ENCODING TO LEGENDRE CURVE, KUMMER LINE AND TWISTED EDWARDS CURVE

Gourab Chandra Saha and Sabyasachi Karati
Indian Statistical Institute, 203, B.T. Road, Kolkata, India

Abstract. For applications of elliptic curve cryptography in censorship circumvention, the traffic generated by a cryptographic protocol must appear indistinguishable from uniformly random strings to blend in with random traffic. To address this challenge, previous works have proposed various mappings that map finite field elements to elliptic curve points, focusing primarily on short Weierstrass, Montgomery, and (twisted) Edwards curve forms. In this article, we primarily focus on the Legendre curve $\mathsf{E}_\lambda : y^2 = x(x-1)(x-\lambda)$ targeting the Kummer lines, ensuring no exception points and a constant-time algorithm. We present two such mappings: Elligator-L3 and Elligator-L1. Elligator-L3 maps elements of a prime field $\mathbb{F}_q$, where $q \equiv 3 \pmod 4$, to a Legendre curve E_λ with $\chi(\lambda) = -1$, while Elligator-L1 maps elements of $\mathbb{F}_q$, where $q \equiv 1 \pmod 4$, to E_λ with $\chi(\lambda) = 1$. We also extend these mappings to Kummer lines, resulting in Elligator-K3 and Elligator-K1.

Previously, Bernstein et al. [2] proposed two efficient encoding-decoding functions: Elligator-1 and Elligator-2. Elligator-1 maps elements of a prime field $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$ to an Edwards curve $E_{1,d} : x^2 + y^2 = 1 + dx^2y^2$ with $\chi(d) = -1$ and vice versa. Elligator-2, in contrast, considers Montgomery curves over a prime field and can be extended to twisted Edwards curves. However, to operate on any element of the prime field, Elligator-2 requires primes of the form $1 \pmod 4$. Addressing this, we propose a new map, Elligator-T, which enables encoding from a prime field $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$ to a complete twisted Edwards curve with no exception points. Further, we extend it to a y-coordinate only mapping called Elligator-T$_y$.

Elligator-T is crucial in verifiable XEdDSA (VXEdDSA) signatures [25]. However, VXEdDSA requires the computation of square roots to manage compressed point representations. To overcome this, we introduce the verifiable quotient Edwards curve Digital Signature Algorithm (VqEdDSA), which utilises Elligator-T$_y$ and relies solely on y-coordinate arithmetic. VqEdDSA eliminates the need for square root computations, replacing them with a few field multiplications. We propose several twisted Edwards curves and squared Kummer lines over prime fields for cryptographic applications, leveraging the newly introduced Elligator maps.

1. Introduction.

Elliptic curve cryptography (ECC), introduced by Koblitz [19] and Miller [22], has emerged as a leading research area due to its ability to offer short key and signature sizes alongside efficient implementation without compromising security. Moreover, the geometric intricacy inherent in elliptic curves has facilitated the development of various cryptographic protocols over the past decades. Notable examples include Joux's tripartite key agreement [17] and Boneh and Franklin's

Key words and phrases. Encoding, Elligator, twisted Edwards curve, Legendre curve, Kummer line, VqEdDSA.

identity-based encryption scheme [3]. Across the internet, widespread applications such as TLS, SSH, and WhatsApp, as well as anonymity and privacy-preserving tools like Tor and Bitcoin, rely on elliptic curves for necessary security.

However, in circumvention applications, ECC exhibits a security vulnerability. ECC protocols transmit elliptic curve points openly as long-term or ephemeral public keys, ciphertext prefixes, and other elements. In their natural representation, these elliptic curve points are distinguishable from uniform binary strings, making them susceptible to identification. Even when considering the compressed form of elliptic curve points, which primarily consist of the x-coordinates, roughly half correspond to points on the actual elliptic curve. In contrast, the remainder corresponds to points on a twist of the elliptic curve. This inherent structure facilitates attackers in distinguishing, blocking, or tampering with ECC traffic.

Bernstein et al. [2] classify these distinguishers into three categories: least severe, more severe, and most severe. For instance, they analyse the NIST prime curve P-256: $y^2 = x^3 - 3x + b$, where b is a standard constant. This curve operates over the prime field $\mathbb{F}_p$, where $p = 2^{256} - 2^{224} + 2^{219} + 2^{96} - 1$. The least severe distinguisher monitors the traffic and confidently identifies ECC traffic if the strings are all less than $2^{256} - 2^{224}$. In contrast, the more severe distinguisher not only observes but also verifies whether a 512-bit string satisfies the curve equation when interpreted as (x, y). Although many systems transmit a compressed version of the point, consisting of x and a sign bit, the computational overhead of square root calculations often outweighs the benefits of reduced point size for regular users. Finally, the most severe distinguisher examines whether the term $x^3 - 3x + b$ is a quadratic residue, with a probability of $\frac{1}{2}$. If this occurs over numerous consecutive iterations, the distinguisher reasonably concludes that the traffic is ECC traffic.

1.1. **Möller's approach.** A proposed solution to the problem involves the "curve-or-twist" technique introduced by Möller [23]. In his research, Möller outlines a practical public-key encryption method designed to withstand adaptive chosen-ciphertext attacks (CCA) while ensuring pseudo-randomness in ciphertexts. This pseudo-randomness is achieved through a novel Key Encapsulation Mechanism (KEM) rooted in the elliptic curve Diffie-Hellman. The proposed technique employs a pair of elliptic curves where each curve serves as a twist of the other. Möller adapts the ElGamal encryption by transmitting points randomly situated either on the elliptic curve or its non-trivial quadratic twist over a binary field. In this modified scheme, a user's public key consists of a pair of points $(aP, a'P')$, where P denotes a point on the elliptic curve, P' represents a point on the twist of the elliptic curve, and (a, a') constitutes the private key. When sending a message, the sender selects a point randomly from $(aP, a'P')$, denoted as $\hat{a}\hat{P}$, and an arbitrary integer b. Subsequently, the sender encrypts the message using $b\hat{a}\hat{P}$. Upon receiving the point $b\hat{P}$ and the encrypted message, the receiver initially verifies whether the received point belongs to the curve or its twist. Then, the user computes $b\hat{a}\hat{P}$ and proceeds to decrypt the message. Bernstein et al. [2] suggest that opting for a' equal to a enables Montgomery scalar multiplication to manage both computations [5, 20, 24].

Building on this framework, Young and Yung successfully attained DDH security within the standard model and put forth a secure key exchange protocol [30], alongside an encryption scheme [31]. Additionally, Möller's methodology has found practical application in censorship circumvention tools. For instance, StegoTorus, a

concealment proxy designed for the Tor anonymity system [28], and Telex, a mechanism for anticensorship within network infrastructure [29], have both implemented Möller's approach.

1.2. **Elligator.** Bernstein et al. proposed a different approach in [2]. Their idea is based on an efficiently computable algebraic function ι from the set $S = \{0, 1, \ldots, \frac{(p-1)}{2}\}$ to an elliptic curve $E(\mathbb{F}_p)$, where p is a prime. The map is injective and efficiently invertible. The mapping is subject to suitable p and E. Bernstein et al. noticed that a point $P \in \iota(S) \subset E(\mathbb{F}_p)$ has a uniform random preimage in S. Therefore, one can map a point P to a uniformly random bit string, however unique integer $\iota^{-1}(P)$, if it exists.

In the paper [2], the authors provide two constructions: Elligator-1 and Elligator-2. Elligator-1 deals with Edwards curve over a prime field $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$. Elligator-1 takes an injective encoding function implicitly mentioned in [10]. On the other hand, Elligator-2 maps any field element to a Montgomery curve over a prime field $\mathbb{F}_p$ with $p \equiv 1 \pmod 4$. Using Elligator-2, one can map a field element to a twisted Edwards curve via the Montgomery curve. For the primes of the form $3 \pmod 4$, Elligator-2 has two or six exception points. Furthermore, twisted Edwards curves are essential because they provide the fastest digital signature [15].

1.2.1. *Advantage of Elligator over Möller's approach.* Elligator has several advantages over Möller's approach. Elligator not only achieves ciphertext indistinguishability but also achieves public-key indistinguishability. In Möller method, the length of the public key is double, while Elligator needs only a minimal length public key. While Möller's method is limited to Elgamal-type schemes, Elligator can be applied to a wider range of elliptic curve protocols. Elligator does not require extra security requirements like Twist security, which is essential for Möller's approach. Also, Elligator is easier to adapt to existing protocols without modifying them.

1.3. **Mapping strings to elliptic-curve points.** This research area originated from an algorithmic number theoretic question: Given an elliptic curve E and an element from the underlying sufficiently large finite field $\mathbb{F}_q$, is there any algorithm to construct a point on the curve $E(\mathbb{F}_q)$? There are provably easy probabilistic algorithms to use. Then, how about a provably deterministic polynomial-time algorithm? Shallue and Woestijne first proposed a mapping that answers the question [26]. They give a deterministic polynomial-time algorithm that computes a nontrivial rational point on an elliptic curve over a finite field, given a Weierstrass equation for the curve by providing a map $\varphi : \mathbb{F}_q \to E(\mathbb{F}_q)$. For this, they reduce the problem to finding a rational point on a curve of genus zero. Their work shows that each element of $E(\mathbb{F}_q)$ has a fixed number of preimages, say k. Trying $k+1$ elements of $\mathbb{F}_q$, they produce a $\varphi(t) \in E(\mathbb{F}_q)$ given E, $\mathbb{F}_q$ and t. Icart and subsequent authors explored many other replacements of φ [4, 16, 12, 11, 7, 13, 8].

1.4. **Our contribution.**

1. In this work, we explicitly address the problem of mapping a field element to a point on a Legendre curve, which is crucial for mapping to a Kummer line. We present two distinct constant-time mappings for finite fields of odd prime characteristic: (i) Elligator-L3, which maps an element of a finite field $\mathbb{F}_q$ to a point on a Legendre curve E_λ with $\chi(\lambda) = -1$ when $q \equiv 3 \pmod 4$; and (ii) Elligator-L1, which maps an element of $\mathbb{F}_q$ to a Legendre curve E_λ with

$\chi(\lambda) = 1$ when $q \equiv 1 \pmod 4$. Moreover, both the mappings do not have any exception points. Furthermore, we also provide efficient inversion algorithms for both mappings and proofs for both the encoding and inversion.

2. Next, we introduce two mappings, Elligator-K3 and Elligator-K1, to the Kummer line, constructed based on the Elligator-L3 and Elligator-L1 mappings, respectively. Elligator-K3 maps an element of the prime field $\mathbb{F}_q$ to the Kummer line when $q \equiv 3 \pmod 4$, while Elligator-K1 handles the case when $q \equiv 1 \pmod 4$.
   - To comprehensively compare all existing encodings applicable to Legendre curves, we provide a constant-time variant of the encoding proposed in [6], along with its inverse mapping. We also extend this encoding to the Kummer Line. Further details are provided in Appendix H. This article also includes an encoding map that in general covers all forms of elliptic curves, including Legendre, Montgomery, and Hessian of prime orders and with $j \neq 0, 1728$.
3. In the paper [2], authors provide a mapping Elligator-2 that maps a field element to a Montgomery curve defined over a prime field $\mathbb{F}_q$ with q being a prime. From the obtained point via this mapping, one can compute a point on the associated twisted Edwards curve. However, the necessary condition for the construction to work for all elements of $\mathbb{F}_q$ is $q \equiv 1 \pmod 4$. For $q \equiv 3 \pmod 4$, we cannot convert all elements of $\mathbb{F}_q$ to a point of the twisted Edwards curve. This paper presents a mapping, Elligator-T, that addresses this gap[1]. Theorem 5.1 ensures the existence of such a map to a twisted Edwards curve. Also, the twisted Edwards curves in the construction support a complete addition formula.
4. A major application of encoding to twisted Edwards curve is the verifiable Edwards curve digital signature in WhatsApp [25]. But in the algorithm, one has to recreate the full point of twisted Edwards from a compressed point where one bit is used to identify the x-coordinate. [2] comments that the cost of square root computation for common users outweighs the benefit of the reduced point size. Using Elligator-T$_y$ (a reduced version of Elligator-T), we propose an y-coordinate only verifiable Edwards curve digital signature (called VqEdDSA). We also provide suitable curves for the applications.

   We show the applicability of Elligator-K* (both K3 and K1) in the context of the Diffie-Hellman Key exchange protocol using squared Kummer Lines. We also suggest some suitable Kummer lines for applications.

All the test codes are written in Magma and are publicly available at:

https://github.com/gourabsaha1992/Encodings-to-Legendre-curve.

2. **Definitions.** In this paper, we provide mappings that take elements of a finite field $\mathbb{F}_q$ to and from three major curves: Twisted Edwards curve, Legendre curve, and Kummer line. Thus, we briefly introduce these three curves in this section. The quadratic character is an essential ingredient in the mappings and in their proofs of correctness. Therefore, we begin by describing the quadratic character.

[1]Performance-wise, Elligator-2 is better than Elligator-T. The probability of hitting an exception point is negligible; however, for Elligator-T, this probability is zero.

2.1. **Quadratic character.** Let q be a prime integer. Then the function $\chi : \mathbb{F}_q \to \{0, 1, -1\}$ is defined by $\chi(a) = a^{(q-1)/2}$ for any element $a \in \mathbb{F}_q$. χ is called quadratic character [2]. For any $a \in \mathbb{F}_q$, it can also be defined as

$$\chi(a) = \begin{cases} 0 & \text{if } a \text{ is zero,} \\ 1 & \text{if } a \text{ is a square,} \\ -1 & \text{if } a \text{ is non-square.} \end{cases}$$

χ is multiplicative in nature, that is, $\chi(ab) = \chi(a)\chi(b)$. Trivially, $\chi(a^2) = 1$. Therefore, $\chi(1) = \chi(a \cdot 1/a)$ and in turn we have $\chi(1/a) = 1/\chi(a) = \chi(a)$ for a non-zero a. Let a and b both be either squares or non-squares, then $\chi(ab) = \chi(a)\chi(b) = 1$. Also, if $\chi(ab) = -1$, one of a and b is square and the other is non-square.

Now, we consider some properties of χ specific to the primes of the form $q \equiv 3 \pmod 4$. First $\chi(\chi(a)) = \chi(a)$. As $(q-1)/2$ is odd, $(-1)^{(q-1)/2} = -1$. This implies that -1 is a non-square in $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$. Also $a^{(q+1)/4}$ is a square root of a if $\chi(a) = 1$. We call it the principal square root of a, the unique square root that is a square, and the other root is non-square. Notice that if $a \in \mathbb{F}_q$ is a square, then $a^{(q+1)/2} = a^{(q-1)/2}a = \chi(a)a = a$ as $\chi(a) = 1$. For any square root of b of a, $b = \chi(b)a^{(q+1)/4}$.

Now, we provide some features of χ relevant to primes $q \equiv 1 \pmod 4$. In this case $(-1)^{(q-1)/2} = 1$ since $(q-1)/2$ is even. Therefore, -1 is a square here. Also, there is no concept of principal square root because both roots are either squares or non-squares. Define a square root function $\sqrt{\ } : \mathbb{F}_q^2 \to \mathbb{F}_q$ such that $\sqrt{a^2} \in \{a, -a\}$ where $\mathbb{F}_q^2 = \{a^2 : a \in \mathbb{F}_q\}$. Let us define $\sqrt{\mathbb{F}_q^2} = \left\{0, 1, \ldots, \frac{q-1}{2}\right\}$. One can also define $\sqrt{\mathbb{F}_q^2}$ by the negation of $\left\{0, 1, \ldots, \frac{q-1}{2}\right\}$.

2.2. **Twisted Edwards curve.** Let $\mathbb{F}_q$ be a finite field with characteristic $\neq 2$. The twisted Edwards curve [1] over $\mathbb{F}_q$ is defined by

$$\mathsf{E}_{a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

where $a, d \in \mathbb{F}_q$ are non-zero and distinct.

For applications, Twisted Edwards curves with $a = -1$ are widely used. By [9], the projective addition formula for $\mathsf{E}_{a,d}$ is complete if and only if $\chi(ad) = -1$. If $\mathbb{F}_q$ is a prime field with $q \equiv 3 \pmod 4$, then -1 is non-square. Consequently, the projective addition formula for the twisted Edwards curve $\mathsf{E}_{-1,d}$ over $\mathbb{F}_q$, where d is a square, is complete.

2.3. **Legendre curve.** Let $\mathbb{F}_q$ be a finite field with characteristic $\neq 2$. Let $\lambda \in \mathbb{F}_q$ such that $\lambda(\lambda - 1) \neq 0$. The Legendre form [27] of an elliptic curve is defined by

$$\mathsf{E}_\lambda : y^2 = x(x-1)(x-\lambda).$$

2.4. **Kummer line.** Let $\tau \in \mathbb{C}$ with a positive imaginary part and $w \in \mathbb{C}$. Let $\xi_1, \xi_2 \in \mathbb{Q}$. Then Theta functions with characteristics $\vartheta[\xi_1, \xi_2](w, \tau)$ are defined by

$$\vartheta[\xi_1, \xi_2](w, \tau) = \sum_{n \in \mathbb{Z}} \exp\left[\pi i(n + \xi_1)^2\tau + 2\pi i(n + \xi_1)(w + \xi_2)\right],$$

where $i = \sqrt{-1}$.

For a fixed τ, $\vartheta_1(w)$ and $\vartheta_2(w)$ are defined as $\vartheta[0, 0](w, \tau)$ and $\vartheta[0, 1/2](w, \tau)$. Let $\mathbb{P}^1(\mathbb{C})$ be the projective line over $\mathbb{C}$. The Kummer line ($\mathcal{K}$) associated with τ is the image of the map ϖ from $\mathbb{C}$ to $\mathbb{P}^1(\mathbb{C})$ defined by $\varpi : w \mapsto [\vartheta_1(w) : \vartheta_2(w)]$.

The mappings are defined over $\mathbb{C}$. However, the Lefschetz principle [14] shows that the identities proved over the complex field are also valid over a large prime field. Consequently, the arithmetic of Kummer lines defined over the complex field also applies over large prime fields.

Let $\mathsf{E}_\lambda : y^2 = x(x-1)(x-\lambda)$ be an elliptic curve of Legendre form and the corresponding projective form is $Y^2Z = X(X-Z)(X-\lambda Z)$. For simplicity we are using the projective form E_λ, that has three point of order 2, namely $(0:0:1), (1:0:1)$ and $(\lambda:0:1)$.

A (squared) Kummer line $\mathcal{K}_{a^2,b^2}$ [18] can be associated with a E_λ where $\lambda = \frac{a^4}{a^4-b^4}$. Let $\varrho : \mathsf{E}_\lambda \to \mathsf{E}_\lambda$ be an automorphism which map a point to its inverse point. A map $\Pi : \mathcal{K}_{a^2,b^2} \setminus \{[b^2:a^2]\} \to \mathsf{E}_\lambda/\varrho$ is defined by

$$\Pi([x^2:z^2]) = \begin{cases} (1:\cdot:0), \text{ if } [x^2:z^2] = [a^2:b^2] \\ (a^2x^2:\cdot:a^2x^2 - b^2z^2), \text{ otherwise, and} \end{cases} \tag{1}$$

$$\Pi^{-1}((X:\cdot:Z)) = \begin{cases} [a^2:b^2], \text{ if } (X:\cdot:Z) = (1:\cdot:0) \\ [b^2X : a^2(X-Z)], \text{ otherwise.} \end{cases} \tag{2}$$

The map Π does not preserve the consistency of addition and doubling between $\mathcal{K}_{a^2,b^2}$ and E_λ. To establish the consistency, we need to add $\mathbf{T} = (\lambda:0:1)$, a point of order 2 of E_λ, with the image point of Π. The updated maps are defined by

$$\hat{\Pi}(P) = \Pi(P) + \mathbf{T}, \text{ and}$$
$$\hat{\Pi}^{-1}(\mathbf{P}) = \Pi^{-1}(\mathbf{P} + \mathbf{T}).$$

Now the map $\hat{\Pi}$ preserves the consistency of addition and doubling. We refer [18] for further details.

3. **Encodings to Legendre curve.** The existing literature primarily focuses on the Weierstrass, Montgomery, and Edwards forms of elliptic curves. However, there is no explicit encoding dedicated solely to Legendre curves. Elligator-2 [2] addresses elliptic curves of the form $y^2 = x^3+Ax^2+Bx$, excluding the specific case $y^2 = x^3+x$. For Legendre curves, we observe that $A = -(\lambda+1)$ and $B = \lambda$. Nevertheless, Elligator-2 introduces exception points when applied to Legendre curves.

In this section, we propose two encodings: **Elligator-L3** and **Elligator-L1**, which map an element of the finite field $\mathbb{F}_q$ to a point on a Legendre curve. Both constructions are constant-time and free of exception points. Elligator-L3 is defined for primes of the form 3 (mod 4) and supports λ when $\chi(\lambda) = -1$. In contrast, Elligator-L1 is defined for primes of the form 1 (mod 4) and is applicable when $\chi(\lambda) = 1$. Notably, Elligator-L1 achieves the lowest operation count among all known constant-time encodings for Legendre curves. Given the practical importance of such encodings, we present several concrete Legendre curve proposals, each offering the desired security level, and the encodings are applicable.

Additionally, [6] proposes an encoding for elliptic curves of the form $y^2 = x^3 + Ax^2 + Bx$ that also avoids exception points. However, it does not operate in constant-time. In Appendix H, we introduce a constant-time variant of this encoding and offer a comparative analysis of all proposals in Section 4.3.

We also note that [10] implicitly includes a map to Legendre curves for primes of the form 3 (mod 4), and it is quite similar to our proposed Elligator-L3 encoding. However, our work is applicable to a wider range of Legendre curves compared to the encoding of [10] (See Section 4.3). Furthermore, our proposal is accompanied by simple and compact proofs.

