GLV/GLS Scalar Multiplication on Twisted Edwards Curves

Chuangui Ma[1], Ruijie Zhang[2(✉)], Lei Niu[1], and Fushan Wei[2]

[1] Department of Basic, Army Aviation Institution, Beijing, China
[2] Information Engineering University, Zhengzhou, Henan, China

Abstract. At present, GLV/GLS scalar multiplication mainly focuses on finding and constructing more and more efficient computable endomorphisms. We research on the applications of GLV/GLS algorithms on twisted Edwards curves. Firstly, we present the concrete construction of efficiently computable endomorphism for this type of curves over prime field by exploiting birational equivalence between curves, and obtain 2-dimensional GLV method. Using birational equivalence and Frobenius mapping between curves, we present methods to construct efficiently computable endomorphisms of this type of curves and obtain 2-dimensional GLS method. Finally, we obtain the 4-dimensional GLV algorithm by using higher degree twists. The experimental conclusion demanstrates that the speedups of 2-dimensional and 4-dimensional GLV methods than 5-NAF method exceed 37.4% and 104.9% for twisted Edwards curves respectively.

Keywords: Elliptic curve · Twisted edwards curve · Scalar multiplication · GLV method · Computable endomorphism

1 Introduction

In the past three decades, Elliptic curve cryptography (ECC) becomes the mainstream of public key mechanism in cryptology because its high security level with small key size. Due to the advantage of storage space, processing speed and bandwidth, ECC is particularly suitable for use in wireless environments, such as the IoT and edge computing application scenarios. Since the devices in these environments are usually resource-constrained ones with limited battery, it is very important to speed up the computation of ECC in these applications. Among all the computation operations, scalar multiplication is the most computation-expensive operation in ECC. Consequently, it is of utmost importance to accelerate the computation of the scalar multiplication.

How to accelerate the scalar multiplication based on the efficiently computable endomorphism is a hot topic in ECC. Gallant et al. [1] put forward the GLV algorithm on a class of elliptic curves using endomorphism to accelerate the scalar multiplication. Their algorithm is efficient and also general. Since then, more and more researchers pay attention to the GLV method. The authors in [2, 3] have studied the decomposition of the scalar k in 2-dimensional GLV, they gives the bounds for the decomposition coefficients k_1 and k_2. The reason why the GLV algorithm is useful to accelerate the scalar

W. Shi et al. (Eds.): SPNCE 2021, LNICST 423, pp. 319–330, 2022.
https://doi.org/10.1007/978-3-030-96791-8_24

multiplication operation is that the endomorphism on the elliptic curve is effective to speed up the calculation. As a result, find out more and more efficiently computable endomorphisms are critical for the GLV algorithm. Many researchers make progress to find more endomorphism [5–7].

In recent years, a lot of effort are paid to acceralate the scalar multiplication speed of genus-2 hyperelliptic curves. In general, the Jacobian group of genus-2 curve has a wider endomorphism range than other ordinary elliptic curves, therefore the highest possible dimension of GLV decomposition on genus-2 curves is twice as large as that of the elliptic curve under the same condition. In 2013, Bos et al. [8] proposed to accelerate the scalar multiplication using 4-dimensional GLV technique, they considered the BK curves $y^2 = x^5 + b$ [9] and FKT curves $y^2 = x^5 + ax$ [10]. Guillevic and Ionica [11] proposed a 4-dimension GLV algorithm on elliptic curves. Bos et al. [12] considered the genus-2 curves over quadratic extension field F_{p^2} and studied an 8-dimensional scalar decomposition for the first time.

In recent years, different forms of elliptic curves have been proposed and widely concerned, such as twisted Edwards curve, Jacobi Quartic curve and so on. These curves have stronger resistance to side channel attacks and faster point calculation formulas, and have been considered as candidates for the next generation elliptic curve standards. At present, GLV/GLS scalar multiplication mainly focuses on the Weierstrass curves, attempting to find and construct more and higher degree efficient computable endomorphism. However, the GLV method has rarely been studied on other curve forms. In order to sovle the problem, we research on how to use the GLV/GLS algorithms in twisted Edwards curves and evaluate its efficiency. We present the concrete construction of efficiently computable endomorphism for this type of curves by exploiting birational equivalence, Frobenius mapping and twisting isomorphism between curves, and give some instances of efficiently computable endomorphism on curves. We generalize the main results of GLV/GLS method on weierstrass curve to the twisted Edwards curve, and obtain the 2-dimensional and 4-dimensional GLV method accordingly. We use experiments to evaluate the GLV method on twisted Edwards curves. The experimental results show that the speedups of 2-dimensional GLV method and 4-dimensional GLV method than 5-NAF method exceed 37.4% and 104.9% in twisted Edwards curves respectively.

2 Preliminaries

We briefly introduce some basic preliminaries for the rest of the paper, including the properties of isomorphism and GLS method. One can refer to reference [13–15] for more details. There are two special types of curves: $E_B : y^2 = x^3 + B$ and $E_A : y^2 = x^3 + Ax$, whose j invariant are 0 and 1728, respectively.

