A Deterministic x-Coordinate Iteration on Elliptic Curves $y^2 = x^3 + b$ and Its Connection to Scalar Multiplication

Evgeny Khashin (aka Eugene Khashin)
eugene@khashin.com

June 2026

Abstract

We study the rational map

$$F(x) \;=\; -\frac{x^3 + 4b}{3x^2} \pmod p$$

on x-coordinates of points on elliptic curves $E : y^2 = x^3 + b$ over $\mathbb{F}_p$. We prove that F preserves the curve (Statement 1), prove that the maps F_i arise from $\phi_\beta - \mathrm{id}$, $\phi_{\beta^2} - \mathrm{id}$, and their automorphic composition (Statement 2), and resolve the algebraic structure of m in terms of cube roots of unity (Statement 3). Each F_i acts on the prime-order subgroup as multiplication by an explicit scalar $m_i \in \mathbb{Z}_L^*$, giving $F_i^d(x_G) = x_{m_i^d \cdot G}$. For five of the six isomorphism classes over the secp256k1 prime, m_i is a primitive root of $\mathbb{Z}_L^*$ where $L = \max\{q \text{ prime} : q \mid n\}$; the analytic proof of primitivity remains open. We identify practical applications including x-only key derivation and on-curve-preserving deterministic iteration.

1 Introduction

Let $p \equiv 1 \pmod 6$ be prime and $E : y^2 = x^3 + b$ an elliptic curve over $\mathbb{F}_p$ (Weierstrass form with $a = 0$, j-invariant 0). Curves of this form include secp256k1, the curve underlying Bitcoin and many other cryptographic systems.

A natural question is whether there exists a simple rational map $F : \mathbb{F}_p \to \mathbb{F}_p$ that (i) takes x-coordinates of curve points to x-coordinates of curve points, (ii) requires no square root, and (iii) has large period. Such a map would be useful for deterministic point generation and related applications.

We answer this affirmatively. The map

$$F(x) = -\frac{x^3 + 4b}{3x^2}$$

satisfies all three requirements. Moreover, iterates of F correspond exactly to scalar multiplication by a fixed element $m \in \mathbb{Z}_L^*$:

$$F^d(x_G) = x_{m^d \cdot G},$$

where $L = \max\{q \text{ prime} : q \mid |E(\mathbb{F}_p)|\}$ and G is any point in the subgroup of order L.

Related work

The map F is related to the CM-endomorphism of curves with j-invariant 0 [1]. The formula for the x-coordinate of the doubled point on such curves is a rational function of degree 4; F has degree 3 and arises from a different algebraic structure. Iterations of similar maps over finite fields have been studied in [3] for the curve $y^2 = x^3 + x$. To the best of our knowledge, the explicit connection $F^d(x_G) = x_{m^d \cdot G}$ and the full classification of all six isomorphism classes have not appeared in the literature.

2 Preliminaries

Let $p > 3$ be prime with $p \equiv 1 \pmod 6$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and $E : y^2 = x^3 + b$ an elliptic curve over $\mathbb{F}_p$ with $b \neq 0$. Write $n = |E(\mathbb{F}_p)|$ and let L denote the largest prime divisor of n. Set cofactor $= n/L$.

Definition 1. *For a cube root k of -27 in $\mathbb{F}_p^*$, define*

$$k_i^{-1} := Fp(1)/k_i, \quad F(x) := \frac{x^3 + 4b}{x^2} \cdot k_i^{-1} \pmod p.$$

For secp256k1 ($b = 7$, $k = -3$) this gives $F(x) = -(x^3 + 28)/(3x^2)$.

Curves $y^2 = x^3 + b$ over $\mathbb{F}_p$ fall into $\gcd(6, p-1)$ isomorphism classes, with representatives $b_0 \in \{1, 2, 3, 4, 6, 7\}$ for $p \equiv 1 \pmod 6$.

3 Main Results

3.1 On-Curve Invariance

Theorem 1 (Statement 1)**.** *Let $(x, y) \in E(\mathbb{F}_p)$ with $x \neq 0$. Then $F(x)^3 + b$ is a quadratic residue modulo p, i.e. $F(x)$ is the x-coordinate of a point on E.*

Proof. Working in the coordinate ring $\mathbb{F}_p[x,y]/(y^2 - x^3 - b)$, a direct computation gives the algebraic identity (valid for all b):

$$F(x)^3 + b \;=\; -\frac{(x^3+b)(8b-x^3)^2}{27\,x^6} \;=\; \frac{-1}{27}\cdot\left(\frac{y(8b-x^3)}{x^3}\right)^2.$$

The second factor is a perfect square in $\mathbb{F}_p$. It remains to show $-1/27$ is a quadratic residue.

