Simultaneously simple universal and indifferentiable hashing to elliptic curves

Dmitrii Koshelev[0000−0002−4796−8989] *

Abstract. The present article explains how to generalize the hash function SwiftEC (in an elementary quasi-unified way) to any elliptic curve E over any finite field $\mathbb{F}_q$ of characteristic > 3. The new result apparently brings the theory of hash functions onto elliptic curves to its logical conclusion. To be more precise, this article provides compact formulas that define a hash function $\{0,1\}^* \to E(\mathbb{F}_q)$ (deterministic and indifferentible from a random oracle) with the same working principle as SwiftEC. In particular, both of them equally compute only one square root in $\mathbb{F}_q$ (in addition to two cheap Legendre symbols). However, the new hash function is valid with much more liberal conditions than SwiftEC, namely when $3 \mid q-1$. Since in the opposite case $3 \mid q-2$ there are already indifferentiable constant-time hash functions to E with the cost of one root in $\mathbb{F}_q$, this case is not processed in the article. If desired, its approach nonetheless allows to easily do that mutatis mutandis.

Keywords: absolute irreducibility · conics · hyperelliptic curves · hashing to elliptic curves · unirationality problem.

1 Introduction

Hashing to an elliptic $\mathbb{F}_q$-curve E plays an important role in elliptic curve cryptography (ECC). To be exact, we are talking about a map $\mathcal{H}\colon \{0,1\}^* \to E(\mathbb{F}_q)$ from the set of binary strings of arbitrary length to the $\mathbb{F}_q$-point group of E. The given primitive already arose in Koblitz's pioneering work [14, Section 3] on ECC under the name "imbedding plaintext". It is not surprising, because many classical public-key encryption schemes, including *Massey–Omura* and *El Gamal* ones (see, e.g., [14, Section 4]), represent a secret message $m \in \{0,1\}^*$ as an elliptic curve point $\mathcal{H}(m)$. Thus, the need for $\mathcal{H}$ appeared long before other more mainstream primitives on elliptic curves such as pairings and isogenies.

To prevent leakage of m the running time of $\mathcal{H}$ must depend exclusively on the length of m, not on its content. In the early years of development of ECC, people did not know how to safely construct $\mathcal{H}$ unless the j-invariant $j(E) = 0$ and $3 \mid q-2$ or, similarly, $j(E) = 1728$ and $4 \mid q-3$ thanks to Kaliski Jr. [13, Section 3] in 1991. In both situations, E is necessarily a supersingular curve. In the same year it became clear [23] that supersingular curves are weaker for ECC than ordinary (a.k.a. non-supersingular) ones. Therefore, a large layer of

[*] https://www.researchgate.net/profile/dimitri-koshelev
`dimitri.koshelev@gmail.com`

cryptographic protocols based on the discrete logarithm problem (DLP) essentially remained for a long time untransferable to $E(\mathbb{F}_q)$ from the multiplicative group $\mathbb{F}_q^*$. Undoubtedly, constant-time hashing of the form $\{0,1\}^* \to \mathbb{F}_q^*$ does not present any difficulties. By contrast, a required hash function to ordinary elliptic curves was independently invented only in the mid-2000s by Skałba [29] and Shallue–van de Woestijne [28].

Since in some scenarios $\mathcal{H}$ is called many times, it is desirable that the given primitive be as cheap as possible. This is the case, e.g., for *incremental (i.e., homomorphic) multiset hashing* [21] and for numerous signature schemes among which a ring signature utilized in *CryptoNote cryptocurrencies* [26]. In the latter, a hash-to-curve function is the principal component of so-called *key image* [24]. For information, it is basically a non-homomorphic map from $E(\mathbb{F}_q)$ to itself designed to hide the discrete logarithm between input and output points. According to an established tradition in the research area under consideration, the operating time of $\mathcal{H}$ is measured in the number of radicals $\sqrt[n]{\cdot} \in \mathbb{F}_q$ (usually with an even $n \in \mathbb{N}$) containing in $\mathcal{H}$. Moreover, each of them is frequently expressed through one exponentiation in $\mathbb{F}_q$. By the way, hashing over highly 2-adic fields is discussed in [11,18], [19, Section 4].

Indifferentiability (from a random oracle) in the sense of [22] is yet another indispensable cryptographic property imposed on hash functions. The point is that this property periodically occurs in reliability proofs of cryptographic protocols and it is not always possible to get rid of it. That is why it is desirable for versatility of use that $\mathcal{H}$ maintain the indifferentiability. For instance, Kaliski Jr.'s hash functions are random oracles, because they are built upon specific readily computable bijective maps $\mathbb{P}^1(\mathbb{F}_q) \to E(\mathbb{F}_q)$ (see a detailed explanation in [30]).

For a long time, there was an open question about the existence of indifferentiable (and still deterministic) hash functions to ordinary elliptic curves with the cost of one root. The first example of such a hash function $\mathcal{H}_3$ was invented several years ago in [16] for curves of j-invariant 0 having, at the same time, an $\mathbb{F}_q$-point of order 3. Subsequently, a number of other constructions arose in the literature. Unfortunately, each of them is applicable solely under certain restrictions on E and $\mathbb{F}_q$. Indeed, $\mathcal{H}_3$ (as well as the hash function $\mathcal{H}_4$ from [17]) inherently exploits a non-trivial automorphism on curves of j-invariant 0 (1728, respectively). In turn, the hashing solution $\mathcal{H}_6$ from [19, Section 2.1] works whenever $3 \mid q - 2$ and, conversely, $j(E) \neq 0, 1728$. The index i in the notation $\mathcal{H}_i$ coincides with the degree of the root incorporated in $\mathcal{H}_i$.

Another indifferentiable deterministic hash function $\mathcal{H}_2$ (dubbed *SwiftEC*) was proposed in Chávez-Saab–Rodríguez-Henríquez–Tibouchi's paper [6]. It was recognized as one of the three best papers at Asiacrypt 2022, one of the three flagship cryptographic conferences under the auspices of IACR (International Association for Cryptologic Research). Apart from one square root, $\mathcal{H}_2$ has to determine the values of two Legendre symbols. Since recently, it is realized [2] that the Legendre symbol is a significantly faster operation than (square) root extraction even in the constant-time setting. As a consequence, $\sqrt{\cdot} \in \mathbb{F}_q$ is the unique bottleneck of $\mathcal{H}_2$, i.e., this function is computationally equivalent to the functions $\mathcal{H}_3$, $\mathcal{H}_4$, $\mathcal{H}_6$ that do not need to compute any (non-trivial) multiplicative characters $\mathbb{F}_q^* \to \mathbb{C}^*$.

The definitions of $\mathcal{H}_i$ are quite sophisticated and their implementation details may slightly vary. In a nutshell, we deal with the compositions $\mathcal{H}_i = h_i \circ \eta$, where $\eta\colon \{0,1\}^* \to (\mathbb{F}_q^*)^2$ is an auxiliary hash function and $h_i\colon (\mathbb{F}_q^*)^2 \to E(\mathbb{F}_q)$. Throughout the article, η is considered as deterministic and indifferentiable. Except for h_6, the other maps h_i are themselves the compositions $h_i = h_i' \circ \chi_i$ of a certain cornerstone map $h_i' : T_i(\mathbb{F}_q) \to E(\mathbb{F}_q)$ and of a rational $\mathbb{F}_q$-map $\chi_i : \mathbb{A}^2 \to T_i$ restricted on $(\mathbb{F}_q^*)^2$. Here, T_i is the three-dimensional quotient-variety with respect to a specific diagonal action of a finite group G_i on the direct product of three carefully selected (possibly trivial) twists of E.

In particular, SwiftEC is built upon the threefold $T = T_2 := E^3/G$, where $G = G_2 := \langle i_1, i_2\rangle \simeq (\mathbb{Z}/2)^2$ is the group generated by $i_1 := (1,-1,-1)$ and $i_2 := (-1,1,-1)$. By the way, $i_1 \circ i_2 = i_2 \circ i_1 = (-1,-1,1)$. It is easily checked that an $\mathbb{F}_q$-point of T corresponds to the orbit having at least one vector $\overline{P} = (P_1, P_2, P_3) \in E^3$ with at least one $\mathbb{F}_q$-point P_i. The map $h' = h_2'$ is nothing but restoring P_i given $\overline{P}$. What is more, this can be done in constant time. A precise description of h' is contained, e.g., in [6, Section 3.1].