3.1. **Elligator-L3 map.** Elligator-L3 map is an encoding map from $\mathbb{F}_q$ to Legendre curve $\mathsf{E}_\lambda : y^2 = x(x-1)(x-\lambda)$ where the prime q is of the form $q \equiv 3 \pmod 4$. The next theorem explicitly provides the encoding map, and the pseudocode is given in Table 8 of Appendix A.

Theorem 3.1. *Let $\mathbb{F}_q$ be a finite field with a prime $q \equiv 3 \pmod 4$. Let $c \in \mathbb{F}_q \setminus \{-1, 0, 1\}$. Define $r = c - \frac{1}{c}$, $\alpha_1 = -2 + c + \frac{1}{c}$, and $\alpha_2 = -2 - c - \frac{1}{c}$. Then either α_1 or α_2 is a quadratic residue in $\mathbb{F}_q$. Without loss of generality, assume α_1 is a square and β is a square root of α_1. Define $\lambda = \frac{\alpha_2}{\alpha_1}$. Then for each $t \in \mathbb{F}_q \setminus \{\pm 1\}$, the following quantities are defined:*

$$u = \frac{1-t}{1+t},\ v = -u^5 + (r^2+2)u^3 - u,\ \epsilon = -\chi(v)^2 + \chi(v) + 1,$$
$$X = \epsilon u,\ Y = (\epsilon v)^{\frac{q+1}{4}} \epsilon \chi\left(u^2 - \frac{1}{c^2}\right),$$
$$x' = r^2 \frac{X}{(1+X)^2},\ y' = r^2 \frac{Y}{(1+X)^3},\ x = x'/\alpha_1,\ y = y'/\beta^3.$$

Furthermore, the point (x, y) lies on the Legendre curve $y^2 = x(x-1)(x-\lambda)$, and the point (X, Y) satisfies $Y^2 = -X^5 + (r^2+2)X^3 - X$.

Proof.

- **At least one of α_1 or α_2 is a sqaure**: By hypothesis, $\alpha_1 = -2+c+\frac{1}{c}$ and $\alpha_2 = -2-c-\frac{1}{c}$. Since $\alpha_1\alpha_2 = -\left(c - \frac{1}{c}\right)^2$ and -1 is a non-square in $\mathbb{F}_q$ (as $q \equiv 3 \pmod 4$), exactly one of α_1 or α_2 must be a quadratic residue.
- **$\mathbf{u}$ and $\mathbf{v}$ is defined and $\mathbf{u \neq 0}$** : Since $t \notin \{\pm 1\}$, both $1+t$ and $1-t$ are nonzero. Thus, u is well-defined and nonzero, and v is consequently defined.
- **$\mathbf{X + 1 \neq 0}$, so x' and y' are defined** : Suppose $X + 1 = 0$. Then, we have $X = -1 = \epsilon u$.
  - If $u = -1$, then $1 - t = -(1 + t)$, which implies $1 = -1$, a contradiction.
  - If $u = 1$, then $v = r^2$ and hence $X = 1$, again a contradiction.

  Therefore, $X + 1 \neq 0$, and so x' and y' are well-defined
- **x and y are defined** : If $\alpha_1 = 0$, then $-2 + c + \frac{1}{c} = 0 \Rightarrow c = 1$ which contradicts to $c \in \mathbb{F}_q \setminus \{-1, 0, 1\}$. Similarly, $\alpha_2 = 0 \Rightarrow c = -1$, which is another contradiction.

  Without loss of generality, let α_1 be a non-zero square and β be a square root of α_1. Then $\beta \neq 0$. Therefore, x and y are defined.
- **$(\mathbf{X}, \mathbf{Y})$ satisfies $\mathbf{Y^2 = -X^5 + (r^2 + 2)X^3 - X}$** : If $v \neq 0$, then $X = \epsilon u = \chi(v)u$. Furthermore, $-X^5 + (r^2+2)X^3 - X = \chi(v)(-u^5 + (r^2+2)u^3 - u) = \chi(v)v$. Since $\chi(\chi(v)v) = \chi(v)^2$, $\chi(v)v$ is a square. Therefore, we have $(\chi(v)v)^{\frac{q+1}{2}} = \chi(v)v$ and thus $(\chi(v)v)^{\frac{q+1}{4}}$ is the principal square root. On the other hand,

$$Y^2 = \left((\chi(v)v)^{\frac{q+1}{4}} \chi(v) \chi\left(u^2 - \frac{1}{c^2}\right)\right)^2 = (\chi(v)v)^{\frac{q+1}{2}} = \chi(v)v.$$

  Also, if $v = 0$, then $u \in \{\pm c, \pm\frac{1}{c}\}$, which implies $X \in \{\pm c, \pm\frac{1}{c}\}$. Then, $-X^5 + (r^2+2)X^3 - X = 0$. Therefore, (X, Y) lies on the curve $Y^2 = -X^5 + (r^2+2)X^3 - X$.

- $(\mathbf{x}', \mathbf{y}')$ **satisfies** $\mathbf{y'^2 = x'^3 + 4x'^2 - r^2x'}$:

$$\begin{aligned} y'^2 &= r^4 \frac{Y^2}{(1+X)^6} \\ &= \frac{r^4\left(-X^5 + (r^2+2)X^3 - X\right)}{(1+X)^6} \\ &= \frac{Xr^2}{(1+X)^2}\left(\frac{X^2r^4}{(1+X)^4} + \frac{4r^2X}{(1+X)^2} - r^2\right) \\ &= x'(x'^2 + 4x' - r^2) \\ &= x'^3 + 4x'^2 - r^2x. \end{aligned}$$

  Therefore, x' and y' satisfy $y'^2 = x'^3 + 4x'^2 - r^2x'$.

- $(\mathbf{x}, \mathbf{y})$ **satisfies** $\mathbf{y^2 = x(x-1)(x-\lambda)}$ where $\lambda = \alpha_2/\alpha_1$:

  The discriminant of $x'^2 + 4x' - r^2$ is $16 + 4r^2 = 16 + 4(c - \frac{1}{c})^2 = 4\left(c + \frac{1}{c}\right)^2$, a square. Therefore, $y'^2 = x'^3 + 4x'^2 - r^2x'$ can be written as

$$y'^2 = x'\left(x'^2 + 4x' - r^2\right) = x'\left(x'^2 + 4x' - \left(c - \frac{1}{c}\right)^2\right) = x'\left(x' - \alpha_1\right)\left(x' - \alpha_2\right).$$

  Without loss of generality, let α_1 be quadratic residue and $\beta = \alpha_1^{\frac{q+1}{4}}$ be the principal square root of α_1. Using the change of variables: $x = x'/\alpha_1$ and $y = y'/\beta^3$, we get

$$\begin{aligned} x(x-1)(x-\lambda) &= \frac{x'}{\alpha_1}\left(\frac{x'}{\alpha_1} - 1\right)\left(\frac{x'}{\alpha_1} - \lambda\right) \\ &= \frac{x'(x'-\alpha_1)(x'-\alpha_1\lambda)}{\alpha_1^3} \\ &= \frac{x'\left(x'-\alpha_1\right)\left(x'-\alpha_2\right)}{\alpha_1^3} \\ &= \frac{y'^2}{\beta^6} \\ &= y^2. \end{aligned}$$

  Therefore, (x, y) lies on the curve $y^2 = x(x-1)(x-\lambda)$.

□

Definition 3.2. Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$ and $\mathsf{E}_\lambda : y^2 = x(x-1)(x-\lambda)$ be a Legrendre curve over $\mathbb{F}_q$ with $\chi(\lambda) = -1$ and $\lambda \notin \{0, \pm 1\}$. Then, in the situation of Theorem 3.1, an encoding map $\psi_1 : \mathbb{F}_q \to \mathsf{E}_\lambda$ is defined by $\psi_1(\pm 1) = (0, 0)$ and if $t \neq \pm 1$ then $\psi_1(t) = (x, y)$.

3.1.1. *Existence of c for E_λ.* Let $\lambda \in \mathbb{F}_q \setminus \{0, \pm 1\}$ be fixed. Suppose there exists an element c such that:

$$\alpha_1 = -2 + c + \frac{1}{c}, \quad \alpha_2 = -2 - c - \frac{1}{c}.$$

We analyse two cases based on the quadratic residuosity of α_1 and α_2:

1. α_1 **is a quadratic residue and** α_2 **is not:** In this case, define $\lambda = \frac{\alpha_2}{\alpha_1}$. A straightforward simplification leads to the quadratic equation:

$$(\lambda + 1)c^2 - (2\lambda - 2) + (\lambda + 1) = 0.$$

This equation is solvable in $\mathbb{F}_q$ if and only if its discriminant, -16λ, is a square in the field. Therefore, we require $\chi(\lambda) = -1$.

2. α_1 **is not a quadratic residue and** α_2 **is:** In this scenario, $\frac{1}{\lambda} = \frac{\alpha_2}{\alpha_1}$, and the same algebraic steps apply. Thus, as in the previous case, we conclude that $\chi(\lambda) = -1$ must hold.

3.1.2. *Inversion of Elligator-L3 map.* The following theorem shows the invertibility of the Elligator-L3 map ψ_1, and the pseudocode is given in Table 8 of Appendix A.

Theorem 3.3. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$ and $\psi_1 : \mathbb{F}_q \to \mathsf{E}_\lambda$ be the encoding map defined in Definition 3.2. Then the following statements hold:*

1. *If $t \in \mathbb{F}_q$, then the set of preimage of $\psi_1(t)$ under the encoding ψ_1 is $\{t, -t\}$.*
2. *$\psi_1(\mathbb{F}_q)$ is the set of $(x, y) \in \mathsf{E}_\lambda(\mathbb{F}_q)$ satisfying*
   (a) if $x = 0$, then $y = 0$.
   (b) if $x \neq 0$, then $(1 - \zeta r^2)^2 - 1$ is a square where $\zeta = \frac{1}{2x\alpha_1}$.
   (c) if $\zeta r^2 = 2$, then $y = \frac{r^3\chi_1(c)}{8\beta^3}$.
3. *Let $(x, y) \in \psi_1(\mathbb{F}_q)$. If $(x, y) = (0, 0)$, then $\bar{t} = 1$ and if $x \neq 0$, the following elements $\bar{X}, z, \bar{u}, \bar{t}$ of $\mathbb{F}_q$ are defined and $\psi_1(\bar{t}) = (x, y)$:*

$$\bar{X} = -\left(1 - \zeta r^2\right) + \left(\left(1 - \zeta r^2\right)^2 - 1\right)^{\frac{q+1}{4}},$$
$$z = \chi\left(\beta^3(1 + \bar{X})^3 y\left(\bar{X}^2 - \frac{1}{c^2}\right)\right),$$
$$\epsilon = -z^2 + z + 1,\ \bar{u} = \epsilon\bar{X},\ \bar{t} = \frac{1 - \bar{u}}{1 + \bar{u}}.$$

Proof. Statement 1 has a forward part asserting $\psi_1(t) = \psi_1(-t)$, and the reverse part states that there is no other preimage. Similarly, statement 2 consists of both forward and reverse parts. The forward part states that any point $(x, y) \in \psi_1(\mathbb{F}_q)$ satisfies conditions (a), (b) and (c). The reverse part claims that any point $(x, y) \in \mathsf{E}_\lambda(\mathbb{F}_q)$ satisfying those conditions lies in $\psi_1(\mathbb{F}_q)$.

- First, we shall show that t and $-t$ map to the same point on $\mathsf{E}_\lambda(\mathbb{F}_q)$. If $t \in \{\pm 1\}$, then by definition, $\psi_1(t) = \psi_1(-t) = (0, 0)$.

  Assume $t \in S = \left\{\pm\frac{1-c}{1+c}, \pm\frac{1+c}{1-c}\right\}$. If $t = \pm\frac{1-c}{1+c}$, then $x = 1$ and $y = 0$. Similarly, if $t = \pm\frac{1+c}{1-c}$, then $x = \lambda$ and $y = 0$.

  Assume from now on that $t \in \mathbb{F}_q \setminus (S \cup \{\pm 1\})$. Then $v \neq 0$ which implies $\epsilon = \chi(v)$. Define u, v, X, Y, x', y', x, y from t as in Theorem 3.1. By definition $\psi_1(t) = (x, y)$.

  Let $t_1 = -t$. Let $u_1, v_1, \epsilon_1, X_1, Y_1, x'_1, y'_1, x_1, y_1$ be the values corresponding to t_1, as defined in Theorem 3.1. Then $u_1 = \frac{1-t_1}{1+t_1} = \frac{1+t}{1-t} = \frac{1}{u}$, and consequently $v_1 = -u_1^5 + (r^2 + 2)u_1^3 - u_1 = -\frac{1}{u^5} + (r^2 + 2)\frac{1}{u^3} - \frac{1}{u} = \frac{v}{u^6}$. Since u and v are both non-zero, it follows that $\epsilon_1 = \chi(v_1) = \chi(v)\chi(\frac{1}{u^6}) = \chi(v)$ as u^6 is a square.

  Next, we have that $X_1 = \chi(v_1)u_1 = \frac{1}{X}$, and $x'_1 = r^2\frac{X_1}{(1+X_1)^2} = r^2\frac{X}{(1+X)^2} = x'$. Thus, $x_1 = \frac{x'_1}{\alpha} = \frac{x'}{\alpha} = x$.

  Now let us focus on Y_1 and recall that $Y_1 = (\epsilon v_1)^{\frac{q+1}{4}}\epsilon\chi\left(u_1^2 - \frac{1}{c^2}\right)$. Note that $\chi(u)u^3$ is square, and hence it is the principal square root of u^6, that is,

$(u^6)^{\frac{q+1}{4}} = (u^3)^{\frac{q+1}{2}} = (u^3)^{\frac{q-1}{2}}u^3 = \chi(u^3)u^3 = \chi(u)u^3 = \epsilon u^3$. Then

$$\begin{aligned}
Y_1 &= (\epsilon_1 v_1)^{\frac{q+1}{4}}\epsilon_1\chi\left(u_1^2 - \frac{1}{c^2}\right)\\
&= (\chi(v_1)v_1)^{\frac{q+1}{4}}\chi(v_1)\chi\left(u_1^2 - \frac{1}{c^2}\right)\\
&= \left(\chi(v)\frac{v}{u^6}\right)^{\frac{q+1}{4}}\chi(v_1)\chi\left(u_1^2 - \frac{1}{c^2}\right) \text{ [Putting } v_1 = v/u^6\text{]}\\
&= (\chi(v)v)^{\frac{q+1}{4}}\left(\frac{1}{u^6}\right)^{\frac{q+1}{4}}\chi(v_1)\chi\left(u_1^2 - \frac{1}{c^2}\right)\\
&= (\chi(v)v)^{\frac{q+1}{4}}\left(\frac{1}{\chi(u)u^3}\right)\chi(v_1)\chi\left(u_1^2 - \frac{1}{c^2}\right)\\
&= (\chi(v)v)^{\frac{q+1}{4}}\left(\frac{\chi(u)}{u^3}\right)\chi(v_1)\chi\left(u_1^2 - \frac{1}{c^2}\right) \text{ [note that } \chi(u) = 1/\chi(u)\text{]}\\
&= (v\chi(v))^{\frac{q+1}{4}}\frac{\chi(u)}{u^3}\chi(v)\chi\left(\frac{1}{u^2} - \frac{1}{c^2}\right) \text{ [Putting } \chi(v) = \chi(v_1) \text{ and } u_1 = 1/u\text{]}\\
&= (v\chi(v))^{\frac{q+1}{4}}\frac{\chi(uv)}{u^3}\chi\left(c^2u^4\left(\frac{1}{u^2} - \frac{1}{c^2}\right)\left(u^2 - \frac{1}{c^2}\right)^2\right) \left[\text{As } \chi(a) = \chi(ab^2)\right]\\
&= (v\chi(v))^{\frac{q+1}{4}}\frac{\chi(uv)}{u^3}\chi\left(uv\left(u^2 - \frac{1}{c^2}\right)\right) \left[\text{Putting } v = -u(u^2 - c^2)\left(u^2 - \frac{1}{c^2}\right)\right]\\
&= (v\chi(v))^{\frac{q+1}{4}}\frac{1}{u^3}\chi\left(u^2 - \frac{1}{c^2}\right)\\
&= \frac{(v\chi(v))^{\frac{q+1}{4}}\chi(v)\chi\left(u^2 - \frac{1}{c^2}\right)}{u^3\chi(v)}\\
&= \frac{(v\epsilon)^{\frac{q+1}{4}}\epsilon\chi\left(u^2 - \frac{1}{c^2}\right)}{u^3\chi(v)}\\
&= \frac{Y}{(u\epsilon)^3}\\
&= \frac{Y}{X^3}.
\end{aligned}$$

Therefore, $y_1' = r^2\frac{Y_1}{(1+X_1)^3} = r^2\frac{\frac{Y}{X^3}}{(1+\frac{1}{X})^3} = y'$ and $y_1 = \frac{y_1'}{\beta^3} = \frac{y'}{\beta^3} = y$. Hence, $\psi_1(-t) = (x, y)$ and forward part of statement 1 is proved. The latter part of the proof contains the proof of the reverse of statement 1.

- Next, we will prove the forward part of statement 2. Let $(x, y) \in \mathsf{E}_\lambda(\mathbb{F}_q)$. By Theorem 3.1, there are two cases (a) if $t \in \{\pm 1\}$ then $x = 0$, and (b) if $t \notin \{\pm 1\}$ then $x \neq 0$.

  By definition of ψ_1, $\psi_1(\pm 1) = (0, 0)$. Now assume $x \neq 0$. Then, by Theorem 3.1, we know that $x = r^2\frac{X}{\alpha_1(1+X)^2}$ which can be rearranged into

$$X^2 + 2\left(1 - \zeta r^2\right)X + 1 = 0. \tag{3}$$

  Equation (3) has a root if the discriminant is a square. The discriminant is

$$4\left(1 - r^2\frac{1}{2\alpha_1 x}\right)^2 - 4 = 4((1 - \zeta r^2)^2 - 1).$$

Thus, a solution exists if $(1-\zeta r^2)^2-1$ is a square in $\mathbb{F}_q$, proving statements 2a and 2b.

Dividing equation (3) by X, we obtain $X+\frac{1}{X}=-2\left(1-\zeta r^2\right)$, which will be useful latter.

To prove statement 2c, substitute $\zeta r^2=2$ into equation (3):

$$X^2+2(1-2)X+1=0 \Rightarrow X^2-2X+1=0 \Rightarrow (X-1)^2=0 \Rightarrow X=1.$$

From Theorem 3.1, we have $X=\epsilon u$. Since $X=1$, it follows that $u\in\{\pm 1\}$. If $u=-1$, then $1-t=-(1+t)\Rightarrow 1=-1$ which is a contradiction. Therefore, $u=1$ and then $t=0$. Now compute $v=-1^5+(r^2+2)1^3-1=r^2$. Then $Y=(r^2)^{\frac{q+1}{4}}\chi(1-\frac{1}{c^2})=\chi(r)r\chi(r/c)=\chi(r)r\chi(rc/c^2)=\chi(r)r\chi(rc)=r\chi(c)$, since $\chi(1/c^2)=1$ and $\chi(r^2)=1$. Therefore, $x=\frac{r^2}{4\alpha_1}$ and $y=\frac{r^3\chi(c)}{8\beta^3}$, so $\psi_1(0)=\left(\frac{r^2}{4\alpha_1},\frac{r^3\chi(c)}{8\beta^3}\right)$. This completes the proof of the forward part of statement 2c. These final expressions of x and y will be used latter.

- Now, we prove statement 3 of the theorem. As before, there are two cases: (a) if $t\in\{\pm 1\}$ then $(x,y)=(0,0)$, and (b) if $t\notin\{\pm 1\}$ then $(x,y)\neq(0,0)$.

  The first case is straightforward. For the second case, assume $(x,y)\neq(0,0)$. Define u,v,X,Y,x',y',x,y from $t\in\mathbb{F}_q\setminus\{\pm 1\}$ as in Theorem 3.1. Then, by definition, $\psi_1(t)=(x,y)$.

  Now fix $t_1=-t$ and define the corresponding values $u_1,v_1,X_1,Y_1,x_1',y_1',x_1,y_1$ for t_1.

  By the construction of $\bar{X}$, we know that $1-\zeta r^2+\bar{X}$ is a square root of $(1-\zeta r^2)^2-1$. Hence $(1-\zeta r^2+\bar{X})^2=(1-\zeta r^2)^2-1$ which simplifies to the equation

$$\bar{X}^2+2(1-\zeta r^2)\bar{X}+1=0. \tag{4}$$

  Observe that $X_1=\frac{1}{X}$ and thus $X+X_1=-2(1-\zeta r^2)$, where $\zeta=\frac{1}{2\alpha_1 x}$. Then, $(\bar{X}-X)(\bar{X}-X_1)=\bar{X}^2-(X+X_1)\bar{X}+XX_1=\bar{X}^2+2(1-\zeta r^2)\bar{X}+1$. This confirms that X and X_1 are two roots of equation (4).

  Now consider the case $\bar{X}=X$. Then $y=r^2\frac{Y}{\beta^3(1+X)^3}$ and hence,

$$z=\chi\left(Y\left(X^2-\frac{1}{c^2}\right)\right)=\chi(Y)\chi\left(X^2-\frac{1}{c^2}\right) \text{ and } \epsilon=-z^2+z+1.$$

  If $v\neq 0$, then $\epsilon=\chi(v)$ and $(\epsilon v)^{\frac{q+1}{4}}$ is a square. Also, $\chi(u^2-1/c^2)=\chi(X^2-1/c^2)$. Therefore, $\chi(Y)=\chi\left((\epsilon v)^{\frac{q+1}{4}}\epsilon\chi\left(X^2-\frac{1}{c^2}\right)\right)=\epsilon\chi\left(X^2-\frac{1}{c^2}\right)$ which implies $\epsilon=\chi(v)=z$. Furthermore, if $v=0$, then $\epsilon=1$.

