Ready-Made Short Basis for GLV+GLS on High Degree Twisted Curves

[1]Bei Wang, [2]Songsong Li, [3]Yi Ouyang and [1]Honggang Hu

[1]Key Laboratory of Electromagnetic Space Information, CAS
University of Science and Technology of China
[2]School of Cyber Science and Engineering
Shanghai Jiao Tong University
[3]CAS Wu Wen-Tsun Key Laboratory of Mathematics,
School of Mathematical Sciences,
University of Science and Technology of China

Abstract

The crucial step in elliptic curve scalar multiplication based on scalar decompositions using efficient endomorphisms—such as GLV, GLS or GLV+GLS—is to produce a short basis of a lattice involving the eigenvalues of the endomorphisms, which usually is obtained by lattice basis reduction algorithms or even more specialized algorithms. Recently, lattice basis reduction is found to be unnecessary. Benjamin Smith (AMS 2015) was able to immediately write down a short basis of the lattice for the GLV, GLS, GLV+GLS of quadratic twists using elementary facts about quadratic rings. Certainly it is always more convenient to use a ready-made short basis than to compute a new one by some algorithm.

In this paper, we extend Smith's method on GLV+GLS for quadratic twists to quartic and sextic twists, and give ready-made short bases for 4-dimensional decompositions on these high degree twisted curves. In particular, our method gives a unified short basis compared with Hu et. al's method (DCC 2012) for 4-dimensional decompositions on sextic twisted curves.

Keywords. Endomorphism; Ready-made short basis; Twist; GLV+GLS
Mathematics Subject Classification (2010) 14H52 · 14G50

1 Introduction

Scalar multiplication on elliptic curves is the key operation in elliptic curve cryptography. It is thus extremely important to speed-up the scalar multiplication. The Gallant-Lambert-Vanstone (GLV) method [1], its generalizations the Galbraith-Lin-Scott (GLS) method [2] and the GLV+GLS method by Longa and Sica [3], use fast endomorphisms to decompose the scalar multiplication into shorter ones. The basic idea of GLV can be explained as follows.

Let $(E, \mathcal{O}_E)$ be an elliptic curve defined over a finite field $\mathbb{F}_q$. Suppose n is a large prime such that $n \| \#E(\mathbb{F}_q)$, so there is only one subgroup $G \subset E(\mathbb{F}_q)$ of order n. Suppose $\phi_1 = 1, \ldots, \phi_m$ are efficiently

computable $\mathbb{F}_q$-endomorphisms of E (in practice $m = 2$ or 4). For an integer $k \in [1, n-1]$ and a point $P \in G$, if there exists an m-dimensional decomposition

$$[k]P = [k_1]P + [k_2]\phi_2(P) + \ldots + [k_m]\phi_m(P) \text{ such that } |k_i|_\infty \leq Cn^{1/m} \tag{1}$$

for some constant C, then one can speed up the scalar multiplication $[k]P$ by computing the right hand side of (1). This approach is called the m-dimensional GLV method.

By hypothesis $\phi_i(G) \subseteq G$ for $1 \leq i \leq m$, then $\phi_i|_G = [\lambda_{\phi_i}]_G$ for a unique $\lambda_{\phi(i)} \in \mathbb{Z}/n\mathbb{Z}$, which we call the eigenvalue of ϕ_i modulo n. Consider the m-dimensional reduction map

$$F : \mathbb{Z}^m \to \mathbb{Z}/n\mathbb{Z}, \quad (x_1, x_2, \ldots, x_m) \mapsto x_1 + x_2\lambda_{\phi_2} + \ldots + x_m\lambda_{\phi_m} \mod n. \tag{2}$$

Clearly F is a surjective homomorphism, its kernel

$$\mathcal{L} := \ker F = \{(x_1, x_2, \ldots, x_m) \in \mathbb{Z}^m \mid x_1 + x_2\lambda_{\phi_2} + \ldots + x_m\lambda_{\phi_m} \equiv 0 \mod n\} \tag{3}$$

is a full sublattice of $\mathbb{Z}^m$. Note that for any $k \in \mathbb{Z}/n\mathbb{Z}$, $[k]P = [x_1]P + [x_2]\phi_2(P) + \ldots + [x_m]\phi_m(P)$ for all $P \in G$ if and only if $(x_1, \cdots, x_m) \in F^{-1}(k) = (k, 0, \ldots, 0) + \mathcal{L}$. If a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_m\}$ for $\mathcal{L}$ is known, let $(\alpha_1, \ldots, \alpha_m)$ be the (unique) solution in $\mathbb{Q}^m$ to the linear system $(k, 0, \ldots, 0) = \sum_{i=1}^m \alpha_i \mathbf{b}_i$. Then