2.1 The Homomorphism

Definition 2.1. Let E_1 and E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ satisfying $\phi(\mathcal{O}) = \mathcal{O}$. The two elliptic curves E_1 and E_2 are isogenous if there is an isogeny from E_1 to E_2 with $\phi(E_1) \neq \{\mathcal{O}\}$.

Let $\mathrm{Hom}(E_1, E_2)$ be the set of isogenies from E_1 to E_2, then $\mathrm{Hom}(E_1, E_2)$ forms a group. Let $E_1 = E_2 = E$, then $\mathrm{Hom}(E, E)$ is a ring, which is called the endomorphism ring of E, denoted as $End(E)$. Let $\phi, \varphi \in End(E)$ and $P \in E$, then $(\phi + \varphi)(P) = \phi(P) + \varphi(P)$ and $(\phi \circ \varphi)(P) = \phi(\varphi(P))$. The invertible elements of $\mathrm{End}(E)$ form the automorphism group of E, which is denoted by $\mathrm{Aut}(E)$. The endomorphism ring of an elliptic curve E is an important invariant of E.

Theorem 2.2. Let $\phi : E_1 \to E_2$ is an isogeny, whose dual isogeny is denoted by $\widehat{\phi}$, then

(1) Let $m = \deg \phi$, then

$$\widehat{\phi} \circ \phi = [m] \text{ on } E_1,$$

$$\widehat{\phi} \circ \phi = [m] \text{ on } E_2.$$

(2) Let $\psi : E_2 \to E_3$ be an isogeny, then $\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}$.
(3) Let $\varphi : E_1 \to E_2$ be another isogeny, then $\widehat{\phi + \varphi} = \widehat{\phi} + \widehat{\varphi}$.
(4) For all integer $m \in \mathbb{Z}$, then $\widehat{[m]} = [m]$ and $\deg[m] = m^2$.

Let π be the p - Frobenius endomorphism of elliptic curve E and $(x, y) \in E$, then

$$\pi(x, y) = (x^p, y^p).$$

The quantity $t = q + 1 - \#E(F_q)$ is called the trace of Frobenius, and the Frobenius endomorphism π satisfies the characteristic equation $\pi^2 - t\pi + q = 0$ with $|t| \leq 2\sqrt{q}$.

2.2 Twisted Edwards Curves

In 2007, the twiseted Edward cureves is presented in [16]. Because of its substantial advantages [17, 18], EdDSA has been officially released in RFC 8032 [24] and deployed in many password products and libraries, such as OpenSSL [25].

Definition 2.3. Let F_q be a non-binary field, the twisted Edwards curve over F_q is a curve.

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

where $a, d \in F_q$ and $ad(a - d) \neq 0$.

Let (x_1, y_1), (x_2, y_2) be points on the twisted Edwards curve $E_{a,d}$. The sum of these points on $E_{a,d}$ is

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1y_1x_2y_2} + \frac{y_1y_2 - ax_1x_2}{1 - dx_1y_1x_2y_2} \right),$$

The point $(0, 1)$ is the neutral element, and the inverse of (x_1, y_1) is $(-x_1, y_1)$. The addition formula is unified, that is, it can also be applied to double a point.

In the inverted Edwards coordinates [21], we can use coordinates $(X : Y : Z)$ to represent the point $(Z/X, Z/Y)$ on an Edwards curve. Then the general form of the twisted Edwards curve is given below.

$$(X^2 + aY^2)Z^2 = X^2Y^2 + dZ^4.$$

The formulas for curve addition in inverted Edwards coordinates needs only 9M + 1S, where M and S denote the multiplication and squaring on finite field respectively.

Theorem 2.4. Let F_q be a non-binary field, every twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ over F_q is birationally equivalent to a Weierstrass curve $E : v^2 = u^3 + 2(a+d)u^2 + (a-d)^2u$, the rational map is

$$\varphi : E_{a,d} \to E, (x, y) \mapsto (u, v) = \left((a-d)\tfrac{1+y}{1-y}, 2(a-d)x \cdot \tfrac{a-dy^2}{(1-y)^2}\right)$$
$$\psi : E \to E_{a,d}, (u, v) \mapsto (x, y) = \left(\tfrac{2v}{(u-2a)^2-4d}, \tfrac{u^2-4(a^2-d)}{(u-2a)^2-4d}\right)$$

2.3 GLS Method

Theorem 2.5. Let E be an elliptic curve defined over F_q such that $\#E(F_q) = q + 1 - t$. Let $\phi : E \to E'$ be a separable isogeny of degree d defined over F_{q^k} where E' is an elliptic curve defined over F_{q^m} with $m|k$. Let $r|\#E'(F_{q^m})$ be a prime such that $r > d$ and $r||\#E'(F_{q^k})$. Let π be the q-power Frobenius map on E and let $\hat{\phi} : E' \to E$ be the dual isogeny of ϕ. Define $\psi = \phi\pi\hat{\phi}$, then

1. $\psi \in End_{q^k}(E')$.
2. For every point $P \in E'(F_{q^k})$, we have $\psi^k(P) - [d^k]P = \mathcal{O}$ and $\psi^2(P) - [dt]\psi(P) + [d^2q]P = \mathcal{O}$.
3. There exists a integer $\lambda \in \mathbb{Z}/r\mathbb{Z}$ with $\lambda^k - d^k \equiv 0 \mod r$ and $\lambda^2 - dt\lambda - d^2q \equiv 0 \mod r$ such that $\psi(P) = [\lambda]P$ for all $P \in E'(F_{q^m})[r]$.

