Indifferentiable Hashing to Barreto–Naehrig Curves

Pierre-Alain Fouque, Mehdi Tibouchi

Indifferentiable Hashing to Barreto–Naehrig Curves

Pierre-Alain Fouque[1] and Mehdi Tibouchi[2]

[1] École normale supérieure and INRIA Rennes
pierre-alain.fouque@ens.fr
[2] NTT Secure Platform Laboratories
tibouchi.mehdi@lab.ntt.co.jp

Abstract. A number of recent works have considered the problem of constructing constant-time hash functions to various families of elliptic curves over finite fields. In the relevant literature, it has been occasionally asserted that constant-time hashing to certain special elliptic curves, in particular so-called BN elliptic curves, was an open problem. It turns out, however, that a suitably general encoding function was constructed by Shallue and van de Woestijne back in 2006.

In this paper, we show that, by specializing the construction of Shallue and van de Woestijne to BN curves, one obtains an encoding function that can be implemented rather efficiently and securely, that reaches about 9/16ths of all points on the curve, and that is *well-distributed* in the sense of Farashahi *et al.*, so that one can easily build from it a hash function that is indifferentiable from a random oracle.

Keywords: Elliptic curve cryptography, BN curves, hashing, random oracle.

1 Introduction

Many elliptic curve-based cryptographic protocols require hashing to an elliptic curve group $\mathbb{G}$: they involve one or more hash functions $\mathfrak{H} : \{0,1\}^* \to \mathbb{G}$ mapping arbitrary values to points on the elliptic curve.

For example, in the Boneh-Franklin identity-based encryption scheme [6], the public key for identity $\mathrm{id} \in \{0,1\}^*$ is a point $\mathbf{Q}_{\mathrm{id}} = \mathfrak{H}(\mathrm{id})$ on the curve. This is also the case in many other pairing-based cryptosystems including IBE and HIBE schemes [1,22,23], signature and identity-based signature schemes [5,7,8,13,39] and identity-based signcryption schemes [10,29].

Hashing into elliptic curves is also required for some passwords-based authentication protocols such as the SPEKE [25] and PAK [11] protocols, as well as various signature schemes based on the hardness of the discrete logarithm problem, like [14], when they are instantiated over elliptic curves.

In all of those cases, the hash functions are modeled as random oracles in security proofs. However, it is not clear how such a hash function can be instantiated in practice. Indeed, random oracles to groups like $\mathbb{Z}_p^*$ can be easily

constructed from random oracles to fixed-length bit strings, for which conventional cryptographic hash functions usually provide acceptable substitutes. On the other hand, constructing random oracles to an elliptic curve even from random oracles to bit strings appears difficult in general, and some of the more obvious instantiations actually break security completely.

For example, to construct a hash function $\mathfrak{H} : \{0,1\}^* \to \mathbb{G}$ to an elliptic curve cyclic group $\mathbb{G}$ of order N and generated by a given point $\mathbf{G}$, a simple idea might be to choose $\mathfrak{H}(m) = [\mathfrak{h}(m)] \cdot \mathbf{G}$, where $\mathfrak{h}$ is a hash function $\{0,1\}^* \to \mathbb{Z}_N$. However, this typically breaks security proofs in the random oracle model. Suppose the proof involves programming the random oracle $\mathfrak{H}$ by choosing its value $\mathbf{P}$ on some input m_0. If we instantiate $\mathfrak{H}$ in this naive way, the programming stage requires setting $\mathfrak{h}(m_0)$ to the discrete logarithm of $\mathbf{P}$, which is normally unknown. In fact, in the case of a primitive like BLS signatures [9], this instantiation leads to very simple and devastating attacks (see the discussions in [37, Ch. 3] or [38]).

In their original short signatures paper [8], Boneh, Lynn and Shacham introduced the first generic construction of a secure hash function to elliptic curves, in the sense that it applies to any target elliptic curve: the so-called "try-and-increment" algorithm. Basically, to hash a message m, one concatenates it with a fixed-length counter c initialized to 0 and computes $\mathfrak{h}(c\|m)$, where $\mathfrak{h}$ is a hash function to the base field of the elliptic curve. If that digest value is the abscissa of a point on the curve, $\mathfrak{H}(m)$ is set to that point; otherwise, one increments the counter c and tries again. This construction can be shown to be secure provided that the counter length is large enough; however, it is somewhat inefficient, since one may need many iterations before finding a suitable point, and the fact that the length of the computation depends on the input yields to possible side-channel attacks, especially in protocols such as password authenticated key exchange (a concrete attack is given is [38] for a variant of SPEKE [25]).

In response, more robust, "constant-time" methods have been proposed, starting with a paper by Icart at CRYPTO 2009 [24], and including a number of extensions, generalizations and refinements afterwards [33,12,19,27,16,15]. In essence, these methods are all based on the construction of a suitable algebraic or piecewise algebraic function from the affine line to the target elliptic curve.

Our contributions. None of the methods mentioned above is fully generic: they all rely on certain arithmetic or geometric properties of the target curve. Some involve taking arbitrary cube roots in the base field $\mathbb{F}_q$, for example, and hence only apply to the case when $q \equiv 2 \pmod 3$. The remaining ones only work for curves of nonzero j-invariant. In particular, none of those more efficient encodings yield a construction of hash functions to the very important class of Barreto–Naehrig (BN) elliptic curves [3], which are the preferred curves for implementing asymmetric pairings nowadays, as they provide essentially optimal parameters for the 128-bit security level. This has led several authors to assert that constant-time hashing to BN curves was an open problem [19,31].

It turns out, however, that several years prior to Icart's work, Shallue and van de Woestijne had presented a construction [35] that applies to all curves of odd characteristic, as pointed out in [38]. This paper is devoted to making that construction explicit in the case of BN curves, and establishing some properties of it. More precisely, our contributions are as follows:

- we propose an explicit, optimized definition of the Shallue–van de Woestijne encoding to a BN elliptic curve (in Section 3);
- using an extension of the technique from [18,20], we establish an estimate for the number of points in the image of that encoding (in Section 4): we find that the encoding reaches about 9/16ths of all points on the curve;
- like Icart's encoding and many others, this encoding f will not yield a generically secure hash function construction if we simply compose it with a random oracle to the base field (e.g. it is easy to distinguish such a hash function from a random oracle to the curve since its image has a simple algebraic description and only contains a constant fraction of all points). However, we show (in Section 5) that it is *well-distributed* in the sense of Farashahi *et al.* [17]. This implies that if $\mathfrak{h}_1$, $\mathfrak{h}_2$ are random oracles to the base field, then $m \mapsto f\big(\mathfrak{h}_1(m)\big) + f\big(\mathfrak{h}_2(m)\big)$ is a good, generically secure hash function to the BN curve (it is *indifferentiable* from a random oracle);
- finally, we also suggest (in Section 6) a way to implement this encoding function that should thwart side-channel analysis and other physical attacks.

