A New Twofold Cornacchia-Type Algorithm for 4-GLV Decompositions and Its Applications

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

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

Abstract

Until now, there are two different methods to compute 4-GLV decompositions on the elliptic curves over $\mathbb{F}_{p^2}$ which are quadratic twists and possess a "restricted" endomorphism ψ satisfying $\psi^2 + 1 = 0$. They are Longa and Sica's twofold Cornacchia-type algorithm (ASIACRYPT 2012) and Benjamin Smith's method–ready-made short bases (AMS 2015). In this paper, we first extend Smith's method from the case of quadratic twists to the case of quartic or sextic twists and give ready-made short bases for 4-GLV decompositions on these high degree twisted curves. After our supplements, Smith's method can be used to compute 4-GLV decompositions on more elliptic curves. Secondly, we focus on exploring more potential of Longa and Sica's algorithm, which is an elaborate iterated Cornacchia algorithm that can compute short bases for 4-GLV decompositions. The algorithm consists of two sub-algorithms, the first one in the ring of integers $\mathbb{Z}$ and the second one in the Gaussian integer ring $\mathbb{Z}[i]$. We observe that $\mathbb{Z}[i]$ in the second sub-algorithm can be replaced by another Euclidean domain $\mathbb{Z}[\omega]$ ($\omega = \frac{-1+\sqrt{-3}}{2}$). As a consequence, we design a new twofold Cornacchia-type algorithm with a theoretic upper bound of output $C \cdot n^{1/4}$, where $C = \frac{3+\sqrt{3}}{2}\sqrt{1+|r|+|s|}$ with small values r, s given by the curve.

The new twofold algorithm can be used to compute 4-GLV decompositions on two classes of curves. First it gives a new and unified method to compute all 4-GLV decompositions on j-invariant 0 elliptic curves over $\mathbb{F}_{p^2}$. We exploit the fact that this family of curves must have an endomorphism ϕ satisfying $\phi^2 + \phi + 1 = 0$ (and hence $\mathbb{Z}[\phi] = \mathbb{Z}[\omega]$). Of the two previous methods on this class of elliptic curves, the first one was proposed by Hu, Longa and Xu in 2012 (Designs, Codes and Cryptography) but is applicable only to curves which are twists of degree 6 and possess a "restricted" endomorphism ψ satisfying $\psi^4 - \psi^2 + 1 = 0$, the second one follows from the the work of Longa and Sica (ASIACRYPT 2012) and is applicable only to curves with a "restricted" endomorphism ψ satisfying $\psi^2 + 1 = 0$. Second it can be used to compute the 4-GLV decomposition on the Jacobian of the hyperelliptic curve defined as $\mathcal{C}/\mathbb{F}_p : y^2 = x^6 + ax^3 + b$, which has an endomorphism ϕ with the characteristic equation $\phi^2 + \phi + 1 = 0$ (hence $\mathbb{Z}[\phi] = \mathbb{Z}[\omega]$).

Keywords. Elliptic curves · 4-GLV decompositions · Twofold Cornacchia-type algorithm
Mathematics Subject Classification (2010) 14H52 · 14G50

1 Introduction

The 2-GLV method, introduced by Gallant, Lambert and Vanstone [1] in 2001, is a generic approach to speed up the computation of scalar multiplication on certain elliptic curves (GLV curves) defined over fields with large prime characteristic by using endomorphisms of the curves to decompose the scalar multiplication. A GLV curve is certain elliptic curve E over $\mathbb{F}_q$ possessing an endomorphism ϕ whose characteristic polynomial is $x^2+rx+s \in \mathbb{Z}[x]$. Let $G \subset E(\mathbb{F}_q)$ be a cyclic subgroup of large prime order n, for a point $P \in G$, then $\phi(P) = [\lambda]P$ for some $\lambda \in [1, n-1]$ satisfying $\lambda^2 + r\lambda + s \equiv 0 \bmod n$. For any $k \in [1, n-1]$, one can find $|k_1|, |k_2| \leq c\sqrt{n}$ for some constant $c > 0$ such that $k = k_1 + k_2\lambda \mod n$. The 2-dimensional decomposition of $[k]P$ is then $[k]P = [k_1]P + [k_2]\phi(P)$. By this decomposition one can speed up the scalar multiplication for GLV curves.

The GLV curves, however, are special curves with special j-invariants, one might wonder whether it matters in practice. In 2002, for elliptic curves over $\mathbb{F}_{p^2}$ with j-invariant in $\mathbb{F}_p$, Iijima, Matsuo, Chao and Tsujii [2] constructed an efficient computable homomorphism arising from the Frobenius map on a twist of E. In 2009, Galbraith, Lin and Scott [3] generalized the construction of [2] to a large class of elliptic curves over $\mathbb{F}_{p^2}$ so that the GLV method is applicable. The construction in [3] is as follows: Let E be an 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. $E'/\mathbb{F}_{p^2}$ is a twist of $E/\mathbb{F}_p$ with $\tau : E_0 \to E'$ the twist isomorphism. Let $G \subset E'(\mathbb{F}_{p^2})$ be a cyclic subgroup of large prime order n. Then $\psi = \tau\pi_0\tau^{-1}$ is an endomorphism of E', which is defined over $\mathbb{F}_{p^2}$. When E' is a quadratic twist of E, ψ acting on points in $E'(\mathbb{F}_{p^2})$ satisfies the equation $\psi^2 + 1 = 0$. One can decompose $[k]P$ as $[k]P = [k_1]P + [k_2]\psi(P)$ for $P \in G$. When E' is a quartic or sextic twist of E, ψ acting on points in $E'(\mathbb{F}_{p^2})$ satisfies a quartic equation. In this case, Galbraith et al. gave 4-GLV expansions on $E'(\mathbb{F}_{p^2})$, they decomposed $[k]P$ as $[k]P = [k_1]P + [k_2]\psi(P) + [k_3]\psi^2(P) + [k_4]\psi^3(P)$ for $P \in G$.

Note that the characteristic equation of ψ is $\psi^2 - t_{\pi_0}\psi + p = 0$, for any point $Q \in E'(\bar{\mathbb{F}}_{p^2})$, we have $\psi^2(Q) - t_{\pi_0}\psi(Q) + [p]Q = \mathcal{O}_{E'}$. Furthermore, when ψ acts on points in $E'(\mathbb{F}_{p^2})$, it also satisfies $\psi^2 + 1 = 0$ or a quartic equation for the degree of twist 2 or 4,6. Here, we call the endomorphism restricted to points in $E'(\mathbb{F}_{p^2})$ the "restricted" endomorphism. The curves $E'/\mathbb{F}_{p^2}$ are called the GLS curves and the 2-dimensional decomposing method using the "restricted" endomorphism ψ satisfying $\psi^2 + 1 = 0$ is called the GLS method.