Corollary 2.6. Let $p > 3$ be a prime and let E be an elliptic curve defined over F_p with $\#E(F_p) = p + 1 - t$. Let E' over F_{p^2} be the quadratic twist of $E(F_{p^2})$. Then $\#E'(F_{p^2}) = (p-1)^2 + t^2$. Let $\phi : E \to E'$ be the twisting isomorphism defined over F_{p^4} and let π be the p-power Frobenius map on E. Let $r|\#E'(F_{p^2})$ be a prime such that $r > 2p$. Define $\psi = \phi\pi\phi^{-1}$, then

1. For every point $P \in E'(F_{p^2})[r]$, we have $\psi^2(P) + P = \mathcal{O}$.
2. $\psi(P) = [\lambda]P$ with $\lambda = t^{-1}(p-1) \mod r$.

Let $p \equiv 1 \mod 6$, and define elliptic curve $E : y^2 = x^3 + B$ over F_p. Choose $u \in F_{p^{12}}^*$ such that $u^6 \in F_{p^2}$ and define elliptic curve $E' : y^2 = x^3 + u^6B$ over F_{p^2}. Repeatedly choose the parameters p, B, u until $\#E'(F_{p^2})$ is prime (or almost prime). The

isomorphism $\phi : E \to E'$ is given by $\phi(x, y) = \left(u^2 x, u^3 y\right)$ and is defined over $F_{p^{12}}$. The homomorphism $\psi = \phi\pi\phi^{-1}$ is defined over F_{p^2}, where π is the p-power Frobenius map on E. It follows that ψ satisfies the characteristic equation $\psi^4 - \psi^2 + 1 = 0$, then one obtains 4-dimensional GLV scalar multiplication.

3 Application of GLV/GLS Method on Twisted Edwards Curves

3.1 GLV Method on Twisted Edwards Curve

In this section, we consider the GLV method on the twisted Edwards curve and present the concrete construction of efficiently computable endomorphism for this type of curves over prime field. Let $p > 3$ be a prime and let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over F_p. According to the literature [18], we know elliptic curve E is birationally equivalent over F_p to a twisted Edwards curve if and only if the group $E(F_p)$ has an element of order 4.

Theorem 3.1. Let $p > 3$ be a prime and let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over F_p. Let $n|\#E(F_p)$ be a prime let ψ be an efficiently-computable endomorphism on E such that there exists $\lambda \in \mathbb{Z}$ satisfying $\psi(P) = \lambda P$ for every point $P \in E(F_p)[n]$. Suppose that E has a point of order 4, then there exists Edwards curve E_e and endomorphism ψ_e such that $\psi_e(P) = \lambda P$ for every point $P \in E_e(F_p)[n]$.

Proof. Let R_1 be a point of order 4 on elliptic curve E and let $2R_1 = (r_2, 0)$. Let $a_2 = 3r_2$ and $a_4 = 3r_2^2 + A$, define the elliptic curve $E_1 : y^2 = x^3 + a_2x^2 + a_4x$, then there is an isomorphism φ_1 from E to E_1 with $\varphi_1(x, y) = (x - r_2, y)$. Suppose point R_1 can be represented as $R_1 = (r_1, s_1)$, then $s_1 \neq 0$ and $r_1 \neq 0$, otherwise R_1 is a point of order 2. Below we show that coefficients a_2 and a_4 be represented by r_1 and s_1.

Due to $2R_1 = (0, 0)$, the tangent line of curve E_1 at point R_1 passes through the point $(0, 0)$, then we have

$$\frac{s_1}{r_1} = \frac{3r_1^2 + 2a_2r_1 + a_4}{2s_1},$$

Hence

$$2s_1^2 = 3r_1^3 + 2a_2r_1^2 + a_4r_1 \tag{1}$$

Since point $R_1 = (r_1, s_1)$ is on the curve E, then

$$s_1^2 = r_1^3 + a_2r_1^2 + a_4r_1 \tag{2}$$

By Eqs. (1) and (2), we have $r_1^3 - a_4r_1 = 0$. Due to $r_1 \neq 0$, then $a_4 = r_1^2$.

On the other hand, substitute $a_4 = r_1^2$ into Eq. (2), we obtain $a_2 = s_1^2/r_1^2 - 2r_1$. Let $d = 1 - \frac{4r_1^3}{s_1^2}$, then $a_2 = 2r_1(1 + d)/(1 - d)$.