  From Theorem 3.1, we have $X=\epsilon u$, so $\bar{u}=\epsilon X=u$ and thus $\bar{t}=t$.

  Similarly, if $\bar{X}=X_1$, then $\epsilon=\chi(v_1)$, $\bar{u}=u_1$ and $\bar{t}=t_1=-t$. This proves statement 3. Using the same reasoning, it follows that for any fixed $(x,y)\in\mathsf{E}_\lambda(\mathbb{F}_q)$, the only possible preimages under ψ_1 are $\{t,-t\}$, which completes the proof of the reverse direction of statement 1.

- Now, we come to the final part of the proof: the reverse direction of statement 2. Let, $(x,y)\in\mathsf{E}_\lambda(\mathbb{F}_q)$ such that (a) if $x=0$, then $y=0$, and (b) if $x\neq 0$, then $(1-\zeta r^2)^2-1$ is a square where $\zeta=\frac{1}{2\alpha_1 x}$. Also, if $\zeta r^2=2$, then $x=\frac{r^2}{4\alpha_1}$. We must show that $(x,y)\in\psi_1(\mathbb{F}_q)$.

  If $x=0$, then $y=0$ from the equation of E_λ, and by definition, $(x,y)=(0,0)=\psi_1(1)\in\psi_1(\mathbb{F}_q)$. So, the claim holds in this case.

Next, assume that $x \neq 0$. Set $X = -(1-\zeta r^2) + ((1-\zeta r^2)^2 - 1)^{\frac{q+1}{4}}$. Then, $1-\zeta r^2+X$ is a square root of $(1-\zeta r^2)^2-1$. Thus $X^2+2(1-\zeta r^2)X+1 = 0$. This quadratic identity, established earlier, leads to several key implications. First, $X \neq 0$. Second, $X \neq -1$. If $X = -1$ then $X^2+2(1-\zeta r^2)X+1 = 0 \Rightarrow \zeta r^2 = 0$. Substituting $\zeta = \frac{1}{2\alpha_1 x}$ and $r^2 = -\alpha_1\alpha_2$, we get $\frac{\alpha_2}{2x} = 0 \Rightarrow \alpha_2 = 0$. This further implies $c = -1$, since $\alpha_2 = -2 - c - \frac{1}{c}$. But this leads to a contradiction, so $X \neq -1$. Third, substituting $\zeta = \frac{1}{2\alpha_1 x}$ into $X^2 + 2(1-\zeta r^2)X + 1 = 0$ gives $x = r^2\frac{X}{\alpha_1(1+X)^2}$.

If $X = 1$, then $x = \frac{r^2}{4\alpha_1}$. Also, $\zeta r^2 = 2$ implies $y = \frac{r^3\chi(c)}{8\beta^3}$. Thus, $(x, y) = \psi_1(0) \in \psi_1(\mathbb{F}_q)$.

If $X \neq 1$, then

$$\begin{aligned}
y^2 &= x(x-1)(x-\lambda)\\
&= \frac{1}{\alpha_1^3(1+X)^6}(r^2X(r^2X - \alpha_1(1+X)^2)(r^2X - \lambda\alpha_1(1+X)^2))\\
&= \frac{1}{\alpha_1^3(1+X)^6}(r^2X(r^2X - \alpha_1(1+X)^2)(r^2X - \alpha_2(1+X)^2))\\
&\quad [\text{As } \lambda = \alpha_2/\alpha_1]\\
&= \frac{r^2X}{\alpha_1^3(1+X)^6}(r^4X^2 - (\alpha_1+\alpha_2)r^2X(1+X)^2 + \alpha_1\alpha_2(1+X)^4)\\
&= \frac{r^2X}{\alpha_1^3(1+X)^6}(r^4X^2 + 4r^2X(1+X)^2 - r^2(1+X)^4)\\
&= \frac{r^4}{\alpha_1^3(1+X)^6}(-X^5 + (r^2+2)X^3 - X).
\end{aligned}$$

Define $Y = y\beta^3(1+X)^3/r^2$, where β is a square root of α_1. Then,

$$Y^2 = y^2\beta^6(1+X)^6/r^4 = -X^5 + (r^2+2)X^3 - X.$$

Next, define $z = \chi(Y(X^2 - \frac{1}{c^2}))$ and $\epsilon = -z^2 + z + 1$. Clearly, $\epsilon \in \{\pm 1\}$.

Define $u = \epsilon X$. Then, $u \in \{\pm X\}$, and since $X \neq \pm 1$, $u \neq \pm 1$.

Now define $v = -u^5 + (r^2+2)u^3 - u$. Substituting $u = \epsilon X$ and using the identity for Y^2, we find that $v = \epsilon Y^2$. If $y = 0$, then $Y = 0$, and so $X \in \{\pm c, \pm\frac{1}{c}\}$. Consequently, $z = 0$ and $\epsilon = 1$. Now if, $y \neq 0$, then $Y \neq 0$, and we compute $\chi(v) = \chi(\epsilon Y^2) = \chi(\epsilon) = \epsilon$. Then, $X = \epsilon u$ and $Y^2 = \epsilon v$. Since $Y \neq 0$, then $v \neq 0$ and $\chi(v) = z = \epsilon = \chi(Y(X^2 - \frac{1}{c^2})) = \chi(Y(u^2 - \frac{1}{c^2}))$, so again we have $\chi(Y) = \epsilon\chi(u^2 - \frac{1}{c^2})$. Now, taking the principal square root, we get $Y = (\epsilon v)^{\frac{q+1}{4}}\epsilon\chi(u^2 - \frac{1}{c^2})$. Define $t = \frac{1-u}{1+u}$. Then, $t \notin \{\pm 1\}$ and $u = \frac{1-t}{1+t}$. The formulas for u, v, X, Y, x', y', x, y are satisfied and so we conclude, $\psi_1(t) = (x, y) \in \psi_1(\mathbb{F}_q)$.

□

3.1.3. *Encoding as strings.* The following theorem is an adaptation of Theorem 4 of [2]. However, we include it here to make this article self-contained. Let q be a prime number of b bits. Let R be the set of all b-bit binary stings whose decimal values lie in the set $\{0, 1, \ldots, \frac{q-1}{2}\}$. The theorem below shows that the mapping ψ_1 induces an injection from R to $\mathsf{E}_\lambda(\mathbb{F}_q)$.

Theorem 3.4. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$. Let $\psi_1 : \mathbb{F}_q \to \mathsf{E}_\lambda$ be the map defined in Definition 3.2. Fix $b = \lfloor \log_2 q \rfloor$ and define a map $\sigma : \{0,1\}^b \to \mathbb{F}_q$ by $\sigma(\rho_0, \rho_1, \ldots, \rho_{b-1}) = \sum_i \rho_i 2^i$. Define a set $R = \sigma^{-1}\left(\left\{0, 1, 2, \ldots, \frac{q-1}{2}\right\}\right)$. Define $\tau_1 : R \to \mathsf{E}_\lambda(\mathbb{F}_q)$ by $\tau_1(\rho) = \psi_1(\sigma(\rho))$. Then, R has exactly $\frac{q+1}{2}$ elements, τ_1 is injective and $\tau_1(R) = \psi_1(\mathbb{F}_q)$.*

Proof. Since $2^b \leq q$, the integers in the set $\{0, 1, \ldots, 2^b - 1\}$ are all distinct in $\mathbb{F}_q$. Hence, the mapping σ is injective. Furthermore, since $2^b > \frac{q}{2}$, it follows that the set $\left\{0, 1, 2, \ldots, \frac{q-1}{2}\right\}$ is a subset of $\left\{0, 1, 2, \ldots, 2^b - 1\right\}$. Therefore, every element in $\left\{0, 1, \ldots, \frac{q-1}{2}\right\}$ has a preimage under σ, and thus the set R contains exactly $\frac{q+1}{2}$ elements.

Now, suppose $\tau_1(\rho) = \tau_1(\rho')$. Then $\psi_1(\sigma(\rho)) = \psi_1(\sigma(\rho'))$, which implies that $\sigma(\rho) = \pm\sigma(\rho')$. Since both $\sigma(\rho)$ and $\sigma(\rho')$ lie in the range $\left\{0, 1, \ldots, \frac{q-1}{2}\right\}$, it must be that $\sigma(\rho) = \sigma(\rho')$, and hence $\rho = \rho'$. This shows that τ_1 is injective.

Each element of $\tau_1(R)$ is of the form $\psi_1(\sigma(\rho))$, and so $\tau_1(R) \subseteq \psi_1(\sigma(R))$. Conversely, let $x \in \psi_1(\mathbb{F}_q)$, so $x = \psi_1(t)$ for some $t \in \mathbb{F}_q$. By Theorem 3.3, we also have $x = \psi_1(-t)$. Since at least one of t or $-t$ lies in the range $\left\{0, 1, \ldots, \frac{q-1}{2}\right\}$, it follows that $x \in \tau_1(R)$. Therefore, $\psi_1(\sigma(R)) \subseteq \tau_1(R)$, and we conclude that $\tau_1(R) = \psi_1(\mathbb{F}_q)$. □

3.2. **Elligator-L1 map.** This section focuses on mapping elements from finite field $\mathbb{F}_q$ with prime $q \equiv 1 \pmod 4$ to a Legendre curve. The following theorem explicitly describes the map, which we call Elligator-L1, and the pseudocode is given in Table 9 of Appendix B.

Theorem 3.5. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 1 \pmod 4$. Let $\lambda \in \mathbb{F}_q$ with $\chi(\lambda) = 1$ and $\lambda \notin \{0, \pm 1\}$, and u be a non-square in $\mathbb{F}_q$. For any non-zero $t \in \mathbb{F}_q$, the following quantities are defined:*

$$v = \frac{\lambda + 1}{1 + ut^2}, \quad \epsilon = \chi(v(v-1)(v-\lambda)),$$
$$x = \epsilon v + (1 - \epsilon)(\lambda + 1)/2, \quad y = -\epsilon\sqrt{x(x-1)(x-\lambda)}.$$

Furthermore, $y^2 = x(x-1)(x-\lambda)$.

Proof.

- **$\mathbf{v}$ is defined and $\mathbf{v \neq 0}$** : Suppose $1 + ut^2 = 0$. Then $t^2 = -\frac{1}{u}$, which is a contradiction since -1 is a square and u is a non-square. Thus, $1 + ut^2 \neq 0$, so $v = \frac{\lambda+1}{1+ut^2}$ is defined. Also, since $\lambda \notin \{0, \pm 1\}$, it follows that $v \neq 0$.
- **$\mathbf{v(v-1)(v-\lambda)}$ is non-zero:** Assume $v(v-1)(v-\lambda) = 0$. Since $v \neq 0$, we must have either $v = 1$ or $v = \lambda$. If $v = 1$, then $\frac{\lambda+1}{1+ut^2} = 1 \Rightarrow \lambda = ut^2$. But then $\chi(\lambda) = \chi(u)\chi(t^2) = -1$, contradicting the assumption that $\chi(\lambda) = 1$. If $v = \lambda$, then $\frac{\lambda+1}{1+ut^2} = \lambda \Rightarrow \lambda ut^2 = 1$, which again contradicts the fact that λut^2 is a non-square, while 1 is a square. Hence, $v(v-1)(v-\lambda) \neq 0$.
- **$\mathbf{x(x-1)(x-\lambda)}$ is non-zero and square:** If $\epsilon = 1$, then $x = v$, and so $x(x-1)(x-\lambda) = v(v-1)(v-\lambda)$, which is non-zero and a square.

  If $\epsilon = -1$, then $x = -v + (\lambda + 1) = vut^2$. Each term of x is non-zero and hence $x \neq 0$. Let $x(x-1)(x-\lambda) = 0$. Now either $x = 1$ or λ where $x = vut^2$. If $vut^2 = 1$, then $\left(\frac{\lambda+1}{1+ut^2}\right) ut^2 = 1 \Rightarrow \lambda ut^2 = 1$. Now λut^2 is a non-square from the assumptions of the theorem. However, 1 is a square, which is a contradiction. Similarly if $vut^2 = \lambda$, then $\left(\frac{\lambda+1}{1+ut^2}\right) ut^2 = \lambda \Rightarrow ut^2 = \lambda$, which again forms a similar contradiction. Hence, $x(x-1)(x-\lambda)$ is non-zero.

Again for $\epsilon = -1$, $x = vut^2$ gives that $\chi(x) = -\chi(v)\chi(u)\chi(t^2) = -\chi(v)$ since u is a non-square. Notice that $v = \frac{\lambda+1}{1+ut^2} \Rightarrow vut^2 = -v+(\lambda+1)$ and thus $x = -v + (\lambda+1)$. Now $x(x-(\lambda+1)) = (-v+(\lambda+1))(-v) = v(v-(\lambda+1))$ and therefore $x^2-(\lambda+1)x+\lambda = v^2-(\lambda+1)v+\lambda$. Then $\chi(x(x-1)(x-\lambda)) = \chi(x)\chi((x-1)(x-\lambda)) = -\chi(v)\chi((v-1)(v-\lambda)) = -\chi(v(v-1)(v-\lambda)) = -\epsilon = 1$. Hence, $x(x-1)(x-\lambda)$ is a square.

- **$\mathbf{y}$ is defined, $\mathbf{y \neq 0}$ and $(\mathbf{x}, \mathbf{y})$ satisfies $\mathbf{y^2 = x(x-1)(x-\lambda)}$** : Since $x(x-1)(x-\lambda)$ is non-zero and a square, $y = \sqrt{x(x-1)(x-\lambda)}$ is defined and non-zero. By construction, $y^2 = x(x-1)(x-\lambda)$.

□

Definition 3.6. Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 1 \pmod 4$ and $\mathsf{E}_\lambda : y^2 = x(x-1)(x-\lambda)$ be a Legrendre curve over $\mathbb{F}_q$ with $\chi(\lambda) = 1$ and $\lambda \notin \{0, \pm 1\}$. Then, in the situation of Theorem 3.5, an encoding map $\psi_2 : \mathbb{F}_q \to \mathsf{E}_\lambda$ is defined by $\psi_2(0) = (0,0)$ and if $t \neq 0$ then $\psi_2(t) = (x, y)$.

3.2.1. *Inversion of Elligator-L1 map.* In this section, we provide the inversion of the Elligator-L1 map ψ_2, and the pseudocode is given in Table 9 of Appendix B.

Theorem 3.7. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 1 \pmod 4$ and $\psi_2 : \mathbb{F}_q \to \mathsf{E}_\lambda$ be the encoding map defined in Definition 3.6. Then the following statements hold:*

1. *If $t \in \mathbb{F}_q$, then the set of preimage of $\psi_2(t)$ under the encoding ψ_2 is $\{t, -t\}$.*
2. *For any (x, y) in $\mathsf{E}_\lambda(\mathbb{F}_q), (x, y)$ is in $\psi_2(\mathbb{F}_q)$ if and only if*
   (a) $x \neq \lambda + 1$ and if $y = 0$ then $x = 0$.
   (b) $-xu(x-\lambda-1)$ is square in $\mathbb{F}_q$.
3. *If $(x, y) \in \psi_2(\mathbb{F}_q)$, then $\bar{t}$ is defined and $\psi_2(\bar{t}) = (x, y)$:*

$$\bar{t} = \begin{cases} \sqrt{-x/((x-\lambda-1)u)}, & \text{if } y \in \sqrt{\mathbb{F}_q^2}, \\ \sqrt{-(x-\lambda-1)/(xu)}, & \text{if } y \notin \sqrt{\mathbb{F}_q^2}. \end{cases}$$

Proof. This proof is identical to the proof of Theorem 7 of [2] with A replaced by $-(\lambda+1)$ and B replaced by λ. □

3.2.2. *Encoding as strings.* Let q be a prime that is b-bit long. Define R as the set of all binary strings of length b, whose decimal values range from 0 to $\frac{q-1}{2}$. The following theorem shows that the map ψ_2 induces an injection from the set R into the elliptic curve $\mathsf{E}_\lambda(\mathbb{F}_q)$.

Theorem 3.8. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 1 \pmod 4$ and $\psi_2 : \mathbb{F}_q \to \mathsf{E}_\lambda$ be the encoding map defined in Definition 3.6. Fix $b = \lfloor \log_2 q \rfloor$ and define a map $\sigma : \{0,1\}^b \to \mathbb{F}_q$ by $\sigma(\rho_0, \rho_1, \ldots, \rho_{b-1}) = \sum_i \rho_i 2^i$. Define a set $R = \sigma^{-1}(\{0, 1, 2, \ldots, \frac{q-1}{2}\})$. Now we can define an injective map $\tau_2 : R \to \mathsf{E}_\lambda(\mathbb{F}_q)$ by $\tau_2(\rho) = \psi_2(\sigma(\rho))$. Then, R has exactly $\frac{q+1}{2}$ elements, τ_2 is injective and $\tau_2(R) = \psi_2(\mathbb{F}_q)$.*

Proof. This proof is almost identical to Theorem 3.4. Therefore, we omit the proof. □

4. **Maps to Kummer line.** In this section, we extend Elligator-L3 and Elligator-L1 maps to Kummer lines. To do so, we first reduce to Elligator-L3 and Elligator-L1 map up to x-coordinate only version and then compose those reduced maps with the mapping Π^{-1} from the Legendre curve to the Kummer Line to achieve the desired mappings. The details of the final maps are given below.

4.1. **Elligator-K3 map.** In this section, we consider the extension of Elligator-L3 map to Kummer lines over finite field $\mathbb{F}_q$ with prime $q \equiv 3 \pmod 4$. The following lemma gives the explicit map, and the pseudocode is given in Table 10 of Appendix C.

Lemma 4.1. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$. Let $c \in \mathbb{F}_q \setminus \{-1, 0, 1\}$, $r = c - \frac{1}{c}$ and $S = \left\{\pm\frac{1-c}{1+c}, \pm\frac{1+c}{1-c}\right\}$. Then either $\alpha_1 = -2 + c + \frac{1}{c}$ or $\alpha_2 = -2 - c - \frac{1}{c}$ is a square. Without loss of generality, assume that α_1 is square and β is a square root of α_1. Let $\mathcal{K}_{a^2,b^2}$ be the Kummer Line associated with Legendre curve E_λ where $\lambda = \frac{a^4}{a^4-b^4} = \frac{\alpha_2}{\alpha_1}$ over a finite field $\mathbb{F}_q$.*

1. *First we define the x-coordinate only version of map ψ_1 of Theorem 3.1 as given below and we call it ψ_{1x}. If $t \neq \pm 1$, then*
$$u = \frac{1-t}{1+t},\ v = -u^5 + (r^2+2)u^3 - u,\ \epsilon = -\chi(v)^2 + \chi(v) + 1,$$
$$X = \epsilon u,\ x' = r^2\frac{X}{(1+X)^2},\ x = \frac{x'}{\alpha_1},$$
where $(x, \cdot)$ is a point on E_λ.
2. *Now composition of ψ_{1x} and Π^{-1} of equation (2), we get a map $\hat{\psi_{1x}} = \Pi^{-1} \circ \psi_{1x} : \mathbb{F}_q \setminus \{S \cup \{\pm 1\}\} \to \mathcal{K}_{a^2,b^2}$ defined as follows:*
$$u = \frac{1-t}{1+t},\ v = -u^5 + (r^2+2)u^3 - u,\ \epsilon = -\chi(v)^2 + \chi(v) + 1,$$
$$X = \epsilon u,\ x' = r^2\frac{X}{(1+X)^2},\ x = \frac{x'}{\alpha_1},$$
$$\mathsf{X} = b^2 x,\ \mathsf{Z} = a^2(x-1).$$

Proof. 1. First let us define $Y = (\epsilon v)^{\frac{q+1}{4}}\epsilon\chi\left(u^2 - \frac{1}{c^2}\right)$, and $y = r^2\frac{Y}{\beta^3(1+X)^3}$. Now by the proof of Theorem 3.1, we can show that (x, y) satisfies $\mathsf{E}_\lambda : y^2 = x(x-1)(x-\lambda)$. This implies that there exists a y corresponding to x defined in the proposed theorem such that (x, y) is a point on the Legendre curve E_λ.
2. As there exists a birational equivalence between E_λ and $\mathcal{K}_{a^2,b^2}$ by the mappings of equations (1) and (2), we can convert the projective version of $(x, \cdot)$, that is $(x : \cdot : 1)$, to a birational equivalent point $(\mathsf{X} : \mathsf{Z})$ as
$$\Pi^{-1}(x : \cdot : 1) = (b^2 x : a^2(x-1)) = (\mathsf{X} : \mathsf{Z}).$$

□

Definition 4.2. Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$ and $\mathcal{K}_{a^2,b^2}$ be a Kummer line over $\mathbb{F}_q$. Then, in the situation of Lemma 4.1, an encoding map $\hat{\psi_1} : \mathbb{F}_q \to \mathcal{K}_{a^2,b^2}$ is defined by (i) if $t \in \{\pm 1\} \cup S$, then $\hat{\psi_1}(t) = (b^2 : a^2)$, and (ii) otherwise, $\hat{\psi_1}(t) = (\mathsf{X} : \mathsf{Z})$.

4.1.1. *Inversion of Elligator-K3.* In the follwoing section, we show that Elligator-K3 is efficiently invertible. First, in Lemma 4.3, we show that the map ψ_{1x} is efficiently invertible and then we extend the invertibility from the Kummer line to a field element by Corollary 4.4. The corresponding pseudocode is given in Table 10 of Appendix C.