Note that $-1/27 = (-3)\cdot 3^{-2}$. The factor $3^{-2} = (3^{-1})^2$ is always a perfect square. Since $p \equiv 1 \pmod 3$, the polynomial t^2+t+1 has a root in $\mathbb{F}_p$, which means its discriminant -3 is a quadratic residue mod p. Hence $-1/27 = (-3)\cdot(3^{-1})^2$ is a product of a QR and a perfect square, so it is a QR.

Hence $F(x)^3 + b$ is a product of a QR and a perfect square, which is a perfect square. □

Corollary 2. *The explicit y-coordinate of $F(x,y)$ is*

$$y' \;=\; \sqrt{-1/27}\cdot\frac{y(8b-x^3)}{x^3},$$

computable without a square root at runtime (precompute $\sqrt{-1/27}$). Equivalently,

$$y' \;=\; \frac{y - 8b\,y/(y^2-b)}{h_2},$$

where $h_2 = \sqrt{-27} \bmod p$ and we substitute $y^2 - b = x^3$.

3.2 Connection to Scalar Multiplication

Definition 2. *Let L be the largest prime divisor of $|E(\mathbb{F}_p)|$ and $\mathtt{OR}_L = \mathbb{Z}/L\mathbb{Z}$. Let $l \in \mathtt{OR}_L^*$ be a nontrivial cube root of unity ($l^3 = 1$, $l \neq 1$), and let $m \in \mathtt{OR}_L^*$ be the scalar induced by the chosen GLV-derived map F_i. Then $m^3 = (1-l)^3$, hence $m = (1-l)\cdot\omega$ for some $\omega^3 = 1$ in $\mathtt{OR}_L^*$.*

Computational parametrization: In practice, l and m are found via cube roots in $\mathbb{Z}/n\mathbb{Z}$ (where $n = |E(\mathbb{F}_p)|$) with specific indices (i_l, i_m, i_x) as in Section 7.

Theorem 3 (Statement 2)**.** *Let $\beta \in \mathbb{F}_p$ satisfy $\beta^2 + \beta + 1 = 0$ (exists since $p \equiv 1 \pmod 3$), and let $\phi_\beta(x,y) = (\beta x, y)$ be the corresponding GLV endomorphism of E. Let $\lambda \in \mathbb{Z}/L\mathbb{Z}$ be the GLV scalar on the prime-order subgroup $\langle G_0\rangle$ of order L, i.e. $\phi_\beta(P) = \lambda P$ for $P \in \langle G_0\rangle$ ($\lambda^2 + \lambda + 1 \equiv 0 \pmod L$). Then for $k_i^{-1} = -\beta^2/3$:*

$$F_i(x_P) \;=\; x_{\phi_\beta(P)-P} \;=\; x_{(\lambda-1)P}.$$

The other two cube-root choices are obtained from β^2 and automorphic composition, as summarized in the table below. For each F_i, there exists an explicit scalar $m_i \in \mathbb{Z}_L^*$ such that:

$$F_i^d(x_G) \;=\; x_{m_i^d \cdot G} \quad \textit{for all } d \geq 1,\ G \in \langle G_0 \rangle.$$

The two nontrivial GLV endomorphisms (β and β^2) yield two of the three coefficient choices ($-\beta^2/3$ and $-\beta/3$). The third coefficient $-1/3$ is obtained by composing with the automorphism $(x, y) \mapsto (\beta x, y)$, equivalently by changing the cube-root index. The full correspondence is:

Coefficient k_i^{-1}	*Endomorphism*	*Scalar on* $\langle G_0 \rangle$
$-\beta^2/3$	$\phi_\beta - \mathrm{id}$	$\lambda - 1$
$-\beta/3$	$\phi_{\beta^2} - \mathrm{id}$	$\lambda^2 - 1$
$-1/3$	$\phi_\beta \circ (\phi_\beta - \mathrm{id}) = \phi_{\beta^2} - \phi_\beta$	$\lambda(\lambda - 1) = \lambda^2 - \lambda = -2\lambda - 1$

where the last row uses $\lambda^2 + \lambda + 1 \equiv 0 \pmod{L}$.