$$(k_1, \ldots, k_m) := (k, 0, \ldots, 0) - \sum_{i=1}^m \lfloor \alpha_i \rceil \, \mathbf{b}_i = \sum_{i=1}^m (\alpha_i - \lfloor \alpha_i \rceil) \, \mathbf{b}_i$$

satisfies $\|(k_1, \ldots, k_m)\|_\infty \leq \frac{m}{2} \max_i \|\mathbf{b}_i\|_\infty$ as $|x - \lfloor x \rceil| \leq 1/2$ for any $x \in \mathbb{Q}$. If the basis vectors are bounded by $O\left(n^{1/m}\right)$, then the decomposition in (1) and as a result faster computation for $[k]P$ are achieved. So the crucial step in the GLV method is to find a basis of short length for the lattice $\mathcal{L}$.

In practice, knowledge of the eigenvalues allows us to write down a long basis for $\mathcal{L}$. To obtain a shorter basis, lattice basis reduction algorithms, such as the Euclidean algorithm ($m = 2$) [1], LLL [11], or even a more specialized algorithm ($m = 4$) [3], are then used. However, in recent development, lattice basis reduction was found to be unnecessary. One can simply write down short vectors of length at most $O\left(n^{1/m}\right)$ directly from the elliptic curve. Galbraith et al. [2] constructed an endomorphism equipped with a convenient ready-made basis for 2-dimensional decompositions and Benjamin Smith [6] constructed more families of endomorphisms from $\mathbb{Q}$-curves equipped with ready-made bases. Then, Smith [5] generalized these ready-made bases to all other known efficient endomorphism constructions for curves. He used elementary facts about quadratic rings to immediately write down ready-made short bases of the lattices for the GLV, GLS, GLV+GLS of quadratic twists, for $\mathbb{Q}$-curve construction on elliptic curves [4, 6], and for Jacobians with real multiplication construction [8, 7].

In this paper, we extend Smith's method to give a ready-made short basis of the lattice for GLV+GLS with degree of twist 4 or 6. We note that Longa and Sica [3]'s algorithm can be used to calculate a

short basis of the lattice for this class of quartic twisted elliptic curves. What's more, for the class of sextic twisted curves $E'/\mathbb{F}_{p^2}$, Hu et al. [10] described different short bases for the lattice according to the order $\#E'(\mathbb{F}_{p^2})$. However, we give a unified short basis of the lattice for the two classes of curves without discussions about their orders. Morever, these short bases of lattices constructed by us from the scalar decompositions can be read off from simple endomorphism ring relations which in practice are known in advance.

This paper is organized as follows. In §2, we give an overview of Smith's method on GLV+GLS with quadratic twists. In §3, we give supplements to Smith's method on high degree twisted elliptic curves. In §4, we give examples to verify our supplements.

2 Preliminary

2.1 GLV+GLS

The original GLV method by Gallant, Lambert and Vanstone [1] was about the 2-dimensional decomposition on special elliptic curves with an efficient endomorphism $\phi_2 = \rho$. The characteristic polynomial of ρ is X^2+rX+s with $r, s \in \mathbb{Z}$. Six examples of ordinary elliptic curves (identified with their j-invariants) defined over $\mathbb{F}_p$ with the endomorphism ρ be the complex multiplication map $P \mapsto [a]P$ were found to be applicable of their method:

$$j = 1728,\ a = \sqrt{-1}; \qquad j = 0,\ a = \frac{-1+\sqrt{-3}}{2}; \qquad j = 8000,\ a = \sqrt{-2};$$

$$j = 54000,\ a = \sqrt{-3}; \qquad j = -3375,\ a = \frac{1+\sqrt{-7}}{2}; \qquad j = -32768,\ a = \frac{1+\sqrt{-11}}{2}.$$

These curves are called the GLV curves. Note that $\mathbb{Z}[\rho] = \mathbb{Z}[\frac{-r+\sqrt{r^2-4s}}{2}]$ is either the maximal order or of an order of index 2 to the maximal order of the quadratic field $\mathbb{Q}(\rho) = \mathrm{End}(E) \otimes \mathbb{Q}$.

Galbraith, Lin and Scott [2] proved the following theorem:

Theorem 1 ([2]). *Let $p > 3$ be a prime and E an ordinary elliptic curve defined over $\mathbb{F}_p$. Let π_0 be the p-power Frobenius map on E and t_{π_0} the trace of π_0. Let $E'/\mathbb{F}_{p^2}$ be the quadratic twist of $E(\mathbb{F}_{p^2})$ and $\tau : E \to E'$ be the twist isomorphism defined over $\mathbb{F}_{p^4}$. Let $\psi = \tau\pi_0\tau^{-1}$.*

(1) The characteristic polynomial of ψ is $X^2 - t_{\pi_0}X + p$, i.e. $\psi^2(P) - [t_{\pi_0}]\psi(P) + [p]P = \mathcal{O}_{E'}$ for $P \in E'(\overline{\mathbb{F}}_p)$.