Our approach to establishing the results of Sections 4 and 5, while quite technical, is also of independent interest. Indeed, the Shallue–van de Woestijne encoding fits in a family of various encoding functions to elliptic curves based on works by Schinzel and Skałba [34,36], and while Fouque and Tibouchi [20] and Farashahi *et al.* [17] did tackle a function of that type before, they had to consider only a special case and tweak the formulas significantly, so as to simplify the computations. In this paper, we show how image size estimates and well-distributedness can be obtained for this type of encoding functions without simplifications or generality loss.

Our results apply almost without change to any elliptic curve of the form $y^2 = x^3 + b$ with $b \neq -1$ over a finite field $\mathbb{F}_q$ with $q \equiv 7 \pmod{12}$. Pairing-friendly curves obtained by the CM method for discriminant -3 are typically of that form: this includes in particular the curves constructed by Barreto, Lynn and Scott in [2, §3.1] and the curves of embedding degree 18 and 36 obtained by Kachisa, Schaefer and Scott in [26], all of which are recommended for pairing implementations at higher security levels (192 to 256-bit security). The elliptic curve group in those cases is not usually of prime order, however (those cases have $\rho > 1$), so hashing to the prime order subgroup requires multiplying the point obtained with the technique described herein by the cofactor. This does not affect indifferentiability, as was shown in [12, §6.1].

Notation. In the paper, p will always be an odd prime and q an odd prime power. In $\mathbb{F}_q$, the finite field with q elements, we denote by $\chi_q \colon \mathbb{F}_q \to \{-1, 0, 1\}$

the nontrivial quadratic character of $\mathbb{F}_q^*$ extended by zero to $\mathbb{F}_q$ (i.e. $\chi_q(0) = 0$ and for $a \neq 0$, $\chi_q(a) = 1$ if a is a square and -1 otherwise). When $q \equiv 3 \pmod 4$, we write $\sqrt{a} = a^{(q+1)/4}$ for any square $a \in \mathbb{F}_q$.

2 Preliminaries

2.1 Barreto–Naehrig elliptic curves

BN curves are a family of pairing-friendly elliptic curves over large prime fields, introduced in 2005 by Barreto and Naehrig [3]. They are one of the preferred families for implementing asymmetric pairings nowadays, as they achieve essentially optimal parameters for obtaining bilinear groups at the 128-bit security level. Indeed, BN curves are of prime order (in particular they satisfy $\rho = 1$) and embedding degree $k = 12$; thus, the pairing on a BN curve over a 256-bit prime field $\mathbb{F}_p$ takes its values in the field $\mathbb{F}_{p^{12}}$ of size $256 \times 12 = 3072$. Then, solving the discrete logarithm problem both in the group of points of the curve and in $\mathbb{F}_{p^k}^\times$ takes time about 2^{128} as required [3].

The details of the construction of BN curves, based on the CM method, is not really relevant for our purposes. Suffice it to say that Barreto and Naehrig's algorithm outputs an elliptic curve of the form:

$$E\colon y^2 = x^3 + b \tag{1}$$

over a field $\mathbb{F}_p$ with $p \equiv 1 \pmod 3$ (for convenience, they suggest to pick a p satisfying, more precisely, $p \equiv 31 \pmod{36}$), such that $\#E(\mathbb{F}_p)$ is prime, together with the generator[3] $\mathbf{G} = (1, \sqrt{b+1} \bmod p) \in E(\mathbb{F}_p)$. Moreover, b is typically a very small integer (the smallest > 0 such that $b + 1$ is a quadratic residue mod p).

2.2 Chebotarev density theorem

In [18,20], Farashahi, Shparlinski and Voloch on the one hand, and Fouque and Tibouchi on the other, proposed an approach to counting the number of points in the image of an elliptic curve encoding function, based on the Chebotarev density theorem for function fields. We will apply a similar technique to the encoding to BN curves presented hereafter, and will therefore need an effective version of the Chebotarev density theorem. One such version is given in [21, Proposition 6.4.8], and if we specialize it to our cases of interest, we obtain:

Lemma 1 (Chebotarev). *Let K be an extension of $\mathbb{F}_q(x)$ of degree $d < \infty$ and L a Galois extension of K of degree $m < \infty$. Assume $\mathbb{F}_q$ is algebraically closed in L, and fix some subset $\mathscr{S}$ of $\mathrm{Gal}(L/K)$ stable under conjugation. Let*

[3] Later works such as [31] use a different point as the generator, and the corresponding construction does no longer ensure that $1 + b$ is a square. This only causes a minor inconvenience for our purposes, namely two extra elements of $\mathbb{F}_q$ that have to be treated separately in the encoding given in Section 3.

$s = \#\mathscr{S}$ and $N(\mathscr{S})$ the number of places v of K of degree 1, unramified in L, such that the Artin symbol $\left(\frac{L/K}{v}\right)$ (defined up to conjugation) is in $\mathscr{S}$. Then

$$\left|N(\mathscr{S}) - \frac{s}{m}q\right| \leq \frac{2s}{m}\big((m+g_L)\cdot q^{1/2} + m(2g_K+1)\cdot q^{1/4} + g_L + dm\big)$$

where g_K and g_L are the genera of the function fields K and L.

2.3 Admissible encodings and indifferentiability

Brier *et al.* [12] use Maurer's indifferentiability framework [30] to analyze the conditions under which their hash function constructions can be plugged into essentially any scheme[4] that is proved secure in the random oracle model in such a way that the proof of security goes through. As shown by Maurer, it suffices that the hash function construction be indifferentiable from a random oracle.

Then, Brier *et al.* [12] establish a sufficient condition for a hash function construction into an elliptic curve E to be indifferentiable from a random oracle. It applies to hash functions of the form:

$$\mathfrak{H}(m) = F(\mathfrak{h}(m)),$$

where $F\colon S \to E(\mathbb{F}_q)$ is a deterministic encoding, and $\mathfrak{h}$ is seen as a random oracle to S. Assuming that $\mathfrak{h}$ is a random oracle, the construction is indifferentiable whenever F is an *admissible encoding* into $E(\mathbb{F}_q)$, in the sense that it satisfies the following properties:

1. Computable: F is computable in deterministic polynomial time;
2. Regular: for s uniformly distributed in S, the distribution of $F(s)$ is statistically indistinguishable from the uniform distribution in $E(\mathbb{F}_q)$;
3. Samplable: there is an efficient randomized algorithm $\mathscr{I}$ such that for any $\mathbf{P} \in E(\mathbb{F}_q)$, the distribution of $\mathscr{I}(\mathbf{P})$ is statistically indistinguishable from the uniform distribution in $F^{-1}(\mathbf{P})$.

