Injective Encodings to Elliptic Curves

Pierre-Alain Fouque, Antoine Joux, Mehdi Tibouchi

Injective Encodings to Elliptic Curves

Pierre-Alain Fouque[1], Antoine Joux[2], and Mehdi Tibouchi[3]

[1] University of Rennes
pierre-alain.fouque@ens.fr
[2] CryptoExperts and Université de Versailles–Saint-Quentin
antoine.joux@m4x.org
[3] NTT Secure Platform Laboratories
tibouchi.mehdi@lab.ntt.co.jp

Abstract. For a number of elliptic curve-based cryptographic protocols, it is useful and sometimes necessary to be able to encode a message (a bit string) as a point on an elliptic curve in such a way that the message can be efficiently and uniquely recovered from the point. This is for example the case if one wants to instantiate CPA-secure ElGamal encryption directly in the group of points of an elliptic curve. More practically relevant settings include Lindell's UC commitment scheme (EUROCRYPT 2011) or structure-preserving primitives.

It turns out that constructing such an encoding function is not easy in general, especially if one wishes to encode points whose length is large relative to the size of the curve. There is a probabilistic, "folklore" method for doing so, but it only provably works for messages of length less than half the size of the curve.

In this paper, we investigate several approaches to injective encoding to elliptic curves, and in particular, we propose a new, essentially optimal geometric construction for a large class of curves, including Edwards curves; the resulting algorithm is also quite efficient, requiring only one exponentiation in the base field and simple arithmetic operations (however, the curves for which the map can be constructed have a point of order two, which may be a limiting factor for possible applications). The new approach is based on the existence of a covering curve of genus 2 for which a bijective encoding is known.

Keywords: Elliptic Curve Cryptography, Injective Encoding, Algebraic Curves

1 Introduction

Various cryptographic protocols based on the hardness of Diffie-Hellman-like problems in a group $\mathbb{G}$, such as ElGamal encryption [7] or Lindell's recent universally-composable commitment scheme [14], assume the existence of an efficient (possibly randomized) algorithm f mapping messages $m \in \{0,1\}^\ell$ to elements of $\mathbb{G}$, in such a way that m can also be recovered efficiently from $f(m)$.

For example, ElGamal encryption is *a priori* defined on group elements, so that a message needs to be mapped to an element of $\mathbb{G}$ before encrypting it,

and mapped back to a bit string upon decryption. Similarly, such a function f is an important ingredient for structure-preserving cryptography [1]: indeed, inputs and outputs of structure-preserving primitives are all group elements; this offers convenient composability properties, but to use e.g. commitments or encryption on actual bit strings, a way to map strings to the group and conversely is required.

Moreover, the size ℓ of supported bit strings should preferably be as close as possible to the bit size of $\mathbb{G}$ to optimize bandwidth. We call such an algorithm f an injective encoding.

For certain groups $\mathbb{G}$, like multiplicative groups of finite fields or some supersingular elliptic curves, it is not difficult to construct injective encodings achieving the optimal value of ℓ. On the other hand, for a general group $\mathbb{G}$, it is not obvious how to construct a function f with ℓ even super-logarithmic in the size of $\mathbb{G}$. In §2.3, we prove that this is not possible with a deterministic generic group algorithm.

When $\mathbb{G}$ is the group of points of any elliptic curve over a finite field, one can construct a probabilistic injective encoding with ℓ equal to about half of the size of $\mathbb{G}$, as we show in §2.4, but we do not know of provable constructions achieving a better ℓ in general. Works on deterministic hashing to elliptic curves, such as [17,11], typically do *not* help addressing this problem, as the functions they construct are not injective, and it is not clear how to find a convenient subset of their domain on which they become injective. Recently, however, a solution was proposed by Farashahi [8] in the special case of Hessian elliptic curves over finite fields $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$.

In §3, we propose an essentially optimal construction for all ordinary elliptic curves over fields $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$ with group order divisible by 4; this includes the well-known Edwards curves studied by Edwards and Bernstein–Lange [2], as well as twisted Huff curves, as studied by Joye et. al. [13]. Our construction is based on the bijective encoding from [10] to certain hyperelliptic curves of genus 2, and on the observation from [12] that those curves are quadratic covers of elliptic curves.

2 Injective encodings

2.1 Definition

To fix ideas, and although it is not essential for our main purpose, let us first give a formal definition of what we mean by an "injective encoding".

Let us say that a *cyclic group family* $(\mathbb{G}_k)_{k\in\mathbb{N}}$ consists in the data of a sequence of integers $n_k \geq 1$ converging to infinity, a sequence of integers $s_k \geq 0$ that is at most polynomial in $\log n_k$, and for each k, an efficiently computable bijection σ_k between the cyclic group $\mathbb{Z}/n_k\mathbb{Z}$ of order n_k and a set $\mathbb{G}_k \subset \{0,1\}^{s_k}$ of bit strings of length s_k, as well as efficient algorithms:

$$\oplus_k \colon \{0,1\}^{s_k} \times \{0,1\}^{s_k} \to \{0,1\}^{s_k} \cup \{\perp\} \qquad \ominus_k \colon \{0,1\}^{s_k} \to \{0,1\}^{s_k} \cup \{\perp\}$$

which induce on the $\mathbb{G}_k$ the group addition and negation obtained by transport of structure via σ_k. Here, "efficient" means with a time complexity polynomial in $\log n_k$ (or equivalently, in s_k).

For example, if q_k is an increasing sequence of positive primes, we can construct a cyclic group family $\mathbb{G}_k = \mathbb{F}_{q_k}^*$ with $n_k = q_k - 1$ and $s_k = O(\log q_k)$ by representing invertible elements in $\mathbb{F}_{q_k}$ as integers in $\{1, \ldots, q_k\}$ (themselves regarded as bit strings). Similarly, if E is an elliptic curve over $\mathbb{Z}[1/N]$ with N coprime with the q_k's such that $E(\mathbb{F}_{q_k})$ is cyclic for all k, we have a cyclic group family $\mathbb{G}_k = E(\mathbb{F}_{q_k})$ with $n_k = q_k + O(\sqrt{q_k})$ and $s_k = O(\log q_k)$ obtained by representing curve points in e.g. affine coordinates (with a special string for the point at infinity).