In 2012, Longa and Sica [5] introduced a 4-GLV method by combining GLV and GLS methods (GLV+GLS), which is a natural extension of Zhou et al. idea [4] of constructing 3-GLV decompositions. When E is a GLV curve with an efficient complex multiplication, then two endomorphisms ϕ and ψ can be constructed on the GLS curve $E'/\mathbb{F}_{p^2}$. The two "restricted" endomorphisms satisfying $\phi^2+r\phi+s = 0$ and $\psi^2+1 = 0$ were used to get the 4-GLV decomposition $[k]P = [k_1]P+[k_2]\phi(P)+[k_3]\psi(P)+[k_4]\phi\psi(P)$

for $P \in G$. The GLV method can also be extended to genus 2 curves, one can refer [6] for the 4-GLV decomposition and [10] for the 8-GLV decomposition.

Scalar decomposition is the crucial step to make the GLV method successful, and it can be reduced to solving the closest vector problem (CVP), as a result the LLL algorithm [12] is used. For the 2-GLV decomposition, Gallant et al. [1] exploited the efficient Cornacchia's algorithm, an application of the extended Euclidean algorithm. For the 4-GLV decomposition on the special class of elliptic curves with j-invariant 0, Hu, Longa and Xu [7] proposed an explicit lattice-based decomposition method with an almost optimal upper bound of coefficients $O(2\sqrt{2}n^{1/4})$. For the general 4-GLV decompositions, Longa and Sica [5] assumed that the "restricted" endomorphisms ϕ and ψ, when viewed as algebraic integers, generate disjoint quadratic extensions of $\mathbb{Q}$. Under the assumption, they designed a specific and more efficient reduction algorithm called the twofold Cornacchia-type algorithm, which consists two parts, the first part in the ring of integers $\mathbb{Z}$ and the second part in the Gaussian integer ring $\mathbb{Z}[i]$.

Recently, in most cryptographic situations, lattice basis reduction is not necessary to find a short basis for the scalar decomposition, one can simply write down short vectors from scratch. Galbraith et al. [3] constructed an endomorphism equipped with a convenient ready-made basis for 2-dimensional decompositions and Benjamin Smith [18] constructed more families of endomorphisms from $\mathbb{Q}$-curves equipped with a ready-made basis. Then, Smith [17] generalized these ready-made bases to all of the other known efficient endomorphism constructions for curves. He used elementary facts about quadratic rings to immediately write down a ready-made short basis of the lattice for the GLV, GLS, GLV+GLS, and $\mathbb{Q}$-curve constructions on elliptic curves [6, 18], and for genus 2 real multiplication constructions [20, 19]. His method is mainly adapt to ordinary curves. He did not pretend that this represents a significant optimization in scalar multiplication, since the lattice reduction step is always an offline precomputation – but it does give a better insight into the structure of scalar decompositions.

Our contributions here are two parts. First, for GLV+GLS, Smith's method can not compute 4-GLV decompositions on GLS curves with degree of twist 4 or 6. In §3, we make supplements to Smith's method under the same assumption that $\mathbb{Z}[\phi]$ contains $\mathbb{Z}[\psi]$ so as to make his method adapt to more elliptic curves over $\mathbb{F}_{p^2}$.

Second, we focus on exploring more potential of Longa and Sica's algorithm, which is an easy-to-implement and very efficient algorithm with complexity $O(\log^2(n))$. It is our observation that the second part of Longa and Sica's algorithm can be implemented not only in $\mathbb{Z}[i]$ but also in other imaginary quadratic orders which are Euclidean, for example, the orders $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$. In this paper we only consider the ring of integers $\mathbb{Z}[\omega] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ of $\mathbb{Q}(\sqrt{-3})$, the discussion of the other cases is similar. We construct a new twofold Cornacchia-type algorithm for scalar decomposition, the first part in $\mathbb{Z}$ and the second part in $\mathbb{Z}[\omega]$. Moreover, our new algorithm gain

a theoretic upper bound of output $C \cdot n^{1/4}$, where $C = \frac{3+\sqrt{3}}{2}\sqrt{1+|r|+|s|}$ with small values r, s given by the curve. The upper bound is very close to Hu et al.'s [7] and better than Longa and Sica's [5] and Yi et al.'s [8].

Our new twofold Cornacchia-type algorithm can be used to compute 4-GLV decompositions on two classes of curves. The first class of curves are j-invariant 0 elliptic curves over $\mathbb{F}_{p^2}$. There are two 4-GLV decompositions have been proposed on this class of elliptic curves, each used under certain conditions. The first decomposition uses the "restricted" endomorphism ψ coming from twists of degree 6 and satisfying the equation $\psi^4 - \psi^2 + 1 = 0$, the algorithm in [7] can be used to compute it. The second 4-GLV decomposition uses the "restricted" endomorphism ψ satisfying $\psi^2 + 1 = 0$, the twofold Cornacchia-type algorithm in [5, 8] can be used to compute it. In both cases, we observe the existence of an endomorphism ϕ satisfying $\phi^2 + \phi + 1 = 0$, thus $\mathbb{Z}[\phi] = \mathbb{Z}[\omega]$ and our new twofold algorithm can be used compute all 4-GLV decompositions on this class of curves simultaneously. The second class of curves are hyperelliptic curves defined as $\mathcal{C}/\mathbb{F}_p : y^2 = x^6 + ax^3 + b$, it has an endomorphism ϕ with characteristic equation $\phi^2 + \phi + 1 = 0$ (hence $\mathbb{Z}[\phi] = \mathbb{Z}[\omega]$), our algorithm can be used to compute 4-GLV decompositions on the Jacobians of this class of hyperelliptic curves. Meanwhile, after some supplements to Smith's method on high degree twisted curves, we can use ready-made short bases to compute all 4-GLV decompositions on the first class of curves. However, we note that this method can not be used to compute 4-GLV decompositions on Jacobians of the second class of curves.