2.4 Well-distributed elliptic curve encodings

Building upon this work by Brier *et al.*, Farashahi *et al.* introduced a general framework [17] to obtain well-behaved hash function construction to elliptic and hyperelliptic curves. The main notion in that framework is that of a *well-distributed* encoding. In the case of an elliptic curve E, it is defined as follows.

[4] It has recently been pointed out by Ristenpart, Shacham and Shrimpton [32] that this type of composition result does not apply to literally *all* cryptographic protocols, but only those which admit so-called "single-stage security proofs". This is not a significant restriction for the purpose at hand, as all protocols constructed so far using elliptic curve-valued hashing satisfy that requirement.

Definition 1 (Farashahi *et al.*). *A function $f\colon \mathbb{F}_q \to E(\mathbb{F}_q)$ is said to be B-well-distributed for some $B > 0$ if, for all nontrivial characters χ of $E(\mathbb{F}_q)$, the following bound holds:*

$$|S_f(\chi)| \leq B\sqrt{q}, \quad \textit{where} \quad S_f(\chi) = \sum_{u \in \mathbb{F}_q} \chi\big(f(u)\big). \tag{2}$$

Let $f\colon \mathbb{F}_q \to E(\mathbb{F}_q)$ be a well-distributed encoding to the elliptic curve E. Then Farashahi *et al.* prove that the tensor square $f^{\otimes 2}\colon \mathbb{F}_q^2 \to E(\mathbb{F}_q)$ defined by $f^{\otimes 2}(u, v) = f(u) + f(v)$ is a *regular* encoding to $E(\mathbb{F}_q)$. More precisely, the statistical distance between the distribution defined by $f^{\otimes 2}$ on $E(\mathbb{F}_q)$ and the uniform distribution is bounded above by $B^2 \cdot \sqrt{\#E(\mathbb{F}_q)}/q$, which is negligible.

If the function f is also efficiently computable and samplable in the sense of Section 2.3, then $f^{\otimes 2}$ is *admissible*, which implies that the hash function:

$$m \mapsto f\big(\mathfrak{h}_1(m)\big) + f\big(\mathfrak{h}_2(m)\big)$$

is indifferentiable from a random oracle, and hence can be used in lieu of a random oracle to $E(\mathbb{F}_q)$ in essentially any scheme proved secure in the random oracle model.

Another important result of [17] is the following consequence of the Riemann hypothesis for curves, which makes it possible to establish the bound (2) in practice.

Lemma 2 ([17, Th. 7]). *Let $h : X \to E$ be a non constant morphism to the elliptic curve E, and χ be any nontrivial character of $E(\mathbb{F}_q)$. Assume that h does not factor through a nontrivial unramified morphism $Z \to E$. Then:*

$$\left| \sum_{\mathsf{P} \in X(\mathbb{F}_q)} \chi(h(P)) \right| \leq (2g_X - 2)\sqrt{q} \tag{3}$$

where g_X is the genus of X. Furthermore, if φ is a non constant rational function on X:

$$\left| \sum_{\mathsf{P} \in X(\mathbb{F}_q)} \chi(h(P)) \cdot \chi_q(\varphi(\mathsf{P})) \right| \leq (2g_X - 2 + 2\deg\varphi)\sqrt{q}. \tag{4}$$

2.5 The Shallue–van de Woestijne encoding

Let E be any elliptic curve over a finite field $\mathbb{F}_q$ of odd characteristic with $\#\mathbb{F}_q > 5$, written is Weierstrass form:

$$E\colon y^2 = g(x) = x^3 + Ax^2 + Bx + C.$$

Shallue and van de Woestijne [35] construct an encoding function $f\colon \mathbb{F}_q \to E(\mathbb{F}_q)$ as follows.

Following the ideas of Schinzel and Skałba [34,36], they first introduce the algebraic threefold $V \subset \mathbb{P}^4$ with affine equation

$$V\colon y^2 = g(x_1) \cdot g(x_2) \cdot g(x_3),$$

and observe that if (x_1, x_2, x_3, y) is an $\mathbb{F}_q$-rational point on V, then at least one of x_1, x_2, x_3 is the abscissa of a point in $E(\mathbb{F}_q)$. Indeed, the product $g(x_1) \cdot g(x_2) \cdot g(x_3) \in \mathbb{F}_q$ is a square, so at least one of the factors must be square as well. Then, they establish the following result.

Lemma 3 ([35, Lemma 6]). *Put $h(u, v) = u^2 + uv + v^2 + A(u + v) + B$, and define:*

$$\begin{aligned} &S\colon y^2 \cdot h(u, v) = -g(u), \\ &\psi\colon (u, v, y) \mapsto \big(v, -A - u - v, u + y^2, g(u + y^2) \cdot h(u, v) \cdot y^{-1}\big). \end{aligned}$$

Then ψ is a rational map from the surface S to V that is invertible on its image.

In particular, any point in $S(\mathbb{F}_q)$ where ψ is well-defined (i.e. satisfying $y \neq 0$) maps to a point in $V(\mathbb{F}_q)$, and hence yields a point in $E(\mathbb{F}_q)$. Finally, to construct points on S, the authors of [35] note that any plane section of S of the form $u = u_0$ is birational to a conic, which is non-degenerate as long as:

$$g(u_0) \neq 0 \quad \text{and} \quad 3u_0^2 + 2Au_0 + 4B - A^2 \neq 0. \tag{5}$$

If we fix one such value u_0 (it necessarily exists since $\#\mathbb{F}_q > 5$), the corresponding conic admits a rational parametrization, which gives a rational map $\phi\colon \mathbb{A}^1 \to S$.

The encoding function $f\colon \mathbb{F}_q \to E(\mathbb{F}_q)$ is then obtained as mapping a point $t \in \mathbb{F}_q$ to one of the points on $E(\mathbb{F}_q)$ of abscissa x_i, where $\psi \circ \phi(t) = (x_1, x_2, x_3, y)$ and $i \in \{1, 2, 3\}$ is the smallest index such that $g(x_i)$ is a square.