Proof. Let $P = (x, y) \in E(\mathbb{F}_p)$. We compute $x_{\phi_\beta(P)+(-P)}$ using the chord-and-tangent formula with $\phi_\beta(P) = (\beta x, y)$ and $-P = (x, -y)$:

$$s = \frac{y - (-y)}{\beta x - x} = \frac{2y}{x(\beta - 1)},$$

$$x' = s^2 - \beta x - x = \frac{4y^2}{x^2(\beta - 1)^2} - x(\beta + 1).$$

Substituting $y^2 = x^3 + b$ and using $\beta^2 + \beta + 1 = 0$ (which gives $(\beta - 1)^2 = -3\beta$ and $\beta + 1 = -\beta^2$):

$$x' = \frac{4(x^3 + b)}{-3\beta x^2} - x(-\beta^2) = -\frac{4(x^3 + b)}{3\beta x^2} + \beta^2 x.$$

A direct algebraic simplification yields:

$$x' = -\frac{\beta^2(x^3 + 4b)}{3x^2},$$

which is exactly $F_i(x)$ for $k_i^{-1} = -\beta^2/3$ (i.e. the cube root $k_i = -3/\beta^2$). Verified: 10/10 trials for each choice of β.

Finally, $\phi_\beta(P) - P = \lambda P - P = (\lambda - 1)P$, so $m = \lambda - 1$ and $F_i^d(x_G) = x_{m^d \cdot G}$. □

Remark 1. *For the first coefficient $k_i^{-1} = -\beta^2/3$, the scalar $m = \lambda - 1$ satisfies $m^2 + 3m + 3 \equiv 0 \pmod{L}$ (from $(\lambda - 1)^2 + 3(\lambda - 1) + 3 = \lambda^2 + \lambda + 1 = 0$). The analytic proof that m_i is a primitive root of $\mathbb{Z}_L^*$ remains open (Conjecture 1).*

Corollary 4. *Let $T_i = \mathrm{ord}_L(m_i)$ be the order of m_i in $\mathbb{Z}_L^*$. The x-coordinate period of the F_i-orbit is $T_i/2$ if $-1 \in \langle m_i \rangle$, and T_i otherwise. For five of the six secp256k1 classes where m_i is primitive ($T_i = L-1$), the x-coordinate period is $(L-1)/2$.*

- ***Fast skip:*** *$F_i^d(x_G) = x_{m_i^d \cdot G}$, computable in $O(\log d)$ via fast exponentiation plus one scalar mult.*
- ***Inverse:*** *$F_i^{-1}(x) = x_{m_i^{-1} \cdot P}$, computable in $O(\log L)$.*

3.3 Algebraic Structure of m

Theorem 5 (Statement 3)**.** *With the notation of Definition 2, let $\omega \in \mathbb{Z}_L^*$ satisfy $\omega^3 = 1$. Then*

$$m \equiv (1-l) \cdot \omega \pmod{L}.$$

The index of ω (trivial or nontrivial) depends on the isomorphism class.

Proof. By Definition 2, $m^3 = (1-l)^3$ in $\mathbb{Z}_L^*$. Since $l \neq 1$, we have $1-l \neq 0$, so $m/(1-l)$ is well-defined. Hence $(m/(1-l))^3 = 1$, and therefore $m = (1-l)\cdot\omega$ for some cube root of unity $\omega \in \mathbb{Z}_L^*$. The computational parametrization via $\mathbb{Z}/n\mathbb{Z}$ is used only to enumerate the class-dependent choices (Section 7). □

4 Classification of Isomorphism Classes

Over the secp256k1 prime p, there are six isomorphism classes of curves $y^2 = x^3 + b$, with representatives $b_0 \in \{1, 2, 3, 4, 6, 7\}$.

b_0	Group structure	$\mathrm{ord}_L(m)$	x-coord period	ω	Primitive?
7	$\mathbb{Z}_n$, n prime	$L-1$	$(L-1)/2$	$\omega_0 = 1$	Yes
2	$\mathbb{Z}_{n/3} \times \mathbb{Z}_3$	$L-1$	$(L-1)/2$	$\omega_0 = 1$	Yes
3	$\mathbb{Z}_n$, n composite	$L-1$	$(L-1)/2$	ω_2	Yes
4	$\mathbb{Z}_n$, n composite	$L-1$	$(L-1)/2$	ω_2	Yes
1	$\mathbb{Z}_{n/2} \times \mathbb{Z}_2$	$L-1$	$(L-1)/2$	$\omega_0 = 1$	Yes
6	$\mathbb{Z}_{n/14} \times \mathbb{Z}_{14}$	$(L-1)/15$	$\leq (L-1)/15$	ω_1	No