Given such a cyclic group family $(\mathbb{G}_k)$ and a sequence of non negative integers ℓ_k, we define an *ℓ_k-injective encoding* to $(\mathbb{G}_k)$ be the data consisting of a pair of efficient, possibly randomized algorithms:

$$\mathscr{F}_k \colon \{0,1\}^{\ell_k} \to \mathbb{G}_k \subset \{0,1\}^{s_k} \qquad \mathscr{I}_k \colon \{0,1\}^{s_k} \to \{0,1\}^{\ell_k} \cup \{\perp\}$$

for all k, which satisfy $\mathscr{I}_k(\mathscr{F}_k(m)) = m$ for all $m \in \{0,1\}^{\ell_k}$ with overwhelming probability over the randomness involved. We will typically express ℓ_k in terms of $\nu_k = \lfloor \log_2 n_k \rfloor$, which is the optimal bound, in the sense that we clearly have $\ell_k \leq \nu_k$ for all k by injectivity.

In what follows, the indices k, as well as references to sequences of integers and groups, will be omitted most of the time for simplicity's sake.

2.2 Some simple, optimal examples

Let p be an odd prime number. The bijection $[1, p-1] \to \mathbb{F}_p^*$ yields an obvious injective encoding to the multiplicative group $\mathbb{G} = \mathbb{F}_p^*$ which is optimal, in the sense that $\ell = \nu$.

Similarly, we obtain an optimal injective encoding to the group of squares $\mathbb{G} = (\mathbb{F}_p^*)^2 \subset \mathbb{F}_p^*$ from the bijection $[1, \frac{p-1}{2}] \to (\mathbb{F}_p^*)^2$ given by $x \mapsto x^2$. The inversion algorithm $\mathscr{I}$ then computes the unique square root of an element in $(\mathbb{F}_p^*)^2$ contained in $[1, \frac{p-1}{2}]$. This is sufficient to obtain IND–CPA ElGamal encryption in the group $(\mathbb{F}_p^*)^2$ when p is a safe prime, assuming the Decisional Diffie–Hellman assumption in that group (though one typically wouldn't want to use it for efficiency reasons). On the other hand, it is not clear how to construct a close to optimal injective encoding to the subgroup of prime order q in $\mathbb{F}_p^*$ when p is a Diffie–Hellman prime $p = 2r \cdot q + 1$.

Some elliptic curve groups also have optimal injective encodings. This is for example the case for the supersingular elliptic curves given by an equation of the form:

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

over a field $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$. Then, as observed e.g. by Boneh and Franklin [4], the map $\mathbb{F}_q \to E(\mathbb{F}_p) \setminus \{\infty\}$ given by $u \mapsto \big((u^2 - b)^{1/3}, u\big)$ is an efficient bijection, and its inverse is clearly efficient as well. This gives, again, an optimal injective encoding to $\mathbb{G} = E(\mathbb{F}_q)$. Similarly, the genus 1 case of the construction

proposed in [10] provides an optimal injective encoding to supersingular elliptic curves of the form:

$$E\colon y^2 = x^3 + ax$$

over fields $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$. However, we are not aware of any strictly optimal injective encoding to groups of points of ordinary elliptic curves, or even supersingular curves of embedding degree greater than 2.

2.3 Generic injective encodings

It is easy to construct ℓ_k-injective encodings to any cyclic group family $(\mathbb{G}_k)$ provided that $\ell_k = O(\log \nu_k)$ (and of course $\ell_k \leq \nu_k$ for all k). Indeed, in that case, the set $\{0,1\}^{\ell_k}$ of elements to be encoded contains only polynomially many elements: therefore, $\mathscr{F}_k$ and $\mathscr{I}_k$ can be defined as mutually inverse dictionary lookups for each k, and still be efficient. For example, we can define $\mathscr{F}_k$ to be the restriction of σ_k to $\{0, 1, \ldots, 2^{\ell_k} - 1\} \subset \mathbb{Z}/n_k\mathbb{Z}$ (coded as bit strings in the obvious way), and $\mathscr{I}_k$ as a series of 2^{ℓ_k} successive comparisons. Moreover, $\mathscr{F}_k$ and $\mathscr{I}_k$ are generic, in the sense that they only require black-box access to $\mathbb{G}_k$ (see [15]).

On the other hand, if $\ell_k = \omega(\log \nu_k)$, then it is easy to see that $\mathscr{F}_k$ and $\mathscr{I}_k$ cannot be both generic for all k if the $\mathscr{F}_k$'s are deterministic. Indeed, suppose that it were the case. Since it doesn't take any group element as input, $\mathscr{F}_k$ must be of the form:

$$\mathscr{F}_k(m) = \sigma_k\big(f_k(m)\big)$$

for some efficiently computable function $f_k\colon \{0,1\}^{\ell_k} \to \mathbb{Z}/n_k\mathbb{Z}$. Then, let $S = \mathscr{F}_k(\{0,1\}^{\ell_k})$ be the image of $\mathscr{F}_k$. In the terminology of Shoup [18], the algorithm $f_k \circ \mathscr{I}_k$ is a generic group algorithm for $\mathbb{Z}/n_k\mathbb{Z}$ on $\{0,1\}^{s_k}$ that computes the discrete logarithm $\sigma_k^{-1}(g)$ of any element $g \in S$ with overwhelming probability in $\mathrm{poly}(\nu_k)$ steps, regardless of the choice of the bijection σ_k. As a result, by Shoup's argument in op. cit., we must have $\#S = \mathrm{poly}(\nu_k)$: a contradiction.

This means that deterministic injective encodings from sets of superlogarithmic bit size must use the particular representation of individual group elements. We conjecture that no *probabilistic* generic $\omega(\log \nu)$-injective encoding exists either, although this seems less easy to establish.

2.4 Injective encodings to elliptic curves

For groups of points of arbitrary (even ordinary) elliptic curves over finite prime fields, it is possible to construct ℓ-injective encodings for much larger values ℓ than in the generic case. We describe one such construction here, which is more or less folklore.

