to hash into elliptic curves. In: Halevi, S. (ed.) Advances in Cryptology – CRYPTO 2009. Lecture Notes in Computer Science, vol. 5677, pp. 303–316. Springer, Berlin, Heidelberg (2009)
26. Janson, S.: Roots of polynomials of degrees 3 and 4 (2010), `https://arxiv.org/abs/1009.2373`
27. Joye, M., Quisquater, J.J.: Efficient computation of full Lucas sequences. Electronics Letters **32**(6), 537–538 (1996)
28. Kammerer, J.G., Lercier, R., Renault, G.: Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing-Based Cryptography – Pairing 2010. Lecture Notes in Computer Science, vol. 6487, pp. 278–297. Springer, Berlin, Heidelberg (2010)
29. Katsura, T., Oort, F.: Families of supersingular abelian surfaces. Compositio Mathematica **62**(2), 107–167 (1987)
30. Koshelev, D.: Indifferentiable hashing to ordinary elliptic $\mathbb{F}_q$-curves of $j = 0$ with the cost of one exponentiation in $\mathbb{F}_q$. Designs, Codes and Cryptography **90**(3), 801–812 (2022)
31. Koshelev, D.: Optimal encodings to elliptic curves of j-invariants 0, 1728. SIAM Journal on Applied Algebra and Geometry **6**(4), 600–617 (2022)
32. Koshelev, D.: Magma code (2023), `https://github.com/dishport/Hashing-to-elliptic-curves-over-highly-2-adic-fields-Fq-with-O-log-q-operations-in-Fq`
33. Koshelev, D.: Some remarks on how to hash faster onto elliptic curves (2023), `https://eprint.iacr.org/2021/1082`
34. Koval, A.: On Lucas sequences computation. International Journal of Communications, Network and System Sciences **3**(12), 943–944 (2010)
35. Käsper, E.: Fast elliptic curve cryptography in OpenSSL. In: Danezis, G., Dietrich, S., Sako, K. (eds.) Financial Cryptography and Data Security. FC 2011. Lecture Notes in Computer Science, vol. 7126, pp. 27–39. Springer, Berlin, Heidelberg (2012)
36. Maier, R.S.: On rationally parametrized modular equations (2008), `https://arxiv.org/abs/math/0611041`
37. Mula, M., Murru, N., Pintore, F.: Random sampling of supersingular elliptic curves (2022), `https://eprint.iacr.org/2022/528`
38. Müller, S.: On the computation of square roots in finite fields. Designs, Codes and Cryptography **31**(3), 301–312 (2004)

39. Petit, C., Kosters, M., Messeng, A.: Algebraic approaches for the elliptic curve discrete logarithm problem over prime fields. In: Cheng, C.M., Chung, K.M., Persiano, G., Yang, B.Y. (eds.) Public-Key Cryptography – PKC 2016. Lecture Notes in Computer Science, vol. 9615, pp. 3–18. Springer, Berlin, Heidelberg (2016)
40. Pornin, T.: Optimized binary GCD for modular inversion (2020), `https://eprint.iacr.org/2020/972`
41. Pornin, T.: X25519 implementation for ARM Cortex-M0/M0+ (2020), `https://github.com/pornin/x25519-cm0`
42. Postl, H.: Fast evaluation of Dickson polynomials. Contributions to General Algebra **6**, 223–225 (1988)
43. Sarkar, P.: Computing square roots faster than the Tonelli–Shanks/Bernstein algorithm. Advances in Mathematics of Communications (2022), `https://www.aimsciences.org/article/doi/10.3934/amc.2022007`
44. Smith, B.: The $\mathbb{Q}$-curve construction for endomorphism-accelerated elliptic curves. Journal of Cryptology **29**(4), 806–832 (2016)
45. Smith, P.J., Lennon, M.J.: LUC: A new public key system. In: Graham Dougall, E. (ed.) International Conference on Information Security (SEC 1993). IFIP Transactions, vol. A-37, pp. 103–117. North-Holland, Amsterdam (1993)
46. Tibouchi, M.: Impossibility of surjective Icart-like encodings. In: Chow, S.S.M., Liu, J.K., Hui, L.C.K., Yiu, S.M. (eds.) Provable Security. ProvSec 2014. Lecture Notes in Computer Science, vol. 8782, pp. 29–39. Springer, Cham (2014)
47. Wahby, R.S., Boneh, D.: Fast and simple constant-time hashing to the BLS12-381 elliptic curve. IACR Transactions on Cryptographic Hardware and Embedded Systems **2019**(4), 154–179 (2019)