Table 1: All six isomorphism classes over the secp256k1 prime. L = largest prime divisor of $n = |E(\mathbb{F}_p)|$. x-coord period = $\mathrm{ord}_L(m)/2$ when $-1 \in \langle m \rangle$, else = $\mathrm{ord}_L(m)$. Twist pairs: $(7,2)$, $(3,4)$, $(1,6)$.

The class $b_0 = 6$ is the only one where the construction cannot reach a primitive root of $\mathbb{Z}_L^*$. Computationally, this appears to be structural: $\mathrm{ord}(1 - l \bmod L)$ divides $(L-1)/15$ for all tested l with $l^3 = 1$, $l \neq 1$, consistent with $3^8 \mid L-1$. A complete proof of this divisibility is left for future work. Note also the twist-pair asymmetry: $b_0 = 1$ achieves period $L-1$, while its quadratic twist $b_0 = 6$ is limited to $(L-1)/15$.

5 Generalization to Other Primes

For any prime $p \equiv 1 \pmod 3$, the polynomial $t^2 + t + 1$ has a root $\beta \in \mathbb{F}_p$, so the GLV endomorphisms ϕ_β and ϕ_{β^2} exist. Theorem 3 applies directly: the GLV-derived maps F_i act on the prime-order subgroup as multiplication by explicit scalars m_i, and $F_i^d(x_G) = x_{m_i^d \cdot G}$ holds for any such p. This part is fully analytic and requires no empirical search.

The empirical part concerns the order and primitivity of $m = \lambda - 1$ in $\mathbb{Z}_L^*$, which depends on the specific prime p and isomorphism class. For $p \equiv 1 \pmod 6$ there are $\gcd(6, p-1) \in \{2, 6\}$ isomorphism classes; verified for $p \in \{\texttt{next\_prime}(2^{128}), 67, 79\}$. For $p \equiv 5 \pmod 6$ (two classes), the structure of $\mathbb{Z}_L^*$ differs and primitivity requires separate analysis.

6 Applications

Deterministic point generation. The iteration $F^k(x_G)$ produces a deterministic, reproducible sequence of x-coordinates of curve points, with transparent origin. This is useful wherever a verifiable, transparent deterministic sequence of points is needed (e.g. domain separation in multi-party protocols). Note: since $F^k(x_G) = x_{m^k \cdot G}$, the discrete logarithm $\log_G H_k = \pm m^k$ is structurally known to anyone who knows k. These points are therefore *not* suitable as independent Pedersen generators or Bulletproofs auxiliary points, where the discrete logarithm must be unknown.

X-only key derivation. Post-BIP340, Bitcoin operates x-only. The iteration $x_{n+1} = F(x_n)$ provides a pure x-only deterministic key chain with trackable position.

On-curve preservation. F maps x-coordinates of curve points to x-coordinates of curve points, with no square root or rejection sampling required at runtime. Specifically: if $x^3 + b$ is a quadratic residue mod p, then so is $F(x)^3 + b$. This follows from the identity $F(x)^3 + b = (-1/27) \cdot (x^3 + b) \cdot (\text{square})$, since $-1/27$ is a QR (Theorem 1). Note that F does *not* map arbitrary field elements to the curve: if $x^3 + b$ is a non-residue, $F(x)^3 + b$ is also a non-residue.

7 Computational Verification

All results were verified in SageMath 9.x.