This paper is organized as follows. In §2, we give an overview of previous work on the GLV decomposition. In §3, we give supplements to Smith's method on high degree twisted elliptic curves. §4 contains the main work of this paper, the construction of the new twofold Cornacchia-type algorithm. In §5 we give applications of our new twofold Cornacchia-type algorithm. In §6, we give some examples and experimental results. Finally, in §7 we make a conclusion.

2 An overview of previous work

2.1 The GLV elliptic curves

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ with infinity point denoted by $\mathcal{O}_E$. Suppose n is a large prime such that $n \| \#E(\mathbb{F}_q)$ and so there is only one subgroup $G \subset E(\mathbb{F}_q)$ of order n. Assume $P \in G$ is a point of order n and ρ is a fast endomorphism of E defined over $\mathbb{F}_q$ with the characteristic polynomial $x^2 + rx + s$. By hypothesis $\rho(P) = [\lambda]P \in E(\mathbb{F}_q)[n]$ and λ is a root of $x^2 + rx + s = 0 \bmod n$. For $k \in [1, n-1]$, the 2-GLV decomposition of $[k]P$ is

$$[k]P = [k_1]P + [k_2]\rho(P), \tag{1}$$

where k_1 and $k_2 \in \mathbb{Z}$ are bounded by $c\sqrt{n}$ for some constant $c > 0$. To compute the coefficients k_1 and k_2, Gallant et al. [1] constructed the reduction map

$$f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (i, j) \mapsto i + \lambda j \mod n.$$

Since f is of finite image, its kernel

$$\mathcal{K} := \{(i, j) \mid i + \lambda j = 0 \mod n\} \tag{2}$$

is a sublattice of $\mathbb{Z} \times \mathbb{Z}$ of full rank. Gallant et al. exploited an efficient algorithm, the Cornacchia's algorithm, to compute a short basis of $\mathcal{K}$. Assume that υ_1, υ_2 are two linearly independent vectors of $\mathcal{K}$ satisfying $\max\{|\upsilon_1|, |\upsilon_2|\} < c\sqrt{n}$ for some positive constant c, where $|\cdot|$ denotes the maximum norm. Express $(k, 0) = \beta_1\upsilon_1 + \beta_2\upsilon_2$ where $\beta_i \in \mathbb{Q}$ and then round β_i to the nearest integer b_i. Then $(k_1, k_2) = (k, 0) - (b_1, b_2)$ satisfies the decomposition condition. By further analysis in [9], one can choose the constant $c = \sqrt{1 + |r| + s}$.

Remark 1. *Gallant et al. provided examples of curves with a fast endomorphism ϕ given by complex multiplication by $\sqrt{-1}$ ($j = 1728$), $\frac{-1+\sqrt{-3}}{2}$ ($j = 0$), $\sqrt{-2}$ ($j = 8000$), $\sqrt{-3}$ ($j = 54000$), $\frac{1+\sqrt{-7}}{2}$ ($j = -3375$) and $\frac{1+\sqrt{-11}}{2}$ ($j = -32768$). In particular, the endomorphism ring of these curves is equal to $\mathbb{Z}[\phi]$, which is either the maximal order of its field of fractions, or (exceptionally) an order of index two in the maximal order. These curves are called GLV curves.*

2.2 The GLS elliptic curves

Galbraith, Lin and Scott [3] implemented the 2-GLV method by using an efficiently computable endomorphism on a large class of elliptic curves. Let E be an elliptic curve defined over $\mathbb{F}_p$ and $E'/\mathbb{F}_{p^2}$ be a twist of $E/\mathbb{F}_p$. By the definition of twist in [11], E and E' are isomorphic over $\mathbb{F}_{p^{2d}}$ with the degree of twist $d \in \{2, 3, 4, 6\}$. Galbraith, Lin and Scott described how to obtain the 2-GLV decomposition on $E'(\mathbb{F}_{p^2})$ for $d = 2$ and the 4-GLV decompositions on $E'(\mathbb{F}_{p^2})$ for $d = 4$ and 6.

Theorem 1 ([3])**.** *Let $p > 3$ be a prime and E an 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 $n \mid \#E'(\mathbb{F}_{p^2})$ such that $n > 2p$ and $\psi = \tau\pi_0\tau^{-1}$. The characteristic equation of ψ is $\psi^2 - t_{\pi_0}\psi + p = 0$. $\psi^2(P) + P = \mathcal{O}_{E'}$ for $P \in E'(\mathbb{F}_{p^2})$. Moreover, for $P \in E'(\mathbb{F}_{p^2})[n]$, we have $\psi(P) = [\mu]P$ where $\mu \equiv t_{\pi_0}^{-1}(p - 1) \mod n$.*

Consider the lattice $\mathcal{K} = \{(i, j) \in \mathbb{Z}^2 \mid i + \mu j \equiv 0 \mod n\}$. Galbraith et al. used the basis $\{(t_{\pi_0}, p - 1), (1 - p, t_{\pi_0})\}$ of some lattice $\mathcal{K}' \subset \mathcal{K}$ to get the 2-dimensional decomposition, with each coefficient bounded by $(p + 1)/\sqrt{2}$.

To construct a 4-GLV decomposition, it is necessary to use twists of degree 4 or 6. Hence the only two examples of interest are $y^2 = x^3 + b$ (having a sextic twist) and $y^2 = x^3 + ax$ (having a quartic twist) with $a, b \in \mathbb{F}_p^*$. Here we only recall the case of constructing a 4-GLV decomposition on the sextic twist of a curve with j-invariant 0.

Theorem 2 ([3]). *Let $p \equiv 1 \mod 6$ and $E : y^2 = x^3 + b$ ($b \in \mathbb{F}_p^*$). Choose $\omega \in \mathbb{F}_{p^{12}}^*$ such that $\omega^6 \in \mathbb{F}_{p^2}$ and set $E' : y^2 = x^3 + \omega^6 b$. Then $E'/\mathbb{F}_{p^2}$ is a sextic twist of $E(\mathbb{F}_{p^2})$ with the twist isomorphism $\tau : E \to E'$, $\tau(x, y) = (\omega^2 x, \omega^3 y)$. Then $\psi = \tau\pi_0\tau^{-1}$ is an endomorphism of E' given by $\psi(x, y) = (\omega^2 x^p/\omega^{2p}, \omega^3 y^p/\omega^{3p})$, which is defined over $\mathbb{F}_{p^2}$. The characteristic equation of ψ is $\psi^2 - t_{\pi_0}\psi + p = 0$. For $P \in E'(\mathbb{F}_{p^2})$, we have $\psi^4(P) - \psi^2(P) + P = \mathcal{O}_{E'}$.*

Hence, the 4-GLV decomposition can be efficiently applied to these curves. Let $n > 2p$ be a prime factor of $\#E'(\mathbb{F}_{p^2})$. For $P \in E'(\mathbb{F}_{p^2})[n]$ and $k \in [1, n-1]$, $[k]P$ can be decomposed as

$$[k]P = [k_1]P + [k_2]\psi(P) + [k_3]\psi^2 P + [k_4]\psi^3(P). \tag{3}$$

Hu et al. [7] described the complete implementation of the 4-GLV method on GLS curves with j-invariant 0. They essentially exploited a specific way and led to an almost optimal upper bound of coefficients $2\sqrt{2}p = O(2\sqrt{2}n^{1/4})$.