In their seminal paper [28] Shallue–van de Woestijne found an embedding $\varphi\colon S \hookrightarrow T$ of an $\mathbb{F}_q$-surface S equipped with a *conic bundle* structure $\pi\colon S \to \mathbb{A}^1$. This means that a general fiber of π is a smooth conic. Choosing in advance any non-degenerate fiber $\pi^{-1}(t)$ for $t \in \mathbb{F}_q$ and an $\mathbb{F}_q$-point on it, those researchers eventually obtained an $\mathbb{F}_q$-parametrization $\mathbb{A}^1 \to \pi^{-1}(t)$ and thereby a one-parametric $\mathbb{F}_q$-map $\mathbb{A}^1 \to T$. If the hash function $\mathcal{H}_2$ is not claimed to be indifferentiable, then it is sufficient to take the latter map (supplemented by $\{0,1\}^* \to \mathbb{F}_q^*$) instead of $\chi = \chi_2$.

The merit of Chávez-Saab et al. consists in that they analyzed the cases when the bundle π has an $\mathbb{F}_q$-section, that is, (the image of) an $\mathbb{F}_q$-map $s\colon \mathbb{A}^1 \to S$ such that $\pi \circ s = \mathrm{id}$. Its existence is known to give rise to a proper (i.e., birational) $\mathbb{F}_q$-parametrization $\psi\colon \mathbb{A}^2 \to S$, leading ultimately to the sought two-parametric $\mathbb{F}_q$-map $\chi := \varphi \circ \psi\colon \mathbb{A}^2 \to T$. Moreover, it costs nothing to derive explicit formulas of ψ and hence of χ. In the language of algebraic geometry, the authors of SwiftEC established $\mathbb{F}_q$-*rationality* (see, e.g., [9]) of the surface S subject to the conditions represented in [6, Theorem 3]. Unfortunately, they are quite restrictive, although ordinary curves of j-invariant 0 (popular in practice) are completely covered.

This article aims to bring to life the idea of [19, Section 3], i.e., to concretize the hash function noted as “Shallue, van de Woestijne (modification)” in Table 1 of that article. The idea lies in the suggestion (correct as we will see) that for indifferentiability of $\mathcal{H}_2$, the $\mathbb{F}_q$-rationality condition of the surface S can be painlessly relaxed to $\mathbb{F}_q$-*unirationality* in the sense of [12, Section 4]. This means that an $\mathbb{F}_q$-parametrization $\psi : \mathbb{A}^2 \to S$ is allowed not to be invertible or, equivalently, not to have $\deg(\psi) = 1$. Incidentally, any $\mathbb{F}_q$-parametrization of a rational curve can be made proper (still over $\mathbb{F}_q$), e.g., with the help of

[27, Section 6.1]. Thereby, the unirationality notion is meaningless as a separate notion in dimension one.

The new (quadratic) map ψ will be based on a so-called *bisection* of π (see, e.g., [9, Section 3.2]). By definition, this is a rational $\mathbb{F}_q$-curve $C \subset S$ intersecting twice (each) fiber of π, that is, the induced cover $\pi : C \to \mathbb{A}^1$ is two-sheeted. Unlike an $\mathbb{F}_q$-section, it turns out that an $\mathbb{F}_q$-bisection on S almost always exists and moreover has a simple equation. The formulas-free origin of ψ is explained in the proof of [12, Theorem 4.2]. As will become clear later, for more comfortable work with concrete formulas of ψ, it is reasonable to impose the restrictions $3 \mid q-1$ (the first one for SwiftEC) and $j(E) \neq 0$. They do not affect the generality, bearing in mind Kaliski Jr.'s hash functions, $\mathcal{H}_4$, $\mathcal{H}_6$, and SwiftEC when $j(E) = 0$ (cf. Section 2.1).

As said at the end of [28, Section 5], the surface S is not $\mathbb{F}_q$-rational in general (maybe even under the introduced restrictions). So, the bisection-based map ψ appears to be an optimal $\mathbb{F}_q$-parametrization of S if one wants to deal with (pretty) universal formulas. Of course, in a series of situations (including those of SwiftEC) it is possible to replace ψ with a birational $\mathbb{F}_q$-map $\mathbb{A}^2 \to S$. Intuitively, the latter should possess slightly more compact formulas (as it turns out for $j(E) = 0$), albeit this does not formally follow from anywhere. In any case, such formulas can at best economize (during their evaluation) only a few multiplications in $\mathbb{F}_q$. As a downside, independent treatment of the opposite scenarios $\deg(\psi) \in \{1, 2\}$ will require additional work when implementing $\mathcal{H}_2$ in cryptographic software libraries.

It is impossible not to note that another quasi-universal $\mathbb{F}_q$-map to T was obtained in Skałba's article [29]. However, its formulas are more bulky compared to those of this article. In this regard, as far as the author knows, Skałba's formulas have never been implemented in practice. Much more importantly, their cumbersomeness is a substantial computational obstacle to a (simple) proof of a theorem (if any) analogous to Theorem 2 whose proof is itself not pleasant. This theorem is at the heart of why the hash function $\mathcal{H}_2$ is indifferentiable. Thus, security of Skałba's map is not confirmed (although not disproved), which is the prevailing applicability criterion in cryptography. It is also worth emphasizing that in Skałba's approach the requirement $j(E) \neq 0$ is crucial as opposed to the current approach.

To summarize, the new $\mathbb{F}_q$-map $\chi\colon \mathbb{A}^2 \to T$ enjoys the advantages (and does not have the drawbacks) of those from the all three previous articles [6,28,29] on hashing to elliptic curves via the threefold T, justifying the title of this article. In the author's taste, the proposed hashing solution is not very interesting from the mathematical viewpoint because of the remaining Legendre symbols in $\mathcal{H}_2$. Nonetheless, the practical significance of the result greatly outweighs this circumstance. That is why the author decided to share the given solution with the R&D community. Since cryptography is a pragmatic science (unlike pure mathematics), the stated view has a right to exist. It is hoped that the below formulas will be used sooner or later in real-world cryptosystems.

2 Formulas

Let's mainly stick to the notation of [19, Section 3]. Hereafter, the reader is invited to look in parallel at the program code [20] written in Magma to verify or leverage encountered (at least core) formulas. Implementers can skip the majority of the present section except for the resulting formulas (2) (cf. (3) when $j(E) = 0$) of the map χ.

Consider an elliptic curve $E\colon y^2 = f(x) := x^3 + ax + b$ over a finite field $\mathbb{F}_q$ of characteristic 5 or greater. Recall that the discriminant

$$D(E) = D(f) = -16(4a^3 + 27b^2) \neq 0.$$

Every specialist knows that $j(E) = 0 \Leftrightarrow a = 0$ and, similarly, $j(E) = 1728 \Leftrightarrow b = 0$.

The threefold T and Shallue–van de Woestijne surface S respectively have the equations

$$T\colon y^2 = f(x_1)f(x_2)f(x_3) \quad \subset \quad \mathbb{A}^4_{(x_1,x_2,x_3,y)}$$

and

$$S\colon y^2 + h(t)x^2 + f(t) = 0 \quad \subset \quad \mathbb{A}^3_{(x,y,t)},$$

where $h(t) := 3t^2 + 4a$. Let's borrow from [28, Section 5] the embedding

$$\varphi\colon S \hookrightarrow T \qquad (x, y, t) \mapsto \Big(s,\ -t-s,\ r,\ \frac{f(r)g(t,s)}{2x}\Big),$$

where

$$s := \frac{y - tx}{2x}, \qquad r := t + 4x^2, \qquad g := t^2 + ts + s^2 + a.$$

For the rest of the article, it is necessary to remember that $3 \mid q - 1$ if and only if the cubic root $\omega := \sqrt[3]{1}$ (such that $\omega \neq 1$) or, equivalently, the square root $\sqrt{-3} = 2\omega + 1$ belongs to $\mathbb{F}_q$.