(2) If $n > 2p$ is a prime factor of $\#E'(\mathbb{F}_{p^2}) = (p-1)^2 + t_{\pi_0}^2$, then for $P \in E'(\mathbb{F}_{p^2})[n]$, $\psi^2(P) + P = \mathcal{O}_{E'}$, and the eigenvalue of ψ modulo n is $\lambda_\psi = t_{\pi_0}^{-1}(p-1) \bmod n$.

Based on Theorem 1, Galbraith et. al constructed the 2-dimensional GLV decomposition on the quadratic twist $E'(\mathbb{F}_{p^2})$. The curve $E'/\mathbb{F}_{p^2}$ which is a twist of $E(\mathbb{F}_{p^2})$ is called the GLS curve and

the 2-dimensional decomposing method using the restricted endomorphism ψ on $E'(\mathbb{F}_{p^2})$ satisfying $\psi^2 + 1 = 0$ is called the GLS method. Moreover, for quartic and sextic twists, Galbraith et. al also described how to obtain the 4-dimensional decompositions on $E'(\mathbb{F}_{p^2})$ by $\psi = \tau\pi_0\tau^{-1}$ satisfying certain quartic equations, which we will give in §3. In particular, Hu et al. [10] described the complete implementation of 4-dimensional decompositions on sextic twisted GLS elliptic curves.

Longa and Sica [3] combined GLV and GLS method (GLV+GLS) to get a 4-dimensional decomposition for twists of any GLV curve over $\mathbb{F}_{p^2}$. Let $E/\mathbb{F}_p$ be a GLV curve with ρ being the GLV endomorphism, let $E'/\mathbb{F}_{p^2}$ be a quadratic twist of E via the twist map $\tau : E \to E'$. We thus get two endomorphisms $\phi = \tau\rho\tau^{-1}$ and $\psi = \tau\pi_0\tau^{-1}$ of E' defined over $\mathbb{F}_{p^2}$, with characteristic polynomials $X^2 + rX + s$ and $X^2 - t_{\pi_0}X + p$ respectively. Let $\mathbb{Z}[\phi]$ and $\mathbb{Z}[\psi]$ be the $\mathbb{Z}$-modules over $\mathbb{Z}$ generated by the roots of the respected characteristic polynomials. If E' is ordinary, we know $\mathbb{Q}(\phi) = \mathbb{Q}(\psi)$.

Now if n satisfies the condition in Theorem 1 and $G \subset E'(\mathbb{F}_{p^2})$ is a cyclic subgroup of order n, then for $P \in G$, $\psi^2(P) + P = \mathcal{O}_{E'}$. The root of $\psi^2 + 1 = 0$ generates the quadratic ring $\mathbb{Z}[\sqrt{-1}]$ over $\mathbb{Z}$.

For any scalar $k \in [1, n-1]$, Longa and Sica obtained a 4-dimensional GLV decompositions

$$[k]P = [k_1]P + [k_2]\phi(P) + [k_3]\psi(P) + [k_4]\phi\psi(P). \tag{4}$$

Moreover, Longa and Sica [3] proposed a specialized algorithm (the twofold Cornacchia-type algorithm) to find a short basis for $\mathcal{L}$ under the assumption that $\mathbb{Z}[\phi]$ and $\mathbb{Z}[\sqrt{-1}]$ are $\mathbb{Z}$-linearly independent. They also treated the case $E/\mathbb{F}_p$ with j-invariant 1728 and E' a quartic twist of E in [3, Appendix B].

2.2 Ready-Made short bases on GLV+GLS of quadratic twists

First, we review the following result in [5], from which we can see that to produce the ready-made basis is mostly based on the simple order relations.

Lemma 1 ([5]). *Let ζ and ζ' be endomorphisms of an abelian variety $\mathcal{A}/\mathbb{F}_q$ such that $\mathbb{Z}[\zeta]$ and $\mathbb{Z}[\zeta']$ are quadratic rings and $\mathbb{Z}[\zeta] \subseteq \mathbb{Z}[\zeta']$, so $\zeta = c\zeta' + b$ for some integers b and c. Let $G \subset \mathcal{A}$ be a cyclic subgroup of order n such that $\zeta(G) \subseteq G$ and $\zeta'(G) \subseteq G$, and let λ and λ' be the eigenvalues in $\mathbb{Z}/n\mathbb{Z}$ of ζ and ζ' on G, respectively. Then*

$$\lambda - c\lambda' + b \equiv 0 \mod n$$

and

$$\lambda\lambda' - t_{\zeta'}\lambda - b\lambda' + cn_{\zeta'} + bt_{\zeta'} \equiv 0 \mod n,$$

where $t_{\zeta'}$ is the trace of ζ' and $n_{\zeta'}$ is the norm of ζ'.