In the following sections, we make that function f explicit when E is a BN curve as in Section 2.1 (or rather, belongs to a class of elliptic curves that contains BN curves), and establish a number of its properties.

3 An Encoding to BN Curves

Let us apply the previous construction to the case of an elliptic curve of the form:

$$E\colon y^2 = g(x) = x^3 + b$$

over a field $\mathbb{F}_q$ of characteristic ≥ 5. We also assume that $q \equiv 7 \pmod{12}$ and that $g(1) = 1 + b$ is a nonzero square in $\mathbb{F}_q$. As seen in Section 2.1, all those properties are in particular satisfied for BN curves.[5]

[5] Technically, one can consider BN curves over fields $\mathbb{F}_p$ with $p \equiv 1 \pmod{12}$ as well, but they are usually avoided in practice, as the condition $p \equiv 3 \pmod{4}$ makes square roots more convenient to compute.

The equation of the surface S defined in Section 2.5 becomes:

$$S\colon y^2 \cdot (u^2 + uv + v^2) = -u^3 - b.$$

We consider its section by the plane of equation $u = u_0 = 1$. This gives a curve of equation:

$$y^2 \cdot \left(\frac{3}{4} + \left(v + \frac{1}{2}\right)^2\right) = -1 - b,$$

and by setting $z = v + 1/2$ and $w = 1/y$, we see that it is birational to the conic:

$$z^2 + (1+b)w^2 = -\frac{3}{4}, \tag{6}$$

which is non-degenerate since $g(1) = 1+b \neq 0$. We can give a convenient rational parametrization of that conic as follows. Since $q \equiv 1 \pmod 3$, (-3) is a quadratic residue in $\mathbb{F}_q$. Thus, $(z_0, w_0) = (\sqrt{-3}/2, 0)$ is an $\mathbb{F}_q$-rational point on the conic (6). We parametrize all the other points by setting $z = z_0 + tw$, which gives:

$$\sqrt{-3} \cdot t + t^2 \cdot w + (1+b) \cdot w = 0,$$

and hence:

$$\begin{aligned} y &= \frac{1}{w} = -\frac{1+b+t^2}{\sqrt{-3} \cdot t} \\ v &= z_0 + tw - 1 = \frac{-1+\sqrt{-3}}{2} + \frac{\sqrt{-3} \cdot t^2}{1+b+t^2}. \end{aligned}$$

This is well-defined (and y is nonzero) if and only if $t \neq 0$ and $t^2 \neq -1-b$, and the second condition is always verified since $\chi_q(-1-b) = -\chi_q(1+b) = -1$. Thus, for any $t \neq 0$, it follows from Lemma 3 that at least one of the three values:

$$x_1 = v = \frac{-1+\sqrt{-3}}{2} - \frac{\sqrt{-3} \cdot t^2}{1+b+t^2}, \tag{7}$$

$$x_2 = -1 - v = \frac{-1-\sqrt{-3}}{2} + \frac{\sqrt{-3} \cdot t^2}{1+b+t^2}, \tag{8}$$

$$x_3 = 1 + y^2 = 1 - \frac{(1+b+t^2)^2}{3t^2} \tag{9}$$

is the abscissa of a point in $E(\mathbb{F}_q)$. Furthermore, we see that these values only depend on t^2, and hence are invariant under a change of sign for t. As a result, it is natural to map t and $-t$ to opposite points on $E(\mathbb{F}_q)$ with one of the previous coordinates.

Therefore, we can define the Shallue–van de Woestijne encoding to the BN curve E as follows.

Definition 2. *For all $t \in \mathbb{F}_q^*$, let $x_1, x_2, x_3 \in \mathbb{F}_q$ be as in Eqs.* (7) *to* (9)*. The* SW encoding *to the BN curve E is the map:*

$$\begin{aligned} f\colon \mathbb{F}_q^* &\longrightarrow E(\mathbb{F}_q) \\ t &\longmapsto \Big(x_i,\ \chi_q(t) \cdot \sqrt{g(x_i)}\Big), \end{aligned}$$

where for each t, $i \in \{1,2,3\}$ is the smallest index such that $g(x_i)$ is a square in $\mathbb{F}_q$.

The encoding can be extended to all of $\mathbb{F}_q$ by sending 0 to some arbitrary point in $E(\mathbb{F}_q)$. Since x_1 is well-defined and equal to $(-1+\sqrt{-3})/2$ for $t = 0$, and $g(x_1) = 1 + b$ is a square, a relatively natural choice may be to set:

$$f(0) = \left(\frac{-1+\sqrt{-3}}{2},\ \sqrt{1+b}\right).$$

4 Computing the Image Size

In this section, we estimate the number of points in the image of the Shallue–van de Woestijne encoding f to $E(\mathbb{F}_q)$, using a refinement of the techniques from [18,20]. We will show that f reaches roughly 9/16ths of all points on the curve, or more precisely, that $\#f(\mathbb{F}_q^*) = (9/16) \cdot q + O(\sqrt{q})$ (where the constant in the big-O is universal and will be made explicit).

To obtain that estimate, we first write $\mathbb{F}_q^*$ as the disjoint union of the subsets T_1, T_2, T_3 of field elements t such that the corresponding index i in Definition 2 is 1, 2, 3 respectively. In other words:

$$\begin{aligned} T_1 &= \{t \in \mathbb{F}_q^* \mid g(x_1) \text{ is a square}\}; \\ T_2 &= \{t \in \mathbb{F}_q^* \mid g(x_1) \text{ is not a square but } g(x_2) \text{ is}\}; \\ T_3 &= \{t \in \mathbb{F}_q^* \mid \text{neither } g(x_1) \text{ nor } g(x_2) \text{ are squares}\}. \end{aligned}$$

Then, we examine the points in $f(T_i)$ for $i = 1, 2, 3$.

Clearly, a point $(x, y) \in f(T_1)$ satisfies:

$$x = x_1(t) = \frac{-1+\sqrt{-3}}{2} - \frac{\sqrt{-3} \cdot t^2}{1 + b + t^2}$$

for some $t \neq 0$, or equivalently:

$$t^2 = -\frac{(1+b) \cdot (x - \zeta)}{x - \zeta^2} \quad \text{where} \quad \zeta = \frac{-1+\sqrt{-3}}{2}. \tag{10}$$

We denote by $\omega_1 \in \mathbb{F}_q(x)$ the rational function on the right-hand side of Eq. (10). The set $f(T_1)$ is thus contained in the set of points $(x, y) \in E(\mathbb{F}_q)$ such that ω_1 is a nonzero square. And conversely, if $(x, y) \in E(\mathbb{F}_q)$ satisfies that $\omega_1 = t^2$ for some $t \neq 0$, we get $x = x_1(t)$ and hence $(x, y) = f(t)$ or $f(-t)$ depending on the sign of $\chi_q(y)$.