Theorem 1. *Suppose that $a \neq 0$ or $3 \mid q-1$. Then, the Shallue–van de Woestijne surface S is $\mathbb{F}_q$-unirational of degree at most 2.*

Proof. The other affine model

$$S'\colon y^2 + h(t) + f(t)z^2 = 0 \quad \subset \quad \mathbb{A}^3_{(y,z,t)}$$

of S is obtained by means of the transformation

$$\tau_2\colon S' \to S \qquad (y, z, t) \mapsto \Big(\frac{1}{z}, \frac{y}{z}, t\Big),$$
$$\tau_2^{-1}\colon S \to S' \qquad (x, y, t) \mapsto \Big(\frac{y}{x}, \frac{1}{x}, t\Big).$$

The surface S' obviously inherits from S the conic bundle structure π. At the same time, there is the natural embedding

$$\iota\colon C \hookrightarrow S' \qquad (y, t) \mapsto (y, 0, t)$$

of the diagonal conic

$$C\colon y^2 + h(t) = 0 \quad \subset \quad \mathbb{A}^2_{(y,t)}.$$

Evidently, the intersection number $\iota(C)\cdot\pi^{-1}(t) = 2$. In the scenario $a = 0$ and $3 \mid q-1$, the conic C is the union of the two $\mathbb{F}_q$-lines $L_\pm\colon y = \pm\sqrt{-3}\cdot t$. Each of them is the (usual) $\mathbb{F}_q$-section of π taken in the construction of SwiftEC (see [6, Section 5.1]), hence we literally rediscover Chávez-Saab et al.'s fact about $\mathbb{F}_q$-rationality of S in the given sporadic case. In the opposite one $a \neq 0$ (regardless of the remainder of q modulo 3), the conic C is non-degenerate. Since over finite fields there is no existence question of a rational point on C, it remains to apply [12, Theorem 4.2]. □

As a useful observation, when the theorem premise is not fulfilled (i.e., $a = 0$ and $3 \mid q-2$), the lines $L_\pm$ are Frobenius-conjugate. Thereby, we do not have a clearly visible absolutely (i.e., geometrically) irreducible $\mathbb{F}_q$-(bi)section of π. But the surface S is still somehow $\mathbb{F}_q$-unirational if one believes [15]. In the author's opinion, derivation of explicit formulas parametrizing S is a surmountable task in all the cases.

Nonetheless, unless stated otherwise, it will be assumed that $a \neq 0$ **and** $3 \mid q-1$. The reason is that by virtue of [6, Lemma 5], the weaker or-condition from the previous theorem is not sufficient (unlike the and-condition) for C to be a smooth conic enjoying an $\mathbb{F}_q(a)$-point. Of course, as well as in the above proof we could refer to the fact that $C(\mathbb{F}_q) \neq \emptyset$ for each fixed $a \in \mathbb{F}_q^*$. However, this would require involving two more dependent variables $(y_0, t_0) \in C$, cluttering the following formulas. As said in the introduction, this strategy is employed (for lack of an alternative) by Shallue–van de Woestijne.

To notice an announced $\mathbb{F}_q(a)$-point on C it is proposed to switch to the affine model

$$C'\colon y^2 + 3 + 4av^2 = 0 \quad \subset \quad \mathbb{A}^2_{(y,v)}$$

via the transformation

$$\tau_1\colon C' \to C \qquad (y,v) \mapsto \left(\frac{y}{v}, \frac{1}{v}\right),$$
$$\tau_1^{-1}\colon C \to C' \qquad (y,t) \mapsto \left(\frac{y}{t}, \frac{1}{t}\right).$$

As predicted, we have $P_1 := (\sqrt{-3}, 0) \in C'$. The projection from P_1 is the invertible map

$$pr_{P_1}\colon C' \to \mathbb{A}^1_{t_1} \qquad (y,v) \mapsto \frac{y - \sqrt{-3}}{v}$$

such that

$$\tau_1 \circ pr_{P_1}^{-1}\colon \mathbb{A}^1_{t_1} \to C \qquad t_1 \mapsto \big(f_y(t_1), f_t(t_1)\big),$$

where

$$f_y := \frac{t_1^2 - 4a}{2t_1}, \qquad f_t := \frac{t_1^2 + 4a}{-2\sqrt{-3}\cdot t_1}.$$

As usual, the surfaces S, S' can be interpreted as $\mathbb{F}_q(t)$-conics on $\mathbb{A}^2_{(x,y)}$, $\mathbb{A}^2_{(y,z)}$, respectively. There is the point $P_2 := (y_0, 0) \in S'$ over the quadratic extension $\mathbb{F}_q(t, y_0)$ generated by the root $y_0 := \sqrt{-h(t)}$. The composition of the inverse to the projection map

$$pr_{P_2}\colon S' \to \mathbb{A}^1_{t_2} \qquad (y,z) \mapsto \frac{y - y_0}{z}$$

and of the $\mathbb{F}_q(t)$-isomorphism $\tau_2\colon S' \to S$ has the form

$$\psi := \tau_2 \circ pr_{P_2}^{-1}\colon \mathbb{A}^1_{t_2} \to S \qquad t_2 \mapsto \big(g_x(t, y_0, t_2),\ g_y(t, t_2)\big),$$

where

$$g_x := \frac{t_2^2 + f(t)}{-2y_0t_2}, \qquad g_y := \frac{t_2^2 - f(t)}{2t_2}.$$

It is worth emphasizing that $(y_0 \circ f_t)(t_1) = f_y(t_1)$ if one looks at y_0 as a non-rational function in t. Realizing S again as an $\mathbb{F}_q$-surface in $\mathbb{A}^3_{(x,y,t)}$, we thus get the **rational** $\mathbb{F}_q$-parametrization

$$\psi\colon \mathbb{A}^2_{(t_1,t_2)} \to S \qquad (t_1, t_2) \mapsto \Big(g_x\big(f_t(t_1), f_y(t_1), t_2\big),\ g_y\big(f_t(t_1), t_2\big),\ f_t(t_1)\Big).$$

Explicitly,

$$\psi\colon \mathbb{A}^2_{(t_1,t_2)} \to S \qquad (t_1, t_2) \mapsto (\mathfrak{g}_x, \mathfrak{g}_y, f_t), \tag{1}$$

where $\mathfrak{g}_x = n_+/d_x$ and $\mathfrak{g}_y = n_-/d_y$,

$$n_\pm := t_1^6 + 2^3 3\sqrt{-3}\cdot bt_1^3 + 2^6a^3 \pm 2^3 3\sqrt{-3}\cdot t_1^3t_2^2$$

and

$$d_x := -2^3 3\sqrt{-3}(t_1^2 - 2^2a)t_1^2t_2, \qquad d_y := -2^4 3\sqrt{-3}\cdot t_1^3t_2.$$

Everywhere below, $i \in \{1,2,3\}$ and $j \in \{1,2\}$. Finally, we come to the two-parametric $\mathbb{F}_q$-map

$$\chi := \varphi \circ \psi\colon \mathbb{A}^2_{(t_1,t_2)} \to T \qquad (t_1, t_2) \mapsto (X_1, X_2, X_3, Y) \tag{2}$$

whose x-coordinate functions $X_i = n_i/d_i$ possess the numerators

$$\begin{aligned} n_j := {} & t_1^8 + 2^2\omega^{2j}at_1^6 + 2^3 3\sqrt{-3}\cdot bt_1^5 + 2^5 3\sqrt{-3}\cdot\omega^{2j}abt_1^3 + 2^6a^3t_1^2 + 2^8\omega^{2j}a^4 + \\ & 2^3 3\sqrt{-3}(\omega^{2j}t_1^2 + 2^2a)t_1^3t_2^2, \end{aligned}$$

$$\begin{aligned} n_3 := {} & t_1^{12} + 2^4 3\sqrt{-3}\cdot bt_1^9 + 2^6(2a^3 - 3^3b^2)t_1^6 + 2^{10} 3\sqrt{-3}\cdot a^3bt_1^3 + 2^{12}a^6 - \\ & 2^3 3\sqrt{-3}\Big(t_1^6 - 2^2 3at_1^4 - 2^4 3\sqrt{-3}\cdot bt_1^3 - 2^4 3a^2t_1^2 + 2^6a^3 - 2^3 3\sqrt{-3}\cdot t_1^3t_2^2\Big)t_1^3t_2^2 \end{aligned}$$

and the denominators

$$\begin{aligned} d_j &:= -2\sqrt{-3}\cdot\omega^j\Big(t_1^6 + 2^3 3\sqrt{-3}\cdot bt_1^3 + 2^6a^3 + 2^3 3\sqrt{-3}\cdot t_1^3t_2^2\Big)t_1, \\ d_3 &:= -2^4 3^3(t_1^2 - 2^2a)^2t_1^4t_2^2. \end{aligned}$$