Define curve $E_2 : (r_1/(1-d))y^2 = x^3 + a_2x^2 + a_4x$, then there exists an isomorphism φ_2 from E_1 to E_2 with $\varphi_2(x, y) = (x, y/t)$,where $t = \pm\sqrt{\frac{r_1}{1-d}} = \pm\frac{s_1}{2r_1}$. Further, define

curve $E_3 : \frac{1}{1-d}y^2 = x^3 + \frac{2(1+d)}{1-d}x^2 + x$, then there exists an isomorphism φ_3 from E_2 to E_3 with $\varphi_3(x, y) = (x/r_1, y/r_1)$. Define curve $E_e : X^2 + Y^2 = 1 + dX^2Y^2$, then E_3 is birationally equivalent over F_p to E_e according to the literature [17], and the rational map is

$$\varphi_4(x, y) = (2x/y, (x - 1)/(x + 1)).$$

By using the isomorphisms and birational maps above, we obtain a birational map from E to E_e with $\varphi = \varphi_4\varphi_3\varphi_2\varphi_1$ satisfying $\varphi(x, y) = \left(\frac{2t(x-r_2)}{y}, \frac{x-r_2-r_1}{x-r_2+r_1}\right)$.

Hence we obtain an endomorphism $\psi_e = \varphi\psi\varphi^{-1}$ of the curve E_e.

Let $P \in E_e(F_p)[n]$ and suppose the endomorphism ψ satisfies the characteristic equation $X^2 + rX + s$, then there exists $\lambda \in [0, n - 1]$ such that $\psi(P) = \lambda P$, where λ is a root of equation $X^2 + rX + s \bmod n$. Due to $\psi^2 + r\psi + s = 0$, we obtain.

$$\psi_e^2 + r\psi_e + s = \varphi\psi^2\varphi^{-1} + r\varphi\psi\varphi^{-1} + s = \varphi(-r\psi - s)\varphi^{-1} + r\varphi\psi\varphi^{-1} + s = 0.$$

That is to say, ψ_e and ψ have the same characteristic equation.

Hence, for $P \in E_e(F_p)[n]$, we have $\psi_e(P) = \lambda P$.

Theorem 3.1 extends the endomorphism on Weierstrass curve to twisted Edwards curve, so that we can obtain 2-dimensional GLV scalar multiplication algorithm on twisted Edwards curve.

Example 3.2. Let $p \equiv 1 \bmod 4$ be a prime and let $\alpha \in F_p$ be an element of order 4. We consider the elliptic curve $E_1 : y^2 = x^3 + ax$ defined over F_p, then the map $\psi(x, y) \mapsto (-x, \alpha y)$ is an endomorphism defined over F_p satisfying $\psi^2 + 1 = 0$. Suppose $R_1 = (r_1, s_1)$ is a point of order 4 on the curve E_1, then $2R_1 = (0, 0)$. According to the proof of Theorem 3.1, there exists a birational equivalence between E_1 and Edwards curve $E_e : X^2 + Y^2 = 1 + dX^2Y^2$ with $d = 1 - \frac{4r_1^3}{s_1^2}$, and the rational map is

$$\varphi : E_1 \to E_e, (x, y) \mapsto (X, Y) = \left(\frac{2tx}{y}, \frac{x - r_1}{x + r_1}\right),$$

$$\varphi^{-1} : E_e \to E_1, (X, Y) \mapsto (x, y) = \left(-\frac{r_1(Y + 1)}{Y - 1}, -\frac{2tr_1(Y + 1)}{X(Y - 1)}\right),$$

where $t = \frac{s_1}{2r_1}$. Hence we obtain the efficiently-computable endomorphism ψ_e on E_e

$$\psi_e(X, Y) = \left(-\frac{X}{\alpha}, \frac{1}{Y}\right).$$

It is easy to verify $\psi_e^2 + 1 = 0$.

Example 3.3. Let $p \equiv 1 \bmod 3$ be a prime and let $\beta \in F_p$ be an element of order 3. We consider the elliptic curve $E_2 : y^2 = x^3 + b$ defined over F_p, then the map $\psi(x, y) \mapsto (\beta x, y)$ is an endomorphism defined over F_p satisfying $\psi^2 + \psi + 1 = 0$. Suppose $R_1 = (r_1, s_1)$ is a point of order 4 on the curve E_2, then $2R_1 = (0, 0)$. According to the proof of Theorem 3.1, there exists a birational equivalence between E_2 and Edwards curve $E_e : X^2 + Y^2 = 1 + dX^2Y^2$ with $d = 1 - \frac{4r_1^3}{s_1^2}$, and the rational map is.