Thus, we obtain that $f(T_1)$ is the set of points $(x, y) \in E(\mathbb{F}_q)$ such that ω_1 is a nonzero square. If we denote by K the function field of E, this set is thus in bijection with the set of places of degree 1 in K that split in the quadratic extension L_1/K with $L_1 = K[t]/(t^2 - \omega_1)$. We can thus apply Lemma 1 with $s = 1$ and $m = d = 2$ to get:

$$\left| \#f(T_1) - \frac{1}{2}q \right| \leq (2 + g_{L_1}) \cdot q^{1/2} + 6q^{1/4} + g_{L_1} + 4,$$

where g_{L_1} is the genus of the function field L_1. After extending the field of scalars to $\overline{\mathbb{F}}_q$, we can see that L_1 is ramified above exactly 4 places of K (corresponding to the two opposite points in $E(\overline{\mathbb{F}}_q)$ where the rational function ω_1 vanishes and the two others where it has a pole), so the Riemann–Hurwitz formula gives $g_{L_1} = 3$. Hence:

$$\left| \#f(T_1) - \frac{1}{2}q \right| \leq 5q^{1/2} + 6q^{1/4} + 7. \tag{11}$$

Similarly, a point $(x, y) \in f(T_2)$ satisfies:

$$x = x_2(t) = \frac{-1 - \sqrt{-3}}{2} + \frac{\sqrt{-3} \cdot t^2}{1 + b + t^2},$$

for some $t \neq 0$, or equivalently:

$$t^2 = -\frac{(1 + b)(x - \zeta^2)}{x - \zeta} \quad \text{where, again,} \quad \zeta = \frac{-1 + \sqrt{-3}}{2}. \tag{12}$$

Thus, for any point $(x, y) \in f(T_2)$, the rational function ω_2 on the right-hand side of Eq. (12) is a nonzero square. But we clearly have:

$$\omega_1 = \frac{(1 + b)^2}{\omega_2},$$

and it follows that if ω_2 is a nonzero square, then so is ω_1. As a result, we must have $f(T_2) \subset f(T_1)$.[6] Therefore:

$$f(\mathbb{F}_q^*) = f(T_1) \cup f(T_2) \cup f(T_3) = f(T_1) \cup \big(f(T_3) \setminus f(T_1)\big)$$

and we can thus complete our estimate if we can evaluate the cardinality of $f(T_3) \setminus f(T_1)$.

Again, a point $(x, y) \in E(\mathbb{F}_q)$ is in $f(T_3)$ if and only if there exists some $t \in \mathbb{F}_q^*$ such that neither $g(x_1(t))$ nor $g(x_2(t))$ is a square, and $x = x_3(t) = 1 - (1 + b + t^2)^2/(3t^2)$. The last relation is equivalent to:

$$t^4 + \big[3(x - 1) + 2(1 + b)\big]t^2 + (1 + b)^2 = 0. \tag{13}$$

[6] It does not matter for our purposes, but that inclusion is usually strict: indeed, $f(T_2)$ is smaller that the set of points in $E(\mathbb{F}_q)$ with an abscissa of the form $x_2(t)$, because the corresponding parameter t must satisfy the additional condition that $g(x_1(t))$ is not a square.

As a biquadratic polynomial over the function field K of E, that polynomial in t, which we denote $P(t)$, is clearly irreducible and has Galois group V_4 (since its constant coefficient is a square; see [28, Th. 2 and 3]). In particular, $L'_3 = K[t]/(P)$ is a Galois extension of K, and its 4 automorphisms send t to $\pm t$ and $\pm(1+b)/t$.

Now, the set $f(T_3)$ is in bijection with the set of places of K where the polynomial P has at least one root t (necessarily nonzero; and in that case, P splits completely) that further satisfies that neither $g(x_1(t))$ nor $g(x_2(t))$ is a square, or equivalently, that both $-g(x_1(t))$ and $-g(x_2(t))$ are nonzero squares. By construction of the Shallue–van de Woestijne encoding, we know that $g(x_1(t)) \cdot g(x_2(t)) \cdot g(x_3(t))$ is a nonzero square for all $t \in \mathbb{F}_q^*$, so that for any t as above, $-g(x_1(t))$ is a nonzero square if and only if $-g(x_2(t))$ is a nonzero square. Furthermore, the automorphisms of $L'_3 = K[t]/(P)$ that send t to $\pm t$ fix x_1 and x_2, whereas those that send t to $\pm(1+b)/t$ exchange them, as we can see from the fact that $\omega_2 = (1+b)^2/\omega_1$. This ensures that the quadratic extension $L''_3 = L'_3[z]/\big(z^2 + g(x_1(t))\big)$ of L'_3 is in fact Galois of degree 8 over K, and $f(T_3)$ is in bijection with the set of places of K that split completely in L''_3.

Finally, an element $(x, y) \in f(T_3)$ is *not* in $f(T_1)$ exactly when ω_1 isn't a nonzero square, i.e. when $-\omega_1$ is a square. As a result, up to possibly two points where $-\omega_1$ vanishes, $f(T_3) \setminus f(T_1)$ has the same number of elements as the set of places in K which split completely in the compositum $L_3 = L''_3 \cdot K[w]/(w^2 + \omega_1)$ (a Galois extension of degree 16, since the two fields are linearly disjoint by inspection of their ramification, as seen below). Thus, we can apply Lemma 1 with $s = 1$, $d = 2$ and $m = 16$ to get:

$$\left| \#\big(f(T_3) \setminus f(T_1)\big) - \frac{1}{16}q \right| \leq \left(2 + \frac{g_{L_3}}{8}\right) \cdot q^{1/2} + 6q^{1/4} + \frac{g_{L_3}}{8} + 4 + 2,$$

where g_{L_3} is the genus of the function field L_3. To compute that genus, we examine the ramification of the various fields involved, after an extension of scalars to $\overline{\mathbb{F}}_q$. Clearly, $(\overline{\mathbb{F}}_q K)[w]/(w^2 + \omega_1)$ is simply ramified over the four places corresponding to the points in $E(\overline{\mathbb{F}}_q)$ with $x = \zeta$ or ζ^2. Thus, that field has genus 4 again. On the other hand, since the discriminant of P is:

$$\Delta = 48 \cdot (1+b)^2 \cdot (x-1)^2 \cdot \big(3(x-1) + 4(1+b)\big)^2,$$

the field $\overline{\mathbb{F}}_q L'_3$ is ramified with ramification type $(2, 2)$ over the places corresponding to the points in $E(\overline{\mathbb{F}}_q)$ with $x = 1$ or $x = -(1+4b)/3$. In turn, $\overline{\mathbb{F}}_q L''_3$ is ramified over the places in $\overline{\mathbb{F}}_q L'_3$ where $x_1(t)^3 = -b$ or $x_1(t) = \infty$. This gives 8 values of t, or 16 places of $\overline{\mathbb{F}}_q L'_3$ (since each value of t corresponds to one value of x and two of y). Putting everything together and using Abhyankar's lemma, we obtain that the ramification divisor of $\overline{\mathbb{F}}_q L_3$ over $\overline{\mathbb{F}}_q K$ has degree $4 \cdot 8 + (4 \cdot 2 \cdot 2 + 16) \cdot 2 = 96$. Thus, the Riemann–Hurwitz formula gives $2g_{L_3} - 2 = 16 \cdot 0 + 96$, hence $g_{L_3} = 49 < 7 \cdot 8$, and thus:

$$\left| \#\big(f(T_3) \setminus f(T_1)\big) - \frac{1}{16}q \right| \leq 9q^{1/2} + 6q^{1/4} + 13. \tag{14}$$

Combining Eqs. (11) and (14), we get the following result, as expected.

Theorem 1. *The number of points in the image $f(\mathbb{F}_q^*)$ of the Shallue–van de Woestijne encoding to a BN curve is bounded as:*

$$\left| \#f(\mathbb{F}_q^*) - \frac{9}{16}q \right| \leq 14q^{1/2} + 12q^{1/4} + 20.$$

Remark 1. While somewhat arbitrary, the numbering of the points x_1, x_2, x_3 in the definition of the Shallue–van de Woestijne encoding actually matters for the computation of the number of points: for example, it is not difficult to adapt the argument above to see that if the order was reversed, the image size would only be about $7/16 \cdot q$ instead of $9/16 \cdot q$.

5 Obtaining Indifferentiability

In this section, we prove that, while f itself is clearly not an admissible encoding in the sense of Section 2.3, the tensor square $f^{\otimes 2}$, as defined in Section 2.4, is indeed admissible, and hence the hash function:

$$m \mapsto f\big(\mathfrak{h}_1(m)\big) + f\big(\mathfrak{h}_2(m)\big) \tag{15}$$

is indifferentiable from a random oracle when $\mathfrak{h}_1, \mathfrak{h}_2$ are seen as independent random oracles to $\mathbb{F}_q^*$.

To see this, first note that $f^{\otimes 2}$ is obviously efficiently computable, and it is also samplable: a sketch of a sampling function is as follows. To find a uniformly random preimage (u, v) of some point $\mathbf{P} \in E(\mathbb{F}_q)$, pick $v \in \mathbb{F}_q^*$ at random, and find all the preimages of $\mathbf{P} - f(v)$ (which can be done by solving three algebraic equations, corresponding to the three "branches" of f). There are at most 4 such preimages. Then pick $i \in \{1, 2, 3, 4\}$ at random and return the i-th preimage if it exists. Otherwise, start over with another v. The image size computation of the previous section guarantees that the expected number of iterations is finite, which ensures samplability. See [4] for a complete formal treatment of the samplability of Icart's function, which is easily adapted to our case along the lines of the previous sketch.

Thus, all that remains to see to prove admissibility is that $f^{\otimes 2}$ is regular. We will show that using the results of Section 2.4, by proving that f is a *well-distributed* encoding. We have to bound the following sum:

$$S_f(\chi) = \sum_{t \in \mathbb{F}_q^*} \chi(f(t))$$

for every nontrivial character χ of $E(\mathbb{F}_q)$. As in the previous section, we break the sum into sums over T_1, T_2 and T_3 which we treat separately.

To estimate the sum over T_1, we introduce the covering curve $h_1 \colon X_1 \to E$ corresponding to the extension of function fields L_1/K (with the notation of Section 4). In other words, a rational point in $X_1(\mathbb{F}_q)$ is a tuple (x, y, t) such

that $(x, y) \in E(\mathbb{F}_q)$ and $x = x_1(t)$ (or equivalently $t^2 = \omega_1(x)$). In particular, for any $t \in T_1$, there are two rational points of X_1 whose third coordinate is t: if we let $(x, y) = f(t)$, these two points are (x, y, t) and $(x, -y, t)$, which map to $\chi(f(t))$ and $\chi(f(t))^{-1}$ under $\chi \circ h_1$. Thus, we get:

$$\sum_{\mathbf{P} \in X_1(\mathbb{F}_q)} \chi(h_1(\mathbf{P})) = \sum_{t \in T_1} \chi(f(t)) + \sum_{t \in T_1} \chi(f(t))^{-1} + O(1),$$

where the constant $O(1)$ accounts for a bounded number of exceptional points (ramification, points at infinity). We would like to get rid of the second sum on the right-hand side. For that purpose, note that the "correct" y value corresponding to a given t is the one such that $\chi_q(ty) = 1$. It follows that:

$$\sum_{\mathbf{P} \in X_1(\mathbb{F}_q)} \frac{1 + \chi_q(ty)}{2} \chi(h_1(\mathbf{P})) = \sum_{t \in T_1} \chi(f(t)) + O(1),$$

and hence, by Lemma 2:

$$\left| \sum_{t \in T_1} \chi(f(t)) \right| \leq \big(2g_{X_1} - 2 + \deg_{X_1}(ty)\big) \cdot \sqrt{q} + O(1) = 12\sqrt{q} + O(1), \quad (16)$$

since $g_{X_1} = g_{L_1} = 3$ as seen before, and the rational functions t and y over X_1 are of degree 2 and 6 respectively.