From Lemma 1, Smith constructed explicit short bases for the GLV [1], GLS [2], GLV+GLS [3], and other constructions on $\mathbb{Q}$-curve [4, 6] and genus 2 Jacobians [7, 8].

In this paper, we only recall Smith's method on GLV+GLS of quadratic twists. The notations are defined as above. Let λ_ϕ and λ_ψ be the eigenvalues of ϕ and ψ on G, respectively. Then λ_ϕ satisfies $\lambda_\phi^2 + r\lambda_\phi + s = 0 \mod n$, λ_ψ satisfies $\lambda_\psi^2 - t_{\pi_0}\lambda_\psi + p = 0 \mod n$ and $\lambda_\psi^2 + 1 = 0 \mod n$. Since ϕ is constructed by a GLV endomorphism, $\mathbb{Z}[\phi] \cong \mathbb{Z}[\rho]$ is either the maximal order of the endomorphism algebra of E', or very close to it—so it makes sense to assume that $\mathbb{Z}[\phi]$ contains $\mathbb{Z}[\psi]$, so that $\psi = c\phi + b$, where

$$b = \frac{1}{2}(t_{\pi_0} + cr) \text{ and } c^2 = \frac{t_{\pi_0}^2 - 4p}{r^2 - 4s}. \tag{5}$$

Theorem 2 ([5]). *With ϕ and ψ defined as above, suppose we can construct a 4-dimensional decomposition (see the Eq. (4)) with $(1, \phi, \psi, \phi\psi)$. The vectors*

$$\mathbf{b}_1 = (1, 0, b, c), \qquad \mathbf{b}_2 = (0, 1, -cs, -cr + b),$$
$$\mathbf{b}_3 = (-b, -c, 1, 0), \qquad \mathbf{b}_4 = (cs, cr - b, 0, 1)$$

generate a sublattice of determinant $\#E'(\mathbb{F}_{p^2})$ in $\mathcal{L}$. These vectors are short with $\|\mathbf{b}_i\|_\infty = O(n^{1/4})$ for $1 \le i \le 4$. If $G = E'(\mathbb{F}_{p^2})$, then $\mathcal{L} = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4 \rangle$.

3 Ready-Made short bases on GLV+GLS of quartic and sextic twists

Smith [5] only considered the ready-made short bases for quadratic twisted curves over $\mathbb{F}_{p^2}$. In this paper, we consider the cases of twisted curves over $\mathbb{F}_{p^2}$ of degree 4 and 6 and provide ready-made short bases for 4-dimensional decompositions on these curves.

In the following, let $E/\mathbb{F}_p$ be a GLV curve with a GLV endomorphism ρ. Let π_0 be the p-power Frobenius on E and t_{π_0} be the trace of π_0. Let $E'/\mathbb{F}_{p^2}$ be a quartic (thus $j(E) = 1728$) or sextic twist ($j(E) = 0$) of $E(\mathbb{F}_{p^2})$ and $\tau : E \to E'$ be the twist isomorphism. Let $\phi = \tau\rho\tau^{-1}$ and $\psi = \tau\pi_0\tau^{-1}$, which are defined over $\mathbb{F}_{p^2}$ on E'. Let $G \subset E'(\mathbb{F}_{p^2})$ be a cyclic subgroup of large prime order n.

Since ρ is a GLV endomorphism, $\mathbb{Z}[\phi] \cong \mathbb{Z}[\rho]$ is the maximal order of the endomorphism algebra of E' for the case j-invariant 0 or 1728, then $\mathbb{Z}[\psi]$ is contained in $\mathbb{Z}[\phi]$. Then $\psi = c\phi + b$, where b, c can be computed as Eq. (5) by the characteristic equations of ϕ and ψ.