$$\varphi : E_2 \to E_e, (x, y) \mapsto (X, Y) = \left(\frac{2t(x - r_2)}{y}, \frac{x - m_1}{x + m_2}\right),$$

$$\varphi^{-1} : E_e \to E_2, (X, Y) \mapsto (x, y) = \left(-\frac{m_2 Y + m_1}{Y - 1}, -\frac{2tr_1(Y + 1)}{X(Y - 1)}\right).$$

where $t = \frac{s_1}{2r_1}$, $m_1 = r_1 + r_2$, $m_2 = r_1 - r_2$. Hence we obtain the efficiently-computable endomorphism ψ_e on E_e

$$\psi_e(X, Y) = \left(\frac{(\beta m_2 + r_2)Y + (\beta m_1 - r_2)}{r_1(Y + 1)}X, \frac{(\beta m_2 + m_1)Y + (\beta m_1 - m_1)}{(\beta m_2 - m_2)Y + (\beta m_1 + m_2)}\right).$$

It can be verified that $\psi_e^2 + \psi_e + 1 = 0$.

3.2 GLS Method on Twisted Edwards Curves

Let F_q be a finite field of characteristic $p > 3$ and let $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$ be an twisted Edwards curve defined over F_q with $a, d \in F_q$ and $ad(a - d) \neq 0$. According to the literature [18], $E_{\overline{a},\overline{d}}$ is a quadratic twist of $E_{a,d}$ if and only if $\overline{d}/\overline{a} = d/a$. Let $u = \frac{\overline{a}}{a}$ be quadratic non-residue, then there exists an isomorphism $F_{q^4}\phi : E_{a,d} \to E_{\overline{a},\overline{d}}$ defined over with $\phi(x, y) = (\sqrt{u}x, y)$.

Next, we extend the GLS method [4] to the twisted Edwards curves, and obtain the Theorem 3.4 below.

Theorem 3.4. Let $p > 3$ be a prime and let $E_{a,d}$ be an twisted Edwards curve defined over F_p with $\#E_{a,d}(F_p) = p + 1 - t$. Let $E_{\overline{a},\overline{d}}$ is a quadratic twist of $E_{a,d}(F_{p^2})$, then $\#E_{\overline{a},\overline{d}}(F_{p^2}) = (p - 1)^2 + t^2$. Let $\phi : E_{a,d} \to E_{\overline{a},\overline{d}}$ be an twisting isomorphism defined over F_{p^4} and let π be p-power Frobenius map on $E_{a,d}$. Let $r|\#E_{\overline{a},\overline{d}}(F_{p^2})$ be a prime such that $r > 2p$. Define $\psi = \phi\pi\phi^{-1}$. For $P \in E_{\overline{a},\overline{d}}(F_{p^2})[r]$, we have $\psi^2(P) + P = \mathcal{O}_{E_{\overline{a},\overline{d}}}$.

Proof. We have $\#E_{a,d}(F_{p^2}) = p^2 + 1 - (t^2 - 2p)$. Let u be a non-square in F_{p^2} and define $\overline{a} = au, \overline{d} = du$ and $E_{\overline{a},\overline{d}} : \overline{a}x^2 + y^2 = 1 + \overline{d}x^2y^2$, then $E_{\overline{a},\overline{d}}$ is the quadratic twist of $E_{a,d}(F_{p^2})$ and $\#E_{\overline{a},\overline{d}}(F_{p^2}) = p^2 + 1 + (t^2 - 2p) = (p - 1)^2 + t^2$. The isomorphism $\phi : E_{a,d} \to E_{\overline{a},\overline{d}}$ is given by

$$\phi(x, y) = (\sqrt{u}x, y),$$

and is defined over F_{p^4}.

It is easy to know that $\psi = \phi\pi\phi^{-1}$ is a endomorphism on $E_{\overline{a},\overline{d}}$. If $r|\#E_{\overline{a},\overline{d}}(F_{p^2})$ is a prime such that $r > 2p$, then $r \not| \#E_{a,d}(F_{p^2})$ and $\#E_{a,d}(F_{p^2}) = (p + 1 - t)(p + 1 + t)$. So $r||\#E_{\overline{a},\overline{d}}(F_{p^4}) = \#E_{\overline{a},\overline{d}}(F_{p^2}) \cdot \#E_{a,d}(F_{p^2})$. Hence, for every point $P \in E_{\overline{a},\overline{d}}(F_{p^2})[r]$, there exists $\lambda \in \mathbb{Z}$ such that $\psi(P) = \lambda P$. Below we show that for $P \in E_{\overline{a},\overline{d}}(F_{p^2})[r]$, we have $\psi^2(P) + P = \mathcal{O}_{E_{\overline{a},\overline{d}}}$.

By definition, $\psi(x, y) = \phi\pi\phi^{-1}(x, y) = (\sqrt{u}x^p/\sqrt{u}^p, y^p)$. Since u be a non-square in F_{p^2}, then $\sqrt{u} \notin F_{p^2}$ and $\sqrt{u}^{p^2} = -\sqrt{u}$. If $P = (x, y) \in E_{\overline{a},\overline{d}}(F_{p^2})$, then $x^{p^2} = x$, $y^{p^2} = y$ and so

$$\begin{aligned}\psi^2(x, y) &= (\sqrt{u}x^{p^2}/\sqrt{u}^{p^2}, y^{p^2}) \\ &= (-x, y) \\ &= -(x, y)\end{aligned}$$

The result of Theorem 3.4 can be applied to the twisted Edwards curves defined over $F_p (p > 3)$, and 2-dimensional GLV scalar multiplication algorithm on twisted Edwards curve is obtained.