Remark 2. *The characteristic equation of ψ is $\psi^2 - t_{\pi_0}\psi + p = 0$, for any point $Q \in E'(\bar{\mathbb{F}}_{p^2})$, we have $\psi^2(Q) - t_{\pi_0}\psi(Q) + [p]Q = \mathcal{O}_{E'}$. Furthermore, when ψ acts on points in $E'(\mathbb{F}_{p^2})$, it also satisfies $\psi^2 + 1 = 0$ or a quartic equation for the degree of twist 2 or 4,6. Here, we call the endomorphism restricted to points in $E'(\mathbb{F}_{p^2})$ the "restricted" endomorphism. 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-GLV decomposing method using the "restricted" endomorphism ψ with $\psi^2 + 1 = 0$ is called the GLS method.*

2.3 Combining GLV and GLS (GLV+GLS)

Longa and Sica [5] showed how to get a 4-GLV decomposition for twists of any GLV curve over $\mathbb{F}_{p^2}$. Let $E/\mathbb{F}_p$ be a GLV curve. As in §2.2, let $E'/\mathbb{F}_{p^2}$ be a quadratic twist of E via the twist map $\tau : E \to E'$. Let ρ be the GLV endomorphism coming with the definition of a GLV curve. Then ρ satisfies the equation $\rho^2 + r\rho + s = 0$. We thus get two endomorphisms $\phi = \tau\rho\tau^{-1}$ and $\psi = \tau\pi_0\tau^{-1}$ of E', both defined over $\mathbb{F}_{p^2}$. For $P \in E'(\mathbb{F}_{p^2})$ of a large prime order n, then ϕ and ψ satisfy $\phi^2(P) + r\phi(P) + sP = \mathcal{O}_{E'}$ and $\psi^2(P) + P = \mathcal{O}_{E'}$ respectively. For any scalar $k \in [1, n-1]$, we obtain a 4-GLV decomposition

$$[k]P = [k_1]P + [k_2]\phi(P) + [k_3]\psi(P) + [k_4]\phi\psi(P) \quad \text{with} \quad \max_i(|k_i|) < 2Cn^{1/4} \tag{4}$$

for some constant C.

Similar to the 2-GLV method, we consider the 4-GLV reduction map $F : \mathbb{Z}^4 \to \mathbb{Z}/n\mathbb{Z}$ with respect to $\{1, \phi, \psi, \phi\psi\}$. It is easy to know $\mathcal{L} := \ker F$ is a full sublattice of $\mathbb{Z}^4$. To compute a short basis of $\mathcal{L}$, Longa and Sica proposed the twofold Cornacchia-type algorithm under the assumption that the "restricted" endomorphisms ϕ and ψ are $\mathbb{Z}$-linearly independent. Review the implementation of the algorithm: the "restricted" endomorphism ψ satisfies $\psi^2 + 1 = 0$, then $\mathbb{Q}(\psi) = \mathbb{Q}(i)$ and $\mathbb{Q}(\phi, i)$ is a biquadratic (Galois of degree 4, with Galois group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) number field. They considered the ring $\mathbb{Z}[\phi, i]$ of $\mathbb{Q}(\phi, i)$ to factor the reduction map F and constructed the twofold Cornacchia-type algorithm, which is an easy-to-implement algorithm in two parts, the first part in $\mathbb{Z}$ and the second part in $\mathbb{Z}[i]$. In particular, for the case $E/\mathbb{F}_p$ with j-invariant 1728, this can be treated separately with a quartic twist as described in [5, Appendix B].

The twofold algorithm is efficient, but more importantly, it gives a better and uniform upper bound with constant $C = 51.5\sqrt{1 + |r| + s}$. Recently, Yi et al. [8] obtained an improved twofold Cornacchia-type algorithm and showed that it possesses a better theoretic bound of output $Cn^{1/4}$ with $C = 3.41\sqrt{1 + |r| + s}$. In particular, their proof is much simpler than Longa and Sica's.

Remark 3. *When E' is ordinary, we always have $\mathbb{Q}(\phi) = \mathbb{Q}(\psi)$ for $\phi, \psi \in \mathrm{End}(E')$. Even so, Longa and Sica's algorithm can still be implemented on ordinary curves over $\mathbb{F}_{p^2}$. Since they consider the "restricted" endomorphisms ϕ and ψ acting on $E'(\mathbb{F}_{p^2})$, in this case, $\phi^2 + r\phi + s = 0$ and $\psi^2 + 1 = 0$. The assumption that the two "restricted" endomorphisms, when viewed as algebraic integers, generate disjoint quadratic extensions of $\mathbb{Q}$, holds on some ordinary curves, see examples in [5, §8].*

2.4 Ready-Made short bases on GLV, GLS or GLV+GLS

Galbraith, Lin, and Scott [3] and Benjamin Smith [18] have already constructed families of endomorphisms equipped with a convenient ready-made basis. Then Smith [17] generalized these ready-made bases to all of the other known efficient endomorphism constructions for elliptic curves and to real multiplication techniques for genus 2 Jacobians.

First, we review some results in [17], from which we can see that to produce the ready-made basis is mostly based on the simple order relations.

Lemma 1 ([17])**.** *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'.

Following the Lemma, Smith gave general two-dimensional decompositions for elliptic curves.