Our main results are Theorems 3 and 4:

Theorem 3. *Let $E/\mathbb{F}_p$ be an elliptic curve with j-invariant 1728 and ρ a GLV endomorphism. Suppose $E'/\mathbb{F}_{p^2}$ is a quartic twist of $E(\mathbb{F}_{p^2})$ and $\tau : E \to E'$ is the twist isomorphism defined over $\mathbb{F}_{p^8}$. Let$\phi = \tau\rho\tau^{-1}$ and $\psi = \tau\pi_0\tau^{-1}$, then the characteristic equations of ϕ and ψ are $\phi^2 + 1 = 0$ and $\psi^2 - t_{\pi_0}\psi + p = 0$*

respectively. Moreover, when restricted on $E'(\mathbb{F}_{p^2})$, ψ *also satisfies* $\psi^4+1=0$. *With* ϕ *and* ψ, *we can construct a 4-dimensional decomposition with* $(1,\phi,\psi,\phi\psi)$. *Then vectors*

$$\mathbf{b}_1=(1,0,-c,b), \qquad \mathbf{b}_2=(0,1,-b,-c),$$
$$\mathbf{b}_3=(-b,-c,1,0), \quad \mathbf{b}_4=(c,-b,0,1)$$

generate a sublattice of determinant $\#E'(\mathbb{F}_{p^2})$ *in* $\mathcal{L}$. *These vectors are short with* $\|\mathbf{b}_i\|_\infty = O(n^{1/4})$ *for* $1\le i\le 4$. *If* $G=E'(\mathbb{F}_{p^2})$, *then* $\mathcal{L}=\langle \mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3,\mathbf{b}_4\rangle$.

Proof. For the fact $\psi^4(P)+P=\mathcal{O}_{E'}$ for any $P\in E'(\mathbb{F}_{p^2})$ one can refer to [2, §3]. Let λ_ϕ and λ_ψ be the eigenvalues of ϕ and ψ on G, respectively. Applying Lemma 1 to the inclusion $\mathbb{Z}[\psi]\subset\mathbb{Z}[\phi]$ with $t_\phi=0$ and $n_\phi=1$, we obtain relations

$$\lambda_\psi - c\lambda_\phi - b \equiv 0 \mod n \text{ and } \lambda_\psi\lambda_\phi - b\lambda_\phi + c \equiv 0 \mod n, \tag{6}$$

which corresponding to the vectors $\mathbf{b}_3$ and $\mathbf{b}_4$. Note that when restricted on $E'(\mathbb{F}_{p^2})$, then $\pm\psi^2$ has the same characteristic equation as ϕ. Changing ϕ to $-\phi$ if necessary, we may identify ϕ with ψ^2. Multiplying the relations in (6) by λ_ψ, using $\lambda_\psi^2=\lambda_{\psi^2}=\lambda_\phi \mod n$ and $\lambda_\phi^2=-1$, we obtain new relations

$$\lambda_\phi - c\lambda_\phi\lambda_\psi - b\lambda_\psi \equiv 0 \mod n \text{ and } 1 + b\lambda_\phi\lambda_\psi - c\lambda_\psi \equiv 0 \mod n, \tag{7}$$

which corresponding to the vectors $\mathbf{b}_1$ and $\mathbf{b}_2$.

The claim that $\det\langle \mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3,\mathbf{b}_4\rangle = \#E'(\mathbb{F}_{p^2})$ will be proved later. □

Theorem 4. *Let* $E/\mathbb{F}_p$ *be an elliptic curve with* j*-invariant 0 and* ρ *a GLV endomorphism. Suppose* $E'/\mathbb{F}_{p^2}$ *is a sextic twist of* $E(\mathbb{F}_{p^2})$ *and* $\tau: E\to E'$ *is the sextic twisted isomorphism defined over* $\mathbb{F}_{p^{12}}$. *Let* $\phi=\tau\rho\tau^{-1}$ *and* $\psi=\tau\pi_0\tau^{-1}$, *then the characteristic equations of* ϕ *and* ψ *are* $\phi^2+\phi+1=0$ *and* $\psi^2-t_{\pi_0}\psi+p=0$ *respectively. Moreover, when restricted on* $E'(\mathbb{F}_{p^2})$, ψ *also satisfies* $\psi^4-\psi^2+1=0$. *With* ϕ *and* ψ, *we can construct a 4-dimensional decomposition with* $(1,\phi,\psi,\phi\psi)$. *Then short vectors*

$$\mathbf{b}_1=(1,0,c-b,-b), \quad \mathbf{b}_2=(0,1,b,c),$$
$$\mathbf{b}_3=(-b,-c,1,0), \qquad \mathbf{b}_4=(c,c-b,0,1)$$

generate a sublattice of determinant $\#E'(\mathbb{F}_{p^2})$ *in* $\mathcal{L}$. *These vectors are short with* $\|\mathbf{b}_i\|_\infty = O(n^{1/4})$ *for* $1\le i\le 4$. *If* $G=E'(\mathbb{F}_{p^2})$, *then* $\mathcal{L}=\langle \mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3,\mathbf{b}_4\rangle$.