Example 3.5. Let $p = 2^{127} - 1$ and let $u = 2 + i$ be a non-square in F_{p^2}. Define the twisted Edwards curve $E : -x^2 + y^2 = 1 + 109x^2y^2$ over F_p, then $E' : -ux^2 + y^2 = 1 + 109ux^2y^2$ is the quadratic twist of $E(F_{p^2})$ and, where r is prime of 253 bits

$$\begin{aligned}r = &\ 7237005577332262213973186563042994240709941236554960197665975021634500559269\end{aligned}$$

The endomorphism $\psi(x, y) = (u^{(1-p)/2}x^p, y^p)$ satisfies that $\psi^2 + 1 = 0 \# E'(F_{p^2}) = 4r$.

3.3 4-Dimensional GLV Method on Twisted Edwards Curves

In order to obtain higher-dimensional GLV method on twisted Edwards curves, we usually have two methods. On the one hand, by using the idea of [7], we can combine the GLV method and GLS method and make use of two different endomorphisms at the same time. On the other hand, by using the idea of [4, 6], we can consider the curve with larger automorphism group, such as elliptic curve with j-invariants 0 or 1728.

For the first case, literature [19] has presented a 4-dimensional GLV construction for a class of curve. Consider the elliptic curve E defined over F_p with j-invariant 1728, let $E'(F_{p^2})$ be the quartic twist of $E_{a,d}(F_{p^2})$. Due to $4 \nmid \#E'(F_{p^2})$, therefore $E'(F_{p^2})$ cannot be transformed to the twisted Edwards curve form.

Below, we consider the elliptic curve with j-invariant 0. Let $p \equiv 1 \bmod 6$ be a prime and define elliptic curve $E : y^2 = x^3 + B$ over F_p. Following the Corollary 2.6 in Subsect. 2.3, choose $u \in F_{p^{12}}^*$ such that $u^6 \in F_{p^2}$ and define elliptic curve $E_1 : y^2 = x^3 + u^6B$ over F_{p^2}. Repeatedly Choose the parameters p, B, u until $\#E_1(F_{p^2})$ is almost prime and $4|\#E_1(F_{p^2})$. The isomorphism $\phi_1 : E \to E_1$ is given by $\phi_1(x, y) = (u^2x, u^3y)$ and is defined over $F_{p^{12}}$. Let let π be p-power Frobenius map on E, then the endomorphism $\psi(x, y) = \phi_1\pi\phi_1^{-1}(x, y) = ((u/u^p)^2x^p, (u/u^p)^3y^p)$ is defined over F_{p^2} and satisfies the characteristic equation $\psi^4 - \psi^2 + 1 = 0$. Next, similar to the proof process of Theorem 3.1, we first transform the curve E_1 into the Montgomery curve form, and then transform the endomorphism ψ to the twisted Edwards curve by using birational equivalence.

Let $r_2 \in F_{p^2}$ and suppose $R_2 = (r_2, 0)$ is a point of order 2. Define curve $E_2 : Y^2 = X^3 + 3r_2X^2 + 3r_2^2X$, then $\phi_2(x, y) = (x - r_2, y)$ is an isomorphism from E_1 to E_2. Define curve $E_3 : \frac{1}{\sqrt{3}r_2}y^2 = x^3 + \sqrt{3}x^2 + x$, then $\phi_3(X, Y) = \left(\frac{X}{\sqrt{3}r_2}, \frac{Y}{\sqrt{3}r_2}\right)$ is an isomorphism from E_2 to E_3.

Let $a = (3 + 2\sqrt{3})r_2$, $d = (3 - 2\sqrt{3})r_2$ and define $E_e : aX^2 + Y^2 = 1 + dX^2Y^2$, then there exists a birational equivalence over F_{p^2} between Montgomery curve E_3 and twisted Edwards curve E_e according to [18], where the rational map from E_3 to E_e is

$$\phi_4(x, y) = (x/y, (x - 1)/(x + 1)).$$

Let $\phi = \phi_4\phi_3\phi_2\phi_1$, then it is the birational map from E to E_e and

$$\phi(x, y) = \left(\frac{u^2x - r_2}{u^3y}, \frac{u^2x - b}{u^2x - a}\right),$$

where $a = (1 - \sqrt{3})r_2$, $b = (1 + \sqrt{3})r_2$. Hence we can obtain an endomorphism $\psi_e = \phi\pi\phi^{-1}$ on elliptic curve E_e, which is given by.

$$\psi_e(X, Y) = \left(X^p \cdot \frac{a_1Y^p - a_2}{a_3(Y^p + 1)}, \frac{a_4Y^p - a_5}{a_6Y^p - a_7}\right),$$

where $a_1 = u^{p-1}(a^p - r_2u^{2(p-1)})$, $a_2 = u^{p-1}(b^p - r_2u^{2(p-1)})$, $a_3 = -3\sqrt{3}^p r_2^p$, $a_4 = a^p - bu^{2p}$, $a_5 = b^p - bu^{2p}$, $a_6 = a^p - au^{2p}$, $a_7 = b^p - au^{2p}$ are all constants.