Let E be an elliptic curve over $\mathbb{F}_p$ ($p \geq 5$) in short Weierstrass form, and ℓ an integer such that $\ell \leq (1/2 - \varepsilon)\log_2 p$ for some fixed constant $\varepsilon \in (0, 1/2)$. We define the encoding algorithm $\mathscr{F}\colon \{0,1\}^\ell \to E(\mathbb{F}_p)$ as follows (this encoding is probabilistic: it is not a map). To compute $\mathscr{F}(m)$, pick a random integer x in $[0, p-1]$ whose least significant ℓ bits coincide with m. If there are points in

$E(\mathbb{F}_p)$ of abscissa $x \bmod p$, return one of those (at most two) points; otherwise, start over. The inversion algorithm $\mathscr{I}$ then simply maps a point $(x, y) \in E(\mathbb{F}_p)$ to the bit string m formed by the ℓ least significant bits of x.

To prove that this method works, it suffices to show that $\mathscr{F}$ terminates in expected polynomial time on any input m. We obtain the following, more precise result.

Theorem 1. *If p is large enough, the expected number of iterations in $\mathscr{F}$ on any input is less than 3.*

Proof. Let $P(m)$ be the success probability of $\mathscr{F}$ on input m after a single iteration; in other words, $P(m)$ is the probability that a random integer x in $[0, p-1]$ whose least significant ℓ bits coincide with m is the abscissa of a point in $E(\mathbb{F}_p)$. Since for each such x there are at most two corresponding points in $E(\mathbb{F}_p)$, we have:

$$P(m) \geq \frac{1}{2} \cdot \frac{\#\{(x,y) \in E(\mathbb{F}_p) \mid \mathrm{LSB}_\ell(x) = m\}}{\#\{x \in [0, p-1] \mid \mathrm{LSB}_\ell(x) = m\}} \tag{1}$$

where $\mathrm{LSB}_\ell(x)$ denotes the bit string formed by the ℓ least significant bits of x. Clearly we have

$$\#\{x \in [0, p-1] \mid \mathrm{LSB}_\ell(x) = m\} \leq 2^{-\ell} \cdot p.$$

On the other hand, the value $\#\{(x,y) \in E(\mathbb{F}_p) \mid \mathrm{LSB}_\ell(x) = m\}$ can be estimated as in [9, §6]. It is the number of $\mathbb{F}_p$-points (x, y) of E such that x/p is in a certain interval of $\mathbb{R}/\mathbb{Z}$ of length $\geq 2^{-\ell} \cdot (1 - 2/p)$ (because x can be of the form $m + 2^\ell \cdot r$ at least for any $r \in [0, \lfloor p/2^\ell \rfloor - 1]$). But the values x/p in $\mathbb{R}/\mathbb{Z}$ for $(x, y) \in E(\mathbb{F}_p)$ are close to equidistributed. More precisely, we know from Bombieri's bound on character sums [3] that for any nontrivial additive character ψ of $\mathbb{F}_p$, we have:

$$T(\psi) = \left| \sum_{(x,y) \in E(\mathbb{F}_p) \setminus \{\infty\}} \psi(x) \right| \leq 4\sqrt{p}. \tag{2}$$

As a result, the (1-dimensional) Erdős–Turán–Koksma inequality [6, Th. 1.21] gives, for any interval $I \subset \mathbb{R}/\mathbb{Z}$ of length L and any positive integer $H < p$:

$$\left| \frac{\#\{(x,y) \in E(\mathbb{F}_p) \setminus \{\infty\} \mid \frac{x}{p} \in I\}}{N} - L \right| \leq \frac{3}{H+1} + \frac{3}{N} \sum_{h=1}^{H} \frac{T(\psi_h)}{h}$$

where ψ_h is the additive character $x \mapsto e^{2i\pi hx/p}$ and $N = \#E(\mathbb{F}_p) \setminus \{\infty\}$. Setting $H = \sqrt{p} - 1$, we get, in view of (2):

$$\begin{aligned} \#\{(x,y) \in E(\mathbb{F}_p) \setminus \{\infty\} \mid \frac{x}{p} \in I\} &\geq L \cdot N - \frac{3N}{\sqrt{p}} - 3 \cdot 4\sqrt{p} \log \sqrt{p} \\ &\geq L \cdot p - 2L\sqrt{p} - 3\sqrt{p} - 6 - 6\sqrt{p} \log p \\ &\geq L \cdot p - 12\sqrt{p} \log p \end{aligned}$$

since $|N - p| \leq 2\sqrt{p}$ by the Hasse bound. Plugging this estimate back into (1), we finally obtain:

$$P(m) \geq \frac{1}{2} \cdot \frac{2^{-\ell}(1 - 2/p)p - 12\sqrt{p}\log p}{2^{-\ell} \cdot p} = \frac{1}{2} - \frac{1}{p} - \frac{6\log p}{p^{\varepsilon}}$$

since $\ell \leq (1/2 - \varepsilon)\log_2 p$. Hence, the expected number of iteration in $\mathscr{F}$ is $1/P(m) \leq 3$ for large enough p as required. □

Thus, we can construct ℓ-injective encodings to elliptic curves over prime fields for $\ell = (1/2 - \varepsilon)\nu$: this is much better than the logarithmic bound we get in the generic case, but this still falls short of optimality by a constant factor greater than 2. It is conceivable that the same algorithm does in fact work with a larger ℓ still, possibly as large as $(1 - \varepsilon)\nu$ or even $\nu - \log^{O(1)} \nu$; we doubt that current results on the distribution of points on elliptic curves are sufficient to prove that the algorithm terminates on all inputs on those cases, however (though it might be possible to bound its complexity *on average* over all inputs m).

The only injective encoding to ordinary elliptic curves in the literature achieving a better bound is, to our knowledge, the one proposed by Farashahi in [8]. It applies to Hessian curves (i.e. elliptic curves with a rational point of order 3) over fields $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$, and achieves $\ell = \nu - 1$, a single bit short of optimal. In the next sections, we construct a similar deterministic injective encoding to all ordinary elliptic curves over fields $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$ with group order divisible by 4, also achieving $\ell = \nu - 1$.

3 Our new elliptic curve encoding

3.1 Main construction

As mentioned in the introduction, we now construct a new injective encoding for a large family of elliptic curves that are covered by certain hyperelliptic curves of genus 2.

More precisely, fix some finite field $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$, and constants $c \in \mathbb{F}_q \setminus \{-1, 0, 1\}$, $\delta = \pm 1$. We consider the following hyperelliptic curve of genus 2:

$$H_c^{\delta} \colon y^2 = f(x) = \delta x^5 + \left(c^2 + \frac{1}{c^2}\right) \cdot x^3 + \delta x. \tag{3}$$

The main result of this paper can then be stated as follows.