Proof. ψ satisfies $\psi^4-\psi^2+1=0$, one can see [2, §3]. Note that when restricted on $E'(\mathbb{F}_{p^2})$, $-\psi^2$ satisfies the same characteristic equation $x^2+x+1=0$ as ϕ, we identify ϕ with $-\psi^2$ on $E'(\mathbb{F}_{p^2})$.

Similar to the proof of Theorem 3 with $t_\phi = -1, n_\phi = 1$, we can get the relations

$$\lambda_\psi - c\lambda_\phi - b \equiv 0 \mod n \text{ and } \lambda_\psi\lambda_\phi + \lambda_\psi - b\lambda_\phi + c - b \equiv 0 \mod n, \tag{8}$$

which corresponding to the vectors $\mathbf{b}_3$ and $(c-b, -b, 1, 1) = \mathbf{b}_4 + \mathbf{b}_3$. Then multiplying (8) by $-\lambda_\psi$, we get

$$\lambda_\phi + c\lambda_\phi\lambda_\psi + b\lambda_\psi \equiv 0 \mod n \text{ and } 1 + (c-b)\lambda_\psi - b\lambda_\phi\lambda_\psi \equiv 0 \mod n \tag{9}$$

with $\lambda_\psi^2 = \lambda_{\psi^2} = -\lambda_\phi \mod n$ and $\lambda_\phi^2 = -\lambda_\phi - 1 \mod n$. We can immediately get the vectors $\mathbf{b}_1, \mathbf{b}_2$. Also, the claim that $\det\langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4\rangle = \#E'(\mathbb{F}_{p^2})$ will be proved later. □

The rest proof of Theorem 3 and 4. To verify $\det\langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4\rangle = \#E'(\mathbb{F}_{p^2})$, we need recall some results for the case $q = p^2$ in [12, Proposition 2]. In the following, let t_π be the trace of Frobenius endomorphism $\pi \in \mathrm{End}(E \times \mathbb{F}_{p^2})$, where $E \times \mathbb{F}_{p^2}$ are the base extension of E to $\mathbb{F}_{p^2}$.

Lemma 2 ([12])**.** *Let $E/\mathbb{F}_p$ be an ordinary elliptic curve, then $\#E(\mathbb{F}_p) = p + 1 - t_{\pi_0}$ and $\#E(\mathbb{F}_{p^2}) = p^2 + 1 - t_\pi$, where $t_\pi = t_{\pi_0}^2 - 2p$. $E'/\mathbb{F}_{p^2}$ is a d-th twist of $E(\mathbb{F}_{p^2})$, then the possible group orders of $E'(\mathbb{F}_{p^2})$ are given by the following:*

$$\underline{d = 4:}\ \ \#E'(\mathbb{F}_{p^2}) = p^2 + 1 \pm f \qquad \text{with } t_\pi^2 - 4p^2 = -f^2$$

$$\underline{d = 6:}\ \ \#E'(\mathbb{F}_{p^2}) = p^2 + 1 - (t_\pi \pm 3f)/2 \quad \text{with } t_\pi^2 - 4p^2 = -3f^2$$

Moreover, if we know p and t_{π_0}, we can get $\#E'(\mathbb{F}_{p^2}) = p^2+1\pm t_{\pi_0}\sqrt{4p - t_{\pi_0}^2}$ for $d = 4$ and $\#E'(\mathbb{F}_{p^2}) = p^2 + p + 1 - \frac{t_{\pi_0}^2 \pm t_{\pi_0}\sqrt{3(4p - t_{\pi_0}^2)}}{2}$ for $d = 6$.

When $E'/\mathbb{F}_{p^2}$ is a quartic twist of $E(\mathbb{F}_{p^2})$, with $b = \frac{t_{\pi_0}}{2}$ and $c^2 = \frac{4p - t_{\pi_0}^2}{4}$ by Eq. (5), we have

$$\begin{aligned}\det\langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4\rangle &= (1 - 2bc)^2 + (c^2 - b^2)^2 = \left(1 \pm \frac{t_{\pi_0}\sqrt{4p - t_{\pi_0}^2}}{2}\right)^2 + \left(\frac{2p - t_{\pi_0}^2}{2}\right)^2 \\ &= p^2 + 1 \pm t_{\pi_0}\sqrt{4p - t_{\pi_0}^2} = \#E'(\mathbb{F}_{p^2}).\end{aligned}$$