Lemma 4.3. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$ and $\psi_{1x} : \mathbb{F}_q \to \mathsf{E}_\lambda/\{\pm 1\}$ be the encoding map defined in Lemma 4.1. Then the followings hold:*

1. *For any* $t \in \mathbb{F}_q \setminus \{S \cup \{\pm 1\}\}$, ψ_{1x} *maps* $\left\{\pm t, \pm \frac{1}{t}\right\}$ *to a* x *such that the points* $(x, \cdot) \in \mathsf{E}_\lambda(\mathbb{F}_q)$.
2. $\psi_{1x}(\mathbb{F}_q)$ *is the set of* x *such that* $(x, \cdot) \in \mathsf{E}_\lambda(\mathbb{F}_q)$ *satisfying if* $x \neq 0$, *then* $(1-\zeta r^2)^2 - 1$ *is a square where* $\zeta = \frac{1}{2x\alpha_1}$.
3. *If* $x \in \psi_{1x}(\mathbb{F}_q)$, *then if* $x \neq 0$ *the following elements* $\bar{X}, \bar{t}$ *of* $\mathbb{F}_q$ *are defined and* $\psi_{1x}(\bar{t}) = x$*:*

$$\bar{X} = -\left(1-\zeta r^2\right) + \left(\left(1-\zeta r^2\right)^2 - 1\right)^{\frac{q+1}{4}}, \ \bar{t} = \frac{1-\bar{X}}{1+\bar{X}}.$$

Furthermore, if $x = 0$, *then* $\bar{t} = 1$.

Proof. By Theorem 3.3, we have already shown that ψ_1 maps t and $-t$ to the same point of $\mathsf{E}_\lambda(\mathbb{F}_q)$, that is, $\psi_{1x}(t) = \psi_{1x}(-t)$. To conclude that ψ_{1x} maps $\left\{\pm t, \pm \frac{1}{t}\right\}$ to the points on $\mathsf{E}_\lambda(\mathbb{F}_q)$ whose x-coordinates are the same, we only need to show that t and $\frac{1}{t}$ map to the points $(x, \cdot) \in \mathsf{E}_\lambda(\mathbb{F}_q)$ by ψ_1 that is $\psi_{1x}(t) = \psi_{1x}(\frac{1}{t}) = x$.

For any $t \in \mathbb{F}_q \setminus \{S \cup \{\pm 1\}\}$, u, v, X, x' and x are defined as in Lemma 4.1. Now, let $t_1 = \frac{1}{t}$. Then we have $u_1 = \frac{1-t_1}{1+t_1} = -u$ and $v_1 = -u_1^5 + (r^2+2)u_1^3 - u_1 = -(-u^5 + (r^2+2)u^3 - u) = -v$. This implies $X_1 = \chi(-v)(-u) = \chi(v)u = X, x_1' = x'$ and $x_1 = x$. Conversely, let $t_1, t_2 \in \mathbb{F}_q$ such that $\psi_{1x}(t_1) = \psi_{1x}(t_2) = x$. Then, $\frac{r^2 X_1}{\alpha_1(1+X_1)^2} = \frac{r^2 X_2}{\alpha_1(1+X_2)^2}$ and this implies $X_1 X_2 = 1$ or $X_1 = X_2$. $X_1 X_2 = 1$ implies $t_1 = -t_2$ or $t_1 = -\frac{1}{t_2}$ and $X_1 = X_2$ implies $t_1 = t_2$ or $t_1 = \frac{1}{t_2}$. This proves statement 1 of the lemma.

Statement 2 is already proved in Theorem 3.3.

Now, we come to statement 3 of the lemma. Let $x \in \psi_{1x}(\mathbb{F}_q)$ and $\zeta = \frac{1}{2x\alpha_1}$. This also implies $(x, \cdot) \in \psi_1(\mathbb{F}_q)$. First note that $x \neq 0$ and $((1-\zeta r^2)^2 - 1)$ is a square by statement 2. From statement 3 of Theorem 3.3, the expression z provides the sign using the value of the y-coordinate. Using $\bar{u} = \epsilon \bar{X}$, we get two value of $\bar{t}$ and both the value maps to $(x, \cdot)$ by statement 1. Hence, we omit the computation of z, ϵ and $\bar{u}$, and the inverse map is given by

$$\bar{X} = -\left(1-\zeta r^2\right) + \left(\left(1-\zeta r^2\right)^2 - 1\right)^{\frac{q+1}{4}}, \ \bar{t} = \frac{1-\bar{X}}{1+\bar{X}}.$$

□

Corollary 4.4. *In the situation of Lemma 4.1 and Lemma 4.3, the following statements hold:*

1. *For any* $t \in \mathbb{F}_q$, $\hat{\psi}_1$ *maps* $\left\{\pm t, \pm \frac{1}{t}\right\}$ *to the points* $(\mathsf{X} : \mathsf{Z}) \in \mathcal{K}_{a^2,b^2}$.
2. *Let* $(\mathsf{X} : \mathsf{Z}) \in \mathcal{K}_{a^2,b^2}$ *and* $(x, \cdot) = \left(\frac{a^2 \mathsf{X}}{a^2 \mathsf{X} - b^2 \mathsf{Z}}, \cdot\right) \in \mathsf{E}_\lambda$. *If* x *satisfying statement 2 of Lemma 4.3, then the following elements* $\bar{X}, \bar{t}$ *of* $\mathbb{F}_q$ *are defined and* $\hat{\psi}_1(\bar{t}) = (\mathsf{X} : \mathsf{Z})$*:*

$$\bar{X} = -\left(1-\zeta r^2\right) + \left(\left(1-\zeta r^2\right)^2 - 1\right)^{\frac{q+1}{4}}, \ \bar{t} = \frac{1-\bar{X}}{1+\bar{X}}.$$

4.1.2. *Encoding as strings.* Let q be a b-bit prime and $T_1 \subset \{0,1\}^b$ as defined below. Corollary 4.5 shows the injection between T_1 and the Kummer line.

Corollary 4.5. *Let* $\mathbb{F}_q$ *be a finite field with prime* $q \equiv 3 \pmod 4$. *Fix* $b = \lfloor \log_2 q \rfloor$ *and define a map* $\sigma : \{0,1\}^b \to \mathbb{F}_q$ *by* $\sigma(\rho_0, \rho_1, \ldots, \rho_{b-1}) = \sum_i \rho_i 2^i$. *Let* $\varsigma_1 : t \mapsto \frac{1}{t}$ *and* $\varsigma_2 : t \mapsto -t$ *for* $t \in \mathbb{F}_q$. *Define* $T_1 = \sigma^{-1}\left(\mathbb{F}_q / \langle \varsigma_1, \varsigma_2 \rangle\right)$. *Then, by using Lemma 4.1, the map* $\hat{\tau}_1 = \hat{\psi}_1 \circ \sigma : T_1 \to \mathcal{K}_{a^2,b^2}$ *is defined, then* $\hat{\tau}_1(T_1) = \hat{\psi}_1(\mathbb{F}_q)$.

Proof of this corollary is similar to Theorem 3.4.

4.2. **Elligator-K1 map.** In this section, we consider the extension of the Elligator-L1 map to Kummer lines over a finite field $\mathbb{F}_q$ with prime $q \equiv 1 \pmod 4$. The following lemma gives the explicit map, and the pseudocode is given in Table 11 of Appendix D.

Lemma 4.6. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 1 \pmod 4$. Let $\lambda \in \mathbb{F}_q$ with $\chi(\lambda) = 1$ and $\lambda \notin \{0, \pm 1\}$, and u be a non-square in $\mathbb{F}_q$. Let $\mathcal{K}_{a^2,b^2}$ be a Kummer Line of corresponding Legendre form E_λ where $\lambda = \frac{a^4}{a^4-b^4}$ over a finite field $\mathbb{F}_q$.*

1. *First we define the x-coordinate only version of map ψ_1 of Theorem 3.5 as given below and we call it ψ_{2x}. If $t \neq 0$, then*
$$v = \frac{\lambda+1}{1+ut^2},\ \epsilon = \chi(v(v-1)(v-\lambda)),\ x = \epsilon v + (1-\epsilon)(\lambda+1)/2,$$
where $(x, \cdot)$ is a point on E_λ.
2. *Now composing ψ_{2x} and Π^{-1} of equation (2), we get the map $\hat{\psi_{2x}} = \Pi^{-1} \circ \psi_{2x} : \mathbb{F}_q \to \mathcal{K}_{a^2,b^2}$ defined as follows:*
$$v = \frac{\lambda+1}{1+ut^2},\ \epsilon = \chi(v(v-1)(v-\lambda)),\ x = \epsilon v + (1-\epsilon)(\lambda+1)/2,$$
$$\mathsf{X} = b^2 x,\ \mathsf{Z} = a^2(x-1).$$

Proof. 1. Define $y = -\epsilon\sqrt{x^3 - (\lambda+1)x^2 + \lambda x}$. By the proof of Theorem 3.5, (x, y) satisfies $\mathsf{E}_\lambda : y^2 = x(x-1)(x-\lambda)$.
2. Using similar argument of Lemma 4.1, $(\mathsf{X} : \mathsf{Z})$ is on $\mathcal{K}_{a^2,b^2}$.

□

Definition 4.7. Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 1 \pmod 4$ and $\mathcal{K}_{a^2,b^2}$ be a Kummer line over $\mathbb{F}_q$. Then, in the situation of Lemma 4.6, an encoding map $\hat{\psi_2} : \mathbb{F}_q \to \mathcal{K}_{a^2,b^2}$ is defined by $\hat{\psi_2}(0) = (b^2 : a^2)$ and if $t \neq 0$ then $\hat{\psi_2}(t) = (\mathsf{X} : \mathsf{Z})$.

4.2.1. *Inversion of Elligator-K1.* In the following section, we show that Elligator-K1 is efficiently invertible. First, in Lemma 4.8, we show that the map ψ_{2x} is efficiently invertible and then we extend the invertibility from Kummer line to a field element by Corollary 4.9. The pseudocode is given in Table 11 of Appendix D.

Lemma 4.8. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 1 \pmod 4$ and $\psi_{2x} : \mathbb{F}_q \to \mathsf{E}_\lambda/\{\pm 1\}$ be the encoding map defined in Lemma 4.6. Then the followings hold:*

1. *For any $t \in \mathbb{F}_q \setminus \{0\}$, ψ_{2x} maps $\left\{\pm t, \pm\frac{1}{ut}\right\}$ to a x such that the points $(x, \cdot) \in \mathsf{E}_\lambda(\mathbb{F}_q)$.*
2. *$\psi_{2x}(\mathbb{F}_q)$ is the set of x such that $(x, \cdot) \in \mathsf{E}_\lambda(\mathbb{F}_q)$ stisfying*
   (a) $x \neq \lambda + 1$.
   (b) $-xu(x-\lambda-1)$ is square in $\mathbb{F}_q$.
3. *If $x \in \psi_{2x}(\mathbb{F}_q)$, then $\bar{t}$ is defined and $\psi_{2x}(\bar{t}) = x$:*
$$\bar{t} = \sqrt{-x/((x-\lambda-1)u)}.$$

Proof. By Theorem 3.7, we have already shown that ψ_2 maps t and $-t$ to the same point on the curve E_λ. Now, we want to show that for any $t \in \mathbb{F}_q$, t and $\frac{1}{ut}$ map to points on the curve E_λ by ψ_2 such that $\psi_2(t) = (x, \cdot)$ and $\psi_2(\frac{1}{ut}) = (x, \cdot)$. Then we can conclude that ψ_{2x} maps $\left\{\pm t, \pm\frac{1}{ut}\right\}$ to the points on $\mathsf{E}_\lambda(\mathbb{F}_q)$ whose x-coordinate are the same.

For any $t \in \mathbb{F}_q \setminus \{0\}$, $v(v-1)(v-\lambda) = \frac{\lambda+1}{1+ut^2}\left(\frac{\lambda+1}{1+ut^2}-1\right)\left(\frac{\lambda+1}{1+ut^2}-\lambda\right) = \frac{\lambda+1}{(1+ut^2)^3}(\lambda-ut^2)(1-\lambda ut^2)$. Let $t_1 = \frac{1}{ut}$ and $\epsilon_1 = \chi(v_1(v_1-1)(v_1-\lambda))$, then $v_1(v_1-1)(v_1-\lambda) = ut^2\frac{\lambda+1}{(1+ut^2)^3}(1-\lambda ut^2)(\lambda-ut^2)$ and $\chi(v_1(v_1-1)(v_1-\lambda)) = -\chi(v(v-1)(v-\lambda))$. If $\epsilon = 1$, then $\epsilon_1 = -1$ and $x_1 = v_1ut_1^2 = v = x$. Also, if $\epsilon = -1$, then $\epsilon_1 = 1$ and $x_1 = v_1 = vut^2 = x$. Therefore, for the both cases, $x_1 = x$. Conversely, let $t_1, t_2 \in \mathbb{F}_q$ such that $\psi_2(t_1) = (x_1, y_1)$ and $\psi_2(t_2) = (x_2, y_2)$ are of the form $(x, \cdot)$. If $x_1 = v_1$ and $x_2 = v_2$, then $t_2 = \pm t_1$. Again if $x_1 = v_1ut_1^2$ and $x_2 = v_2ut_2^2$, then $t_2 = \pm t_1$. Now consider the case if $x_1 = v_1$ and $x_2 = v_2ut_2^2$, then $v_1 = v_2ut_2^2 \Rightarrow \frac{\lambda+1}{1+ut_1^2} = u\frac{\lambda+1}{1+ut_2^2}t_2^2 \Rightarrow t_2 = \pm\frac{1}{ut_1}$. This proves statement 1 of the theorem.

Statement 2 of the theorem follows from Theorem 3.7.

By statement 3 of Theorem 3.7, the value of y-coordinate chooses the preimage $\bar{t}$ of the map ψ_2 between $\sqrt{-x/((x-\lambda-1)u)}$ and $\sqrt{-(x-\lambda-1)/xu}$. But, both the values of $\bar{t}$ map to the point of the form $(x, \cdot)$. Therefore, without loss of generality, we can define the inverse function by

$$\bar{t} = \sqrt{-x/((x-\lambda-1)u)}.$$

□

Corollary 4.9. *In the situation of Lemma 4.6 and Lemma 4.8, the following statements hold:*

1. *For any $t \in \mathbb{F}_q$, $\hat{\psi}_2$ maps $\left\{\pm t, \pm\frac{1}{ut}\right\}$ to the points $(\mathsf{X} : \mathsf{Z}) \in \mathcal{K}_{a^2,b^2}$.*
2. *Let $(\mathsf{X} : \mathsf{Z}) \in \mathcal{K}_{a^2,b^2}$ and $(x, \cdot) = \left(\frac{a^2\mathsf{X}}{a^2\mathsf{X}-b^2\mathsf{Z}}, \cdot\right) \in \mathsf{E}_\lambda$. If x satisfying statement 2 of Theorem 4.8, then the following element $\bar{t}$ of $\mathbb{F}_q$ is defined and $\hat{\psi}_2(\bar{t}) = (\mathsf{X} : \mathsf{Z})$:*

$$\bar{t} = \sqrt{-\frac{a^2\mathsf{X}}{(a^2\mathsf{X}-(\lambda+1)(a^2\mathsf{X}-b^2\mathsf{Z}))u}}.$$

4.2.2. *Encoding as strings.* Let q be a b-bit prime and $R_1 \subset \{0,1\}^b$ as defined below. Corollary 4.10 shows the injection between R_1 and the Kummer line.

Corollary 4.10. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 1 \pmod 4$. Fix $b = \lfloor \log_2 q \rfloor$ and define a map $\sigma : \{0,1\}^b \to \mathbb{F}_q$ by $\sigma(\rho_0, \rho_1, ..., \rho_{b-1}) = \sum_i \rho_i 2^i$. Let $\varsigma_2 : t \mapsto -t$ and $\varsigma_3 : t \mapsto \frac{1}{ut}$ for $t \in \mathbb{F}_q$ and u as defined in Lemma 4.6. Define $R_1 = \sigma^{-1}(\mathbb{F}_q/\langle\varsigma_2, \varsigma_3\rangle)$. In the situation of Lemma 4.6, the map $\hat{\tau}_2 = \hat{\psi}_2 \circ \sigma : R_1 \to \mathcal{K}_{a^2,b^2}$ is defined, then $\hat{\tau}_2(R_1) = \hat{\psi}_2(\mathbb{F}_q)$.*

Proof. Proof of this corollary is similar to Theorem 3.4. □

4.3. **Comparison of Encodings for Legendre curve and Kummer line.** This section compares our proposed encodings with those defined in [2, 6, 10]. The encoding proposed in [6], which we refer to as the F-F encoding, is not constant-time. Therefore, we provide a constant-time variant of the F-F encoding in Appendix H and use that variant for our comparisons, to ensure consistency since all other encodings considered here are constant-time.

4.3.1. *Encodings defined for primes of the form* $3 \pmod 4$. Fouque et al., in [10], propose a map from a finite field $\mathbb{F}_q$, $q \equiv 3 \pmod 4$, to a hyperelliptic curve of the form $\mathsf{H}_c^\delta : y^2 = f(x) = \delta x^5 + \left(c^2 + \frac{1}{c^2}\right)x^3 + \delta x$, where $c \in \mathbb{F}_q \setminus \{0, \pm 1\}$, $\delta = \pm 1$, and

subsequently to an elliptic curve of the form $E_{\delta,c} : y^2 = x^3 - 4\delta x^2 + \delta(c + \delta/c)^2 x$. When $\delta = -1$, this map can be extended to the curve of the form $E_{\alpha_1,\alpha_2} : y^2 = x(x - \alpha_1)(x - \alpha_2)$, where $\chi(\alpha_1 + \alpha_1) = -1$ and $\chi(\alpha_1\alpha_2) = -1$. Without loss of generality, putting $\alpha_1 = 1$ and $\alpha_2 = \lambda$, we get Legendre curves, and consequently λ must satisfies that $\chi(\lambda + 1) = -1$ and $\chi(\lambda) = -1$. We refer to this map as the F-J-T map. On the contrary, our construction covers all Legendre curves $E_\lambda : y^2 = x(x - 1)(x - \lambda)$ with $\chi(\lambda) = -1$, a wider range.

Our construction, Elligator-L3, is largely similar to the F-J-T map. however, unlike the F-J-T map, which has exception points[2] in $\mathbb{F}_q$ for injective encoding, Elligator-L3 avoids such exceptions. Both constructions, however, require comparable computational costs for encoding.

Similar to Elligator-L3, the F-F encoding also does not introduce exception points. Moreover, the F-F encoding achieves better performance than Elligator-L3. In contrast, Bernstein et al. [2] proposed Elligator-2, which also applies to the Legendre curve over $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$. However, Elligator-2 *always* exhibits exception points for injective encoding.

4.3.2. *Encodings defined for primes of the form* $1 \pmod 4$. F-J-T map [10] is not applicable in this case. However, Elligator-L1 covers all the Legendre curves with $\chi(\lambda) = 1$. In that sense, the encodings proposed in this paper cover a significantly wider range of Legendre curves, in total, compared to the F-J-T map. The Elligator-2 map is also applicable to the Legendre curve over $\mathbb{F}_q$ with $q \equiv 1 \pmod 4$. While Elligator-2 is similar to our construction Elligator-L1, it does not cover the whole $\mathbb{F}_q$. In contrast, Elligator-L1 avoids exception points entirely. Similar to Elligator-L1, the F-F encoding also has no exception points. However, in terms of performance, Elligator-L1 outperforms the F-F encoding.

Table 1 compares the operation counts of our constructions with those of existing maps applicable to Legendre curves.

TABLE 1. Operation Count for encoding to Legendre curve over prime field $\mathbb{F}_q$, where $\mathsf{S}, \mathsf{M}, \mathsf{I}, \mathsf{C}, \mathsf{C_s}, \chi$ and Sqrt denote a field squaring, a field multiplication, a field inversion, a multiplication by a constant, a multiplication by a small constant, a quadratic character and a square root computation, respectively.

Map	Operation Count	Condition of $\mathbb{F}_q$	$\chi(\lambda)$	Exception Point
Elliagtor-2 [2]	$1\mathsf{S} + 6\mathsf{M} + 1\mathsf{I} + 1\mathsf{C} + 1\mathsf{C_s} + 1\chi + 1\mathsf{Sqrt}$	All	± 1	Yes
F-F Map [6], (Table 14)	$1\mathsf{S} + 8\mathsf{M} + 1\mathsf{I} + 1\mathsf{C} + 1\mathsf{C_s} + 1\chi + 1\mathsf{Sqrt}$	All	± 1	No
F-J-T Map [10]	$2\mathsf{S} + 11\mathsf{M} + 2\mathsf{I} + 2\mathsf{C} + 2\chi + 1\mathsf{Sqrt}$	$3 \pmod 4$	-1	Yes
Elligator-L3 (**This work**)	$2\mathsf{S} + 11\mathsf{M} + 2\mathsf{I} + 2\mathsf{C} + 2\chi + 1\mathsf{Sqrt}$	$3 \pmod 4$	-1	No
Elliagtor-L1 (**This work**)	$1\mathsf{S} + 6\mathsf{M} + 1\mathsf{I} + 1\mathsf{C} + 1\mathsf{C_s} + 1\chi + 1\mathsf{Sqrt}$	$1 \pmod 4$	1	No

4.4. **Encodings for Kummer line.** In this section, we have included Table 2 that compares the operation count of our constructions that map a finite field $\mathbb{F}_q$ to Kummer line via the Legendre curve.

[2]First paragraph of Section 3.2 of [10] ensures the exception points.

TABLE 2. Operation count for encoding to Kummer line map over prime field $\mathbb{F}_q$.

Map	Operation Count	condition of $\mathbb{F}_q$
F-F-K Map (**This work**)	$1\mathsf{S}+5\mathsf{M}+1\mathsf{C}+3\mathsf{C_s}+1\chi$	All
Elligator-K3 (**This work**)	$1\mathsf{S}+3\mathsf{M}+3\mathsf{C}+2\mathsf{C_s}+1\chi$	$3 \pmod 4$
Elliagtor-K1 (**This work**)	$1\mathsf{S}+3\mathsf{M}+3\mathsf{C}+3\mathsf{C_s}+1\chi$	$1 \pmod 4$

5. **Elligator-T.** In this section, we describe our proposed map Elligator-T that takes an element from the prime field $\mathbb{F}_q$ to a twisted Edwards curve. For this mapping, q must be a prime of the form $q \equiv 3 \pmod 4$. Previously, [2] also considered twisted Edwards curve via Montgomery curve using Elligator-2. However, it covers the whole $\mathbb{F}_q$ if $q \equiv 1 \pmod 4$. In that respect, our present work also complements the [2]. In our work, we consider twisted Edwards curve with complete addition formulas.