Theorem 2. *The following properties hold.*

1. *In addition to the hyperelliptic involution $\tau \colon (x, y) \mapsto (x, -y)$, H_c^{δ} admits an additional involution σ defined over $\mathbb{F}_q$ and given by $\sigma(x, y) = (1/x, y/x^3)$.*

2. *The quotient curve* $H_c^\delta/\langle\sigma\rangle$ *is an elliptic curve isomorphic to:*

$$E_c^\delta\colon y^2 = x^3 - 4\delta x^2 + \delta(c+\delta/c)^2 x. \tag{4}$$

The quotient map $G\colon H_c^\delta \to E_c^\delta$ *commutes with hyperelliptic involutions, in the sense that if we denote by* τ' *the involution of* E_c^δ *given by* $(x,y)\mapsto(x,-y)$*, we have* $G\circ\tau = \tau'\circ G$*.*

3. *There is a well-defined map* $F\colon \mathbb{F}_q \to H_c^\delta(\mathbb{F}_q)$ *given by*

$$F(t) = \left(\chi_q(f(t))\cdot t,\ \chi_q\big(ct+\delta t^3/c\big)\sqrt{\chi_q(f(t))\cdot f(t)}\right), \tag{5}$$

where $\chi_q(\cdot)$ *is the quadratic character of* $\mathbb{F}_q^*$ *(extended by zero to all of* $\mathbb{F}_q$*) and* $\sqrt{\cdot}$ *is the usual square root on the squares in* $\mathbb{F}_q$ *(namely exponentiation by* $(q+1)/4$*). This map* F *satisfies, for all* $t\in\mathbb{F}_q^*$*:*

$$F(1/t) = \sigma\big(F(t)\big) \quad \textit{and} \quad F(-t) = \tau\big(F(t)\big).$$

4. *Fix* $I\subset\mathbb{F}_q$ *a subset of* $\mathbb{F}_q$ *with* $(q-1)/2$ *elements such that* $I\cap(-I)=\varnothing$ *and* $-1\notin I$*, and let* I_0 *be the set obtained from* I *by removing all elements of the form* $\frac{1-t}{1+t}$ *for* t *a root of* f*, and adding* 0 *and* 1*. Then, the restriction to* I_0 *of the map* $F_{\mathrm{inj}}\colon u\mapsto G\Big(F\big(\frac{1-u}{1+u}\big)\Big)$ *is injective, and can be computed very efficiently as can its inverse (computing either of them costs one exponentiation in the base field and a few multiplications and divisions).*

Proof. The first claim is clear. To prove the second claim, the idea is to write the equation of H_c^δ in terms of a rational function that transforms in a simple way under σ, such as $t=\frac{1+x}{1-x}$, which satisfies $\sigma^* t = -t$. Concretely, we observe that (when t is regarded as an indeterminate over $\mathbb{F}_q$):

$$\begin{aligned}(1+t)^6 f\left(\frac{1-t}{1+t}\right) &= \delta(1-t)^5(1+t) + \omega(1-t^3)(1+t)^3 + \delta(1-t)(1+t)^5\\ &= -(2\delta+\omega)t^6 - (10\delta-3\omega)t^4 + (10\delta-3\omega)t^2 + (2\delta+\omega).\end{aligned}$$

where $\omega = c^2+1/c^2$. From this relation, it is easily verified that H_c^δ is isomorphic to the curve:

$$H'\colon v^2 = -(2\delta+\omega)t^6 - (10\delta-3\omega)t^4 + (10\delta-3\omega)t^2 + (2\delta+\omega),$$

a pair of mutually inverse rational maps between H_c^δ and H' being given by:

$$\begin{aligned} H_c^\delta &\longrightarrow H'\\ (x,y) &\longmapsto \left(\frac{1-x}{1+x},\ y\Big(\frac{2}{1+x}\Big)^3\right);\\ \left(\frac{1-t}{1+t},\ \frac{v}{(1+t)^3}\right) &\longmapsfrom (t,v).\end{aligned}$$

Moreover, the involution σ on H_c^δ corresponds, under this isomorphism, to the involution $\sigma'\colon (x,y) \mapsto (-x,y)$ of H', and hence $H_c^\delta/\langle\sigma\rangle \cong H'/\langle\sigma'\rangle$ is isomorphic to:

$$E'\colon v^2 = h(u) = -(2\delta+\omega)u^3 - (10\delta - 3\omega)u^2 + (10\delta - 3\omega)u + (2\delta+\omega).$$

Now, since $h(1-u) = (2\delta+\omega)x^3 - 16\delta x^2 + 16\delta x$, we see by applying the change of coordinates $(u,v) \mapsto (1-u,v)$ and then the scaling $(u,v) \mapsto \big((2\delta+\omega)u/4, (2\delta+\omega)v/8\big)$ that E' is itself isomorphic to

$$E_c^\delta\colon y^2 = x^3 - 4\delta x^2 + \delta(2\delta+\omega)x$$

as required (this is the same as (4) since $2\delta+\omega = (c+\delta/c)^2$). Furthermore, the discriminant of this curve is:

$$\Delta = 16(c+\delta/c)^4 \cdot \big(16 - 4\delta(c+\delta/c)^2\big) = -64\delta(c+\delta/c)^4 \cdot (c-\delta/c)^2,$$

which is necessarily non-zero since $c \neq \pm 1$ and -1 is a non quadratic residue. It follows that E_c^δ is indeed an elliptic curve. Finally, each of the maps in the diagram $H_c^\delta \to H' \to E' \to E_c^\delta$ commutes with hyperelliptic involutions, so the compose map G does as well.