We briefly introduce some basic preliminaries for the rest of the paper, including the properties of isomorphism and GLS method. One can refer to reference [13–15] for more details. There are two special types of curves: $E_B : y^2 = x^3 + B$ and $E_A : y^2 = x^3 + Ax$, whose j invariant are 0 and 1728, respectively.

4 Performance Comparison

We evaluate the computation complexity of the GLV/GLS scalar multiplication algorithms by experiments, and then compare performance with the algorithms on the Weierstrass curve. For the generality of comparison results, we do not give specific curve parameter selection. We suppose that the Weierstrass curve E and twisted Edwards curve E_e are selected, p_1 and p_2 are 256-bit and 128-bit prime respectively, where the parameters of curves and finite field can be flexibly selected as needed. We implement the w-NAF method, 2-dimensinal GLV method and 4-dimensional GLV scalar multiplication algorithm via Magma software on the two types of curves above, and compare the performance.

We use "M", "S" and "I" to represent an operation of multiplication, squaring and inversion on F_{p_1}, respectively. Other simple operations are ignored due to its high efficiency. Correspondingly, m, s and i denote the multiplication, squaring and inversion on $F_{p_2^2}$. According to [7], it is assumed that 1i = 66 m, 1s = 0.76 m, 1I = 290M, 1S = 0.85M and M/m = 0.91. Table 1 presents the computation complexity of two curves.

Table 1. The comparison of computation cost of different operations

Curve	DBL	ADD	mADD
InvEdwards	3M + 4S	9M + 1S	8M + 1S
Jacobian	1M + 8S	11M + 5S	7M + 4S

The computation complexity of doubling (DBL), addition (ADD) and mixed addition (mADD) are summarized in the following.

The scalar multiplication algorithms usually include precomputation, evaluation and coordinate conversion phases. According to the analysis result of [22], we choose the optimal implementations for different scalar multiplication algorithms. For the w-NAF method, we use the 5-NAF representation. For the 2-dimensional GLV method, we use the 4-NAF-based interleaving method (denoted as 2GLV + INT(4-NAF)). For the 4-dimensional GLV method, we use the 3-NAF-based interleaving method (denoted as 4GLV + INT(3-NAF)). Using the precomputation algorithm in [23], we only nedd on inversion precomputation. In the first two stages, the cost is $1\mathrm{I} + (15.8L + \lceil (L-2)/L \rceil + 3.4)\mathrm{M}$ for InvEdwards curve and $1\mathrm{I} + (9L)\mathrm{M} + (3L+5)\mathrm{S}$ for Jacobian curve, where L is 1/2 of precomputed points. Since the computation cost of endomorphism only occurs in precomputation stage and has little effect on the whole cost, we neglect the cost of endomorphism here. The computation cost is 1I + 2M for InvEdwards curve and 1I + 3M + 2S for Jacobian curve. Table 2 presents the costs of different algorithms on two types of curves.

Table 2. The cost of different algorithms on two curves

Curve	Implementation	Operation number	Cost	Speedup
$E_e(F_{p_2^2})$	4GLV+INT(3-NAF)	2i + 836.8m + 320s	1212m	104.9%
$E_e(F_{p_1})$	2GLV+INT(4-NAF)	2I + 926.4M + 563.2S	1985.1M ≈ 1806.5m	37.4%
$E_e(F_{p_1})$	5-NAF	2I + 1242.1M + 1066.7S	2728.8M ≈ 2483.2m	-
$E(F_{p_2^2})$	4GLV+INT(3-NAF)	2i + 587m + 798s	1325.5m	114.3%
$E(F_{p_1})$	2GLV+INT(4-NAF)	2I + 561.4M + 1258.8S	2211.4M ≈ 2012.4m	41.1%
$E(F_{p_1})$	5-NAF	2I + 629.7M + 2248.7S	3121.1M ≈ 2840.2m	-

5 Conclusion

At present, GLV/GLS scalar multiplication mainly focuses on the Weierstrass curves, and has rarely been studied on other curve forms. This paper mainly studies the applications of GLV/GLS method on twisted Edwards curves. By exploiting birational equivalence, Frobenius mapping and twisting isomorphism between curves, we present the concrete

construction of efficiently computable endomorphism for Edwards curves, and also give some instances of efficiently computable endomorphism on curves. The main results of GLV/GLS method on the weierstrass curve are generalized to the twisted Edwards curve, and the 2-dimensional and 4-dimensional GLV methods are obtained accordingly.