Given $x \in \mathbb{F}_q$, introduce the hyperplanes $\mathit{\Pi}_{i,x}\colon x_i = x$ in the space $\mathbb{A}^4_{(x_1,x_2,x_3,y)}$ as well as the curves

$$C^{(i)}_x := \varphi^{-1}(\mathit{\Pi}_{i,x}) \subset S, \qquad C_{i,x} := \chi^{-1}(\mathit{\Pi}_{i,x}) = \psi^{-1}(C^{(i)}_x).$$

The latter clearly have the equations $C_{i,x}\colon xd_i = n_i$ on the plane $\mathbb{A}^2_{(t_1,t_2)}$. Besides, we lack the infinity curve $C_\infty = C_{j,\infty}\colon d_j/t_1 = 0$. In a sense, it is $\chi^{-1}(\mathit{\Pi}_{j,\infty})$ up to the coordinate line $t_1 = 0$. It is readily seen that

$$\deg(C_{j,x}) = 8, \qquad \deg(C_{3,x}) = 12, \qquad \deg(C_\infty) = 6.$$

As a consequence, the arithmetic genera

$$p_a(C_{j,x}) = 21, \qquad p_a(C_{3,x}) = 55, \qquad p_a(C_\infty) = 10,$$

e.g., by virtue of [31, Theorem 2.3.18].

It is shown in [6, Section 3.2] that the curves $C^{(i)}_x$ are absolutely irreducible (of geometric genus 2) except for several values x. Nonetheless, this does not automatically result in the analogous statement for $C_{i,x}$ (not to mention C_∞), because the covers $\psi\colon C_{i,x} \to C^{(i)}_x$ are not birational, but only quadratic. Therefore, we are obliged to manually prove it.

Theorem 2. *As before, $a \neq 0$ by assumption. The curves $C_{i,x}$, C_∞ are absolutely irreducible whenever x is outside the degeneracy set*

$$\mathcal{D} := \left\{ \pm\sqrt{\frac{a}{-3}},\ \pm 2\sqrt{\frac{a}{-3}},\ -\frac{b}{a} \right\} \ \cup\ x(E[2]).$$

Proof. Recall that absolute irreducibility of a plane curve $\subset \mathbb{A}^2_{(t_1,t_2)}$ (given by one polynomial) amounts to irreducibility of the corresponding univariate polynomial in t_2 over the field $\overline{\mathbb{F}_q}(t_1)$, where $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$.

For the sake of compactness, put

$$\rho_0 := t_1^6 + 2^3 3\sqrt{-3}\cdot b t_1^3 + 2^6 a^3, \qquad q_i := t_1^2 + 2\sqrt{-3}\cdot\omega^{2i} x t_1 + 2^2\omega^i a.$$

First, there are the transformations

$$\begin{aligned} \sigma_{j,x}\colon C_{j,x} \to H_x \qquad & (t_1, t_2) \mapsto \big(t_1,\ 2^2 3\omega^j q_j(t_1) t_1^2 t_2\big), \\ \sigma_{j,x}^{-1}\colon H_x \to C_{j,x} \qquad & (t_1, t_2) \mapsto \left(t_1,\ \frac{t_2}{2^2 3\omega^j q_j(t_1) t_1^2}\right) \end{aligned}$$

between $C_{j,x}$ and the hyperelliptic curve

$$H_x\colon t_2^2 = h_x(t_1) := 2\sqrt{-3}\cdot\rho_0(t_1) q_1(t_1) q_2(t_1) t_1 \quad \subset \quad \mathbb{A}^2_{(t_1,t_2)}.$$

In particular, $C_{1,x} \simeq C_{2,x}$ with the help of $\sigma_{2,x}^{-1} \circ \sigma_{1,x}$. Since $\sigma_{j,x}$ are birational maps (constant on t_1), absolute (ir)reducibility of $C_{j,x}$, H_x takes place under the same circumstances. Looking ahead, this argument will be tacitly applied also to the transformations $\sigma_{3,x}$, σ_∞.

The discriminants

$$D(\rho_0) = 2^{18}3^6a^6D(E)^3, \qquad D(q_i) = -2^2\omega^i h(x).$$

In turn, the resultants

$$R(\rho_0, q_j) = -2^{12}3^3a^3f(x)^2, \qquad R(q_1, q_2) = -2^43a(a+3x^2).$$

Besides, $(\rho_0q_1q_2)(0) = 0 \Leftrightarrow a = 0$. All this exactly means that the polynomial h_x has a multiple root only if $a = 0$ or $x \in \mathcal{D}$. Otherwise, h_x is certainly not a perfect square in $\overline{\mathbb{F}_q}(t_1)$. Incidentally, $\deg(h_x) = 11$, i.e., the geometric genus $g(C_{j,x}) = g(H_x) = 5$, albeit this fact will not be necessary for us.

By analogy,

$$\begin{aligned}
\sigma_\infty\colon C_\infty \to H_\infty \qquad & (t_1, t_2) \mapsto (t_1,\ -2^23t_1^2t_2),\\
\sigma_\infty^{-1}\colon H_\infty \to C_\infty \qquad & (t_1, t_2) \mapsto \Big(t_1,\ \frac{t_2}{-2^23t_1^2}\Big),
\end{aligned}$$

where

$$H_\infty\colon t_2^2 = h_\infty(t_1) := 2\sqrt{-3}{\cdot}\rho_0(t_1)t_1 \quad \subset \quad \mathbb{A}^2_{(t_1,t_2)}.$$

We already know that $D(\rho_0) \neq 0$. Furthermore, $\rho_0(0) = 0 \Leftrightarrow a = 0$. As a result, the curves C_∞, H_∞ are also absolutely irreducible. By the way, $\deg(h_\infty) = 7$, that is, $g(C_\infty) = g(H_\infty) = 3$.

It remains to analyze absolute (ir)reducibility of the last more awkward curve $C_{3,x}$. Below, we will meet the polynomials

$$\begin{aligned}
\rho_\pm := {} & t_1^6 \pm 2{\cdot}3\sqrt{-3}{\cdot}xt_1^5 \mp 2^23at_1^4 \mp 2^43\sqrt{-3}(ax+\delta_\mp b)t_1^3 \mp 2^43a^2t_1^2 \pm \\
& 2^53\sqrt{-3}{\cdot}a^2xt_1 + 2^6a^3,
\end{aligned}$$

where $\delta_\mp := (3 \mp 1)/2$. It is convenient to simplify a little $C_{3,x}$ as follows:

$$\begin{aligned}
\sigma_{3,x}\colon C_{3,x} \to C'_{3,x} \qquad & (t_1, t_2) \mapsto (t_1,\ 2\sqrt{-3}{\cdot}t_1t_2),\\
\sigma_{3,x}^{-1}\colon C'_{3,x} \to C_{3,x} \qquad & (t_1, t_2) \mapsto \Big(t_1,\ \frac{t_2}{2\sqrt{-3}{\cdot}t_1}\Big).
\end{aligned}$$