We now turn to the third claim. For any $t \in \mathbb{F}_q$, $\chi_q(f(t)) \cdot f(t)$ has a square image under χ_q so it is itself a square, and thus equation (5) correctly defines $F(t) = (x,y)$ as a point in $\mathbb{F}_q^2$. We have to check that it lies in $H_c^\delta(\mathbb{F}_q)$. Suppose first that $f(t) \neq 0$. In that case, we cannot have $ct + \delta t^3/c = 0$ since:

$$(ct + \delta t^3/c) \cdot (ct^2 + \delta/c) = c^2t^3 + \delta t + \delta t^5 + t^3/c^2 = f(t) \neq 0.$$

Therefore, the first factor in y is ± 1, and thus:

$$y^2 = \chi_q(f(t)) \cdot f(t) = f\left(\chi_q(f(t)) \cdot t\right) = f(x)$$

so that $F(t) \in H_c^\delta(\mathbb{F}_q)$ as required. On the other hand, if $f(t) = 0$, we get $x = y = 0$ and again $F(t) \in H_c^\delta(\mathbb{F}_q)$.

It remains to show that $F(1/t) = \sigma\big(F(t)\big)$ and $F(-t) = \tau\big(F(t)\big)$ for all $t \neq 0$. The latter is easy:

$$\begin{aligned} F(-t) &= \left(\chi_q(f(-t)) \cdot (-t),\ \chi_q\big(-ct - \delta t^3/c\big)\sqrt{\chi_q(f(-t)) \cdot f(-t)}\right) \\ &= \left(\chi_q(f(t)) \cdot t,\ -\chi_q\big(ct + \delta t^3/c\big)\sqrt{\chi_q(f(t)) \cdot f(t)}\right) = \tau\big(F(t)\big). \end{aligned}$$

To obtain the former, note that $f(1/t) = f(t)/t^6$. In particular, $f(t)$ and $f(1/t)$ have the same quadratic residue. Moreover, if we let $\alpha(t) = \chi_q\big(ct + \delta t^3/c\big)$, we have:

$$\alpha(t) \cdot \alpha(1/t) = \chi_q\big((ct + \delta t^3/c) \cdot (ct^2 + \delta/c)/t^3\big) = \chi_q\big(f(t)/t^3\big)\,.$$

Now write $F(t) = (x, y)$ and $F(1/t) = (x', y')$. We have:

$$\begin{aligned} x' &= \chi_q(f(t)) \cdot \frac{1}{t} = \frac{1}{x} \\ y' &= \alpha(1/t) \cdot \sqrt{\chi_q(f(t))\,\frac{f(t)}{t^6}} \\ &= \alpha(1/t) \cdot \sqrt{\chi_q(f(t))\,f(t)} \cdot \frac{1}{t^3}\chi_q\big(1/t^3\big) \\ &= \alpha(1/t) \cdot \alpha(t) y \cdot \frac{\chi_q\big(t^3\big)}{t^3} = y \cdot \chi_q(f(t))\,\frac{1}{t^3} = \frac{y}{x^3}, \end{aligned}$$

hence $F(1/t) = \sigma\big(F(t)\big)$ as required.

Regarding the fourth assertion of the theorem, the injectivity claim is a direct consequence of Lemma 1 below. The efficiency claim for F_{inj} follows from the fact that F can be computed at the cost of one exponentiation in the base field, some quadratic character evaluations[4] and a few multiplications, while G is the simple rational function described explicitly above. Similarly, computing G^{-1} costs one square root to lift a point from $E'(\mathbb{F}_q)$ back to $H'(\mathbb{F}_q)$ and a few arithmetic operations for the isomorphisms $E_c^\delta \cong E'$ and $H' \cong H_c^\delta$, whereas the inverse of F (outside of the Weierstrass points of H_c^δ) admits the following simple expression:

$$F^{-1}(x, y) = \alpha(x) \cdot \chi_q(y) \cdot x.$$

Indeed, if $(x, y) = F(t)$, we have $\alpha(x)\chi_q(y) = \alpha(x)\alpha(t) = \chi_q(xt) \cdot \chi_q\big(c + \delta x^2/c\big)^2 = \chi_q(xt)$ since $t^2 = x^2$. Hence the claim on the efficiency of F_{inj}^{-1}. □

Lemma 1. *Let $S \subset \mathbb{F}_q$ be any subset of $\mathbb{F}_q$ containing no root of f, and such that $S \cap S^{-1} = \varnothing$ (i.e. for all $x \in S$, $1/x \notin S$). Then, the restriction of $G \circ F$ to S is injective. Moreover, the result still holds if we replace S by $S \cup \{0, 1\}$.*

Proof. Consider $t, t' \in S$ such that $G\big(F(t)\big) = G\big(F(t')\big)$. We must have either $F(t) = F(t')$ or $F(t) = \sigma\big(F(t')\big) = F(1/t')$.

In the latter case, we see in particular that the first coordinates of $F(t)$ and $F(1/t')$ coincide, so that $t = \pm 1/t'$. By definition of S, $t = 1/t'$ is excluded, so we must have $t = -1/t'$. Now since G commutes with hyperelliptic involutions, we can write:

$$G\big(F(t')\big) = G\big(F(-1/t')\big) = G\big(\tau F(1/t')\big) = \tau' G\big(\sigma F(t')\big) = \tau' G\big(F(t')\big).$$

Therefore, $G\big(F(t')\big)$ is a Weierstrass point on E_c^δ. Given the expression of G, this implies that $F(t')$ is a Weierstrass point on H_c^δ, and hence that t' is a root of f, which is a contradiction.

If on the other hand $F(t) = F(t')$, we see in particular by comparing the first coordinates of $F(t)$ and $F(t')$ that $t' = \pm t$. But since S contains no root of f, $F(t)$ is not a Weierstrass point, so it is not equal to its image $F(-t)$ under the

[4] In fact, using the techniques from [10], they can be optimized away.

hyperelliptic involution τ. Hence $t' = -t$ is impossible, and we must have $t = t'$ as required.