Theorem 3 ([17]). *Let $E/\mathbb{F}_q$ be an ordinary elliptic curve. If π is the q-power Frobenius endomorphism on E and let ϕ be a non-integer endomorphism of E such that $\mathbb{Z}[\pi] \subset \mathbb{Z}[\phi]$, so $\pi = c\phi + b$ for some integers c and b. The vectors*

$$\mathbf{b}_1 = (b-1, c) \quad \textit{and} \quad \mathbf{b}_2 = (c\deg(\phi) + (b-1)t_\phi, 1-b)$$

generate a sublattice of $\mathcal{K}$ (see Equ. (2)) of determinant $\#E(\mathbb{F}_q)$. If $G = \#E(\mathbb{F}_q)$, then $\mathcal{K} = \langle \mathbf{b}_1, \mathbf{b}_2 \rangle$. If $E(\mathbb{F}_q) \cong G \oplus \mathbb{Z}/2\mathbb{Z}$ or $G \oplus (\mathbb{Z}/2\mathbb{Z})^2$, the following simple procedure produces a basis for $\mathcal{K}$:

- *If c is even, then $\mathcal{K} =< \frac{1}{2}\mathbf{b}_1, \frac{1}{2}\mathbf{b}_2 >$.*
- *If c and b are odd and $deg(\phi)$ is even, then $\mathcal{K} =< \mathbf{b}_1, \frac{1}{2}\mathbf{b}_2 >$.*
- *Otherwise, $\mathcal{K} =< \mathbf{b}_1, \frac{1}{2}(\mathbf{b}_1 + \mathbf{b}_2) >$.*

In this way, he constructed explicit short bases for the GLV [1], GLS [3], GLV+GLS [5], Guillevic–Ionica [6], and $\mathbb{Q}$-curve reduction techniques [18], as well as for the Kohel–Smith [19] and Takashima [20] methods for genus 2 Jacobians. Smith [17] can not pretend that the method is a significant optimization for scalar decomposition methods, the construction of these "instant" bases turns out to be an illuminating exercise.

In this paper, we only recall the four-dimensional decompositions for GLV+GLS in [17]. Let $E/\mathbb{F}_p$ be an elliptic curve with a fast endomorphism ρ satisfying $\rho^2 + r\rho + s = 0$. 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 quadratic twist of $E(\mathbb{F}_{p^2})$ and $\tau : E \to E'$ be the twist isomorphism defined over $\mathbb{F}_{p^4}$. Let $\phi = \tau\rho\tau^{-1}$ and $\psi = \tau\pi_0\tau^{-1}$. The characteristic equations of ϕ and ψ are $\phi^2 + r\phi + s = 0$ and $\psi^2 - t_{\pi_0}\psi + p = 0$ respectively. Moreover, the "restricted" endomorphism ψ also satisfies $\psi^2 + 1 = 0$. Let $G \subset E'(\mathbb{F}_{p^2})$ be a cyclic subgroup of large prime order n. 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, $\mathbb{Z}[\phi]$ 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

$$b = \frac{1}{2}(t_{\pi_0} - ct_\phi) \text{ and } c^2 = \frac{t_{\pi_0}^2 - 4p}{t_\phi^2 - 4n_\phi}. \tag{5}$$

Theorem 4 ([17]). *With ϕ and ψ defined as above, suppose we can construct a 4-GLV decomposition with $(1, \phi, \psi, \phi\psi)$. The vectors*

$$\mathbf{b}_1 = (1, 0, b, c), \qquad \mathbf{b}_2 = (0, 1, -cn_\phi, ct_\phi + b),$$
$$\mathbf{b}_3 = (-b, -c, 1, 0), \qquad \mathbf{b}_4 = (cn_\phi, -ct_\phi - b, 0, 1).$$

generate a sublattice of determinant $\#E'(\mathbb{F}_{p^2})$ in $\mathcal{L}$ (see the difinition in §2.3). If $G = E'(\mathbb{F}_{p^2})$, then $\mathcal{L} = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4 \rangle$.

Smith used relations between orders of quadratic fields to produce short lattice vectors. His method is mainly adapt to ordinary curves. Due to the perception of the Menezes–Okamoto–Vanstone and Frey–Rück reductions [25, 26] as "attacks," supersingular curves are widely believed to be "weak" curves and thus not desirable for cryptographic applications. Therefore, in practical applications, ordinary curves are mainly used. In this paper, we mainly consider the implementation of our work on ordinary curves.

3 Supplements to Smith's method on 4-GLV decompositions

Smith's method in §2.4 is only for quadratic twisted curves over $\mathbb{F}_{p^2}$ with the "restricted" endomorphism ψ satisfing $\psi^2 - t_{\pi_0}\psi + p = 0$ and $\psi^2 + 1 = 0$. In this paper, we consider the case of twisted curves over $\mathbb{F}_{p^2}$ of degree 4 or 6 and provide ready-made short bases for 4-GLV decompositions on these curves.

In the following, let $E/\mathbb{F}_p$ be a GLV curve with a fast endomorphism ρ, the j-invariant of E is 0 or 1728. 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 or sextic twist of $E(\mathbb{F}_{p^2})$ and $\tau : E \to E'$ be the twist isomorphism. Defining $\phi = \tau\rho\tau^{-1}$ 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, $\mathbb{Z}[\phi]$ is the maximal order of the endomorphism algebra of E' for the case j-invariant 0 or 1728, it is therefore reasonable to assume $\mathbb{Z}[\psi]$ 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.

Now, we give ready-made short bases for 4-GLV decompositions on quartic or sextic twisted curves over $\mathbb{F}_{p^2}$.

Theorem 5. *If $E/\mathbb{F}_p$ is an elliptic curve with j-invariant 1728, ρ satisfies $\rho^2 + 1 = 0$. $E'/\mathbb{F}_{p^2}$ is a quartic twist of $E(\mathbb{F}_{p^2})$ and $\tau : E \to E'$ is defined over $\mathbb{F}_{p^8}$. With ϕ and ψ defined as above, the characteristic equations of ϕ and ψ are $\phi^2 + 1 = 0$ and $\psi^2 - t_{\pi_0}\psi + p = 0$ respectively. Moreover, the "restricted" endomorphism ψ also satisfies $\psi^4 + 1 = 0$. With ϕ and ψ, we can construct a 4-GLV*

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* $\mathcal{L}$. *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 case that $E'/\mathbb{F}_{p^2}$ is a quartic twisted curve of E, the proof is similar to that of Theorem 5. For the proof of the "restricted" endomorphism ψ satisfying $\psi^4 + 1 = 0$, see [3, §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