The curve $C'_{3,x}$ is defined by the equation

$$C'_{3,x}\colon c_0(t_1) + c_1(t_1)t_2^2 + c_2(t_1)t_2^4 = 0 \quad \subset \quad \mathbb{A}^2_{(t_1,t_2)}$$

with the coefficients

$$c_0 := \rho_0(t_1)^2, \qquad c_1 := 2\sqrt{-3}{\cdot}\rho_+(t_1)t_1, \qquad c_2 := -2^23t_1^2.$$

Consider the univariate quartic and quadratic $\overline{\mathbb{F}_q}(t_1)$-polynomials $Q_4(t_2) := C'_{3,x}(t_1)(t_2)$ and $Q_2(s_2) := Q_4(\sqrt{s_2})$, respectively. The second has the discriminant

$$D(Q_2) = 2^23^2(t_1^2 - 2^2a)^2t_1^2 \cdot h_{3,x}(t_1)$$

with $h_{3,x}(t_1) := q_3(t_1)\rho_-(t_1)$. Therefore, the roots of Q_2 are nothing but

$$r_\pm = \frac{\rho_+(t_1) \pm \sqrt{-3}(t_1^2 - 2^2a)s_1}{-2^2\sqrt{-3}\cdot t_1},$$

where s_1 is a square root of $h_{3,x}(t_1)$. The discriminant $D(q_3)$ was already determined earlier. Meanwhile,

$$D(\rho_-) = 2^{38}3^{12}a^6(ax+b)^2f(x)^2D(E), \qquad R(q_3,\rho_-) = -2^{16}3^3a^3f(x)^2.$$

Thus, $D(Q_2)$ (i.e., $h_{3,x}$) is not a perfect square in $\overline{\mathbb{F}_q}(t_1)$ (as above, unless $a = 0$ or $x \in \mathcal{D}$). Consequently, $r_\pm$ (i.e., s_1) do not belong to $\overline{\mathbb{F}_q}(t_1)$.

Let's involve the hyperelliptic curve $H_{3,x}\colon s_1^2 = h_{3,x}(t_1)$ on the plane $\mathbb{A}^2_{(t_1,s_1)}$. There is on $H_{3,x}$ the point $P_0 := (0, 2^4a^2)$. The tangent line of $H_{3,x}$ at P_0 has the form

$$T_{P_0}\colon 2^5a^2(s_1 - 2^4a^2) = h'_{3,x}(0)t_1.$$

Whenever $a \neq 0$, the left-hand side does not vanish, hence the line $t_1 = 0$ is different from T_{P_0}. As a result, t_1 (as a function on $H_{3,x}$) is known to be a uniformizing (a.k.a. local) parameter at P_0. Note that

$$(r_\pm t_1)(P_0) = \frac{2^5a^3\omega^{\delta_\mp}}{\sqrt{-3}} \neq 0, \infty.$$

We see that the order (a.k.a. valuation) $v_{P_0}(r_\pm) = -1$ is odd. At the same time, the theory of function fields says that $v_{P_0} : \overline{\mathbb{F}_q}(H_{3,x})^* \to \mathbb{Z}$ is a group homomorphism. So, neither of the roots of Q_4 (namely $\pm\sqrt{r_+}$ and $\pm\sqrt{r_-}$) lies in $\overline{\mathbb{F}_q}(H_{3,x}) = \overline{\mathbb{F}_q}(t_1, s_1)$.

To summarize, we demonstrated that

$$\overline{\mathbb{F}_q}(C'_{3,x}) \supsetneqq \overline{\mathbb{F}_q}(H_{3,x}) \supsetneqq \overline{\mathbb{F}_q}(t_1),$$

that is, $\overline{\mathbb{F}_q}(C'_{3,x}) = \overline{\mathbb{F}_q}(t_1, t_2)$ is a quartic extension of $\overline{\mathbb{F}_q}(t_1)$. This is possible if and only if Q_4 is an $\overline{\mathbb{F}_q}(t_1)$-minimal polynomial of t_2 as a function on $C'_{3,x}$. The theorem is proved. □

2.1 The case $a = 0$

Although we worked under the assumption $a \neq 0$ to avoid caveats, the formal substitution $a = 0$ into the formulas of the map ψ (1) gives rise to the equalities

$$\mathfrak{g}_x = \frac{-\mathfrak{g}_y + t_2}{\sqrt{-3}\cdot f_t}, \qquad \mathfrak{g}_y = \frac{f_t^3 + b - t_2^2}{-2t_2}, \qquad f_t = \frac{t_1}{-2\sqrt{-3}}.$$

They coincide with [6, Equalities (15)] up to the swap $x \leftrightarrow y$, the sign $-$ in front of $\mathfrak{g}_y$, and labeling the variables f_t, t_2. The proof of Theorem 1 predicts that ψ should be a birational map in the given sporadic case. For the sake of completeness, here is its inverse

$$\psi^{-1}\colon S \to \mathbb{A}^2_{(t_1,t_2)} \qquad (x,y,t) \mapsto (-2\sqrt{-3}\cdot t,\ \sqrt{-3}\cdot xt + y).$$

In turn, the formulas of the functions X_i (2) are not explicitly written out in [6]. It is useful to have them before our eyes, not pretending to their authorship:

$$X_i = \frac{\mathfrak{n}_i}{\mathfrak{d}_i}, \qquad n_j = \mathfrak{n}_j t_1^4, \qquad n_3 = \mathfrak{n}_3 t_1^6, \qquad d_j = \mathfrak{d}_j t_1^4, \qquad d_3 = \mathfrak{d}_3 t_1^6, \qquad (3)$$

where

$$\mathfrak{n}_j := \Big(t_1^3 + 2^3 3\sqrt{-3}\cdot b + 2^3 3\sqrt{-3}\cdot\omega^{2j} t_2^2\Big) t_1,$$
$$\mathfrak{n}_3 := t_1^6 + 2^4 3\sqrt{-3}\cdot b t_1^3 - 2^6 3^3 b^2 - 2^3 3\sqrt{-3}\Big(t_1^3 - 2^4 3\sqrt{-3}\cdot b - 2^3 3\sqrt{-3}\cdot t_2^2\Big) t_2^2$$

and

$$\mathfrak{d}_j := -2\sqrt{-3}\cdot\omega^j \Big(t_1^3 + 2^3 3\sqrt{-3}\cdot b + 2^3 3\sqrt{-3}\cdot t_2^2\Big), \qquad \mathfrak{d}_3 := -2^4 3^3 t_1^2 t_2^2.$$

Formally speaking, Theorem 2 is not true when $a = 0$. However, this is just a reflection of the fact that the initial numerators n_i and denominators d_i of the functions X_i have common factors (namely powers of t_1) after specializing a in the given way. Since the map ψ is invertible and the curves $C_x^{(i)} \subset S$ remain generally absolutely irreducible, so are their inverse (i.e., direct) images $C_{i,x} = \psi^{-1}(C_x^{(i)})$. Their right equations on $\mathbb{A}^2_{(t_1,t_2)}$ are nothing but $C_{i,x}\colon x\mathfrak{d}_i = \mathfrak{n}_i$. By the way, the infinity curve $C_\infty = C_{j,\infty}\colon \mathfrak{d}_j = 0$ becomes a twist of E. To sum up, the situation encountered for elliptic curves E of j-invariant 0 degenerates not because it is painful, but because it is even simpler.

3 Final remarks

First of all, the function Y of the map χ (2) seemingly does not have (as opposed to X_i) a very short expression, using solely the variables t_1, t_2. Fortunately, evaluating Y is not required, since the map $h'\colon T(\mathbb{F}_q) \to E(\mathbb{F}_q)$ from the introduction in fact does not depend on the y-coordinate of T. Indeed, Y just has to constantly fall into $\mathbb{F}_q$ to be sure that at least one of the values $f(X_i)$ is a quadratic residue in $\mathbb{F}_q$. Besides, it is not important that X_3 structurally does not resemble X_1, X_2. The point is that an implementer must guarantee evaluating all the functions X_i despite a well-defined choice of $\sqrt{f(X_i)} \in \mathbb{F}_q$. Otherwise, constant-time behavior of the hash function $\mathcal{H}_2$ is not respected. Curiously, $X_i(t_1,t_2) = X_i(t_1,-t_2)$, hence the sign of t_2 can serve as the sign of the chosen $\mathbb{F}_q$-root $\sqrt{f(X_i)}$. This proposal is not consistent with [6, Section 3.1], where one additional bit is involved for the given purpose.