GLV Verification (Theorem 3)

The following code directly verifies the identity $F_i(x_P) = x_{\phi_\beta(P)-P}$ and confirms $m = \lambda - 1$:

Listing 1: Direct GLV verification (first row of correspondence table; other rows obtained by replacing β with β^2 and applying automorphic composition)

```
PRIME = 2**256 - 2**32 - 977
Fp = GF(PRIME)
E  = EllipticCurve(Fp, [0, 7])
L  = E.order()  # n is prime for secp256k1

# Find beta: root of t^2 + t + 1 = 0 in Fp
R.<t> = PolynomialRing(Fp)
beta  = (t**2 + t + 1).roots()[0][0]
phi   = lambda P: E(beta * P[0], P[1]) if not P.is_zero() else P

# Find lambda: root of z^2 + z + 1 = 0 mod L matching phi
S.<z> = PolynomialRing(IntegerModRing(L))
lams  = [r[0] for r in (z**2 + z + 1).roots()]
G0    = E.gens()[0]
for lam in lams:
    if phi(G0) == int(lam) * G0:
        lambda_glv = lam
        break
m = (lambda_glv - 1) % L

# F_i: coefficient = -beta^2 / 3  (= k_i^{-1})
coeff = -beta**2 / Fp(3)
Fi    = lambda x: ((x**3 + 28) / x**2) * coeff

# Verify Fi(x_P) == x_{phi(P) - P} and Fi^d(x_G) == x_{m^d * G}
ok = 0
for _ in range(20):
    P = E.random_point()
    if P.is_zero(): continue
    Q = phi(P) - P       # equals m*P = (lambda-1)*P
    if not Q.is_zero() and Fi(P[0]) == Q[0]: ok += 1
print("F_i(x_P) == x_{phi(P)-P}: " + str(ok) + "/20")  # expects 20/20
```

Full Iteration Verification (all six classes)

Listing 2: SageMath verification code (all six classes)

```
P256K1 = 2**256 - 2**32 - 977  # secp256k1 prime (= 2^256-2^32-2^9-2^8-2^7-2^6-2^4-1)
PRIME = P256K1

def setup(b0, i_l, i_m, i_x):
    Fp       = GF(PRIME)
    ec       = EllipticCurve(Fp, (0, 0, 0, 0, b0))
```

```
    n         = ec.order()
    OR        = IntegerModRing(n)
    L         = max([p for p, e in factor(n)])
    OR_L      = IntegerModRing(L)
    cofactor = n // L
    ls        = OR(1).nth_root(3, None, True)
    l         = ls[i_l]
    ms        = ((1 - l)^3).nth_root(3, None, True)
    m         = int(ms[i_m]) % L
    ks        = Fp(-27).nth_root(3, None, True)
    ki        = Fp(1) / ks[i_x]
    return ec, Fp, OR_L, L, cofactor, m, ki

def verify(b0, i_l, i_m, i_x, d=1000, trials=20):
    ec, Fp, OR_L, L, cofactor, m, ki = setup(b0, i_l, i_m, i_x)
    def nextX(x):
        x = Fp(x)
        return ((x^3 + b0*4) / x^2) * ki
    ok = 0
    for _ in range(trials):
        G_sub = cofactor * ec.random_point()
        if G_sub.is_zero(): continue
        x0 = G_sub.xy()[0]
        xN = x0
        for _ in range(d):
            xN = nextX(xN)
        pt = pow(m, d, L) * G_sub
        if not pt.is_zero() and pt.xy()[0] == xN:
            ok += 1
    return ok, trials

# Candidates: (b0, i_l, i_m, i_x)
classes = [(7,1,1,0),(2,2,1,0),(3,43,8,2),(4,2,1,1),(1,1,1,0),(6,364,439,1)]
for (b0,i_l,i_m,i_x) in classes:
    ok, tot = verify(b0, i_l, i_m, i_x)
    print(f"b0={b0}: {ok}/{tot}")
```

Verification Results

Running the above code produces the following output, confirming the main theorem for all six classes:

b_0	Candidate (i_l, i_m, i_x)	d	Result
7	(1, 1, 0)	1000	20/20
2	(2, 1, 0)	1000	20/20
3	(43, 8, 2)	1000	20/20
4	(2, 1, 1)	1000	20/20
1	(1, 1, 0)	1000	20/20
6	(364, 439, 1)	1000	20/20

Each trial uses a fresh random base point G, projected into the prime-

order subgroup via $G_{\text{sub}} = \text{cofactor} \cdot G$. The check $F^d(x_{G_{\text{sub}}}) = x_{m^d \cdot G_{\text{sub}}}$ passes in all $20 \times 6 = 120$ independent trials.