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

corresponding to the vectors $\mathbf{b}_3$ and $\mathbf{b}_4$. Note that the "restricted" endomorphism $\pm\psi^2$ satisfies the characteristic equation $x^2+1 = 0$ and so acts the same as ϕ on $E'(\mathbb{F}_{p^2})$. Changing ψ to $-\psi$ if necessary, here we identify ϕ with ψ^2. Multiplying the relations above through by λ_ψ, using $\lambda_\psi^2 = \lambda_{\psi^2} = \lambda_\phi \mod n$ and $\lambda_\phi^2 = -1$, we obtain new relations

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

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

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

Theorem 6. *If* $E/\mathbb{F}_p$ *is an elliptic curve with j-invariant 0,* ρ *satisfies* $\rho^2 + \rho + 1 = 0$. $E'/\mathbb{F}_{p^2}$ *is a sextic twist of* $E(\mathbb{F}_{p^2})$ *and* $\tau : E \to E'$ *is defined over* $\mathbb{F}_{p^{12}}$. *With* ϕ *and* ψ *defined as above, the characteristic equations of* ϕ *and* ψ *are* $\phi^2 + \phi + 1 = 0$ *and* $\psi^2 - t_{\pi_0}\psi + p = 0$ *respectively. Moreover, the "restricted" endomorphism* ψ *also satisfies* $\psi^4 - \psi^2 + 1 = 0$. *With* ϕ *and* ψ, *we can construct a 4-GLV decomposition with* $(1, \phi, \psi, \phi\psi)$. *Then 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* $\mathcal{L}$. *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 proof of the "restricted" endomorphism ψ satisfying $\psi^4 - \psi^2 + 1 = 0$, see [3, §3]. Note that the "restricted" endomorphism $-\psi^2$ satisfies the characteristic equation $x^2 + x + 1 = 0$ and so acts as the same as ϕ on $E'(\mathbb{F}_{p^2})$. Similar to the proof of Theorem 5 with $t_\phi = -1, n_\phi = 1$, we can get the short vectors immediately by $\lambda_\psi^2 = \lambda_{\psi^2} = -\lambda_\phi \mod n$ and $\lambda_\phi^2 = -\lambda_\phi - 1 \mod n$. Also, the claim that $\det(< \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4 >) = \#E'(\mathbb{F}_{p^2})$ will be proved later. □

The rest proof of Theorem 5 and 6. To verify $\det(<\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3,\mathbf{b}_4>) = \#E'(\mathbb{F}_{p^2})$, we need recall some results for the case $q = p^2$ in [24, 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 $\mathbb{F}_{p^2}$.

Proposition 1 ([24]). *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 $c^2 = \frac{4p-t_{\pi_0}^2}{4}$, we have

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

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 $c^2 = \frac{4p-t_{\pi_0}^2}{3}$, we have

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

So far, we have completed the proof of Theorem 5 and 6.

Smith did not pretend that the ready-made short bases represents a significant optimization in scalar multiplication, but it does give a better insight into the structure of scalar decompositions. It is always more convenient to use a ready-made short basis than it is to compute a new one. Longa and Sina's algorithm [5] or an improved algorithm [8] is also an easy-to-implement and an evry efficient algorithm with complexity $O(\log^2(n))$. Importantly, the output (i.e. short bases) of these algorithms have an exact upper bound, such as $51.5(\sqrt{1+|r|+s})n^{1/4}$ or $3.41(\sqrt{1+|r|+s})n^{1/4}$. In practical applications, users could choose which method to use according to their preferences. In this paper, we will focus on exploring more potential of Longa and Sica's algorithm and construct a new twofold Cornacchia-type algorithm.

4 A new twofold Cornacchia-type algorithm

4.1 Analysis of the new twofold algorithm

First, we consider a curve which has two fast endomorphisms ϕ, ψ with minimal polynomials x^2+x+1 and x^2+rx+s respectively. Let λ and μ be the eigenvalues of ϕ and ψ on a cyclic subgroup of order n, respectively, $\lambda, \mu \in [0, n-1]$. Viewing ϕ and ψ as algebraic integers, then $\mathbb{Q}(\phi) = \mathbb{Q}(\sqrt{-3})$. Moreover, Changing ϕ to $-\phi$ if necessary, then we may identify ϕ with $\omega = \frac{-1+\sqrt{-3}}{2}$. Assume $\mathbb{Q}(\psi) \neq \mathbb{Q}(\sqrt{-3})$, then $K = \mathbb{Q}(\phi, \psi)$ is a biquadratic number field. Let O_K be its ring of integers.

The existence of λ and μ above means that n splits in $\mathbb{Q}(\phi)$ and $\mathbb{Q}(\psi)$, thus n splits completely in K. Hence there exists a prime ideal $\mathfrak{n}$ of O_K of norm n dividing nO_K. Let $\mathfrak{n}' = \mathfrak{n} \cap \mathbb{Z}[\phi, \psi]$ and $\mathfrak{n}'' = \mathfrak{n} \cap \mathbb{Z}[\omega]$. The inclusions $\mathbb{Z} \hookrightarrow \mathbb{Z}[\omega] \hookrightarrow \mathbb{Z}[\phi, \psi] \hookrightarrow O_K$ induce isomorphisms $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}[\omega]/\mathfrak{n}'' \cong \mathbb{Z}[\phi, \psi]/\mathfrak{n}' \cong O_K/\mathfrak{n}$. In particular we can suppose $\phi \equiv \lambda \mod \mathfrak{n}'$ and $\psi \equiv \mu \mod \mathfrak{n}'$. Consider the map F:

$$F : \mathbb{Z}^4 \to \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}[\phi, \psi]/\mathfrak{n}', \quad (x_1, x_2, x_3, x_4) \mapsto x_1 + x_2\lambda + x_3\mu + x_4\lambda\mu \mod n. \tag{6}$$

Then F is a surjective homomorphism and $\ker F = f^{-1}(\mathfrak{n}')$ is a full sublattice of $\mathbb{Z}^4$ of index n where f is the isomorphism $\mathbb{Z}^4 \to \mathbb{Z}[\phi, \psi]$, $(x_1, x_2, x_3, x_4) \mapsto x_1 + x_2\phi + x_3\psi + x_4\phi\psi$.