Clearly, the functions X_i are correctly defined outside the lines $t_j = 0$, $t_1 = \pm 2\sqrt{a}$ and the curve C_∞. Since the latter is an absolutely irreducible curve (due to Theorem 2) and its arithmetic genus is a small number independent of q, we conclude that $\#C_\infty(\mathbb{F}_q) = q + O(\sqrt{q})$. The remark concerning $p_a(C_\infty)$ is essential, because there are (e.g., in [10]) absolutely irreducible plane curves of degree $\geqslant q+1$ (dubbed *plane-filling curves*) containing even the whole set $\mathbb{F}_q^2$. So, X_i are meaningful on a subset of $\mathbb{F}_q^2$ of cardinality $q^2 + O(q)$. The probability for a hash function $\eta\colon \{0,1\}^* \to (\mathbb{F}_q^*)^2$ of falling into the undefined locus of X_i is thereby negligible for finite fields of cryptographic size. If desired, the map $h = h_2 : (\mathbb{F}_q^*)^2 \to E(\mathbb{F}_q)$ can be manually extended to $t_1 = \pm 2\sqrt{a}$ (of course, if $\sqrt{a} \in \mathbb{F}_q$) and $C_\infty(\mathbb{F}_q)$, leading to a little more complicated implementation.

Corollary 1. *The map h is ϵ-regular (i.e., statistically ϵ-indistinguishable from the uniform distribution on the codomain) with $\epsilon = O(q^{-1/2})$.*

It is enough to comment on this statement without a rigorous proof owing to the main work done by Chávez-Saab et al. Fix a non-zero point $P = (x, y) \in E(\mathbb{F}_q)$ such that $x \notin \mathcal{D}$ to be able to refer to Theorem 2. By analogy with C_∞, absolute irreducibility of the curves $C_{i,x}$ (as well as smallness of $p_a(C_{i,x})$) is responsible for the fact that $\#C_{i,x}(\mathbb{F}_q) = q + O(\sqrt{q})$. Taking into account the sign of y (i.e, of t_2) and the careful reasoning from [6, Section 3.2] (cf. [16, Section 4], [17, Section 4]), we easily establish that $\#h^{-1}(P) = q + O(\sqrt{q})$. This equality is indispensable for the resulting one $\epsilon = O(q^{-1/2})$.

Rigorously speaking, without absolute irreducibility one cannot resort to *Hasse–Weil* and *Perret bounds* [6, Lemmas 1, 2]. Fortunately, these bounds hold true for singular curves (as in our situation) if the geometric genus is replaced by the arithmetic one (see [3]). It is not superfluous to also stress that the curves $C_{i,x}$, C_∞ obviously have few $\mathbb{F}_q$-points on the coordinate lines $t_j = 0$ (and on the infinity line of $\mathbb{P}^2$) whose number is hidden in $O(\sqrt{q})$. Therefore, it does not matter that our h acts from $(\mathbb{F}_q^*)^2$ rather than from $\mathbb{F}_q^2$ as in the definition of SwiftEC. Thus, the above cardinality estimations of $C_{i,x}(\mathbb{F}_q)$, $C_\infty(\mathbb{F}_q)$, and $h^{-1}(P)$ are actually fair.

As usual in the theory of hash-to-curve functions, the degenerate elements $x \in \mathcal{D}$ (also as the zero point of E) do not play any (significant) role in estimating ϵ, since they constitute a negligible quantity with respect to q. Furthermore, the proof of [6, Lemma 4] (cf. [16, Corollary 2], [17, Corollary 2]) can be shortened without finding a more or less exact constant c in front of $q^{-1/2}$ in the O-notation. For SwiftEC, $c = 6 + o(1)$, while the current $c = O(1)$ should be a little bit greater, because the arithmetic genera of the curves $C_{i,x}$ slightly exceed those of $C_x^{(i)}$ (naturally, for $a \neq 0$). Nevertheless, this is absolutely not important for huge fields $\mathbb{F}_q$ used in ECC.

We eventually come to the next result identical to [6, Theorem 2].

Corollary 2. *The map h is ϵ-admissible with $\epsilon = O(q^{-1/2})$ and hence the hash function $\mathcal{H}_2 = h \circ \eta\colon \{0,1\}^* \to E(\mathbb{F}_q)$ is indifferentiable from a random oracle.*

In conclusion, we obtain the following eye-catching statement.

Corollary 3. *For every elliptic curve E (supersingular or ordinary) over a finite field $\mathbb{F}_q$ of characteristic > 3, there is an indifferentiable deterministic hash* *function* $\{0,1\}^* \to E(\mathbb{F}_q)$ *with the cost of one radical in* $\mathbb{F}_q$ *(and maybe two Legendre symbols).*

Its extension (mutatis mutandis) to the characteristics 2, 3 is seemingly just the question of necessity, because most of the preliminary work was already done in Shallue–van de Woestijne's original paper [28]. To the author's knowledge, elliptic curves over finite fields of characteristic 3 have never been utilized in real world cryptography. In turn, binary (even ordinary) curves were and continue to be suspicious, despite the fact that they are as a rule faster than prime curves. For example, there is the speed-record curve GLS254 [1,25] preferable (among other things) for multiset hashing [21]. It is remarkable that binary curves are deprecated in the last version of the NIST (National Institute of Standards and Technology) standard [5, Section 3.3] on ECC. What is more, there are quasi-polynomial in ℓ algorithms of solving the DLP in $\mathbb{F}_{2^\ell}^*$. As an illustration, the paper [8] computes a discrete logarithm for $\ell = 30750$, which is today the largest bit length $\ell = \lceil \log_2(q) \rceil$ of a field $\mathbb{F}_q$ with a successfully attacked DLP instance in $\mathbb{F}_q^*$. That is why binary pairing-friendly curves (including supersingular ones) are unsafe, although that cannot be said for plain curves.

References

1. Aardal, M.A., Aranha, D.F.: 2DT-GLS: Faster and exception-free scalar multiplication in the GLS254 binary curve (2022), https://eprint.iacr.org/2022/748
2. Aranha, D.F., Salling Hvass, B., Spitters, B., Tibouchi, M.: Faster constant-time evaluation of the Kronecker symbol with application to elliptic curve hashing. In: CCS 2023: ACM Conference on Computer and Communications Security. pp. 3228–3238. ACM Press, New York (2023)
3. Aubry, Y., Perret, M.: A Weil theorem for singular curves. In: Pellikaan, R., Perret, M., Vlăduţ, S.G. (eds.) Arithmetic, Geometry, and Coding Theory. pp. 1–7. Proceedings in Mathematics, De Gruyter, Berlin (1996)
4. Brier, E., Coron, J.S., Icart, T., Madore, D., Randriam, H., Tibouchi, M.: Efficient indifferentiable hashing into ordinary elliptic curves. In: Rabin, T. (ed.) Advances in Cryptology – CRYPTO 2010. Lecture Notes in Computer Science, vol. 6223, pp. 237–254. Springer, Berlin, Heidelberg (2010)
5. Chen, L., Moody, D., Regenscheid, A., Robinson, A., Randall, K.: Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters (NIST Special Publication 800-186) (2023), https://csrc.nist.gov/publications/detail/sp/800-186/final
6. 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)
7. El Mrabet, N., Joye, M. (eds.): Guide to pairing-based cryptography. Cryptography and Network Security Series, Chapman and Hall/CRC, New York (2017)
8. Granger, R., Kleinjung, T., Lenstra, A.K., Wesolowski, B., Zumbrägel, J.: Computation of a 30750-bit binary field discrete logarithm. Mathematics of Computation **90**(332), 2997–3022 (2021)