Turning to the second claim, we compute the images of 0 and 1 under $G \circ F$. We have $G \circ F(0) = G\big((0,0)\big) = (0,0) \in E_c^\delta(\mathbb{F}_q)$, and similarly, since $f(1) = (c+\delta/c)^2$, we find that $G \circ F(1) = G\big((1, c+\delta/c)\big) = \big((c+\delta/c)^2/4, (c+\delta/c)^3/8\big) \in E_c^\delta(\mathbb{F}_q)$. In particular, these images are distinct. Moreover, it follows from the above that for all $t \in S$, $G\big(F(t)\big)$ is never a Weierstrass point on E_c^δ, and hence is always distinct from $G\big(F(0)\big)$. Finally, if there was some $t \in S$ such that $G\big(F(t)\big) = G\big(F(1)\big)$, then, using the same argument as above, we would have $t = \pm 1$ (or $1/t = \pm 1$, which is equivalent), and this is impossible since $S \cap S^{-1} = \varnothing$. □

3.2 Description of the target curves

The result of Theorem 2 is an injective encoding F_{inj} to any elliptic curve of the form E_c^δ. Its range I_0 is of cardinality exactly $(q-1)/2 + \delta$. Indeed, we can write $f(x)$ for $x \neq 0$ as $x^3 \cdot (cx^2 + \delta/c) \cdot (c/x^2 + \delta/c)$. When $\delta = +1$, none of the factors can vanish for $x \neq 0$, so 0 is the only root of f. Therefore, the range I_0 of F_{inj} is of cardinality $(q+1)/2$; when q is prime, we can take the interval $[0, (q-1)/2]$. On the other hand, when $\delta = -1$, the roots of f are $0, \pm c, \pm 1/c$, and I_0 is then of cardinality $(q+1)/2 - 2 = (q-3)/2$; when q is prime, it is the interval $[0, (q-1)/2]$ from which one has removed $\pm t, \pm 1/t$ where $t = \frac{1-c}{1+c}$.

In both cases, we see that the size of the set from which we encode is a single bit less than the cardinality $\#E_c^\delta(\mathbb{F}_q) = q + O(\sqrt{q})$ of the target group. Hence, we do get a deterministic $(\nu - 1)$-injective encoding as stated.

It is desirable to have a simple description of the class of curves E_c^δ for which we obtain this encoding. It is given by the following theorem.

Theorem 3. *Denoting E_c^δ by E_c^+ or E_c^- for $\delta = 1$ and $\delta = -1$ respectively, the following hold:*

1. *The point $(0,0)$ is the only rational point of exact order 2 on E_c^+ and it is divisible by 2. In particular, the rational 4-torsion subgroup of E_c^+ is equal to $\mathbb{Z}/4\mathbb{Z}$.*
2. *All three points of exact order 2 on E_c^- are rational, but $(0,0)$ is not divisible by 2. In particular, E_c^- has full rational 2-torsion, and the rational 4-torsion of is equal to $(\mathbb{Z}/2\mathbb{Z})^2$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, depending on whether one of the other points of order 2 is divisible by 2.*
3. *Any ordinary elliptic curve over $\mathbb{F}_q$ with rational 4-torsion equal to $\mathbb{Z}/4\mathbb{Z}$ is isomorphic to E_c^+* or to its twist *for some c.*
4. *Any ordinary elliptic curve over $\mathbb{F}_q$ with full rational 2-torsion is isomorphic to E_c^-* or to its twist *for some c.*

Proof. Statements 1 and 2. The curve E_c^δ obviously has a rational point of exact order 2, namely $(0,0)$. When $\delta = +1$, it is the only one; indeed, the trinomial $x^2 - 4x + (c+1/c)^2$ has discriminant $16 - 4(c+1/c)^2 = -4(c-1/c)^2$ which is a non quadratic residue. On the other hand, if $\delta = -1$, all three points of exact order 2

are rational, since $x^2+4x-(c-1/c)^2$ has discriminant $16+4(c-1/c)^2 = 4(c+1/c)^2$ which is a square.

Furthermore, there is a rational point P such that $[2]P = (0,0)$ if and only if $\delta = +1$. To see that, it suffices to show that there is a line through $(0,0)$ which is tangent to the curve, since the intersection point will clearly satisfy the requirement. Now if $y = tx$ is a line through $(0,0)$, the other intersection points with the curve have their abscissa given by $t^2x = x^2 - 4\delta x + \delta(c+\delta/c)^2$, and the line is tangent when the discriminant of this quadratic equation vanishes, i.e. when t satisfies:

$$(4\delta + t^2)^2 = 4\delta \left(c + \frac{\delta}{c}\right)^2.$$

There is no solution when $\delta = -1$ since the right-hand side is not square. On the other hand, when $\delta = +1$, this is equivalent to:

$$t^2 = -4 \pm 2\left(c + \frac{1}{c}\right)$$

and this equation has a solution for one of the two possible signs, because $\big(-4+2(c+1/c)\big)\cdot\big(-4-2(c+1/c)\big) = -4(c-1/c)^2$ is a non quadratic residue, and hence exactly one of the factors must be square.

Thus, in all cases, we see that the curve admits a rational subgroup of order 4. In fact, the rational 4-torsion is of order 4 or 8: namely $\mathbb{Z}/4\mathbb{Z}$ when $\delta = +1$, and $(\mathbb{Z}/2\mathbb{Z})^2$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ when $\delta = -1$ depending on whether one of the points of order 2 other than $(0,0)$ is divisible by two. This completes the proof of statements 1 and 2.

Statement 3. Conversely, we now prove that, *up to a quadratic twist*, any ordinary elliptic curve over $\mathbb{F}_q$ with a point of order 4 and only one point of order 2 is isomorphic to E_c^+ for some c. Indeed, let E be any such elliptic curve. We can put E in Weierstrass form, translate so that the point of order 2 is $(0,0)$, and scale the coordinates to get an equation of the form:

$$E\colon y^2 = x^3 \pm 4x^2 + ax$$

for some $a \in \mathbb{F}_q$, with $a \neq 0, 4$ since the right-hand side must have no double root. Note that the nontrivial quadratic twist of E has the same equation, only with the sign of the coefficient of x^2 reversed.

Since there is a single point of order 2, the discriminant $16 - 4a$ of the trinomial $x^2 \pm 4x + a$ must be a non quadratic residue. Hence, $a - 4$ is a square. Moreover, $(0,0)$ is divisible by two: therefore, there exists a t such that the line of slope t through $(0,0)$ is tangent to the curve. This t is such that the equation $t^2x = x^2 \pm 4x + a$ has a double root, so we must have $(-t^2 \pm 4)^2 - 4a = 0$, hence a is a square. And the discriminant of the trinomial $c^2 - \sqrt{a}\cdot c + 1$ is $a - 4$, so there is a $c \in \mathbb{F}_q \setminus \{0, \pm 1\}$ such that $a = (c + 1/c)^2$. This shows that E is either E_c^+ or its quadratic twist as required.