The essence of the mapping is the function $\phi : \mathbb{F}_q \to \mathsf{E}_{-1,d}(\mathbb{F}_q)$ defined in Theorem 5.1 and Definition 5.2. The only existing collision is that $\phi(t) = \phi(-t)$ for any $t \in \mathbb{F}_q$. Therefore, if we restrict our mapping to $S = \{0, 1, 2, \ldots, (q-1)/2\}$, then the mapping becomes injective.

The proposed map has a constraint that -1 has to be non-square. For prime field $\mathbb{F}_q$, -1 is non-square only when $q \equiv 3 \pmod 4$. Also, the targeted twisted Edwards curve has a coefficient $a = -1$ and d is a square, and the twisted Edwards curve has a complete addition and doubling formula. Theorem 5.1 describes the map, and Theorem 5.3 provides the inversion of the map and gives the condition under which a point on the twisted Edwards curve has a preimage. The pseudocode is given in Table 12 of Appendix E.

5.1. Elligator-T map.

Theorem 5.1. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$. Let $s \in \mathbb{F}_q^*$ such that $(s^2-2)(s^2+2) \neq 0$ and $\left(\left(\frac{2}{s^2} + \frac{s^2}{2} - 2\right)^2 - 4\right)$ is a quadratic non-residue.*

Now fix $c = \frac{2}{s^2}$, $r = c + \frac{1}{c}$ and $d = \frac{(c-1)^2}{(c+1)^2}$. Then the following elements of $\mathbb{F}_q$ are defined for each $t \in \mathbb{F}_q \setminus \{\pm 1\}$:

$$u = \frac{1-t}{1+t},\ v = u^5 + (r^2-2)u^3 + u,$$
$$X = \chi(v)u,\ Y = (\chi(v)v)^{\frac{q+1}{4}}\chi(v)\chi\left(u^2 + \frac{1}{c^2}\right),$$
$$x = (c+1)sX(X+1)/Y,\ \ y = \frac{rX + (1+X)^2}{rX - (1+X)^2}.$$

Furthermore, we have that $Y^2 = X^5 + (r^2-2)X^3 + X$, and $-x^2 + y^2 = 1 + dx^2y^2$.

Proof. The proof given below follows the same proof techniques used by the authors of [2] while proving the Theorem 1 of [2]. The proof of our proposed Theorem 5.1 and the proof of Theorem 1 of [2] are the same for the first six bullet points, that is, they are the same for the statements "$c(c-1)(c+1) \neq 0$", "$r \neq 0$", "u is defined and $u \neq$

0", "$v \neq 0$", "$XY \neq 0$, so x is defined" and "$1 + X \neq 0$, so $x \neq 0$". However, we replicate them to provide a complete understanding of the proof.

- $\mathbf{c(c-1)(c+1) \neq 0}$: By definition, $c = \frac{2}{s^2}$. So, $c \neq 0$. If $c = \pm 1$, then $s^2 = \pm 2$. Therefore, $(s^2 - 2)(s^2 + 2) = 0$ forms a contradiction.
- $\mathbf{r \neq 0}$: $r = 0$ implies that $c + \frac{1}{c} = 0$, that is $c^2 = -1$. But -1 is a quadratic non residue modulo q if $q \equiv 3 \pmod 4$. Therefore, we have a contradiction.
- **u is defined and** $\mathbf{u \neq 0}$: By assumption, $t \in \mathbb{F}_q \setminus \{\pm 1\}$, that is $t \neq \{\pm 1\}$ and this implies $1 \pm t \neq 0$. Therefore, u is defined and non-zero by the definition of the map $u = \frac{1-t}{1+t}$.
- $\mathbf{v \neq 0}$: First notice that $r^2 - 2 = c^2 + \frac{1}{c^2}$. Then, we have $v = u^5 + (r^2 - 2)u^3 + u = u^5 + (c^2 + \frac{1}{c^2})u^3 + u = u(u^2 + c^2)(u^2 + \frac{1}{c^2})$. Since u is non-zero, either $u^2 + c^2$ or $u^2 + \frac{1}{c^2}$ must be zero to make $v = 0$. However, $u^2 + c^2 = 0$ or $u^2 + \frac{1}{c^2} = 0$ implies $(\frac{u}{c})^2 = -1$ or $(uc)^2 = -1$ respectively. In either case, -1 is a square, which is a contradiction.
- $\mathbf{XY \neq 0}$, **so** x **is defined** : As above $(u^2 + \frac{1}{c^2}) \neq 0$, then all factors of X and Y are non-zero and x is defined.
- $\mathbf{1 + X \neq 0}$, **so** $\mathbf{x \neq 0}$: Assume that $X + 1 = 0$. From $X = \chi(v)u$, we get $\chi(v)u = -1$. Multiplying both sides by $\chi(v)$, we get $\chi(v)^2 u = -\chi(v)$, that is, $u = -\chi(v)$. Therefore, $v = (-\chi(v))^5 + (r^2 - 2)(-\chi(v))^3 + (-\chi(v)) = -\chi(v)r^2$ as $(-\chi(v))^2 = 1$. Now we have $\chi(v) = \chi(-1)\chi(\chi(v))\chi(r^2) = -\chi(v)$ and that is a contradiction.
- $(\mathbf{X, Y})$ **satisfies** $\mathbf{Y^2 = X^5 + (r^2 - 2)X^3 + X}$: From $X = \chi(v)u$, $X^5 + (r^2 - 2)X^3 + X = \chi(v)(u^5 + (r^2 - 2)u^3 + u) = \chi(v)v$. Now $\chi(\chi(v)v) = \chi(v)^2$ and thus $\chi(v)v$ is a square. Therefore, we have that $(\chi(v)v)^{\frac{(q+1)}{2}} = \chi(v)v$ as $(\chi(v)v)^{\frac{q+1}{4}}$ is the principal square root. On the other hand,

$$Y^2 = \left((\chi(v)v)^{\frac{q+1}{4}}\chi(v)\chi\left(u^2 + \frac{1}{c^2}\right)\right)^2 = (\chi(v)v)^{\frac{q+1}{2}} = \chi(v)v.$$

  Therefore, (X, Y) satisfies $Y^2 = X^5 + (r^2 - 2)X^3 + X$.
- $\mathbf{rX - (1 + X)^2 \neq 0}$, **so** y **is defined** : Let $rX - (1+X)^2 = 0$, then $X^2 - (r - 2)X + 1 = 0$. Replacing r by $(c + \frac{1}{c})$, we get that $X^2 - (c + \frac{1}{c} - 2)X + 1 = 0$. The quadratic equation has a root over $\mathbb{F}_q$ if and only if the discriminant $(c + \frac{1}{c} - 2)^2 - 4 = \left(\frac{2}{s^2} + \frac{s^2}{2} - 2\right)^2 - 4$ is a quadratic residue, which is a contradiction to the hypothesis. Therefore, y is defined.
- $\mathbf{-x^2 + y^2 = 1 + dx^2y^2}$: Observe that $(c + 1)^2 s^2 = \frac{2}{c}(c + 1)^2 = 2(r + 2)$. So, $Y^2(1 + x^2) = Y^2 + (c + 1)^2 s^2 X^2 (1 + X)^2 = X^5 + (r^2 - 2)X^3 + X + 2(r + 2)X^2(1 + X)^2 = X(rX + (1 + X)^2)^2$.

  Similarly, $d = \left(\frac{c-1}{c+1}\right)^2 = \frac{c-2+1/c}{c+2+1/c} = \frac{r-2}{r+2}$. Now, $Y^2(1 - d^2x^2) = Y^2 - \left(\frac{c-1}{c+1}\right)^2 (c + 1)^2 s^2 X^2 (1 + X)^2 = Y^2 - \left(\frac{r-2}{r+2}\right) 2(r + 2)X^2(1 + X)^2 = (X^5 + (r^2 - 2)X^3 + X) - 2(r - 2)X^2(1 + X)^2 = X(rX - (1 + X)^2)^2$.

  Since $(rX - (1 + X)^2)^2$ and X are non-zero,

$$\frac{1 + x^2}{1 - dx^2} = y^2, \text{ that is } -x^2 + y^2 = 1 + dx^2y^2.$$

□

Definition 5.2. Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$ and $\mathsf{E}_{-1,d} : -x^2 + y^2 = 1 + dx^2y^2$ be a twisted Edwards curve over $\mathbb{F}_q$. Then, in the situation of Theorem 5.1, an encoding function $\phi : \mathbb{F}_q \to \mathsf{E}_{-1,d}(\mathbb{F}_q)$ is defined by the map $\phi(\pm 1) = (0, 1)$ and if $t \neq \{\pm 1\}$ then $\phi(t) = (x, y)$.

5.2. **Inversion map of Elligator-T.** The theorem proposed next shows the existence of an efficient inversion map of the encoding map ϕ, and the pseudocode is given in Table 12 of Appendix E.

Theorem 5.3. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 (mod\ 4)$ and $\phi : \mathbb{F}_q \to \mathsf{E}_{-1,d}$ be the encoding map defined in Definition 5.2. Then the following statements hold:*

1. *If $t \in \mathbb{F}_q$, then the set of preimage of $\phi(t)$ under the encoding map ϕ is $\{t, -t\}$.*
2. *$\phi(\mathbb{F}_q)$ is the set of $(x, y) \in \mathsf{E}_{-1,d}(\mathbb{F}_q)$ satisfying*
   (a) $y + 1 \neq 0$,
   (b) $(1 - \eta r)^2 - 1$ is a square, where $\eta = \frac{y-1}{2(y+1)}$,
   (c) if $\eta r = 2$, then $x = 2s(c + 1)\chi(c)/r$.
3. *If $(x, y) \in \phi(\mathbb{F}_q)$, then the following elements $\bar{X}, z, \bar{u}, \bar{t}$ of $\mathbb{F}_q$ are defined and $\phi(\bar{t}) = (x, y)$:*

$$\bar{X} = -(1 - \eta r) + ((1 - \eta r)^2 - 1)^{\frac{q+1}{4}},$$
$$z = \chi\left((c + 1)s\bar{X}(1 + \bar{X})x\left(\bar{X}^2 + \frac{1}{c^2}\right)\right),$$
$$\bar{u} = z\bar{X}, \quad \bar{t} = \frac{1 - \bar{u}}{1 + \bar{u}}.$$

Proof. The following proof also employs similar techniques used in the proof of Theorem 3 of [2]. Statement 1 has a forward part that says $\phi(t) = \phi(-t)$, and the reverse part says that there is no other preimage. Similarly, statement 2 has a forward part and a reverse part. The forward part states that any point $(x, y) \in \phi(\mathbb{F}_q)$ satisfies conditions (a), (b) and (c). As for the reverse part, it says that any point $(x, y) \in \mathsf{E}_{-1,d}(\mathbb{F}_q)$ satisfying those conditions is in $\phi(\mathbb{F}_q)$.

- First, we shall prove the forward of statement 1: t and $-t$ map to the same point of $\mathsf{E}_{-1,d}(\mathbb{F}_q)$. If $t \in \{\pm 1\}$, then $\phi(t) = \phi(-t) = (0, 1)$, by definition of ϕ.

  Assume from now that $t \in \mathbb{F}_q \setminus \{\pm 1\}$. Define u, v, X, Y, x, y from t as in Theorem 5.1. Then, by definition, $\phi(t) = (x, y)$. Now let $t' = -t$ and u', v', X', Y', x', y' are the values corresponding to t' as in Theorem 5.1. Then $u' = \frac{1-t'}{1+t'} = \frac{1+t}{1-t} = \frac{1}{u}$ and consequently $v' = u'^5 + (r^2 - 2)u'^3 + u' = \frac{1}{u^5} + (r^2 - 2)\frac{1}{u^3} + \frac{1}{u} = \frac{v}{u^6}$ with $\chi(v') = \chi(v)\chi(\frac{1}{u^6}) = \chi(v)$ because u^6 is a square. Then we have $X' = \chi(v')u' = \frac{\chi(v)}{u} = \frac{\chi(v)^2}{\chi(v)u} = \frac{1}{\chi(v)u} = \frac{1}{X}$.

  Next, $y' = \frac{rX' + (1+X')^2}{rX' - (1+X')^2} = \frac{r\frac{1}{X} + (1+\frac{1}{X})^2}{r\frac{1}{X} - (1+\frac{1}{X})^2} = \frac{rX + (X+1)^2}{rX - (X+1)^2} = y$.

  Now let us focus on $Y' = (\chi(v')v')^{\frac{q+1}{4}}\chi(v')\chi\left(u'^2 + \frac{1}{c^2}\right)$. First note that $(u^6)^{\frac{q+1}{4}} = (u^3)^{\frac{q+1}{2}} = (u^3)^{\frac{q-1}{2}}u^3 = \chi(u^3)u^3 = \chi(u)u^3$, and therefore $\chi(u)u^3$ is the principle square root of u^6. Thus $\chi(u)u^3$ is a square. Then

$$Y' = (\chi(v')v')^{\frac{q+1}{4}}\chi(v')\chi\left(u'^2 + \frac{1}{c^2}\right)$$
$$= \left(\chi(v)\frac{v}{u^6}\right)^{\frac{q+1}{4}}\chi(v')\chi\left(u'^2 + \frac{1}{c^2}\right) \text{ [Putting } v' = v/u^6\text{]}$$

$$
\begin{aligned}
&= (\chi(v)v)^{\frac{q+1}{4}} \left(\frac{1}{u^6}\right)^{\frac{q+1}{4}} \chi(v')\chi\left(u'^2 + \frac{1}{c^2}\right) \\
&= (\chi(v)v)^{\frac{q+1}{4}} \left(\frac{1}{\chi(u)u^3}\right) \chi(v')\chi\left(u'^2 + \frac{1}{c^2}\right) \\
&= (\chi(v)v)^{\frac{q+1}{4}} \left(\frac{\chi(u)}{u^3}\right) \chi(v')\chi\left(u'^2 + \frac{1}{c^2}\right) [\text{Note that } \chi(u) = 1/\chi(u)] \\
&= (v\chi(v))^{\frac{q+1}{4}} \frac{\chi(u)}{u^3}\chi(v)\chi\left(\frac{1}{u^2} + \frac{1}{c^2}\right) [\text{As } \chi(v) = \chi(v') \text{ and } u' = 1/u] \\
&= (v\chi(v))^{\frac{q+1}{4}} \frac{\chi(uv)}{u^3}\chi\left(c^2u^4\left(\frac{1}{u^2} + \frac{1}{c^2}\right)\left(u^2 + \frac{1}{c^2}\right)^2\right) [\text{As } \chi(a) = \chi(ab^2)] \\
&= (v\chi(v))^{\frac{q+1}{4}} \frac{\chi(uv)}{u^3}\chi\left(uv\left(u^2 + \frac{1}{c^2}\right)\right) \left[\text{Putting } v = u(u^2 + c^2)\left(u^2 + \frac{1}{c^2}\right)\right] \\
&= (v\chi(v))^{\frac{q+1}{4}} \frac{1}{u^3}\chi\left(u^2 + \frac{1}{c^2}\right) \\
&= \frac{(v\chi(v))^{\frac{q+1}{4}}\chi(v)\chi\left(u^2 + \frac{1}{c^2}\right)}{u^3\chi(v)} \\
&= \frac{Y}{(u\chi(v))^3} \\
&= \frac{Y}{X^3}.
\end{aligned}
$$

Next, $x' = (c+1)sX'(1+X')/Y' = (c+1)s\frac{1}{X}\left(1+\frac{1}{X}\right)/\frac{Y}{X^3} = (c+1)sX(1+X)/Y = x$. Hence, $\phi(-t) = (x, y)$ and forward part of statement 1 is proved. The latter part of the proof contains the proof of the reverse of statement 1.

- Next, we will prove the forward part of statement 2. Let $t \in \mathbb{F}_q$ and define $\phi(t) = (x, y)$. There are two cases, (a) $t \in \{\pm 1\}$ then $(x, y) = (0, 1)$ and (b) $t \notin \{\pm 1\}$ then $(x, y) \neq (0, 1)$.

  Case (a). As $(x, y) = (0, 1)$, $y + 1 = 2 \neq 0$, and thus $\eta = \frac{y-1}{2(y+1)} = 0$. Therefore, $(1 - \eta r)^2 - 1 = 0$ is a square.

  Case (b). First we prove that $y + 1 \neq 0$. Let $y = -1$. Then by Theorem 5.1, $\frac{rX+(1+X)^2}{rX-(1+X)^2} = -1$. Simplifying the expression, we get $rX + (1+X)^2 = -(rX - (1+X)^2)$, that is $rX = 0$. However, r and X are both non-zero by Theorem 5.1 and lead to a contradiction. Now,

$$
\begin{aligned}
y = \frac{rX + (1+X)^2}{rX - (1+X)^2} &\Rightarrow \frac{y-1}{y+1} = \frac{(1+X)^2}{rX} \\
&\Rightarrow X^2 + 2X - \left(\frac{y-1}{y+1}\right) rX + 1 = 0 \\
&\Rightarrow X^2 + 2(1 - \eta r)X + 1 = 0 \text{ where } \eta = \frac{y-1}{2(y+1)}.
\end{aligned}
$$

The last quadratic equation has a root and thus the discriminant $4(1-\eta r)^2 - 4 = 4\left((1-\eta r)^2 - 1\right)$ is a square, that is, $(1-\eta r)^2 - 1$ is a square as claimed. Both cases prove statements 2a and 2b. After dividing $X^2 + 2(1-\eta r)X + 1 = 0$

by X, we get $X + \frac{1}{X} = -2(1 - \eta r)$ and this will be used in the later part of the proof.

For statement 2c, let $\eta r = 2$, then

$$X^2 + 2(1-2)X + 1 = 0 \Rightarrow X^2 - 2X + 1 = 0 \Rightarrow (X-1)^2 = 0 \Rightarrow X = 1.$$

From Theorem 5.1, we have $X = \chi(v)u$. As $X = 1$, $u \in \{\pm 1\}$. If $u = -1$, then $1 - t = -(1 + t)$, that is $1 = -1$ and hence a contradiction. Therefore, u must be 1 and $t = 0$. So, $v = 1^5 + (r^2 - 2)1^3 + 1 = r^2$ and $Y = (r^2)^{\frac{q+1}{4}}\chi(1 + \frac{1}{c^2}) = \chi(r)r\chi(r/c) = \chi(r)r\chi(rc/c^2) = \chi(r)r\chi(rc) = r\chi(c)$, as $\chi(1/c^2) = 1$ and $\chi(r^2) = 1$. Therefore, $x = (c+1)sX(X+1)/Y = 2(c+1)s\chi(c)/r$. This proves statement 2 of the theorem.

For future reference, note that $y = \frac{r+4}{r-4}$. Consequently, we obtain

$$\phi(0) = \left(2(c+1)s\chi(c)/r, \frac{r+4}{r-4}\right).$$

- Now, we will prove statement 3 of the theorem. Let $t \in \mathbb{F}_q$ and define $\phi(t) = (x, y)$. We prove that the quantities $\bar{X}, z, \bar{u}, \bar{t}$ of are defined and for $\bar{t} \in \{t, -t\}$, $\phi(\bar{t}) = (x, y)$. This part of the proof is also divided into two parts: (a) $t \in \{\pm 1\}$ then $(x, y) = (0, 1)$ and (b) $t \notin \{\pm 1\}$ then $(x, y) \neq (0, 1)$.

  Case (a). As $(x, y) = (0, 1)$, $\bar{X} = -(1 - 0) + 0^{\frac{q+1}{4}} = -1$. On the other hand, z contains a factor $(1 + \bar{X})$, thus $z = \chi(0) = 0$. Then we have $\bar{u} = z\bar{X} = 0$ and $\bar{t} = \frac{1-\bar{u}}{1+\bar{u}} = 1 \in \{\pm t\}$. Therefore, $\{1, -1\}$ are the only preimages of $(0, 1)$.

  Case (b). Let, $(x, y) \neq (0, 1)$. Fix $t' = -t$ and then define u', v', X', Y', x', y' for t'. From the construction of $\bar{X}$, we have that $1 - \eta r + \bar{X}$ is a square root of $(1 - \eta r)^2 - 1$. Therefore, $(1 - \eta r + \bar{X})^2 = (1 - \eta r)^2 - 1$ and further simplification gives us

  $$\bar{X}^2 + 2(1 - \eta r)\bar{X} + 1 = 0. \tag{5}$$

  We have already shown that $X' = \frac{1}{X}$ and thus $X + X' = -2(1 - \eta r)$. Therefore, X and X' are two roots of equation (5) and thus we have $(\bar{X} - X)(\bar{X} - X') = \bar{X}^2 - (X + X')\bar{X} + XX' = \bar{X}^2 + 2(1 - \eta r)\bar{X} + 1$. Then, $\bar{X} = X$ or $\bar{X} = X'$. So, $\bar{u} = u$ or $\bar{u} = u'$, since definition of z matches $\chi(v)$ and $\chi(v')$.

  If $\bar{X} = X$, then $(c+1)s\bar{X}(1 + \bar{X}) = xY$. Then we also have

  $$z = \chi\left(x^2 Y\left(X^2 + \frac{1}{c^2}\right)\right) = \chi(Y)\chi\left(X^2 + \frac{1}{c^2}\right).$$

  Further we have that $(\chi(v)v)^{\frac{q+1}{4}}$ is a square and $\chi(u^2 + 1/c^2) = \chi(X^2 + 1/c^2)$. So, $\chi(Y) = \chi\left((\chi(v)v)^{\frac{q+1}{4}}\chi(v)\chi\left(X^2 + \frac{1}{c^2}\right)\right) = \chi(v)\chi\left(X^2 + \frac{1}{c^2}\right), z = \chi(v), \bar{u} = \chi(v)X = u$ and $\bar{t} = t$. Similarly, for $\bar{X} = X'$, we have $z = \chi(v')$, $\bar{u} = u'$ and $\bar{t} = t' = -t$. This proves statement 3 of the theorem.