9. Hassett, B.: Rational surfaces over nonclosed fields. In: Darmon, H., Ellwood, D.A., Hassett, B., Tschinkel, Y. (eds.) Arithmetic Geometry. Clay Mathematics Proceedings, vol. 8, pp. 155–209. Clay Mathematics Institute, Cambridge, MA (2009)
10. Homma, M.: Fragments of plane filling curves of degree $q+2$ over the finite field of q elements, and of affine-plane filling curves of degree $q+1$. Linear Algebra and its Applications **589**, 9–27 (2020)
11. 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)
12. Iskovskikh, V.A.: Rational surfaces with a pencil of rational curves. Mathematics of the USSR-Sbornik **3**(4), 563–587 (1967)
13. Kaliski Jr., B.S.: One-way permutations on elliptic curves. Journal of Cryptology **3**(3), 187–199 (1991)
14. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation **48**(177), 203–209 (1987)
15. Kollár, J., Mella, M.: Quadratic families of elliptic curves and unirationality of degree 1 conic bundles. American Journal of Mathematics **139**(4), 915–936 (2017)
16. 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)
17. Koshelev, D.: The most efficient indifferentiable hashing to elliptic curves of j-invariant 1728. Journal of Mathematical Cryptology **16**(1), 298–309 (2022)
18. Koshelev, D.: Hashing to elliptic curves through Cipolla–Lehmer–Müller's square root algorithm (2023), `https://eprint.iacr.org/2023/390`
19. Koshelev, D.: Some remarks on how to hash faster onto elliptic curves (2023), `https://eprint.iacr.org/2021/1082`
20. Koshelev, D.: Magma code (2024), `https://github.com/Dimitri-Koshelev/Simultaneously-simple-universal-and-indifferentiable-hashing-to-elliptic-curves`
21. Maitin-Shepard, J., Tibouchi, M., Aranha, D.F.: Elliptic curve multiset hash. The Computer Journal. Section D: Security in Computer Systems and Networks **60**(4), 476–490 (2017)
22. Maurer, U.M., Renner, R., Holenstein, C.: Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In: Naor, M. (ed.) Theory of Cryptography Conference. TCC 2004. Lecture Notes in Computer Science, vol. 2951, pp. 21–39. Springer, Berlin, Heidelberg (2004)
23. Menezes, A.J., Vanstone, S.A., Okamoto, T.: Reducing elliptic curve logarithms to logarithms in a finite field. In: STOC 1991: ACM Symposium on Theory of Computing. pp. 80–89. ACM Press, New York (1991)
24. Noether, S.: Understanding ge fromfe frombytes vartime, `https://www.getmonero.org/ru/resources/research-lab/pubs/ge_fromfe.pdf`
25. Pornin, T.: Faster complete formulas for the GLS254 binary curve (2023), `https://eprint.iacr.org/2023/1688`
26. van Saberhagen, N.: CryptoNote v 2.0 (2013), `https://bytecoin.org/old/whitepaper.pdf`
27. Sendra, J.R., Winkler, F., Pérez-Díaz, S.: Rational algebraic curves: A computer algebra approach, Algorithms and Computation in Mathematics, vol. 22. Springer, Berlin, Heidelberg (2008)
28. Shallue, A., van de Woestijne, C.E.: Construction of rational points on elliptic curves over finite fields. In: Hess, F., Pauli, S., Pohst, M. (eds.) Algorithmic Number Theory Symposium. ANTS 2006. Lecture Notes in Computer Science, vol. 4076, pp. 510–524. Springer, Berlin, Heidelberg (2006)

29. Skałba, M.: Points on elliptic curves over finite fields. Acta Arithmetica **117**(3), 293–301 (2005)
30. 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)
31. Tsfasman, M.A., Vlăduţ, S.G., Nogin, D.Y.: Algebraic geometric codes: Basic notions, Mathematical Surveys and Monographs, vol. 139. American Mathematical Society, Providence (2007)
32. 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 (CHES) **2019**(4), 154–179 (2019)

Appendix. How to avoid Legendre symbols in hashing to elliptic curves

As earlier, let E be an elliptic curve over a finite field $\mathbb{F}_q$ (of characteristic > 3). In the main part of the present article we established that there is always an *admissible* (in the sense of [6, Definition 4]) map $h : \mathbb{F}_q^2 \to E(\mathbb{F}_q)$ underlying an indifferentiable deterministic hash function $\mathcal{H}\colon \{0,1\}^* \to E(\mathbb{F}_q)$. Moreover, h requires to compute only one root in $\mathbb{F}_q$ and at worst two instances of the Legendre symbol $\left(\frac{\cdot}{q}\right)$. Unfortunately, fast constant-time algorithms (such as in [2]) of determining $\left(\frac{\cdot}{q}\right)$ are pretty complicated. Hence, being improperly implemented, they may be a potential source of leaking secret information inputted to $\mathcal{H}$. In this connection, it is desirable to completely avoid $\left(\frac{\cdot}{q}\right)$ (if possible) in the structure of $\mathcal{H}$.

It is worth emphasizing once again that admissible maps h (collected in [19, Table 1]) without Legendre (and any other) symbols have quite severe applicability restrictions. The current appendix explains how to circumvent them (almost for free) in the situation when after $\mathcal{H}$ comes a scalar multiplication on E. In other words, the overall computational task is to evaluate the function $[m] \circ \mathcal{H}$ for some scalar m (constant or variable, public or secret) of considerable size. This task arises when producing numerous cryptographic objects among which BLS signatures [7, Section 1.4.3] and key images [26, Section 4.4]. That is why the given batching strategy is really justified.

As is customary, E is of interest for ECC solely if there is a subgroup $G \subset E(\mathbb{F}_q)$ of large prime order r and of cofactor c such that $r \nmid c$. Typically, $c \leqslant 8$ for real-world non-pairing friendly curves, including the NIST standardized ones from [5, Section 3]. Clearly, the hash function $[c] \circ \mathcal{H}\colon \{0,1\}^* \to G$ is still indifferentible and deterministic (with a proper implementation of $[c]$). Therefore, it is usually enough to deal with hashing to E, abstracting from its concrete subgroup. Nevertheless, the below material concerns direct hashing to G because of inevitable technical details. Looking ahead, this material is relevant provided that c is moderate, namely $c = O(\sqrt{q})$. Curiously, the new batching technique partially resembles that of [19, Section 1.2] valid if E is a pairing-friendly curve and, conversely, c is huge, namely $c = \Omega(r)$.

Instead h, it is suggested to consider a map of the form $e\colon \mathbb{F}_q \to E(\mathbb{F}_q)$. Let's suppose that it is *α-weak* (for $\alpha \in \mathbb{N}$) in accordance with [4, Definition 5] (see also [21, Definition 4.1]). In particular, e is *α-bounded* (i.e., $\#e^{-1}(Q) \leqslant \alpha$ for each $Q \in E(\mathbb{F}_q)$) and so the image cardinality $\#\mathrm{Im}(e) \geqslant q/\alpha$. A state-of-the-art classification of such weak maps is exhibited in [19, Table 2], although there the weakness notion is not explicitly addressed. They are free of $\left(\frac{\cdot}{q}\right)$ in most cases, but still dependent on one radical in $\mathbb{F}_q$. Importantly, α is a small number for all maps from that classification. Whenever $j(E) \neq 0, 1728$, it is possible to take as e the *simplified Shallue–van de Woestijne(–Ulas) map* e_{sSWU} appeared originally in [4, Section 7] and optimized in [32, Section 4]. In the case of e_{sSWU}, the bound $\alpha = 8$ according to [4, Lemma 6] and, in fact, $\alpha = 4$ if the sign of the resulting y-coordinate is taken into account.

As we know from [30], maps e are not itself *regular* unless E is a supersingular curve. We are thus forced to search for an alternative for e to serve ordinary curves. There is a series of widespread regular (mostly $\left(\frac{\cdot}{q}\right)$-free) maps to G:

$$\begin{aligned}
&F_0\colon \mathbb{F}_r \to G && n \mapsto [n]P_0,\\
&F_1\colon V \to G && (t,n) \mapsto [c]e(t) + [n]P_0,\\
&F_2\colon \mathbb{F}_q^2 \to G && (t_1,t_2) \mapsto [c]\big(e(t_1) + e(t_2)\big),
\end{aligned}$$

where $P_0 \in G$ is a non-zero fixed point and $V := \mathbb{F}_q \times \mathbb{F}_r$. These maps can be found in any detailed survey of hash-to-curve functions, for example in [4, Section 1]. Note that the index i in the notation F_i means the copy number of e in the structure of F_i.