Statement 4. Finally, consider any elliptic curve E over $\mathbb{F}_q$ with full rational 2-torsion. As above, we can put E in the form:

$$E\colon y^2 = x^3 \pm 4x^2 + ax \tag{6}$$

for some $a \in \mathbb{F}_q$ with $a \neq 0, 4$, and since the right-hand side splits in linear factors, $4 - a$ is a square. Assume for the moment that a is a non quadratic residue, then E is isomorphic to either E_c^- or its twist. Indeed, $-a$ is then a square, and the discriminant of the trinomial $c^2 - \sqrt{-a} \cdot c - 1$ is $-a + 4$ which is a square as well; hence, we can find $c \in \mathbb{F}_q \setminus \{0, \pm 1\}$ such that $a = -(c - 1/c)^2$, as required.

To complete the proof, we need to show that we can always find a Weierstrass equation (6) for E such that a is a non quadratic residue. To see this, first observe that if we start from a Weierstrass equation of the form

$$y^2 = x(x - \lambda)(x - \mu) \tag{7}$$

for E (which certainly exists) and scale the coefficients to get (6), the scaling factor s satisfies $\lambda + \mu = \pm 4s^2$ and $\lambda\mu = as^4$, so that:

$$a = \frac{16\lambda\mu}{(\lambda + \mu)^2}.$$

Now clearly, starting from (7), we can translate the origin to one of the other two points of order 2, and get one of the other two Weierstrass forms:

$$y^2 = x'(x' + \lambda)(x' + \lambda - \mu) \quad \text{or} \quad y^2 = x''(x'' + \mu)(x'' + \mu - \lambda).$$

These correspond to the canonical form (6) with the coefficient of x equal to:

$$a' = \frac{16(-\lambda)(-\lambda + \mu)}{(-2\lambda + \mu)^2}, \quad \text{resp.} \quad a'' = \frac{16(-\mu)(-\mu + \lambda)}{(-2\mu + \lambda)^2}.$$

But at least one of a, a' and a'' must be a non quadratic residue, since:

$$\chi_q(a \cdot a' \cdot a'') = \chi_q(\lambda\mu \cdot (-\lambda)(-\lambda + \mu) \cdot (-\mu)(-\mu + \lambda)) = -1.$$

This concludes the proof. □

Note that elliptic curves with rational 4-torsion equal to $\mathbb{Z}/4\mathbb{Z}$ are birational to Edwards curves $x^2 + y^2 = 1 + dx^2y^2$ with non square d [2]. Bernstein and Lange showed that these curves are quite interesting for computation and cryptography, as they admit a complete addition law, and admit the fastest arithmetic known to date. Similarly, curves with full rational 2-torsion are also isomorphic to curves with fast arithmetic and unified addition laws, namely twisted Huff curves [13]. Together, they comprise all ordinary curves with order divisible by 4.

3.3 Mapping to the twist

The previous paragraph suggests that if E is an elliptic curve with order divisible by 4, then we know an injective encoding to *either* $E(\mathbb{F}_q)$ itself or to its nontrivial quadratic twist. But we can in fact do better and map to $E(\mathbb{F}_q)$ itself.

Indeed, it is classical (see e.g. [16] or [5, Ch. 14]) that H_c^δ does not only cover the elliptic curve $E'\colon v^2 = h(u)$ given by the quotient by σ (using the notations of the proof of Theorem 2), but also $v^2 = u^3 h(1/u)$ given by the quotient by $\sigma\tau$. Moreover, we have $u^3 h(1/u) = -h(u)$, so that $H_c^\delta/\langle\sigma\tau\rangle$ is the nontrivial quadratic twist of E_c^δ.

It is easy to adapt the construction of Theorem 2 to obtain a similar injective function to $H_c^\delta/\langle\sigma\tau\rangle$, and hence a $(\nu-1)$-injective encoding to the twists of the curves E_c^δ. We conclude:

Theorem 4. *Let E be an ordinary elliptic curve over a finite field $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$, such that 4 divides $\#E(\mathbb{F}_q)$. Then there is an efficient, efficiently invertible injective encoding to $E(\mathbb{F}_q)$ from an interval of cardinality $q/2 + O(1)$ (i.e. a $(\nu-1)$-injective encoding, in the terminology of §2.1). Both the encoding and its inverse can be computed with one exponentiation in $\mathbb{F}_q$ and a few multiplications and divisions.*

In Appendix A, we give pseudocode for the encoding to and decoding from E_c^+. The other cases (viz. E_c^- and the twists of $E_c^\pm$) are treated similarly.

4 Conclusion

In this paper, we proposed an efficient injective encoding with almost optimally large image for a new class of elliptic curves including important examples like Edwards curves. The only previous construction in that direction was for Hessian curves.

Note that, from a cryptographic perspective, this does not completely solve the problem of constructing an encoding for ElGamal encryption, as the curves we encode to have a small subgroup which can reveal information about the message (i.e. ElGamal is one-way but not semantically secure in this setting). This is similar to the situation of ElGamal in multiplicative groups $\mathbb{F}_p^*$ when p is not a safe prime. Similarly, since Lindell's UC commitment scheme works in prime order groups, our construction is *a priori* not applicable to that setting.

However, we believe that the possibility of encoding messages as elliptic curve points can be of sufficient interest to protocol designers that designing around this cofactor limitation might be worthwhile.

References

1. M. Abe, G. Fuchsbauer, J. Groth, K. Haralambiev, and M. Ohkubo. Structure-preserving signatures and commitments to group elements. In T. Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 209–236. Springer, 2010.