Similarly, to estimate the character sum:

$$\sum_{t \in T_2} \chi(f(t)), \quad (17)$$

we introduce the extension $L_2 = K[t, z]/\big(t^2 - \omega_2, z^2 + g(x_1(t))\big)$ of K associated to f over T_2, and the corresponding covering curve $h_2 \colon X_2 \to E$. A point in $X_2(\mathbb{F}_q)$ is thus a tuple (x, y, t, z) such that $(x, y) \in E(\mathbb{F}_q)$, $x = x_2(t)$, and z is a square root of $-g(x_1(t))$ ensuring that $g(x_1(t))$ is not a square. For a given $t \in T_2$, there are four rational points of X_1 whose third coordinate is t, namely $(x, \pm y, t, \pm z)$ with $(x, y) = f(t)$ and $z = \sqrt{-g(x_1(t))}$. As with T_1, we can thus write the character sum (17) as:

$$\sum_{t \in T_2} \chi(f(t)) = \frac{1}{2} \sum_{\mathbf{P} \in X_2(\mathbb{F}_q)} \frac{1 + \chi_q(ty)}{2} \chi(h_2(\mathbf{P})) + O(1),$$

where the factor $1/2$ accounts for the two values of z. By Lemma 2, it follows that:

$$\left| \sum_{t \in T_2} \chi(f(t)) \right| \leq \frac{1}{2} \big(2g_{X_2} - 2 + \deg_{X_2}(ty)\big) \cdot \sqrt{q} + O(1) = 20\sqrt{q} + O(1), \quad (18)$$

since $g_{X_2} = g_{L_2} = 13$ by inspection of the ramification, and the rational functions t and y over X_2 are of degree 4 and 12 respectively.

Finally, to estimate the character sum:

$$\sum_{t \in T_3} \chi(f(t)),$$

we introduce the covering curve $h_3 \colon X_3 \to E$ corresponding to the extension $L_3'' = K[t,z]/\big(P(t), z^2 + g(x_1(t))\big)$ of K defined in Section 4. The expression of the character sum is the same as with T_2:

$$\sum_{t \in T_3} \chi(f(t)) = \frac{1}{2} \sum_{\mathbf{P} \in X_3(\mathbb{F}_q)} \frac{1 + \chi_q(ty)}{2} \chi(h_3(\mathbf{P})) + O(1).$$

By Lemma 2, it follows that:

$$\left| \sum_{t \in T_3} \chi(f(t)) \right| \leq \frac{1}{2}\big(2g_{X_3} - 2 + \deg_{X_3}(ty)\big) \cdot \sqrt{q} + O(1) = 30\sqrt{q} + O(1), \quad (19)$$

since $g_{X_3} = g_{L_3''} = 17$ by inspection of the ramification, and the rational functions t and y over X_2 are of degree 4 and 24 respectively.

Putting Eqs. (16), (18) and (19) together, we obtain that $|S_f(\chi)| \leq 62\sqrt{q} + O(1)$ for any nontrivial character χ, and hence f is well-distributed as required.

Using the statistical distance bound given in Section 2.4 together with [12, Th. 1], it follows that for a $2k$-bit BN curve, the hash function given by Eq. (15) is ε-indifferentiable from a random oracle, where:

$$\varepsilon = 4 \cdot \big(62 + O(q^{-1/2})\big)^2 \cdot \frac{\sqrt{\#E(\mathbb{F}_q)}}{q} \cdot q_D \leq \big(2^{14} + o(1)\big) 2^{-k} \cdot q_D$$

if we denote by q_D the number of queries made by the distinguisher.

6 Efficient Computation

Finally, we would like to describe a possible implementation of the Shallue–van de Woestijne encoding from Definition 2 that is both efficient and secure against side-channel analysis and other physical attacks. It is not difficult to meet what is more or less the standard of efficiency for elliptic curve encodings, as set by functions like Icart's [24]—namely, that an evaluation of the function should cost one exponentiation in the base field, plus a small, bounded number of faster operations. In the case of our encoding f, we simply need to compute the values x_1, x_2, x_3, and decide, based on $\chi_q(g(x_1)), \chi_q(g(x_2))$, which of those three values will be the abscissa of the output point.

This simple implementation has two problems with respect to side-channel attacks, however.

One the one hand, computing the quadratic character is difficult to do in constant time, so the length of that part of the computation may leak information about the input. We propose to alleviate that problem using blinding: instead

of computing $\chi_q(g(x_1))$, we evaluate $\chi_q\big(r_1^2 \cdot g(x_1)\big)$ for some random $r_1 \in \mathbb{F}_q^*$. If we then make sure that the quadratic character is implemented in such a way that evaluating $\chi_q(a)$ and $\chi_q(-a)$ takes the same time (which isn't hard to achieve), the duration of the computation of the two quadratic characters we need is completely independent of the input.

On the other hand, the naive way to choose the index i of the output abscissa involves several conditional branches. This opens up a (small) risk of timing attacks, as well as (more serious) possibilities for fault injection (i.e. glitch attacks). We avoid that problem by selecting the index using an algebraic formula depending on the two quadratic character values. It suffices to construct a function ψ of two variables such that:

$$\psi(1,1) = \psi(1,-1) = 1, \quad \psi(-1,1) = 2, \quad \psi(-1,-1) = 3.$$

One such function is given by:

$$\psi(\alpha,\beta) = \big[(\alpha-1)\cdot\beta \bmod 3\big] + 1.$$

Using that function, we propose the implementation of the encoding given in Algorithm 1.

Algorithm 1 Shallue–van de Woestijne encoding to BN curves.

procedure SWEncBN(t) ▷ $t \in \mathbb{F}_q^*$
  $w \leftarrow \sqrt{-3}\cdot t/(1+b+t^2)$
  $x_1 \leftarrow (-1+\sqrt{-3})/2 - tw$
  $x_2 \leftarrow -1 - x_1$
  $x_3 \leftarrow 1 + 1/w^2$
  $r_1, r_2, r_3 \xleftarrow{\$} \mathbb{F}_q^*$
  $\alpha \leftarrow \chi_q\big(r_1^2 \cdot (x_1^3+b)\big)$
  $\beta \leftarrow \chi_q\big(r_2^2 \cdot (x_2^3+b)\big)$
  $i \leftarrow \big[(\alpha-1)\cdot\beta \bmod 3\big] + 1$
  return $\big(x_i, \chi_q\big(r_3^2\cdot t\big)\cdot\sqrt{x_i^3+b}\big)$
end procedure

Acknowledgments

We would like to thank Paulo Barreto for suggesting this problem, Sorina Ionica and himself for fruitful discussions, and the reviewers of LATINCRYPT 2012 for numerous useful comments.

References

1. J. Baek and Y. Zheng. Identity-based threshold decryption. In F. Bao, R. H. Deng, and J. Zhou, editors, *Public Key Cryptography*, volume 2947 of *Lecture Notes in Computer Science*, pages 262–276. Springer, 2004.