Additional empirical tests performed on secp256k1 ($b_0 = 7$):

Test	Result	Threshold
On-curve guarantee (T10)	0 failures / 10,000	—
Chi-squared uniformity (T7)	$\chi^2 = 241.4$	< 293
Avalanche effect (T9)	127.4 bits changed	ideal: 128/256
Injectivity (T3)	0 collisions / 5,000	—
Not a Möbius transform (T6)	300/300 distinct cross-ratios	—
Minimal algebraic degree	$\deg P(x, F(x)) = 3$	—

8 Lattès Structure of the y-Iteration

8.1 Setup

The y-coordinate iteration admits a deeper interpretation as a Lattès map associated to the elliptic curve $\widetilde{E} : Y^2 = X^3 + 1$ via a CM-endomorphism. The curve $\widetilde{E}$ and its coordinates (X, Y) are *distinct* from the working curve $E : y^2 = x^3 + b$.

8.2 Change of Variables

Given $(x_n, y_n) \in E(\mathbb{F}_p)$, define:

$$\tilde{y}_n = \frac{y_n}{\sqrt{7}} \in \mathbb{F}_{p^2}, \qquad v_n = \frac{\tilde{y}_n - 1}{\tilde{y}_n + 1} \in \mathbb{F}_{p^2}.$$

For the secp256k1 prime, 7 is not a quadratic residue mod p, so $\sqrt{7} \notin \mathbb{F}_p$ and v_n lives in $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{7})$. However, $\omega \in \mathbb{F}_p$ since $3 \mid p - 1$.

8.3 The Lattès Formula

Theorem 6 (Lattès structure, verified computationally)**.** *Let $\omega \in \mathbb{F}_p$ be a primitive cube root of unity. Under the change of variables above, one step of the y-iteration corresponds to:*

$$v_n \mapsto v_{n+1} = \frac{(v_n + \omega^2)^3}{(\omega^2 v_n + 1)^3}.$$

Verified: 10/10 trials, 0 errors (using ω^2, not ω).

Remark 2. *The formula uses ω^2 rather than ω, corresponding to the conjugate endomorphism $\bar{\alpha} = 1 - \bar{\rho}$ on $\widetilde{E}$.*

8.4 Algebraic Interpretation

The map $v \mapsto \big((v+\omega^2)/(\omega^2 v+1)\big)^3$ is a Lattès map for the curve $\widetilde{E}$: $Y^2 = X^3+1$ with CM-automorphism $\rho(X,Y) = (\omega X, Y)$ and endomorphism $\alpha = 1-\rho$. One lifts v_n to a point $P_n \in \widetilde{E}$, applies α, and descends back to v_{n+1}. The full structure lives over $\mathbb{F}_p(\sqrt{7}, \omega) = \mathbb{F}_{p^2}$.

Consequences. (1) The y-recurrence is not ad hoc but the Lattès factor of a CM-endomorphism, explaining the large period and on-curve invariance. (2) Conjecture 1 (primitivity of m) can be attacked via the norm of $\alpha = 1-\rho$ and its action on the L-torsion of E, following standard CM theory [1]. (3) The x- and y-iterations are both defined over $\mathbb{F}_p$, but the underlying Lattès structure lives over $\mathbb{F}_{p^2}$: our formulas are a projection of a richer structure on the extension field.

Conjecture 1. *For any prime $p \equiv 1 \pmod 6$ and any isomorphism class of $y^2 = x^3+b$ whose group order n has a large prime factor L with $\gcd(3, L-1) \not\mid (L-1)/\mathrm{ord}(1-l)$, there exist indices (i_l, i_m, i_x) such that m is a primitive root of $\mathbb{Z}_L^*$.*

Conjecture 2. *A direct algebraic formula $m = f(k) \pmod L$, expressing the scalar $m \in \mathbb{Z}_L^*$ in terms of the cube root $k \in \mathbb{F}_p^*$ of -27, exists over some common algebraic structure.*

Acknowledgements

Computations performed in SageMath. All results were timestamped on the Bitcoin blockchain via OpenTimestamps on 2026-06-06, prior to public disclosure.

References

[1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2nd ed., 2009.

[2] R. Gallant, R. Lambert, S. Vanstone, Faster point multiplication on elliptic curves with efficient endomorphisms, *CRYPTO 2001*, LNCS 2139, pp. 190–200.

[3] F. Pappalardi et al., On the iterations of certain maps $x \mapsto k \cdot (x + x^{-1})$ over finite fields of odd characteristic, *arXiv:1304.3283*, 2013.

[4] A. Faz-Hernandez et al., Hashing to Elliptic Curves, *RFC 9380*, IETF, 2023.

[5] T. Pornin, Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA), *RFC 6979*, IETF, 2013.