2. D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In K. Kurosawa, editor, *ASIACRYPT*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer, 2007.
3. E. Bombieri. On exponential sums in finite fields. In *Les Tendances Géom. en Algèbre et Théorie des Nombres*, pages 37–41. Éditions du CNRS, 1966.
4. 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.
5. J. Cassels and E. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*. Number 230 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1996.
6. M. Drmota and R. F. Tichy. *Sequences, discrepancies and applications*. Springer, 1997.
7. T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.
8. 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.
9. R. R. Farashahi, P.-A. Fouque, I. E. Shparlinski, M. Tibouchi, and J. F. Voloch. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. *Math. Comp.*, 82:491–512, 2013.
10. 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.
11. 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.
12. A. Joux and V. Vitse. Cover and decomposition index calculus on elliptic curves made practical. Application to a previously unreachable curve over $\mathbb{F}_{p^6}$. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*. Springer, 2012.
13. M. Joye, M. Tibouchi, and D. Vergnaud. Huff's model for elliptic curves. In G. Hanrot, F. Morain, and E. Thomé, editors, *ANTS*, volume 6197 of *Lecture Notes in Computer Science*, pages 234–250. Springer, 2010.
14. Y. Lindell. Highly-efficient universally-composable commitments based on the DDH assumption. In K. G. Paterson, editor, *EUROCRYPT*, volume 6632 of *Lecture Notes in Computer Science*, pages 446–466. Springer, 2011.
15. U. M. Maurer. Abstract models of computation in cryptography. In N. P. Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2005.
16. J. Paulhus. Decomposing Jacobians of curves with extra automorphisms. *Acta. Arith.*, 132(3):231–244, 2008.
17. 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.
18. V. Shoup. Lower bounds for discrete logarithms and related problems. In W. Fumy, editor, *EUROCRYPT*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer, 1997.

A Pseudocode for the encoding to E_c^+

We give formulas for computing the injective encoding to $E_c^+(\mathbb{F}_q)$ both in short Weierstrass form and in Edwards form. Fix a subset $I_0 \subset \mathbb{F}_q \setminus \{-1\}$ of cardinality $(q+1)/2$ such that $I \cap (-I) = \{0\}$. We can for example pick $I_0 = [0, (q-1)/2]$ if q is prime.

Short Weierstrass form. The image (x, y) of $u \in I_0$ is obtained with the $\textsc{Encode}_{E_c^+}$ algorithm below, and decoding in carried out with the inverse algorithm $\textsc{Decode}_{E_c^+}$.

function $\textsc{Encode}_{E_c^+}(u)$
- $t \leftarrow (1-u)/(1+u)$
- $f \leftarrow t^5 + (c^2 + 1/c^2) \cdot t^3 + t$
- $\varepsilon \leftarrow \chi_q(f)$
- $\alpha \leftarrow \chi_q\big(ct + t^3/c\big)$
- $x_H \leftarrow \varepsilon \cdot t$
- $y_H \leftarrow \alpha \cdot \sqrt{\varepsilon \cdot f}$
- $u_{E'} \leftarrow \left(\frac{1-x_H}{1+x_H}\right)^2$
- $v_{E'} \leftarrow y_H \left(\frac{2}{1+x_H}\right)^3$
- $x \leftarrow (c + 1/c)^2 \cdot (1 - u_{E'})/4$
- $y \leftarrow (c + 1/c)^2 \cdot v_{E'}/8$
- **return** (x, y)

function $\textsc{Decode}_{E_c^+}(x, y)$
- $u_{E'} \leftarrow 1 - 4x/(c + 1/c)^2$
- $v_{E'} \leftarrow 8y/(c + 1/c)^2$
- $u_{H'} \leftarrow \sqrt{u_{E'}}$
- $x_H \leftarrow \frac{1-u_{H'}}{1+u_{H'}}$
- $y_H \leftarrow \frac{v_{E'}}{(1+u_{H'})^3}$
- $\alpha \leftarrow \chi_q\big(cx_H + x_H^3/c\big)$
- $t \leftarrow \alpha \cdot \chi_q(y_H) \cdot x_H$
- $u \leftarrow (1-t)/(1+t)$
- **if** $u \notin I_0$ **then**
  - $u \leftarrow -u$
- **return** u

A number of optimizations of these algorithms are possible: for example, the decoding function only uses the quadratic character of y_H, so it is not necessary to compute y_H in full; similarly, one can speed up the first part of the encoding algorithm by using the implementation techniques from [10] and noticing that $\alpha = \chi_q(c/t + t/c)$. Such improvements, however, only marginally affect the running time, which is dominated in both cases by the square root evaluation, so we chose to closely follow the steps of §3.1.

Edwards form. Clearly, E_c^+ and E_{-c}^+ are identical curves, so we may assume without loss of generality that c is of the form $2s^2$. Then, consider the birational transformation $(X, Y) \mapsto (x, y)$ given by:

$$x = \left(c + \frac{1}{c}\right)\frac{1+Y}{1-Y} \qquad \text{and} \qquad \frac{y}{x} = \frac{c-1}{sX}.$$

It maps E_c^+ to the curve given by the equation:

$$\begin{aligned}
\left(\frac{c-1}{sX}\right)^2 &= x - 4 + \left(c + \frac{1}{c}\right)^2 \frac{1}{x} \\
2\frac{(c-1)^2}{cX^2} &= \left(c + \frac{1}{c}\right) \cdot \left(\frac{1+Y}{1-Y} + \frac{1-Y}{1+Y}\right) - 4 \\
\frac{(c-1)^2}{X^2} &= (c^2+1)\frac{1+Y^2}{1-Y^2} - 2c = \frac{(c-1)^2 + (c+1)^2 Y^2}{1-Y^2} \\
1 - Y^2 &= X^2 \cdot \left(1 + \left(\frac{c+1}{c-1}\right)^2 Y^2\right)
\end{aligned}$$

which is exactly the Edwards curve $\mathscr{E}_d\colon X^2 + Y^2 = 1 + dX^2Y^2$ for:

$$d = -\left(\frac{c+1}{c-1}\right)^2.$$

Since we constrained c to be of the form $2s^2$, this shows that about half of all Edwards curves $\mathscr{E}_d$ with non square d are isomorphic to some E_c^+ (the other half being isomorphic to the twists of those).

We can easily encode to and decode from $\mathscr{E}_d(\mathbb{F}_q)$ using the birational transformation described above. This gives the following algorithms.

function $\textsc{Encode}_{\mathscr{E}_d}(u)$
  $(x, y) \leftarrow \textsc{Encode}_{E_c^+}(u)$
  $X \leftarrow \frac{c-1}{s} \cdot \frac{x}{y}$
  $Y \leftarrow \frac{x+c+1/c}{x-c-1/c}$
  return (X, Y)

function $\textsc{Decode}_{\mathscr{E}_d}(X, Y)$
  $x \leftarrow (c + 1/c) \cdot \frac{1+Y}{1-Y}$
  $y \leftarrow \frac{c-1}{s} \cdot \frac{x}{X}$
  $u \leftarrow \textsc{Decode}_{E_c^+}(x, y)$
  return u