  Using the same logic, it can also be shown that for any fixed $(x, y) \in \mathsf{E}_{-1,d}(\mathbb{F}_q)$, the only possible preimage is $\{t, -t\}$ which proves the reverse part of part the statement 1.
- Now, we come to the last part of the proof that is the reverse of statement 2. Let, $(x, y) \in \mathsf{E}_{-1,d}(\mathbb{F}_q)$ such that $y + 1 \neq 0$ and $(1 - \eta r)^2 - 1$ is a square where $\eta = \frac{y-1}{2(y+1)}$. If $\eta r = 2$ then $x = 2(c+1)s\chi(c)/r$. We must show that $(x, y) \in \phi(\mathbb{F}_q)$.

If $x = 0$, then $(x, y) = (0, \pm 1)$, but $y + 1 \neq 0$. Hence, $y = 1$ and $(x, y) = (0, 1) = \phi(1) \in \phi(\mathbb{F}_q)$.

From now on, assume that $x \neq 0$. If $y = 1$, then $x = 0$ from the curve equation, and it creates a contradiction. Therefore, $y \neq 1$ and it implies $\eta \neq 0$.

Let $X = -(1 - \eta r) + ((1 - \eta r)^2 - 1)^{\frac{q+1}{4}}$. Then, $1 - \eta r + X$ is a square root of $(1 - \eta r)^2 - 1$ and thus $X^2 + 2(1 - \eta r)X + 1 = 0$. Now we can conclude four facts from it. First, by construction, $X \neq 0$. Second, $rX - (1 + X)^2 \neq 0$. Let $rX - (1 + X)^2 = 0$, and that implies

$$\begin{aligned}
&rX = 1 + 2X + X^2 \\
&\Rightarrow X^2 + (2 - r)X + 1 = 0 \\
&\Rightarrow -2(1 - \eta r)X + (2 - r)X = 0 \ \left[\text{As } X^2 + 2(1 - \eta r)X + 1 = 0\right] \\
&\Rightarrow (2\eta - 1)rX = 0 \\
&\Rightarrow 2\eta = 1 \\
&\Rightarrow y - 1 = y + 1 \\
&\Rightarrow 1 = -1, \text{ a contradiction.}
\end{aligned}$$

Hence, $rX - (1 + X)^2 \neq 0$. Third, $X \neq -1$ otherwise $\eta = 0$. Fourth, $y = \frac{rX + (1+X)^2}{rX - (1+X)^2}$ using $\eta = \frac{y-1}{2(y+1)}$.

If $X = 1$, then $y = \frac{r+4}{r-4}$. Also $\eta r = 2$ implies $x = 2s(c + 1)\chi(c)/r$. So, $(x, y) = \phi(0) \in \phi(\mathbb{F}_q)$.

Now, let $X \neq 1$ and $d = \left(\frac{c-1}{c+1}\right)^2 = \frac{r-2}{r+2}$, then

$$\begin{aligned}
(rX - (1 + X)^2)^2(1 - y^2) &= (rX - (1 + X)^2)^2 - (rX + (1 + X)^2)^2 \\
&= -4rX(1 + X)^2
\end{aligned}$$

and

$$\begin{aligned}
&(rX - (1 + X)^2)^2(1 + dy^2) \\
&= (rX - (1 + X)^2)^2 + \frac{r - 2}{r + 2}(rX + (1 + X)^2)^2 \\
&= \frac{1}{r + 2}[(r + 2)(rX - (1 + X)^2)^2 + (r - 2)(rX + (1 + X)^2)^2] \\
&= \frac{2r}{r + 2}(X^4 + (r^2 - 2)X^2 + 1).
\end{aligned}$$

Since d is a square, $1 + dy^2 \neq 0$. Then

$$\begin{aligned}
-x^2 &= \frac{1 - y^2}{1 + dy^2} = -\frac{2(r + 2)X^2(1 + X)^2}{X^5 + (r^2 - 2)X^3 + X} \\
\Rightarrow x^2 &= \frac{2(r + 2)X^2(1 + X)^2}{X^5 + (r^2 - 2)X^3 + X}.
\end{aligned}$$

Define $Y = (c + 1)sX(1 + X)/x$. Then,

$$\begin{aligned}
Y^2 &= (c + 1)^2 s^2 X^2 (1 + X)^2/x^2 \\
&= 2(c + 1)^2 X^2 (1 + X)^2/cx^2 \\
&= 2(c + 1/c + 2)X^2(1 + X)^2/x^2 \\
&= 2(r + 2)X^2(1 + X)^2/x^2
\end{aligned}$$

$$= X^5 + (r^2 - 2)X^3 + X.$$

Define $z = \chi(Y(X^2 + \frac{1}{c^2}))$, both Y and $(X^2 + \frac{1}{c^2})$ are non-zero. Therefore, $z \in \{\pm 1\}$.

Define $u = zX$. Then, $u \in \{\pm X\}$ and $u \neq -1$, since $X \neq \pm 1$. Next, define $v = u^5 + (r^2 - 2)u^3 + u = z(X^5 + (r^2 - 2)X^3 + X) = zY^2$. So, $\chi(v) = \chi(zY^2) = \chi(z) = z$. Then, $X = \chi(v)u$ and $Y^2 = \chi(v)v$. Now, $\chi(v) = z = \chi(Y(X^2 + \frac{1}{c^2})) = \chi(Y(u^2 + \frac{1}{c^2}))$. Then, $\chi(Y) = \chi(v)\chi(u^2 + \frac{1}{c^2})$ and $Y^2 = zv = \chi(v)v$. Taking the principal square root, we get $Y = (\chi(v)v)^{\frac{q+1}{4}}\chi(v)\chi(u^2 + \frac{1}{c^2})$. Define $t = \frac{1-u}{1+u}$. Then, $t \notin \{\pm 1\}$ and $u = \frac{1-t}{1+t}$. The formulas of u, v, X, Y, x, y are defined and so, $\phi(t) = (x, y) \in \phi(\mathbb{F}_q)$. This proves the reverse part of statement 2 of the theorem.

□

5.3. **Encoding as strings.** Let q be a b-bit long prime. Let R be the set of all b-bit long binary strings whose decimal values range from 0 to $\frac{q-1}{2}$. The following theorem shows that the mapping ϕ induces an injection from R to $\mathsf{E}_{-1,d}(\mathbb{F}_q)$.

Theorem 5.4. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$ and $\phi : \mathbb{F}_q \to \mathsf{E}_{-1,d}$ be the encoding map defined in Definition 5.2. Fix $b = \lfloor \log_2 q \rfloor$ and define a map $\sigma : \{0,1\}^b \to \mathbb{F}_q$ by $\sigma(\rho_0, \rho_1, ..., \rho_{b-1}) = \sum_i \rho_i 2^i$. Define a set $R = \sigma^{-1}(\{0, 1, 2, \ldots, \frac{q-1}{2}\})$. Define $\tau_3 : R \to \mathsf{E}_{-1,d}(\mathbb{F}_q)$ by $\tau_3(\rho) = \phi(\sigma(\rho))$. Then, R has exactly $\frac{q+1}{2}$ elements, τ_3 is injective and $\tau_3(R) = \phi(\mathbb{F}_q)$.*

Proof. The proof is identical to the proof of Theorem 4 of [2]. Therefore, we omit it here. □

5.4. **y-coordinate only Elligator-T (Elligator-T$_y$).** In this section, we provide the y-coordinate-only version of the proposed map Elligator-T, and the pseudocode is given in Table 13 of Appendix F.

Lemma 5.5. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$). Let $s \in \mathbb{F}_q^*$ such that $(s^2 - 2)(s^2 + 2) \neq 0$ and $\left(\left(\frac{2}{s^2} + \frac{s^2}{2} - 2\right)^2 - 4\right)$ is a quadratic non-residue. Now fix $c = \frac{2}{s^2}$, $r = c + \frac{1}{c}$ and $d = \left(\frac{c-1}{c+1}\right)^2$. Then for each $t \in \mathbb{F}_q \setminus \{\pm 1\}$, following quantities are defined:*

$$u = \frac{1-t}{1+t},\ v = u^5 + (r^2 - 2)u^3 + u,\ X = \chi(v)u,\ y = \frac{rX + (1+X)^2}{rX - (1+X)^2},$$

and if $t = \pm 1$, $y = 1$. Then, there exists a x such that $-x^2 + y^2 = 1 + dx^2y^2$.

Proof. Define $Y = (\chi(v)v)^{\frac{q+1}{4}}\chi(v)\chi\left(u^2 + \frac{1}{c^2}\right)$, and $x = (c+1)sX(X+1)/Y$. Now the rest of the proof is similar to the proof of Theorem 5.1, and is omitted here. □

Definition 5.6. Let $y(\mathsf{E}_{-1,d}) = \{y \in \mathbb{F}_q : \exists x \in \mathbb{F}_q \text{ such that } (x, y) \in \mathsf{E}_{-1,d}\}$. In the situation of Lemma 5.5, the map $\hat{\phi} : \mathbb{F}_q \to y(\mathsf{E}_{-1,d})$ is defined as: if $t = \pm 1$, $\hat{\phi}(t) = 1$ and if $t \neq \pm 1$, $\hat{\phi}(t) = y$.

5.4.1. *Inversion map of Elligator-T$_y$.* The following lemma shows that there exists an efficient inversion map for Elligator-T$_y$, and the pseudocode is given in Table 13 of Appendix F.

Lemma 5.7. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$ and $\hat{\phi} : \mathbb{F}_q \to y(\mathsf{E}_{-1,d})$ be the encoding map defined in Definition 5.6. Then the following statements hold:*

1. *For any $t \in \mathbb{F}_q$, $\hat{\phi}$ maps $\left\{\pm t, \pm \frac{1}{t}\right\}$ to a y such that $y \in y(\mathsf{E}_{-1,d})$.*
2. *$\hat{\phi}(\mathbb{F}_q)$ is the set of y such that $y \in y(\mathsf{E}_{-1,d})$ satisfying*
   (a) $y + 1 \neq 0$,
   (b) $(1 - \eta r)^2 - 1$ is a square, where $\eta = \frac{y-1}{2(y+1)}$.
3. *If $y \in \hat{\phi}(\mathbb{F}_q) \setminus \{1\}$, then the following elements $\bar{X}, \bar{t}$ of $\mathbb{F}_q$ are defined and $\hat{\phi}(\bar{t}) = y$:*

$$\bar{X} = -(1 - \eta r) + \left((1 - \eta r)^2 - 1\right)^{\frac{q+1}{4}}, \quad \bar{t} = \frac{1 - \bar{X}}{1 + \bar{X}}.$$

Proof. By Theorem 5.3, we have already shown that t and $-t$ map to the same $y \in y(\mathsf{E}_{-1,d})$. Now, we have to show that t and $\frac{1}{t}$ map to the same $y \in y(\mathsf{E}_{-1,d})$. For any $t \in \mathbb{F}_q \setminus \{\pm 1\}$, u, v, X and y are defined as in Lemma 5.5. Now, let $t_1 = \frac{1}{t}$. Then we have $u_1 = \frac{1-t_1}{1+t_1} = -u$ and $v_1 = -u_1^5 - (r^2+2)u_1^3 - u_1 = -(u^5 + (r^2+2)u^3 + u) = -v$. This implies $X_1 = \chi(-v)(-u) = \chi(v)u = X$ and $y_1 = y$. Conversely, let $t_1, t_2 \in \mathbb{F}_q$ such that $\hat{\phi}(t_1) = \hat{\phi}(t_2) = y$. Then, $\frac{rX_1 + (1+X_1)^2}{rX_1 - (1+X_1)^2} = \frac{rX_2 + (1+X_2)^2}{rX_2 - (1+X_2)^2}$ and this implies $X_1 X_2 = 1$ or $X_1 = X_2$. $X_1 X_2 = 1$ implies $t_1 = -t_2$ or $t_1 = -\frac{1}{t_2}$ and $X_1 = X_2$ implies $t_1 = t_2$ or $t_1 = \frac{1}{t_2}$. This proves statement 1 of the lemma.

Statement 2 is already proved in Theorem 5.3.

Now, we come to statement 3 of the lemma. Let $y \in \hat{\phi}(\mathbb{F}_q) \setminus \{1\}$ and $\eta = \frac{y-1}{2(y+1)}$. First note that $y + 1 \neq 0$ and $(1 - \eta r)^2 - 1$ is a square by statement 2. From the statement 3 of Theorem 5.3, the expression z provides the sign using the value of the y-coordinate. Using $\bar{u} = z\bar{X}$, we get two value of $\bar{t}$ and both the value maps to $(\cdot, y)$ by statement 1. Hence, we omit the computation of z and $\bar{u}$, and without loss of generality, the inverse map is given by

$$\bar{X} = -(1 - \eta r) + ((1 - \eta r)^2 - 1)^{\frac{q+1}{4}}, \quad \bar{t} = \frac{1 - \bar{X}}{1 + \bar{X}}.$$

□

5.4.2. *Encoding as strings.* Let q be a b-bit prime and $T_1 \subset \{0,1\}^b$ as defined below. Corollary 5.8 shows the injection between T_1 and y-coordinates of twisted Edwards curve $\mathsf{E}_{-1,d}$.

Corollary 5.8. *Let $\mathbb{F}_q$ be a finite field with prime $q \equiv 3 \pmod 4$. Fix $b = \lfloor \log_2 q \rfloor$ and define a map $\sigma : \{0,1\}^b \to \mathbb{F}_q$ by $\sigma(\rho_0, \rho_1, \ldots, \rho_{b-1}) = \sum_i \rho_i 2^i$. Let $\varsigma_1 : t \mapsto \frac{1}{t}$ and $\varsigma_2 : t \mapsto -t$ for $t \in \mathbb{F}_q$. $T_1 = \sigma^{-1}\left(\mathbb{F}_q / \langle \varsigma_1, \varsigma_2 \rangle\right)$, where σ is define in Theorem 5.4. Then, by using Lemma 5.7, the map $\hat{\tau_3} = \hat{\phi} \circ \sigma : T_1 \to y(\mathsf{E}_{-1,d})$ is defined and if $y \in y(\mathsf{E}_{-1,d})$ satisfies $y + 1 \neq 0$ and $((1 - \eta r)^2 - 1)$ is a square where $\eta = \frac{y-1}{2(y+1)}$, then $\hat{\tau_3}(T_1) = \hat{\phi}(\mathbb{F}_q)$.*

6. **Applications of Elligator-T and Elligator-T$_y$ maps.** To show the applications of Elligator-T and Elligator-T$_y$ maps, we consider the verifiable XEdDSA scheme [25] used in WhatsApp. The verifiable XEdDSA scheme needs to hash a message to a point on a twisted Edwards curve. For a prime field $\mathbb{F}_q$ with $q \equiv 1 \pmod 4$, one can obtain an element $\mathbb{F}_q$ from the message by using any standard cryptographic hash function like the SHA family. After that, this field element can

be mapped to a Montgomery curve using Elligator-2, and subsequently to an isomorphic twisted Edwards curve. However, only for the primes of the form $q \equiv 1 \pmod 4$, Elligator-2 covers the whole field $\mathbb{F}_q$. Thus, our proposed Elligator-T map complements the earlier works. The Elligator-T map can be directly used to verifiable XEdDSA algorithm without any necessary modification. For the application of the Elligator-T$_y$ map, we propose a y-coordinate only variant of the verifiable XEdDSA as given below.

6.1. **y-coordinate only verifiable XEdDSA using Elligator-T$_y$.** During communication, (twisted) Edwards curve points are represented in a compressed form. Let a n-bit string represent the point in little-endian representation. The First $(n-1)$ bits represent the y-coordinate, while the last bit is used for the sign bit. One main caveat is that one square root computation is required to recover the x coordinate. However, the computational overhead of square root calculations often outweighs the benefits of reduced point size for regular users [2]. To overcome this issue, we propose a new verifiable EdDSA algorithm called Verifiable Quotient Edwards Curve Digital Signature Algorithm (VqEdDSA). This algorithm uses only y-coordinate-based arithmetic of the Twisted Edwards curve [21]. This algorithm is one of our contributions and an application of the Elligator-T$_y$ map.

TABLE 3. Key generation.

keyGen:
output: $(a, y(A))$
1. Choose a $a \xleftarrow{\$} \{2, 3. \ldots, p-1\}$
2. Compute $y(A) = y(aB)$.
3. return $(a, y(A))$

TABLE 4. VqEdDSA signature generation and verification.

Parameter: Curve $\mathsf{E}_{-1,\mathsf{d}}$, Base point B	
Sign :	Verify :
Input: $m, (a, y(A))$	Input: $A, m, ((y(V)\|y(R)\|y(R_v)\|s), v)$
Output:$(y(V)\|y(R)\|y(R_v)\|s), v$	Output: Accept/Reject
1. $y(B_v)$=Elligator-T$_y(H(y(A)\|m) \pmod q)$	1. $y(B_v)$=Elligator-T$_y$ $(y(A)\|m)$
2. $y(V) = y(aB_v)$	2. $h = H(A\|y(V)\|y(R)\|y(R_v)\|m) \pmod q$
3. r=$H(a\|y(V))\pmod q$	3. $y_{11} = y(sB)$
4. $y(R) = y(rB)$	4. $y_{12} = y(hA)$
5. $y(R_v) = y(rB_v)$	5. $y_{21} = y(sB_v)$
6. $h = H(A\|y(V)\|y(R)\|y(R_v)\|m) \pmod q$	6. $y_{22} = y(hV)$
7. $s = r + ha \pmod q$	7. If $f(y_{11}, y_{12}, y(R)) == 0$ and $f(y_{21}, y_{22}, y(R_v)) == 0$
8. $v = H(y(cV))\pmod{2^b}$	8. $v = H(y(cV))\pmod{2^b}$
9. return $((y(V)\|y(R)\|y(R_v)\|s), v)$	9. Return v
	10. Else
	11. Return false

The VqEdDSA protocol has two main components. One is signature generation, and the other is a verification algorithm. Both algorithms require hashing a field

element to an elliptic curve point, specifically to a twisted Edwards curve. The VqEdDSA signature generation and verification can be performed by using only the y-coordinate-based arithmetic of the twisted Edwards curve. In VqEdDSA, all the scalar multiplication is done by using the y-coordinate only Montgomery-style scalar multiplication. Let H be a collision-resistant hash function. Let $\mathsf{E}_{-1,d}$ be a twisted Edwards curve over a prime field $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$ and q is of bit-length b-bit. Also, d is square. Let B be the base point of the largest prime subgroup of the curve, and let the order of B be p. If P be a point on the curve, then we denote the y-coordinate by $y(P)$.

The keyGen algorithm returns a pair $(a, y(A))$ where a is the secret key and $y(A)$ is the public key. The details of key generation are given in Table 3. The user converts $y(A)$ into a binary string $\hat{\tau}_3^{-1}(y(A))$. Before using the public key, the signer or verifier retrieves $y(A)$ by computing $y(A) = \hat{\tau}_3(\hat{\tau}_3^{-1}(y(A)))$.

The signing algorithm Sign takes a message m and the user's key pair $(a, y(A))$ as input and generates the signature $((y(V)\|y(R)\|y(R_v)\|s), v)$ as described in Table 4. The signer shares the signature as $(\hat{\tau}_3^{-1}((y(V))\|\hat{\tau}_3^{-1}(y(R))\|\hat{\tau}_3^{-1}(y(R_v))\|s), v)$.

Before verification, verifier converts the binary strings $\hat{\tau}_3^{-1}((y(V)), \hat{\tau}_3^{-1}(y(R))$, and $\hat{\tau}_3^{-1}(y(R_v))$ to y-coordinates of twisted Edwards curve points as $\hat{\tau}_3(\hat{\tau}_3^{-1}((y(V)))$, $\hat{\tau}_3(\hat{\tau}_3^{-1}(y(R)))$, and $\hat{\tau}_3(\hat{\tau}_3^{-1}(y(R_v)))$. Then, the verification algorithm Verify employs the same technique as the verification of qDSA on Kummer line [18]. Let, P_1, P_2 and P_3 be three points on the curve such that $P_1 \pm P_2 = P_3$. We formulate f function from the $y(P_1)$ and $y(P_2)$ such that $y(P_3)$ satisfies the expression. The formulaizations of α_i are given in Appendix G. Let $y_1 = y(P_1)$, $y_2 = y(P_2)$ and $y_3 = y(P_3)$ and the f function is defined as given below.

$$f(y_1, y_2, y_3) = \alpha_0 y_3^2 - \alpha_1 y_3 + \alpha_2$$

where $\alpha_0 = -(y_1^2 - 1)(1 + dy_2^2) + (d+1)y_1^2$, $\alpha_1 = 2(d+1)y_1y_2$ and $\alpha_2 = (y_1^2 - 1)(1 + dy_2^2) + (d+1)y_2^2$. The details of the verification algorithm are also given in Table 4.

Performance comparison between verifiable XEdDSA and proposed VqEdDSA. The signing algorithm of our proposed VqEdDSA eliminates the square root computations of the signing algorithm of the original XEdDSA algorithm [18]. However, the verification algorithm of VqEdDSA replaces two square root computations required to retrieve R and R_v fully with a total of 20 field multiplications and 12 field squarings in projective space. Therefore, it improves the performance of the signing and verification algorithm by avoiding costly square root computation at the cost of a few field multiplications.