Acknowledgment. This work is supported by the National Natural Science Foundation of China (Nos. 61772548, 61672413, 61872449) and the Foundation of Science and Technology on Information Assurance Laboratory (No. KJ-17–001).

References

1. Gallant, R.P., Lambert, R.J., Vanstone, S.A.: Faster point multiplication on elliptic curves with efficient endomorphisms. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 190–200. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44647-8_11
2. Park, Y.-H., Jeong, S., Kim, C.H., Lim, J.: An alternate decomposition of an integer for faster point multiplication on certain elliptic curves. In: Naccache, D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, pp. 323–334. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45664-3_23
3. Sica, F., Ciet, M., Quisquater, J.-J.: Analysis of the Gallant-Lambert-Vanstone method based on efficient endomorphisms: elliptic and hyperelliptic curves. In: Nyberg, K., Heys, H. (eds.) SAC 2002. LNCS, vol. 2595, pp. 21–36. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36492-7_3
4. Galbraith, S.D., Lin, X., Scott, M.: Endomorphisms for faster elliptic curve cryptography on a large class of curves. J. Cryptol. **24**(3), 446–469 (2011)
5. Zhou, Z., Hu, Z., Xu, M., Song, W.: Efficient 3-dimensional GLV method for faster point multiplication on some GLS elliptic curves. Inf. Process. Lett. **110**(22), 1003–1106 (2010)
6. Hu, Z., Longa, P., Xu, M.: Implementing 4-dimensional GLV method on GLS elliptic curves with j-invariant 0. Des. Codes Crypt. **63**(3), 331–343 (2012)
7. Longa, P., Sica, F.: Four-dimensional Gallant-Lambert-Vanstone scalar multiplication. J. Cryptol. **27**(2), 248–283 (2014)
8. Bos, J.W., Costello, C., Hisil, H., Lauter, K.: Fast cryptography in genus 2. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 194–210. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-38348-9_12
9. Buhler, J., Koblitz, N.: Lattice basis reduction, Jacobi sums and hyperelliptic cryptosystems. Bull. Aust. Math. Soc. **58**(1), 147–154 (1998)
10. Furukawa, E., Kawazoe, M., Takahashi, T.: Counting points for hyperelliptic curves of type y2 = x5 + ax over finite prime fields. In: Matsui, M., Zuccherato, R.J. (eds.) SAC 2003. LNCS, vol. 3006, pp. 26–41. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24654-1_3
11. Guillevic, A., Ionica, S.: Four-dimensional GLV via the weil restriction. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8269, pp. 79–96. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42033-7_5
12. Bos, J.W., Costello, C., Hisil, H., Lauter, K.: High-performance scalar multiplication using 8-dimensional GLV/GLS decomposition. In: Bertoni, G., Coron, J.-S. (eds.) CHES 2013. LNCS, vol. 8086, pp. 331–348. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40349-1_19
13. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 106, 2nd edn. Springer, Berlin (2009)

14. Hankerson, D., Menezes, A.J., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer, Berlin (2004)
15. Washington, L.C.: Elliptic Curves: Number Theory and Cryptography. CRC Press, New York (2008)
16. Edwards, H.M.: A normal form for elliptic curves. Bull. Am. Math. Soc. **44**(3), 392–422 (2007)
17. Bernstein, D.J., Lange, T.: Faster addition and doubling on elliptic curves. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 29–50. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76900-2_3
18. Bernstein, D.J., Birkner, P., Joye, M., Lange, T., Peters, C.: Twisted Edwards curves. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 389–405. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-68164-9_26
19. Faz-Hernández, A., Longa, P., Sánchez, A.H.: Efficient and secure algorithms for GLV-based scalar multiplication and their implementation on GLV-GLS curves. J. Cryptogr. Eng. **5**(1), 31–52 (2015)
20. MAGMA Computational Algebra System. http://magma.maths.usyd.edu.au/magma/
21. Bernstein, D.J., Lange, T.: Inverted Edwards coordinates. In: Boztaş, S., Lu, H.-F. (eds.) AAECC 2007. LNCS, vol. 4851, pp. 20–27. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77224-8_4
22. Dou, Y., Weng, J., Ma, C., Wei, F.: Analysis of GLV/GLS method for elliptic curve scalar multiplication. In: Hung, J.C., Yen, N.Y., Hui, L. (eds.) FC 2017. LNEE, vol. 464, pp. 210–219. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-7398-4_23
23. Longa, P., Miri, A.: New composite operations and precomputation scheme for elliptic curve cryptosystems over prime fields. In: Cramer, R. (ed.) PKC 2008. LNCS, vol. 4939, pp. 229–247. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-78440-1_14
24. Josefsson, S., Liusvaara, I.: Edwards-Curve Digital Signature Algorithm (EdDSA). RFC 8032, January 2017 (2017). https://rfc-editor.org/rfc/rfc8032.txt
25. Things that use Ed25519 (2019). https://ianix.com/pub/ed25519-deployment.html