When $E'/\mathbb{F}_{p^2}$ is a sextic twist of $E(\mathbb{F}_{p^2})$, with $b = \frac{t_{\pi_0} + c}{2}$ and $c^2 = \frac{4p - t_{\pi_0}^2}{3}$ by Eq. (5), we have

$$\begin{aligned}\det\langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4\rangle &= (1 + 2bc - b^2)(1 + 2bc - c^2) + (c^2 - b^2)^2 \\ &= p^2 + p + 1 - \frac{t_{\pi_0}^2 \pm t_{\pi_0}\sqrt{3(4p - t_{\pi_0}^2)}}{2} = \#E'(\mathbb{F}_{p^2}).\end{aligned}$$

In the last, we can see that the vectors produced by Theorem 3 and 4 are short: since ϕ is a GLV endomorphism, both r and s are in $O(1)$. Hence, in view of Eq. (5), we observe that b and c are both in $O(\sqrt{p})$, thus $\|\mathbf{b}_i\|_\infty$ is in $O(\sqrt{p}) = O(n^{1/4})$ for $1 \leq i \leq 4$. So far, we have completed the proof of Theorem 3 and 4. □

Remark 1. *For the class of sextic twisted curves $E'/\mathbb{F}_{p^2}$, there are six cases of Frobenius trace t_{π_0} [9, Ch. 18.3,Th. 4]. According to the formula in Lemma 2 with $d = 6$, there are three cases of $\#E'(\mathbb{F}_{p^2})$. Hu et. al [10] constructed three kinds of short bases according to the order of $E'(\mathbb{F}_{p^2})$. Their method is first to find the integral solutions (u, v) of quadratic form $x^2 + xy + y^2 = p$, then six cases of t_{π_0} and three cases of $\#E'(\mathbb{F}_{p^2})$ can be represented by u, v. For each case of $\#E'(\mathbb{F}_{p^2})$, they described a short basis generating a sublattice of determinant $\#E'(\mathbb{F}_{p^2})$ in $\mathcal{L}$, the upper bound of the basis is only depend on the bound of u, v. We note that the lattice $\mathcal{L}$ in their construction is the same as ours in Theorem 4 and there are simple linear relationships between the elements b, c and u, v. Thus, the basis $\langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4 \rangle$ is of the same length $O(n^{1/4})$ as their's. We give a unified short basis without discussion of the order of $E'(\mathbb{F}_{p^2})$.*

4 Examples

Here, we give two examples to immediately write down a short basis of the lattice for GLV+GLS by our Theorem 3 and 4, see the following.

Example 1 ($j = 1728$). Let $p_1 = 2^{127} - 11791$ and $\mathbb{F}_{p_1^2} = \mathbb{F}_{p_1}(u)$ which $u^4 = \sqrt{7}$ in $\mathbb{F}_{p_1^2}$. Let $E_1'/\mathbb{F}_{p_1^2} : y^2 = x^3 + 6u^4x$ with $\#E_1'(\mathbb{F}_{p_1^2}) = 2n_1$, where n_1 is a 253-bit prime. E_1' is the quartic twist of the curve $E_1 : y^2 = x^3 + 6$ with the Frobenius trace $t_{\pi_0,1} = -5387725816103856782$. $\phi_1(x, y) = [\lambda_1]P = (-x, iy)$ and $\psi_1(x, y) = [\mu_1]P = (u^{2(1-p_1)}x^{p_1}, u^{3(1-p_1)}y^{p_1})$. The characteristic equations of ϕ_1 and ψ_1 are $\phi_1^2 + 1 = 0$ and $\psi_1^2 - t_{\pi_0,1}\psi_1 + p_1 = 0$ respectively, ψ_1 also satisfies $\psi_1^4 + 1 = 0$ when restricted on $E_1'(\mathbb{F}_{p_1^2})$. Theorem 3 constructs a short basis of $\mathcal{L}$ in GLV+GLS method with $b = -2693862908051928391$ and $c = 12762612823912321416$:

$$\mathbf{b}_1 = (0, 1, 2693862908051928391, -12762612823912321416),$$

$$\mathbf{b}_2 = (-1, 0, 12762612823912321416, 2693862908051928391),$$

$$\mathbf{b}_3 = (2693862908051928391, -12762612823912321416, 1, 0),$$

$$\mathbf{b}_4 = (12762612823912321416, 2693862908051928391, 0, 1).$$

Example 2 ($j = 0$). Let $p_2 = 2^{128} - 40557$ and $\mathbb{F}_{p_2^2} = \mathbb{F}_{p_2}(u)$ with $u^6 = 3 + \sqrt{-1}$ in $\mathbb{F}_{p_2^2}$. Let $E_2'/\mathbb{F}_{p_2^2} : y^2 = x^3 + 8u^6$ with $\#E_2(\mathbb{F}_{p_2^2}) = n_2$, where n_2 is a 256-bit prime. E_2' is the sextic twist of