We identify $\mathbb{Z}[\phi, \psi]$ with the free $\mathbb{Z}[\omega]$-module of rank 2 with basis $\{e_1, e_2\} = \{1, \psi\}$. To find a short $\mathbb{Z}$-basis of $\mathfrak{n}'$, we first find out a generator $\nu = a + b\omega$ of $\mathfrak{n}''$ in the Euclidean domain $\mathbb{Z}[\omega]$, which is equivalent to finding $a, b \in \mathbb{Z}$ such that $a^2 - ab + b^2 = n$. This can be achieved by using the first Cornacchia's algorithm in $\mathbb{Z}$ (see §4.2 Algorithm 1). Then $\nu = \nu e_1$ and $\psi - \mu = -\mu e_1 + e_2$ are both in $\mathfrak{n}'$, and $\{\nu e_1, -\mu e_1 + e_2\}$ generates a sub-$\mathbb{Z}[\omega]$-module of $\mathbb{Z}[\phi, \psi]$ of index n, so this submodule must be $\mathfrak{n}'$, i.e.,

$$\mathfrak{n}' = \nu\mathbb{Z}[\omega] + (\psi - \mu)\mathbb{Z}[\omega]. \tag{7}$$

We now use the second Cornacchia's algorithm in $\mathbb{Z}[\omega]$ to find a short $\mathbb{Z}[\omega]$-basis $\{v_1, v_2\}$ of $\mathfrak{n}'$ (see §4.2 Algorithm 2) with $\max_i(|v_i|) \leq Cn^{1/4}$ for some constant $C > 0$. Thus we get a short $\mathbb{Z}$-basis $\{v_1, v_1\omega, v_2, v_2\omega\}$ of $\mathfrak{n}'$. Moreover, write $v_1 = (a_1 + b_1\omega) + (c_1 + d_1\omega)\psi$ and $v_2 = (a_2 + b_2\omega) + (c_2 + d_2\omega)\psi$, then

$$\mathfrak{n}' = (a_1 + b_1\omega + (c_1 + d_1\omega)\psi)\mathbb{Z}[\omega] + (a_2 + b_2\omega + (c_2 + d_2\omega)\psi)\mathbb{Z}[\omega]. \tag{8}$$

By $\ker F = f^{-1}(\mathfrak{n}')$, we get a short basis of $\ker F$, which are the rows of the following matrix.

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ -b_1 & a_1 - b_1 & -d_1 & c_1 - d_1 \\ a_2 & b_2 & c_2 & d_2 \\ -b_2 & a_2 - b_2 & -d_2 & c_2 - d_2 \end{pmatrix}. \tag{9}$$

Let $\{\widetilde{v}_1, \widetilde{v}_2, \widetilde{v}_3, \widetilde{v}_4\}$ be the rows of the matrix (9) with $\max_i(|\widetilde{v}_i|) \leq Cn^{1/4}$. For any $k \in [1, n-1]$, write $(k,0,0,0) = \sum_{j=0}^{4} \beta_j \widetilde{v}_j$ with $\beta_j \in \mathbb{Q}$. Then $v := \sum_{j=0}^{4} \lfloor \beta_j \rceil \widetilde{v}_j \in \ker F$. Let $\kappa = (k_1, k_2, k_3, k_4) = (k,0,0,0) - v$. By the triangle inequality, $|\kappa| = |\sum_{i=1}^{4} (\lfloor \beta_i \rceil - \beta_i)\widetilde{v}_i| \leq 4 \times \frac{1}{2} \max_i(|\widetilde{v}_i|) \leq 2Cn^{1/4}$. Then

$$[k]P = [k_1]P + [k_2]\phi(P) + [k_3]\psi(P) + [k_4]\phi\psi(P) \text{ with } \max_i(|k_i|) \leq 2Cn^{1/4}.$$

Second, we consider a curve which has an endomorphism ψ satisfing $\psi^4 - \psi^2 + 1 = 0$. Hence the 4-GLV decomposition can be implemented on the curve as described as in (3). View ψ as an algebraic integer satisfying $x^4 - x^2 + 1 = 0$. Let $K = \mathbb{Q}(\psi)$ be the quartic extension over $\mathbb{Q}$ and O_K be the ring of integers of K. Since ψ is a primitive 12-th root of unity, then $K/\mathbb{Q}$ is a Galois extension and $O_K = \mathbb{Z}[\psi]$. Let μ be the eigenvalue of ψ on a cyclic subgroup of order n, then $\pm\mu$ and $\pm\mu^{-1}$ are the roots of $x^4 - x^2 + 1 = 0$ in $\mathbb{F}_n$, which means that n splits completely in O_K. Denote by $\mathfrak{n}'$ the prime ideal lying over n which contains n and $\psi - \mu$. We also get a map

$$F : \mathbb{Z}^4 \to \mathbb{Z}/n\mathbb{Z} \cong O_K/\mathfrak{n}', \quad (x_1, x_2, x_3, x_4) \mapsto x_1 + x_2\mu + x_3\mu^2 + x_4\mu^3 \mod n. \tag{10}$$

To compute a short basis of $\ker F$ is equivalent to computing a short basis of $\mathfrak{n}'$. Note that $\phi := -\psi^2$ satisfies $x^2 + x + 1 = 0$, hence $\mathbb{Z}[\phi] = \mathbb{Z}[\omega] \subset O_K$. Let $\lambda := -\mu^2 \mod n$, using Algorithm 1 on input n, λ, we can get a generator $\nu = a + b\omega$ of $\mathfrak{n}' \cap \mathbb{Z}[\omega]$. Subsequently, $\mathfrak{n}' = \nu\mathbb{Z}[\omega] + (\psi - \mu)\mathbb{Z}[\omega]$, then we use Algorithm 2 on input ν, μ to find a short $\mathbb{Z}[\omega]$-basis $\{v_1, v_2\}$ of $\mathfrak{n}'$. Moreover, in this case, the new twofold Cornacchia-type algorithm can be used for scalar decomposition as well.