2. P. S. L. M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In S. Cimato, C. Galdi, and G. Persiano, editors, *SCN*, volume 2576 of *Lecture Notes in Computer Science*, pages 257–267. Springer, 2002.
3. P. S. L. M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In B. Preneel and S. E. Tavares, editors, *Selected Areas in Cryptography*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer, 2005.
4. G. Barthe, B. Grégoire, S. Heraud, F. Olmedo, and S. Zanella Béguelin. Verified indifferentiable hashing into elliptic curves. In P. Degano and J. D. Guttman, editors, *POST*, volume 7215 of *Lecture Notes in Computer Science*, pages 209–228. Springer, 2012.
5. A. Boldyreva. Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme. In Y. Desmedt, editor, *Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2003.
6. D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.
7. D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In E. Biham, editor, *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer, 2003.
8. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In C. Boyd, editor, *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2001.
9. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *J. Cryptology*, 17(4):297–319, 2004.
10. X. Boyen. Multipurpose identity-based signcryption (a Swiss army knife for identity-based cryptography). In D. Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 383–399. Springer, 2003.
11. V. Boyko, P. D. MacKenzie, and S. Patel. Provably secure password-authenticated key exchange using Diffie-Hellman. In B. Preneel, editor, *EUROCRYPT*, volume 1807 of *Lecture Notes in Computer Science*, pages 156–171. Springer, 2000.
12. E. Brier, J.-S. Coron, T. Icart, D. Madore, H. Randriam, and M. Tibouchi. Efficient indifferentiable hashing into ordinary elliptic curves. In T. Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 237–254. Springer, 2010.
13. J. C. Cha and J. H. Cheon. An identity-based signature from Gap Diffie-Hellman groups. In Y. Desmedt, editor, *Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 18–30. Springer, 2003.
14. B. Chevallier-Mames. An efficient CDH-based signature scheme with a tight security reduction. In V. Shoup, editor, *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 511–526. Springer, 2005.
15. J.-M. Couveignes and J.-G. Kammerer. The geometry of flex tangents to a cubic curve and its parameterizations. *Journal of Symbolic Computation*, 47(3):266–281, 2012.
16. R. R. Farashahi. Hashing into Hessian curves. In A. Nitaj and D. Pointcheval, editors, *AFRICACRYPT*, volume 6737 of *Lecture Notes in Computer Science*, pages 278–289. Springer, 2011.
17. R. R. Farashahi, P.-A. Fouque, I. E. Shparlinski, M. Tibouchi, and J. F. Voloch. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. *Math. Comput.*, 2012. To appear.

18. R. R. Farashahi, I. E. Shparlinski, and J. F. Voloch. On hashing into elliptic curves. *J. Math. Cryptology*, 3:353–360, 2010.
19. P.-A. Fouque and M. Tibouchi. Deterministic encoding and hashing to odd hyperelliptic curves. In M. Joye, A. Miyaji, and A. Otsuka, editors, *Pairing*, volume 6487 of *Lecture Notes in Computer Science*, pages 265–277. Springer, 2010.
20. P.-A. Fouque and M. Tibouchi. Estimating the size of the image of deterministic hash functions to elliptic curves. In M. Abdalla and P. S. L. M. Barreto, editors, *LATINCRYPT*, volume 6212 of *Lecture Notes in Computer Science*, pages 81–91. Springer, 2010.
21. M. D. Fried and M. Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, second edition, 2005.
22. C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. In Y. Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer, 2002.
23. J. Horwitz and B. Lynn. Toward hierarchical identity-based encryption. In L. R. Knudsen, editor, *EUROCRYPT*, volume 2332 of *Lecture Notes in Computer Science*, pages 466–481. Springer, 2002.
24. T. Icart. How to hash into elliptic curves. In S. Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 303–316. Springer, 2009.
25. D. P. Jablon. Strong password-only authenticated key exchange. *SIGCOMM Comput. Commun. Rev.*, 26:5–26, October 1996.
26. E. J. Kachisa, E. F. Schaefer, and M. Scott. Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. In S. D. Galbraith and K. G. Paterson, editors, *Pairing*, volume 5209 of *Lecture Notes in Computer Science*, pages 126–135. Springer, 2008.
27. J.-G. Kammerer, R. Lercier, and G. Renault. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. In M. Joye, A. Miyaji, and A. Otsuka, editors, *Pairing*, volume 6487 of *Lecture Notes in Computer Science*, pages 278–297. Springer, 2010.
28. L.-C. Kappe and B. Warren. An elementary test for the Galois group of a quartic polynomial. *Amer. Math. Monthly*, 96(2):133–137, 1989.
29. B. Libert and J.-J. Quisquater. Efficient signcryption with key privacy from Gap Diffie-Hellman groups. In F. Bao, R. H. Deng, and J. Zhou, editors, *Public Key Cryptography*, volume 2947 of *Lecture Notes in Computer Science*, pages 187–200. Springer, 2004.
30. U. M. Maurer, R. Renner, and C. Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In M. Naor, editor, *TCC*, volume 2951 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2004.
31. G. C. C. F. Pereira, M. A. Simplício, Jr., M. Naehrig, and P. S. L. M. Barreto. A family of implementation-friendly BN elliptic curves. *The Journal of Systems and Software*, 84(8):1319–1326, 2011.
32. T. Ristenpart, H. Shacham, and T. Shrimpton. Careful with composition: Limitations of the indifferentiability framework. In K. G. Paterson, editor, *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, pages 487–506. Springer, 2011.
33. H. Sato and K. Hakuta. An efficient method of generating rational points on elliptic curves. *J. Math-for-Industry*, 1(A):33–44, 2009.
34. A. Schinzel and M. Skałba. On equations $y^2 = x^n + k$ in a finite field. *Bull. Pol. Acad. Sci. Math.*, 52(3):223–226, 2004.

35. A. Shallue and C. van de Woestijne. Construction of rational points on elliptic curves over finite fields. In F. Hess, S. Pauli, and M. E. Pohst, editors, *ANTS*, volume 4076 of *Lecture Notes in Computer Science*, pages 510–524. Springer, 2006.
36. M. Skałba. Points on elliptic curves over finite fields. *Acta Arith.*, 117:293–301, 2005.
37. M. Tibouchi. *Hachage vers les courbes elliptiques et cryptanalyse de schémas RSA*. PhD thesis, Univ. Paris 7 and Univ. Luxembourg, 2011. Introduction in French, main matter in English.
38. M. Tibouchi. A note on hasing to BN curves. In A. Miyaji, editor, *SCIS*. IEICE, 2012.
39. F. Zhang and K. Kim. ID-based blind signature and ring signature from pairings. In Y. Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 533–547. Springer, 2002.