Consider the one more map

$$F\colon V \to G \qquad (t,n) \mapsto [nc]e(t).$$

Despite its simple shape, the author has never met this map anywhere in the literature. For compactness, let's also label the infinity point $\mathcal{O} := (0:1:0)$ and the complementary subgroup $G' := E(\mathbb{F}_q)/G$ of order c.

Theorem 3. *If e is an α-bounded map, then F is an ϵ-regular map with $\epsilon = 2c\alpha/q$.*

Proof. Given $P \in G$ and $n \in \mathbb{F}_r$, the inverse image

$$[nc]^{-1}(P) = \begin{cases} [(nc)^{-1}]P + G' & \text{if} \quad n \neq 0,\\ \emptyset & \text{if} \quad n = 0 \text{ and } P \neq \mathcal{O},\\ E(\mathbb{F}_q) & \text{if} \quad n = 0 \text{ and } P = \mathcal{O}. \end{cases}$$

Consequently,

$$U := \bigcup_{n \in \mathbb{F}_r} [nc]^{-1}(P) = \begin{cases} E(\mathbb{F}_q) \setminus G' & \text{if} \quad P \neq \mathcal{O},\\ E(\mathbb{F}_q) & \text{if} \quad P = \mathcal{O} \end{cases}$$

and thereby

$$e^{-1}(U) = \begin{cases} \mathbb{F}_q \setminus e^{-1}(G') & \text{if} \quad P \neq \mathcal{O}, \\ \mathbb{F}_q & \text{if} \quad P = \mathcal{O}. \end{cases}$$

It is readily seen that U is in reality a disjoint union $\sqcup$ when $P \neq \mathcal{O}$. In other words, the projection $V \to \mathbb{F}_q$ is bijective between the sets $F^{-1}(P)$ and $e^{-1}(U)$. Note that

$$0 \leqslant \#e^{-1}(G') \leqslant c\alpha \qquad \text{and so} \qquad q - c\alpha \leqslant \#F^{-1}(P) \leqslant q.$$

Meanwhile, $[nc]^{-1}(\mathcal{O}) = G'$ for each $n \in \mathbb{F}_r^*$, which leads to

$$F^{-1}(\mathcal{O}) = \big(\mathbb{F}_q \times \{0\}\big) \sqcup \big(e^{-1}(G') \times \mathbb{F}_r^*\big), \qquad q \leqslant \#F^{-1}(\mathcal{O}) \leqslant q + c\alpha(r-1).$$

This means that

$$\big|\#F^{-1}(P) - q\big| \leqslant \begin{cases} c\alpha & \text{if} \quad P \neq \mathcal{O}, \\ c\alpha(r-1) & \text{if} \quad P = \mathcal{O}. \end{cases}$$

As a result, the sum of

$$\delta(P) := \left| \frac{\#F^{-1}(P)}{\#V} - \frac{1}{\#G} \right| = \frac{\big|\#F^{-1}(P) - q\big|}{qr}$$

is equal to

$$\sum_{P \in G} \delta(P) = \sum_{P \neq \mathcal{O}} \delta(P) + \delta(\mathcal{O}) \leqslant 2(r-1)\frac{c\alpha}{qr} \leqslant 2\frac{c\alpha}{q}.$$

This fits the regularity definition represented, e.g., in [4, Equality (3)]. □

Corollary 4. *Assume that $c = O(\sqrt{q})$, $\alpha = O(1)$, and e is an α-weak map. Then, F is an admissible map and hence the hash function $\mathcal{H} = F \circ \eta\colon \{0,1\}^* \to G$ is indifferentiable whenever so is $\eta\colon \{0,1\}^* \to V$.*

Proof. By virtue of the last theorem, F is ϵ-regular with $\epsilon = O(q^{-1/2})$ (cf. Corollary 1) for the assumed values c, α. This is a sufficient bound on ϵ to satisfy the inequality $\log_2(\epsilon) \lesssim -\lambda$ in view of the classical one $\log_2(q) \gtrsim 2\lambda$, where λ (typically, ≈ 128) is a desirable security level. The given formalization of negligibility for ϵ is first introduced in [19, Section 1.2]. Besides, F is obviously computable in constant time, since weakness of e includes this aspect.

In a nutshell, samplability of F follows from that of e. To be definite, suppose that a point $P \in G$ is different from $\mathcal{O}$. Nothing prevents from sampling uniformly at random $n \in \mathbb{F}_r^*$ and $Q \in [nc]^{-1}(P)$. This is readily done, because it is elementary to determine (in precomputations) at most two generators of G' (and thereby of $E(\mathbb{F}_q) = G \times G'$). Therefore, $Q - [(nc)^{-1}]P$ is one of their linear combinations with samplable coefficients.

At worst, the whole subgroup G' lies in $\mathrm{Im}(e)$, hence

$$\#\big(U \cap \mathrm{Im}(e)\big) \geqslant \#\mathrm{Im}(e) - \#G' \geqslant \frac{q}{\alpha} - c.$$

With the (large) probability

$$\frac{\#\big(U \cap \mathrm{Im}(e)\big)}{\#U} \geqslant \frac{q/\alpha - c}{\#E(\mathbb{F}_q)} = \frac{q - c\alpha}{\alpha\big(q + O(\sqrt{q})\big)} \approx \frac{1}{\alpha},$$

the point $Q \in \mathrm{Im}(e)$. Otherwise, one just tries the other n and Q. It remains to pick uniformly at random $t \in e^{-1}(Q)$, getting ultimately $(t, n) \in F^{-1}(P)$.

The above reasoning can be evidently formalized by analogy with [4, Algorithm 1]. Without any obstacles, the case $P = \mathcal{O}$ is processed separately in a similar way. This finishes the proof of admissibility for F, which as usual implies (see, e.g., [4, Theorem 1]) indifferentiabitity for $\mathcal{H}$. □

It is time to discuss advantages of the new construction F compared to the previous ones F_i. Clearly, F is a modification of F_0 in which the base point is variable. The fixed point P_0 is responsible for why F_0 is vulnerable to a catastrophic attack mentioned in [7, Section 8.1] and at the end of [11, Section 1.1]. It is easily checked that (at least) this attack does not work at all for F. Moreover, the map F_0 is not admissible (namely not samplable), because the discrete logarithm $\log_{P_0}(P) \in \mathbb{F}_r$ is unknown for a general point $P \in G$.

In turn, the maps F_1, F_2 are admissible and widely recognized to be reliable. Nonetheless, they cannot be efficiently batched with a subsequent scalar multiplication $[m]$ in G, where $m \in \mathbb{F}_r$. Meanwhile, for computing $[m] \circ F(t, n)$, it is enough to perform one additional (cheap) multiplication $N := m(nc)$ in the field $\mathbb{F}_r$, since the sought point is expressed as $[N]e(t)$. Thus, we manage to get by with only one scalar multiplication.

In conclusion, it is worth stating explicitly that the new map F is itself an order of magnitude slower than the SwiftEC(-like) map $[c] \circ h_2$, because the same holds true when comparing $[n]$ with two $\big(\frac{\cdot}{q}\big)$. As a result, F is meaningless if a hash function $\mathcal{H}$ is a standalone primitive (or m is small) in a cryptographic scheme. This is the case, e.g., for multiset hashing. However, it is in reality sufficient (owing to [21, Section 4.1, Appendix A]) for this hashing type to employ a weak map e instead of an admissible one. Offhand, it is hard to remember a scheme that requires $\mathcal{H}$ to be simultaneously indifferentiable, deterministic, and not followed by a scalar multiplication. By reason of F, the SwiftEC(-like) map is thereby a slightly less significant achievement than it seems at first glance.