the curve $E_2 : y^2 = x^3 + 8$ with the Frobenius trace $t_{\pi_0,2} = 17641752181631433232$. $\phi_2(x, y) = (\xi x, y)$ ($\xi^3 = 1 \mod p_2$) and $\psi_2(x, y) = [\mu_2]P = (u^{2(1-p_2)}x^{p_2}, u^{3(1-p_2)}y^{p_2})$. The characteristic equations of ϕ_2 and ψ_2 are $\phi_2^2 + \phi_2 + 1 = 0$ and $\psi_2^2 - t_{\pi_0,2}\psi + p_2 = 0$ respectively, ψ_2 also satisfies $\psi_2^4 - \psi_2^2 + 1 = 0$ when restricted on $E_2'(\mathbb{F}_{p_1^2})$. Theorem 4 constructs a short basis of $\mathcal{L}$ in GLV+GLS method with $b = 18174565414845640175$ and $c = 18707378648059847118$:

$$\mathbf{b}_1 = (0, -1, -18174565414845640175, -18707378648059847118),$$

$$\mathbf{b}_2 = (1, 0, 532813233214206943, -18174565414845640175),$$

$$\mathbf{b}_3 = (-18174565414845640175, -18707378648059847118, 1, 0),$$

$$\mathbf{b}_4 = (18707378648059847118, 532813233214206943, 0, 1).$$

Morever, we can compute the decomposed coefficients of 4-dimensional decompositions on E_i' with respect to $\{1, \phi_i, \psi_i, \phi_i\psi_i\}$ through the ready-made short bases, $i = 1, 2$, see the Table 1.

Table 1. The decomposed coefficients with random k of the 128-bit security

Curve	k	$[k_1, k_2, k_3, k_4]$
$E_1'(\mathbb{F}_{p_1^2})$	$k = 2^{128} - 5$	$[23576, -2, 1987161191704607852, 2693862908051928391]$
	$k = 2^{128} - 46$	$[23535, -2, 1987161191704607852, 2693862908051928391]$
$E_2'(\mathbb{F}_{p_2^2})$	$k = 2^{128} - 5$	$[40550, -1, -1065626466428413886, -1065626466428413886]$
	$k = 2^{128} - 865$	$[39691, 0, -1065626466428413886, -532813233214206943]$

References

[1] Gallant, R., Lambert, R., Vanstone, S.: Faster point multiplication on elliptic curves with efficient endomorphisms. In: Kilian, J. (ed.) CRYPTO. LNCS, vol. 2139, pp. 190–200. Springer (2001)

[2] Galbraith S.D., Lin X.B., Scott M.: Endomorphisms for faster elliptic curve cryptography on a Large class of curves. J. Cryptol. 24(3), 446–469 (2011).

[3] Longa P., Sica F.: Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication. J. Cryptol. **27**(2), 248-283 (2014).

[4] Guillevic A., Ionica S.: Four-dimensional GLV via the Weil restriction. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 79-96, Springer, Berlin, Heidelberg (2013).

[5] Smith B.: Easy scalar decompositions for efficient scalar multiplication on elliptic curves and genus 2 Jacobians. Contemporary mathematics, American Mathematical Society, 637 (2015).

[6] Smith B.: Families of Fast Elliptic Curves from Q-Curves. Part I of the Proceedings of the 19th International Conference on Advances in Cryptology - ASIACRYPT 2013. vol. 8269 , 61–78 (2013).

[7] D. R. Kohel and Smith B.: Efficiently computable endomorphisms for hyperelliptic curves. In F. Hess, S. Pauli, and M. Pohst (eds), Algorithmic number theory: ANTS-VII, Lecture Notes in Comput. Sci. 4076, 495–509 (2006).

[8] K. Takashima.: A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application. IEICE Trans. Fundamentals E89-A #1, 124–133 (2006).

[9] Ireland K., Rosen M.: A Classical Introduction to Modern Number Theory, Second Edition. GTM, vol. 84. Springer, New York (1990).

[10] Hu Z., Longa P., Xu M.: Implementing the 4-dimensional GLV method on GLS elliptic curves with j-invariant 0. Designs, Codes and Cryptography. **63**(3), 331-343 (2012).

[11] Cohen, H.: A Course in Computational Algebraic Number Theory. GTM 138. Springer, Heidelberg (2000).

[12] F. Hess, N. Smart, F. Vercauteren, The Eta pairing revisited. IEEE Trans. Inf. Theory, vol. 52, pp. 4595–4602 (2006)