6.2. **Some suitable twisted Edwards curves for Elligator-T.** For the Elligator-T map, we restrict ourselves to the prime fields $\mathbb{F}_p$ with $p \equiv 3 \pmod 4$. For cryptographic implementation purposes, some popular primes of the form $p \equiv 3 \pmod 4$ are $p2519 = 2^{251} - 9$, $p2859 = 2^{285} - 9$. These primes are useful because they are of the form $2^m \pm \delta$ with small δ. Thus, they provide efficient modular reduction. Here, for each prime, one twisted Edwards curve is suggested such that the curve and its quadratic twists both have small cofactors. These curves are parametrised by the coefficient d of the twisted Edwards curve $\mathsf{E}_{-1,d}$. Let l and l_T be the largest primes that divide the cardinality of the twisted Edwards curve and its quadratic twist, respectively. Also, let h and h_T denote the cofactors accordingly.

7. **Application of Elligator-K1 and Elligator-K3 map.** Elligator-K3 and -K1 map a prime field element to Kummer Lines. If the prime is of the form $3 \pmod 4$

TABLE 5. Suitable twisted Edwards curve.

Field	Twisted Edwards Curve(d)	$(\log l, \log l_T)$	(h, h_T)	Base Point$(x : y)$
$p2519$	149321	$(250, 249)$	$(4, 4)$	$(x_1, 14)$
$p2859$	150423	$(283, 284)$	$(4, 4)$	$(x_2, 18)$
$x_1 =$ 0x1589f196fae086c11e9347ce4c86bb73e2aea92c676d0c8bd90e30992b0dd06				
$x_2 =$ 0x8b6d66d398fd1b1f18cd7f4270e116929a1c0de12586f6dfcadee4c796757dd688f32fa				

then one can use Elligator-K3, and if the prime is of the form 1 (mod 4), then one can use Elligator-K1. By [18], the Kummer line provides the fastest scalar multiplication among all forms of elliptic curves. Because of that, we choose Diffie-Hellman key exchange [2] using Kummer line to show the application of Elligator-K* (K3 and K1 both).

7.1. **Diffie-Hellman using Kummer line.** Depending on the prime field, one can use either Elligator-K1 or Elligator-K3 to map on a Kummer line. Here, the user publishes a bit string (field element) instead of a curve point. Let A and B be two parties trying to establish a shared key by Diffie-Hellman key exchange using Kummer Line. User A generates a (public key, secret key) pair by following the steps given below.

1. A chooses a random integer a.
2. Computes $P_A = aP$, where P is the base point of the Kummer line.
3. Check whether P_A is in the image set of Elligator-K. If "False", goto step 1.
4. Compute $\hat{\tau_i}^{-1}(P_A) = \mu_A$ and sends μ_A to B. (From the Corollary 4.5 and 4.10 and $i \in \{1, 2\}$ depending on the prime of the underlying field)

Similarly, B also computes μ_B and sends it to A. Upon receiving μ_B, A computes the following Steps.

1. Computes $P_B = \hat{\tau_i}(\mu_B)$.
2. Computes $c = H(aP_B)$.

Similarly, A computes the same c. Hence, A and B share a secret key.

7.2. **Some suitable Kummer lines.** As mentioned earlier, the primes $p2519$ and $p2859$ are primes of the form 3 (mod 4). For primes of the form 1 (mod 4), we choose two well-known primes commonly used in cryptographic implementations, $p25519 = 2^{255} - 19$ and $p2663 = 2^{266} - 3$. For each prime, one Kummer line is suggested so that the curve and its quadratic twists have a small cofactor. Table 6 and Table 7 enlist the Legendre curves along with the associated Kummer lines that can be used for Diffie-Hellman using Elligator-K3 and Elligator-K1, respectively. Here, l and l_T are the largest prime factors of the cardinalities of the associated Legendre curve and its quadratic twist, respectively. Similarly, h and h_T are the corresponding cofactors.

8. **Conclusion.** In this paper, we have introduced a map, Elligator-T, from a prime field of the form 3 (mod 4) to a complete twisted Edwards curve $\mathsf{E}_{-1,d}$. Additionally, we have proposed a y-coordinate-only verifiable qEdDSA using Elligator-T$_y$. There is no existing literature about the mapping to the Kummer Line. In this context, we have first constructed two maps, Elligator-L3 and Elligator-L1, from

TABLE 6. Kummer lines for Elligator-K3.

Field	Legendre Curve(λ)	Kummer line(a^2, b^2)	($\log l, \log l_T$)	(h, h_T)	Base Point($\mathsf{X} : \mathsf{Z}$)
$p2519$	λ_1	$(122, 202)$	$(248, 249)$	$(8, 8)$	$(2 : 1)$
$p2859$	λ_2	$(268, 273)$	$(282, 283)$	$(8, 8)$	$(13 : 1)$
$\lambda_1 =$ 0x555046cb892a59c20de7faf17633d5046cb892a59c20de7faf17633d5046cb2					
$\lambda_2 =$ 0x9bc6d67407314ea53d9c3ff9f16cee1cf5af2d8589526e59876de063f07aa7222a358f1					

TABLE 7. Kummer lines for Elligator-K1.

Field	Legendre Curve(λ)	Kummer line(a^2, b^2)	($\log l, \log l_T$)	(h, h_T)	Base Point($\mathsf{X} : \mathsf{Z}$)
$p25519$	λ_3	$(289, 515)$	$(252, 253)$	$(16, 4)$	$(2 : 1)$
$p2663$	λ_4	$(211, 345)$	$(263, 263)$	$(16, 12)$	$(56 : 1)$
$\lambda_3 =$ 0x12cadb5b93d7bd5d89e6d2067837a2509694e414dfc0e1c840d4cc46eae96c8a					
$\lambda_4 =$ 0x1f9162ee532e191fdbef659ff49096db4d8b8100da25fd3238ae63036fa17090b2e					

prime fields to a Legendre curve, covering all forms of prime fields. Using these maps, we have introduced the maps Elligator-K3 and Elligator-K1, which map an element of the prime field to the Kummer Line. We have also shown the applicability of Elligator-K3 and Elligator-K1 in the Diffie-Hellman key exchange protocol context. Furthermore, we have suggested some examples of twisted Edwards curves and Kummer lines over popular primes suitable for cryptographic implementation.

REFERENCES

[1] D. J. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters, Twisted Edwards curves, *Proceedings of the 1st International Conference on Cryptology in Africa on Progress in Cryptology – AFRICACRYPT 2008*, Casablanca, Morocco, (2008), 389-405.

[2] D. J. Bernstein, M. Hamburg, A. Krasnova and T. Lange, Elligator: Elliptic-curve points indistinguishable from uniform random strings, *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security – CCS 2013*, Berlin, Germany, (2013), 967-980.

[3] D. Boneh and M. Franklin, Identity-based encryption from the weil pairing, *Proceedings of the 21st Annual Cryptology Conference on Advances in Cryptology – CRYPTO 2001*, Santa Barbara, California, USA, (2001), 213-229.

[4] E. Brier, J.-S. Coron, T. Icart, D. Madore, H. Randriam and M. Tibouchi, Efficient indifferentiable hashing into ordinary elliptic curves, *Proceedings of the 30th Annual Cryptology Conference on Advances in Cryptology – CRYPTO 2010*, Santa Barbara, CA, USA, (2010), 237-254.

[5] É. Brier and M. Joye, Weierstraß elliptic curves and side-channel attacks, *Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems – PKC 2002*, Paris, France, (2002), 335-345.

[6] M. Fadavi and R. R. Farashahi, Uniform encodings to elliptic curves and indistinguishable point representation, *Designs, Codes and Cryptography*, **88** (2020), 1479-1502.

[7] R. R. Farashahi, Hashing into Hessian curves, *Proceedings of the 4th International Conference on Progress in Cryptology in Africa – AFRICACRYPT 2011*, Dakar, Senegal, (2011), 278-289.

[8] R. R. Farashahi, P.-A. Fouque, I. E. Shparlinski, M. Tibouchi and J. F. Voloch, Indifferentiable deterministic hashing to elliptic and hyperelliptic curves, *Mathematics of Computation*, **82** (2013), 491-512.

[9] R. R. Farashahi and S. G. Hosseini, Differential addition on twisted Edwards curves, *Proceedings of the 22nd Australasian Conference on Information Security and Privacy – ACISP 2017*, Auckland, New Zealand, (2017), 366-378.

[10] P.-A. Fouque, A. Joux and M. Tibouchi, Injective encodings to elliptic curves, *Proceedings of the 18th Australasian Conference on Information Security and Privacy – ACISP 2013*, Brisbane, Australia, (2013), 203-218.

[11] P.-A. Fouque and M. Tibouchi, Deterministic encoding and hashing to odd hyperelliptic curves, *Proceedings of the 4th International Conference on Pairing-Based Cryptography – PAIRING 2010*, Yamanaka Hot Spring, Japan, (2010), 265-277.

[12] P.-A. Fouque and M. Tibouchi, Estimating the size of the image of deterministic hash functions to elliptic curves, *Proceedings of the 1st International Conference on Cryptology and Information Security in Latin America – LATINCRYPT 2010*, Puebla, Mexico, (2010), 81-91.

[13] P.-A. Fouque and M. Tibouchi, Indifferentiable hashing to Barreto–Naehrig curves, *Proceedings of the 2nd International Conference on Cryptology and Information Security in Latin America – LATINCRYPT 2012*, Santiago, Chile, (2012), 1-17.

[14] G. Frey and H.-G. Rück, The strong Lefschetz principle in algebraic geometry, *Manuscripta Mathematica*, **55** (1986), 385-401.

[15] H. Hisil, K.-H. K. Wong, G. Carter and E. Dawson, Twisted Edwards curves revisited, *Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2008*, Melbourne, Australia, (2008), 326-343.

[16] T. Icart, How to hash into elliptic curves, *Proceedings of the 29th Annual Cryptology Conference on Advances in Cryptology – CRYPTO 2009*, Santa Barbara, CA, USA, (2009), 303-316.

[17] A. Joux, A one round protocol for tripartite Diffie–Hellman, *Journal of Cryptology*, **17** (2004), 263-276.

[18] S. Karati and P. Sarkar, Kummer for genus one over prime-order fields, *Journal of Cryptology*, **33** (2020), 92-129.

[19] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.*, **48** (1987), 203-209.

[20] J. López and R. Dahab, Fast multiplication on elliptic curves over GF(2^m) without precomputation, *Proceedings of the 1st International Workshop Cryptographic Hardware and Embedded Systems – CHES 1999*, Worcester, MA, USA, (1999), 316-327.

[21] L. Marin, Differential elliptic point addition in twisted Edwards curves, *Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops – WAINA 2013*, Barcelona, Spain, (2013), 1337-1342.

[22] V. S. Miller, Use of elliptic curves in cryptography, *Proceedings of the 5th Annual Cryptology Conference on Advances in Cryptology – CRYPTO 1985*, Santa Barbara, California, USA, 1985, 417-426.

[23] B. Möller, A public-key encryption scheme with Pseudo-random ciphertexts, *Proceedings of the 9th European Symposium on Research Computer Security – ESORICS 2004*, Sophia Antipolis, France, (2004), 335-351.

[24] P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, *Mathematics of Computation*, **48** (1987), 243-264.

[25] T. Perrin, The XEdDSA and VXEdDSA signature schemes, Available from: `https://www.signal.org/docs/specifications/xeddsa/xeddsa.pdf`.

[26] A. Shallue and C. E. van de Woestijne, Construction of rational points on elliptic curves over finite fields, *Proceedings of the 7th international conference on Algorithmic Number Theory – ANTS-VII*, Berlin, Germany, (2006), 510-524.

[27] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2^{nd} edition, Chapman & Hall/CRC, 2003.

[28] Z. Weinberg, J. Wang, V. Yegneswaran, L. Briesemeister, S. Cheung, F. Wang and D. Boneh, StegoTorus: A camouflage proxy for the Tor anonymity system, *Proceedings of the 2012 ACM SIGSAC Conference on Computer and Communications Security – CCS 2012*, Raleigh, North Carolina, USA, (2012), 109-120.

[29] E. Wustrow, S. Wolchok, I. Goldberg and J. A. Halderman, Telex: Anticensorship in the network infrastructure, *Proceedings of the 20th USENIX Conference on Security – USENIX 2011*, San Francisco, CA, USA, 2011.

[30] A. L. Young and M. M. Yung, Space-efficient kleptography without random oracles, *Proceedings of Information Hiding – IH 2007*, Saint Malo, France, (2007), 112-129.

[31] A. L. Young and M. M. Yung, Kleptography from standard assumptions and applications, *Proceedings of the 7th International Conference on Security and Cryptography for Networks–SCN 2010*, Amalfi, Italy, (2010), 271-290.

Received October 26, 2024; 1st revision April 27, 2025; 2nd revision December 4, 2025; early access January 2026.

Appendix A. **Pseudocode for Elligator-L3.** Table 8 includes the pseudocode of the encoding and decoding of Elligator-L3 as given by Theorem 3.1 (and Definition 3.2) and Theorem 3.3.

TABLE 8. Elligator-L3.

Parameter: Fix $q \equiv 3 \pmod 4$, $c \in \mathbb{F}_q \setminus \{-1, 0, 1\}$, $r = c - \frac{1}{c}$, $\alpha_1 = -2 + c + \frac{1}{c}$ and $\alpha_2 = -2 - c - \frac{1}{c}$. α_1 is a square and β is a square root of α_1 and $\lambda = \alpha_2/\alpha_1$, $A = \frac{r^2}{\alpha_1}$,$B = \frac{r^2}{\beta^3}$	
Encoding Input: $t \in \mathbb{F}_q \setminus \{\pm 1\}$ Output: $(x, y) \in \mathsf{E}_\lambda$	**Decoding** Input: $(x, y) \in \psi_1(\mathbb{F}_q) \subset \mathsf{E}_\lambda$ Output: $\bar{t} \in \mathbb{F}_q$
1. $u_0 = 1 - t$ 2. $u_1 = \frac{1}{1+t}$ 3. $u = u_0 \cdot u_1$ 4. $v_0 = u^2$ 5. $v = -u \cdot (v_0 - c^2) \cdot (v_0 - \frac{1}{c^2})$ 6. $\epsilon_1 = -\chi(v)^2 + \chi(v) + 1$ 7. $X = \epsilon_1 \cdot u$ 8. $Y_0 = \mathsf{Sqrt}(\epsilon_1 \cdot v)$ 9. $\epsilon_2 = \chi(v_0 - \frac{1}{c^2})$ 10. $Y = Y_0 \cdot \epsilon_1 \cdot \epsilon_2$ 11. $x_0 = 1 + X$ 12. $x_1 = x_0^2$ 13. $y_0 = x_1 \cdot x_0$ 14. $w = 1/y_0$ 15. $x = A \cdot X \cdot w \cdot x_0$ 16. $y = B \cdot Y \cdot w$ 17. Return (x, y)	1. If $(x, y) = (0, 0)$ 2. Return $\bar{t} = 1$ 3. Else 4. $v_0 = 2 \cdot x \cdot \alpha_1$ 5. $v_1 = \frac{1}{v_0}$ 6. $v_2 = 1 - v_1 \cdot r^2$ 7. $v_3 = v_2 \cdot v_2$ 8. $\bar{X} = -v_2 + \mathsf{Sqrt}(v_3 - 1)$ 9. $x_2 = \bar{X} \cdot \bar{X} - \frac{1}{c^2}$ 10. $z = \chi(\beta \cdot (1 + \bar{X}) \cdot y \cdot x_2)$ 11. $\epsilon = -z^2 + z + 1$ 12. $\bar{u} = \epsilon \cdot \bar{X}$ 13. $t_0 = \frac{1}{1+\bar{u}}$ 14. $\bar{t} = (1 - \bar{u}) \cdot t_0$ 15. Return $\bar{t}$

Appendix B. **Pseudocode for Elligator-L1.** Table 9 includes the pseudocode of the encoding and decoding of Elligator-L1 as given by Theorem 3.5 (and Definition 3.6) and Theorem 3.7.

TABLE 9. Elligator-L1.

Parameter: Fix $q \equiv 1 \pmod 4$, $u \in \mathbb{F}_q$ is a non-square, $\lambda \in \mathbb{F}_q$ is a square, $A = \frac{\lambda+1}{2}$	
Encoding Input: $t \in \mathbb{F}_q \setminus \{0\}$ Output: $(x, y) \in \mathsf{E}_\lambda$	**Decoding** Input: $(x, y) \in \psi_2(\mathbb{F}_q) \subset \mathsf{E}_\lambda$ Output: $\bar{t} \in \mathbb{F}_q$
1. $u_0 = u \cdot t^2$ 2. $u_1 = \frac{1}{1+u_0}$ 3. $u_2 = (\lambda + 1) \cdot u_1$ 4. $v = u_2 \cdot (u_2 - 1) \cdot (u_2 - \lambda)$ 5. $\epsilon = \chi(v)$ 6. $x = \epsilon \cdot (u_2 - A) + A$ 7. $v_1 = x \cdot (x - 1) \cdot (x - \lambda)$ 8. $y = -\epsilon \cdot \mathsf{Sqrt}(v_1)$ 9. Return (x, y)	1. If $y \in \{0, 1, 2, \cdots, \frac{q-1}{2}\}$then 2. $x_1 = (x - \lambda - 1) \cdot u$ 3. $x_2 = 1/x_1$ 4. $x_3 = -x \cdot x_2$ 5. $\bar{t} = \mathsf{sqrt}(x_3)$ 6. Return $\bar{t}$ 7. Else 8. $x_1 = x \cdot u$ 9. $x_2 = 1/x_1$ 10. $x_3 = -(x - \lambda - 1) \cdot x_2$ 11. $\bar{t} = \mathsf{Sqrt}(x_3)$ 12. Return $\bar{t}$

Appendix C. **Pseudocode for Elligator-K3.** Table 10 includes the pseudocode of the encoding and decoding of Elligator-K3 as given by Lemma 4.1 (and Definition 4.2) and Corollary 4.4.

TABLE 10. Elligator-K3.

Parameter: Fix $q \equiv 3 \pmod 4$, $c \in \mathbb{F}_q \setminus \{-1, 0, 1\}$, $r = c - \frac{1}{c}$, $\alpha_1 = -2 + c + \frac{1}{c}$ and $\alpha_2 = -2 - c - \frac{1}{c}$. α_1 is a square and $\lambda = \alpha_2/\alpha_1$,$A = \frac{r^2}{\alpha_1}$	
Encoding Input: $t \in \mathbb{F}_q \setminus (\{\pm 1\} \cup S)$ Output:$(\mathsf{X} : \mathsf{Z}) \in \mathcal{K}_{a^2,b^2}$	**Decoding** Input: $(\mathsf{X} : \mathsf{Z}) \in \hat{\psi}_1(\mathbb{F}_q) \subset \mathcal{K}_{a^2,b^2}$ Output: $\bar{t} \in \mathbb{F}_q$
$u_0 = t^2$	If $(\mathsf{X} : \mathsf{Z}) = (b^2 : a^2)$
$u_1 = t + t$	Return $\bar{t} = 1$
$u_{02} = u_0 - u_1 + 1$	Else
$u_{12} = u_0 + u_1 + 1$	$x_0 = a^2 \cdot \mathsf{X}$
$u_{01} = 1 - u_0$	$x_1 = x_0 - b^2 \cdot \mathsf{Z}$
$v_0 = u_{02} - c^2 \cdot u_{12}$	$x_3 = 2 \cdot x_0 \cdot \alpha_1$
$v_1 = u_{02} - \frac{1}{c^2} \cdot u_{12}$	$v = \frac{1}{x_3}$
$v = -u_{01} \cdot v_0 \cdot v_1$	$v_0 = v \cdot x_1$
$\epsilon = -\chi(v)^2 + \chi(v) + 1$	$v_1 = 1 - v_0 \cdot r^2$
$x_0 = \epsilon \cdot u_{01}$	$v_2 = v_1^2$
$\mathbf{x} = A \cdot x_0$	$\bar{X} = -v_1 + \mathsf{Sqrt}(v_2 - 1)$
$\mathbf{z} = u_{02} + u_{12} + (x_0 + x_0)$	$t_0 = \frac{1}{1+\bar{X}}$
$\mathsf{X} = b^2 \cdot \mathbf{x}$	$\bar{t} = (1 - \bar{X}) \cdot t_0$
$\mathsf{Z} = a^2 \cdot (\mathbf{x} - \mathbf{z})$	Return $\bar{t}$
Return $(\mathsf{X} : \mathsf{Z})$	

Appendix D. **Pseudocode for Elligator-K1.** Table 11 includes the pseudocode of the encoding and decoding of Elligator-K1 as given by Lemma 4.6 (and Definition 4.7) and Corollary 4.9.

TABLE 11. Elligator-K1.

Parameter: Fix $q \equiv 1 \pmod 4$, $u \in \mathbb{F}_q$ is a non-square, $\lambda \in \mathbb{F}_q$ is a square, $A = \frac{\lambda+1}{2}$ and $B = \lambda + 1$	
Encoding Input: $t \in \mathbb{F}_q \setminus \{0\}$ Output: $(\mathsf{X} : \mathsf{Z}) \in \mathcal{K}_{a^2,b^2}$	**Decoding** Input: $(\mathsf{X} : \mathsf{Z}) \in \hat{\psi}_2(\mathbb{F}_q) \subset \mathcal{K}_{a^2,b^2}$ Output: $\bar{t} \in \mathbb{F}_q$
$u_0 = u \cdot t^2$	If $(\mathsf{X} : \mathsf{Z}) = (b^2 : a^2)$
$v_1 = 1 + u_0$	Return $t = 0$
$v = B \cdot v_1 \cdot (\lambda - u_0) \cdot (1 - \lambda \cdot u_0)$	Else
$\epsilon = \chi(v)$	$x_0 = a^2 \cdot \mathsf{X}$
$v_2 = A \cdot v_1$	$x_1 = x_0 - b^2 \cdot \mathsf{Z}$
$\mathbf{x} = \epsilon \cdot (B - v_2) + v_2$	$x_2 = (x_0 - (\lambda + 1) \cdot x_1) \cdot u$
$\mathbf{z} = v_1$	$x_3 = \frac{1}{x_2}$
$\mathsf{X} = b^2 \cdot \mathbf{x}$	$t_0 = -x_3 \cdot x_0$
$\mathsf{Z} = a^2 \cdot (\mathbf{x} - \mathbf{z})$	$\bar{t} = \mathsf{Sqrt}(t_0)$
Return $(\mathsf{X} : \mathsf{Z})$	Return $\bar{t}$

Appendix E. **Pseudocode for Elligator-T.** Table 12 includes the pseudocode of the encoding and decoding of Elligator-T as given by Theorem 5.1 (and Definition 5.2) and Theorem 5.3.

TABLE 12. Elligator-T.

Parameter: Fix $q \equiv 3 \pmod 4$ and $s \in \mathbb{F}_q$ such that $(s^2-2)(s^2+2) \neq 0$ and $\left(\left(\frac{2}{s^2}+\frac{s^2}{2}-2\right)^2-4\right)$ is a quadratic non-residue. Fix $c=\frac{2}{s^2}$, $r=c+\frac{1}{c}$, $d=\left(\frac{c-1}{c+1}\right)^2$ and $B=s\cdot(c+1)$	
Encoding Input: $t \in \mathbb{F}_q \setminus \{\pm 1\}$ Output:$(x,y) \in \mathsf{E}_{-1,d}$	**Decoding** Input: $(x,y) \in \phi(\mathbb{F}_q) \subset \mathsf{E}_{-1,d}$. Output: $\bar{t} \in \mathbb{F}_q$
1. $u_0 = 1-t$ 2. $u_1 = \frac{1}{1+t}$ 3. $u = u_0 \cdot u_1$ 4. $v_0 = u^2$ 5. $v = u\cdot(v_0+c^2)\cdot(v_0+\frac{1}{c^2})$ 6. $\epsilon = \chi(v)$ 7. $X = \epsilon \cdot u$ 8. $Y_0 = \mathsf{Sqrt}(\epsilon \cdot v)$ 9. $Y_1 = \chi(v_0+\frac{1}{c^2})$ 10. $Y = Y_0 \cdot \epsilon \cdot Y_1$ 11. $x_0 = r \cdot X$ 12. $x_1 = (1+X)\cdot(1+X)$ 13. $x_2 = (x_0-x_1)\cdot Y$ 14. $w = \frac{1}{x_2}$ 15. $x = B\cdot X\cdot(1+X)\cdot w\cdot(x_0-x_1)$ 16. $y = (x_0+x_1)\cdot w\cdot Y$ 17. Return (x,y)	1. $x_0 = 2\cdot(y+1)$ 2. $x_1 = \frac{1}{x_0}$ 3. $x_2 = (y-1)\cdot x_1$ 4. $x_3 = 1-x_2\cdot r$ 5. $x_4 = x_3\cdot x_3$ 6. $\bar{X} = -x_3 + \mathsf{Sqrt}(x_4-1)$ 7. $x_5 = \bar{X}^2 + \frac{1}{c^2}$ 8. $z = \chi(B\cdot(1+\bar{X})\cdot\bar{X}\cdot x\cdot x_5)$ 9. $\bar{u} = z\cdot\bar{X}$ 10. $t_0 = \frac{1}{1+\bar{u}}$ 11. $t = (1-\bar{u})\cdot t_0$ 12. Return $\bar{t}$

Appendix F. **Pseudocode for Elligator-T$_y$.** Table 13 includes the pseudocode of the encoding and decoding Elligator-T$_y$ as given by Lemma 5.5 (and Definition 5.6) and Lemma 5.7.

TABLE 13. Elligator-T$_y$.

Parameter: Fix $q \equiv 3 \pmod 4$ and $s \in \mathbb{F}_q$ such that $(s^2-2)(s^2+2) \neq 0$ and $\left(\left(\frac{2}{s^2}+\frac{s^2}{2}-2\right)^2-4\right)$ is a quadratic non-residue. Fix $c=\frac{2}{s^2}$, $r=c+\frac{1}{c}$ and $d=\left(\frac{c-1}{c+1}\right)^2$	
Encoding Input: $t \in \mathbb{F}_q \setminus \{\pm 1\}$ Output: $y \in y(\mathsf{E}_{-1,d})$	**Decoding** Input: $y \in \hat{\phi}(\mathbb{F}_q) \subset y(\mathsf{E}_{-1,d})$ Output: $\bar{t} \in \mathbb{F}_q$
1. $u_0 = t^2$ 2. $u_1 = t+t$ 3. $u_{02} = u_0 - u_1 + 1$ 4. $u_{12} = u_0 + u_1 + 1$ 5. $u_{01} = 1-u_0$ 6. $v_0 = u_{02} + c^2\cdot u_{12}$ 7. $v_1 = u_{02} + \frac{1}{c^2}\cdot u_{12}$ 8. $v = u_{01}\cdot v_0\cdot v_1$ 9. $\epsilon = \chi(v)$ 10. $X_1 = \epsilon\cdot(1-t)$ 11. $X_2 = 1+t$ 12. $y_1 = r\cdot X_1\cdot X_2$ 13. $y_2 = (X_1+X_2)\cdot(X_1+X_2)$ 14. $Y = y_1+y_2$ 15. $Z = y_1-y_2$ 16. $y = Y/Z$ 18. Return y	1. $x_0 = 2\cdot(y+1)$ 2. $x_1 = \frac{1}{x_0}$ 3. $x_2 = (y-1)\cdot x_1$ 4. $x_3 = 1-x_2\cdot r$ 5. $x_4 = x_3\cdot x_3$ 6. $\bar{X} = -x_3 + \mathsf{Sqrt}(x_4-1)$ 7. $t_0 = \frac{1}{1+\bar{X}}$ 8. $t = (1-\bar{X})\cdot t_0$ 9. Return $\bar{t}$

Appendix G. Detailed calculation of $f(y_1, y_2, y)$ in Section 6.1.

Let $\mathsf{E}_{-1,d} : -x^2 + y^2 = 1 + dx^2y^2$ be a twisted Edwards curve over a finite field $\mathbb{F}_q$. Let, (x_1, y_1) and (x_2, y_2) be two points on twisted Edwards $\mathsf{E}_{-1,d}$ and $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$, $(x_4, y_4) = (x_1, y_1) - (x_2, y_2)$. Then,

$$y_3 = \frac{y_1y_2 + x_1x_2}{1 - dx_1x_2y_1y_2} \text{ and } y_4 = \frac{y_1y_2 - x_1x_2}{1 + dx_1x_2y_1y_2}.$$

Now,

$$\begin{aligned}
y_3 + y_4 &= \frac{(y_1y_2 + x_1x_2)(1 + dx_1x_2y_1y_2) + (y_1y_2 - x_1x_2)(1 - dx_1x_2y_1y_2)}{1 - d^2x_1^2x_2^2y_1^2y_2^2} \\
&= \frac{2y_1y_2 + 2dx_1^2x_2^2y_1y_2}{1 - d^2x_1^2x_2^2y_1^2y_2^2} \\
&= \frac{2y_1y_2 + 2d\frac{y_1^2-1}{dy_1^2+1}\frac{y_2^2-1}{dy_2^2+1}y_1y_2}{1 - d^2\frac{y_1^2-1}{dy_1^2+1}\frac{y_2^2-1}{dy_2^2+1}y_1^2y_2^2} \qquad \left[\text{ Since } x_i^2 = \frac{y_i^2 - 1}{dy_i^2 + 1}\right] \\
&= 2y_1y_2\frac{(dy_1^2 + 1)(dy_2^2 + 1) + d(y_1^2 - 1)(y_2^2 - 1)}{(dy_1^2 + 1)(dy_2^2 + 1) - d^2(y_1^2 - 1)(y_2^2 - 1)y_1^2y_2^2} \\
&= 2y_1y_2\frac{d^2y_1^2y_2^2 + dy_1^2 + dy_2^2 + 1 + dy_1^2y_2^2 - dy_1^2 - dy_2^2 + d}{d^2y_1^2y_2^2 + dy_1^2 + dy_2^2 + 1 - d^2y_1^4y_2^4 + d^2y_1^4y_2^2 + d^2y_1^2y_2^4 - d^2y_1^2y_2^2} \\
&= 2y_1y_2\frac{(d + 1)(1 + dy_1^2y_2^2)}{(1 + dy_1^2y_2^2)(dy_1^2 + dy_2^2 - dy_1^2y_2^2 + 1)} \\
&= \frac{2(d + 1)y_1y_2}{dy_1^2 + dy_2^2 - dy_1^2y_2^2 + 1}.
\end{aligned}$$

Also,

$$\begin{aligned}
y_3y_4 &= \frac{y_1^2y_2^2 - x_1^2x_2^2}{1 - d^2x_1^2x_2^2y_1^2y_2^2} \\
&= \frac{y_1^2y_2^2 - \frac{y_1^2-1}{dy_1^2+1}\frac{y_2^2-1}{dy_2^2+1}}{1 - d^2\frac{y_1^2-1}{dy_1^2+1}\frac{y_2^2-1}{dy_2^2+1}y_1^2y_2^2} \qquad \left[\text{ Since } x_i^2 = \frac{y_i^2 - 1}{dy_i^2 + 1}\right] \\
&= \frac{y_1^2y_2^2(dy_1^2 + 1)(dy_2^2 + 1) - (y_1^2 - 1)(y_2^2 - 1)}{(dy_1^2 + 1)(dy_2^2 + 1) - d^2(y_1^2 - 1)(y_2^2 - 1)y_1^2y_2^2} \\
&= \frac{y_1^2y_2^2(d^2y_1^2y_2^2 + 1 + dy_1^2 + dy_2^2) - y_1^2y_2^2 - 1 + y_1^2 + y_2^2}{(dy_1^2 + 1)(dy_2^2 + 1) - d^2(y_1^2 - 1)(y_2^2 - 1)y_1^2y_2^2} \\
&= \frac{(1 + dy_1^2y_2^2)(y_1^2 + y_2^2 + dy_1^2y_2^2 - 1)}{(1 + dy_1^2y_2^2)(dy_1^2 + dy_2^2 - dy_1^2y_2^2 + 1)} \\
&= \frac{y_1^2 + y_2^2 + dy_1^2y_2^2 - 1}{dy_1^2 + dy_2^2 - dy_1^2y_2^2 + 1}.
\end{aligned}$$

Then, y_3 and y_4 are both the roots of the polynomial

$$f(y_1, y_2, y) = y^2 - \frac{2(d + 1)y_1y_2}{dy_1^2 + dy_2^2 - dy_1^2y_2^2 + 1}y + \frac{y_1^2 + y_2^2 + dy_1^2y_2^2 - 1}{dy_1^2 + dy_2^2 - dy_1^2y_2^2 + 1}.$$

Equivalently,

$$\begin{aligned} f(y_1, y_2, y) &= (dy_1^2 + dy_2^2 - dy_1^2y_2^2 + 1)y^2 - 2(d+1)y_1y_2y + (y_1^2 + y_2^2 + dy_1^2y_2^2 - 1) \\ &= (-(y_1^2 - 1)(1 + dy_2^2) + (d+1)y_1^2)y^2 - 2(d+1)y_1y_2y \\ &\quad + ((y_1^2 - 1)(1 + dy_2^2) + (d+1)y_2^2) \\ &= \alpha_0 y^2 - \alpha_1 y + \alpha_2 \end{aligned}$$

where

$$\begin{aligned} \alpha_0 &= -(y_1^2 - 1)(1 + dy_2^2) + (d+1)y_1^2 \\ \alpha_1 &= 2(d+1)y_1y_2 \\ \alpha_2 &= (y_1^2 - 1)(1 + dy_2^2) + (d+1)y_2^2 \end{aligned}$$

Appendix H. **F-F encoding** [6]. Let $\mathbb{F}_q$ be a finite field of odd characteristic. Let $\mathsf{E} : y^2 = x^3 + Ax^2 + Bx$ be an elliptic curve defined over $\mathbb{F}_q$. Note that E_λ is of the form E where $A = -(1+\lambda)$ and $B = \lambda$. In [6], Fadavi et al. proposed a mapping, from hereon we call it F-F, that maps an element of $\mathbb{F}_q$ to a point of E. First, we state Lemma 3 of [6] as Lemma H.1 given below.

Lemma H.1. [6] *Let $\mathbb{F}_q$ be a finite field of odd characteristic, $A, B, C \in \mathbb{F}_q^*$, $(A^2 - 4B) \neq 0$ and $\chi(C) = -1$. Let $f(x) = x^3 + Ax^2 + Bx$ and $\mathsf{E} : y^2 = f(x)$ be an elliptic curve. For any $t \in \mathbb{F}_q^*$, either $X_1 = -\frac{B}{A}\left(1 + \frac{1}{Ct^2}\right)$ or $X_2 = -\frac{B}{A}(1 + Ct^2)$ is the abscissa of $\mathbb{F}_q$-rational point on the elliptic curve E. Also, if $f(X_1(t)) \neq 0$ exactly one of the values $X_1(t)$ or $X_2(t)$ is the abscissa of a point on $\mathsf{E}(\mathbb{F}_q)$.*

Theorem H.2. [6] *Let $\mathbb{F}_q$ be a finite field of odd characteristic, $A, B, C \in \mathbb{F}_q^*$, $(A^2 - 4B) \neq 0$ and $\chi(C) = -1$. Let $R = \left\{0, 1, 2, \cdots, \frac{q-1}{2}\right\}$, $f(x) = x^3 + Ax^2 + Bx$ and $\mathsf{E} : y^2 = f(x)$ be an elliptic curve. Then,*

1. *The function $\Phi : \mathbb{F}_q \to \mathsf{E}(\mathbb{F}_q)$ where*

$$\Phi(t) = \begin{cases} \mathcal{O}, & \text{if } t = 0, \\ (X_1(t), \sqrt{f(X_1(t))}) & \text{if } \chi(f(X_1(t))) \neq -1, \\ (X_2(t), -\sqrt{f(X_2(t))}) & \text{if } \chi(f(X_1(t))) = -1, \end{cases}$$

   and $X_1(t), X_2(t)$ are given in Lemma H.1, is a 2:1 encoding function on $\mathbb{F}_q^*$.
2. *There is an injective encoding function $\Phi : R \to \mathsf{E}(\mathbb{F}_q)$, that Φ^{-1} is efficiently computable.*

The encoding algorithm defined by Φ given in [6] is not constant-time. Theorem H.3 provides the constant-time version of the F-F map. We also include the algorithmic version of the map in Table 14.

Theorem H.3. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, $A, B, C \in \mathbb{F}_q^*$, $(A^2 - 4B) \neq 0$ and $\chi(C) = -1$. For any non-zero $t \in \mathbb{F}_q$, the following quantities are defined:*

$$\begin{aligned} v &= -\frac{B}{A}(1 + Ct^2), \\ \epsilon &= \chi(v^3 + Av^2 + Bv), \\ x &= \epsilon v + (1 - \epsilon)\frac{v(1 + Ct^2)}{2Ct^2}, \\ y &= -\epsilon\sqrt{x^3 + Ax^2 + Bx}. \end{aligned}$$

Furthermore, $y^2 = x^3 + Ax^2 + Bx$.

Proof. The proof of the theorem is straightforward. □

H.1. **Inversion of Φ map.** In this section, we provide the inversion of the Φ map.

Theorem H.4. *Let* $\mathbb{F}_q$ *be a finite field and* $\Phi : \mathbb{F}_q \to \mathsf{E}$ *be the encoding map defined in Theorem H.2. Then the following statements hold:*

1. *For any* (x, y) *in* $\mathsf{E}(\mathbb{F}_q), (x, y)$ *is in* $\Phi(\mathbb{F}_q)$ *if and only if* $-\left(\frac{A}{B}x + 1\right)$ *is non-square in* $\mathbb{F}_q$.
2. *If* $(x, y) \in \Phi(\mathbb{F}_q)$, *then* $\bar{t}$ *is defined and* $\Phi(\bar{t}) = (x, y)$:

$$\bar{t} = \begin{cases} \sqrt{-1/C\left(\frac{A}{B}x + 1\right)}, & \text{if } y \in \sqrt{\mathbb{F}_q^2}, \\ \sqrt{-\frac{1}{C}\left(\frac{A}{B}x + 1\right)}, & \text{if } y \notin \sqrt{\mathbb{F}_q^2}. \end{cases}$$

Proof. The proof of the theorem is similar to Theorem 3.7. □

TABLE 14. F-F Map.

Parameter: $C \in \mathbb{F}_q^*$ and C is a non-square. fix $D = -\frac{B}{A}$	
Encoding Input: $t \in \mathbb{F}_q \setminus \{0\}$ Output: $(x, y) \in \mathsf{E}$	**Decoding** Input: $(x, y) \in \Phi(\mathbb{F}_q) \subset \mathsf{E}$ Output: $t \in \mathbb{F}_q$
1. $u = C \cdot t^2$ 2. $x_1 = D \cdot (1 + u)$ 3. $x_2 = x_1^2$ 4. $v = x_1 \cdot x_2 + A \cdot x_2 + B \cdot x_1$ 5. $\epsilon = \chi(v)$ 6. $u_1 = u + u$ 7. $u_2 = \frac{1}{u_1}$ 8. $u_3 = x_1 \cdot (1 + u) \cdot u_2$ 9. $x = \epsilon \cdot (x_1 - u_3) + u_3$ 10. $v_0 = x^2$ 11. $v_1 = x \cdot v_0 + A \cdot v_0 + B \cdot x$ 12. $y = -\epsilon \cdot \mathsf{Sqrt}(v_1)$ 12. Return (x, y)	1. $x_0 = -\frac{1}{D} \cdot x + 1$ 2. if $y \in \left\{0, 1, 2, \cdots, \frac{q-1}{2}\right\}$ then 3. $\quad \bar{t} = \mathsf{Sqrt}\left(-\frac{1}{c \cdot x_0}\right)$ 4. Else 5. $\quad \bar{t} = \mathsf{Sqrt}\left(-\frac{1}{c} \cdot x_0\right)$ 6. Return $\bar{t}$

H.2. **F-F-K: Encoding to Kummer line using F-F map, and its Pseudocode.**

Theorem H.5. *Let* $\mathbb{F}_q$ *be a finite field of odd characteristic,* $\lambda, C \in \mathbb{F}_q^*$ *with* $\lambda \notin \{\pm 1\}$ *and* $\chi(C) = -1$. *Let* $\mathcal{K}_{a^2,b^2}$ *be a Kummer Line of corresponding Legendre form* E_λ *where* $\lambda = \frac{a^4}{a^4 - b^4}$ *over a finite field* $\mathbb{F}_q$. *For any non-zero* $t \in \mathbb{F}_q$, *define a*

map $\hat{\Phi} : \mathbb{F}_q \to \mathcal{K}_{a^2,b^2}$ *by*

$$\begin{aligned} v &= \frac{\lambda}{\lambda+1}(1+Ct^2), \\ \epsilon &= \chi(v(v-1)(v-\lambda)), \\ x &= \epsilon v + (1-\epsilon)\frac{v(1+Ct^2)}{2Ct^2}, \\ \mathsf{X} &= b^2 x, \mathsf{Z} = a^2(x-1). \end{aligned}$$

Furthermore, if $\hat{\Phi}(0) = (a^2 : b^2)$*. If* $q \equiv 3 \pmod 4$*, then* $-\frac{1}{C}$ *is a square and* $\hat{\Phi}(\pm\sqrt{-\frac{1}{C}}) = (b^2 : a^2)$.

TABLE 15. F-F-K Map.

Parameter: $C \in \mathbb{F}_q$ is a non-square, $A = \frac{\lambda}{\lambda+1}$		
Encoding		**Decoding**
Fix $q \equiv 1 \pmod 4$	Fix $q \equiv 3 \pmod 4$	
Input: $t \in \mathbb{F}_q \setminus \{0\}$	Input: $t \in \mathbb{F}_q \setminus \left\{0 \cup \pm\sqrt{-\frac{1}{C}}\right\}$	Input: $(\mathsf{X} : \mathsf{Z}) \in \hat{\Phi}(\mathbb{F}_q) \subset \mathcal{K}_{a^2,b^2}$
Output: $(\mathsf{X} : \mathsf{Z}) \in \mathcal{K}_{a^2,b^2}$	Output: $(\mathsf{X} : \mathsf{Z}) \in \mathcal{K}_{a^2,b^2}$	Output: $\bar{t} \in \mathbb{F}_q$
1. $u = C \cdot t^2$		1. If $(\mathsf{X} : \mathsf{Z}) = (a^2 : b^2)$
2. $x_1 = A \cdot (1+u)$		2. Return $\bar{t} = 0$
3. $v = x_1 \cdot (x_1 - 1) \cdot (x_1 - \lambda)$		3. Else if $(\mathsf{X} : \mathsf{Z}) = (b^2 : a^2)$
4. $\epsilon = \chi(v)$		4. Return $\bar{t} = \sqrt{-\frac{1}{C}}$
5. $u_2 = u + u$		5. Else
6. $x_{11} = u_2 \cdot x_1$		6. $x_0 = a^2 \cdot \mathsf{X}$
7. $x_{12} = (u+1) \cdot x_1$		7. $x_1 = x_0 - b^2 \cdot \mathsf{Z}$
8. $\mathbf{x} = \epsilon \cdot (x_{11} - x_{12}) + x_{12}$		8. $x_2 = \frac{1}{x_1}$
9. $\mathbf{z} = u_2$		9. $x = x_0 \cdot x_2$
10. $\mathsf{X} = b^2 \cdot \mathbf{x}$		10. $x_3 = -\frac{1}{A} \cdot x + 1$
11. $\mathsf{Z} = a^2 \cdot (\mathbf{x} - \mathbf{z})$		11. $\bar{t} = \mathsf{Sqrt}\left(-\frac{1}{c} \cdot x_3\right)$
12. Return $(\mathsf{X} : \mathsf{Z})$		12. Return $\bar{t}$