Remark 4. *Our method is a variation of the method by Longa and Sica [5] and Yi et al. [8]. In the second Cornacchia's algorithm we use the extended Euclidean algorithm on the Euclidean domain $\mathbb{Z}[\omega]$ instead of $\mathbb{Z}[i]$. See the following relationship diagram.*

$$\begin{array}{cc} \mathbb{Z}[\phi, i] & \mathfrak{n}' \\ \uparrow & \uparrow \\ \mathbb{Z}[i] & \nu\mathbb{Z}[i] \\ \uparrow & \uparrow \\ \mathbb{Z} & n \end{array} \longrightarrow \begin{array}{cc} \mathbb{Z}[\psi, \omega] & \mathfrak{n}' \\ \uparrow & \uparrow \\ \mathbb{Z}[\omega] & \nu\mathbb{Z}[\omega] \\ \uparrow & \uparrow \\ \mathbb{Z} & n \end{array}$$

Method in [5, 8] *Our method*

Moreover, we observe that the second Cornacchia's algorithm can also implemented on orders of imaginary quadratic fields which are Euclidean, for example, the orders $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$. The analysis is similar to the analysis above and the corresponding algorithms are similar to the algorithms below, just paying attention to the different norms when implementing the second Cornacchia's algorithm.

4.2 Specific algorithm

We now describe our new twofold Cornacchia-type algorithm to compute 4-GLV decomposition coefficients. The first part is to find $\nu = a + b\omega \in \mathbb{Z}[\omega]$ such that $\mathrm{Norm}(\nu) = a^2 - ab + b^2 = n$. We can find ν by Cornacchia's algorithm in $\mathbb{Z}$, which is a truncated form of the extended Euclidean algorithm.

Algorithm 1: The first part of the new algorithm

Input: n, $1 < \lambda < n$ such that $\lambda^2 + \lambda + 1 \equiv 0 \mod n$, i.e, $\lambda \equiv \omega \mod n$.
Output: $\nu = a + b\omega$ dividing n, such that $\nu P = 0$.

1. **initialize**
   $r_0 \leftarrow n$, $r_1 \leftarrow \lambda, r_2 \leftarrow n$,
   $t_0 \leftarrow 0$, $t_1 \leftarrow 1, t_2 \leftarrow 0$,
   $q \leftarrow 0$.
2. **main loop**
   while $r_2^2 \geq n$ do
   $q \leftarrow \lfloor r_0/r_1 \rfloor$,
   $r_2 \leftarrow r_0 - qr_1, r_0 \leftarrow r_1, r_1 \leftarrow r_2$,
   $t_2 \leftarrow t_0 - qt_1, t_0 \leftarrow t_1, t_1 \leftarrow t_2$.

return: $\nu = r_1 - \omega t_1,\ a = r_1,\ b = -t_1$

Lemma 2. *Algorithm 1 is valid and the output $\nu = r_1 - \omega t_1$ is really lying over n, i.e., $\nu(P) = 0$.*

Proof. Let $\lambda \in [1, n-1]$ such that $\lambda \equiv \omega \mod n$, with ω being defined by $\phi(P) = \omega P$. To compute the g.c.d of n and λ, the extended Euclidean algorithm produces three terminating sequences of integers $(r_j)_{j\geq 0}$, $(s_j)_{j\geq 0}$ and $(t_j)_{j\geq 0}$ such that

$$\begin{pmatrix} r_{j+2} & s_{j+2} & t_{j+2} \\ r_{j+1} & s_{j+1} & t_{j+1} \end{pmatrix} = \begin{pmatrix} -q_{j+1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{j+1} & s_{j+1} & t_{j+1} \\ r_j & s_j & t_j \end{pmatrix}, \tag{11}$$

for some integers $q_{j+1} > 0$ and the initial data

$$\begin{pmatrix} r_1 & s_1 & t_1 \\ r_0 & s_0 & t_0 \end{pmatrix} = \begin{pmatrix} \lambda & 0 & 1 \\ n & 1 & 0 \end{pmatrix}. \tag{12}$$

This means that at step $j \geq 0$,

$$r_j = q_{j+1}r_{j+1} + r_{j+2}, \quad s_j = q_{j+1}s_{j+1} + s_{j+2}, \quad t_j = q_{j+1}t_{j+1} + t_{j+2}.$$

The sequences (r_j), (s_j) and (t_j) with $q_{j+1} = \lfloor r_j/r_{j+1} \rfloor$ satisfy the following properties, valid for all $j \geq 0$:

P1 $r_j > r_{j+1} \geq 0$ and $q_{j+1} \geq 1$,

P2 $(-1)^j s_j \geq 0$ and $|s_j| < |s_{j+1}|$ (this last inequality valid for $j \geq 1$),

P3 $(-1)^{j+1} t_j \geq 0$ and $|t_j| < |t_{j+1}|$,

P4 $s_{j+1} r_j - s_j r_{j+1} = (-1)^{j+1} \lambda$,

P5 $t_{j+1} r_j - t_j r_{j+1} = (-1)^j n$,

P6 $n s_j + \lambda t_j = r_j$.

P5 can be reformulated as

$$|s_{j+1} r_j| + |s_j r_{j+1}| = \lambda \text{ and } |t_{j+1} r_j| + |t_j r_{j+1}| = n. \tag{13}$$

The algorithm stops at m when $r_m \geq \sqrt{n}$ and $r_{m+1} < \sqrt{n}$. For $j = m$ in (13), this yields $|t_{m+1} r_m| < n$ or $|t_{m+1}| < \sqrt{n}$. Since by P6, we have $r_{m+1} - \lambda t_{m+1} = n s_{m+1} \equiv 0 \mod n$, we deduce that

$$r_{m+1}^2 + r_{m+1} t_{m+1} + t_{m+1}^2 = (r_{m+1} - \lambda t_{m+1})(r_{m+1} + \lambda t_{m+1} + t_{m+1}) \equiv 0 \mod n.$$

Moreover, since $t_{m+1} \neq 0$ by P3,

$$0 < r_{m+1}^2 + r_{m+1} t_{m+1} + t_{m+1}^2 = (r_{m+1} + \frac{1}{2} t_{m+1})^2 + \frac{3}{4} t_{m+1}^2 < \frac{9}{4} n + \frac{3}{4} n = 3n,$$

which implies that $r_{m+1}^2 + r_{m+1} t_{m+1} + t_{m+1}^2 = n$ or $2n$. Since $r_{m+1}^2 + r_{m+1} t_{m+1} + t_{m+1}^2 \not\equiv 2 \mod 4$ but $2n \equiv 2 \mod 4$ (n is a prime), $r_{m+1}^2 + r_{m+1} t_{m+1} + t_{m+1}^2 \neq 2n$. Therefore $r_{m+1}^2 + r_{m+1} t_{m+1} + t_{m+1}^2 = n$. For $\nu = r_{m+1} - \omega t_{m+1}$, $\nu \overline{\nu} = n$. Since n splits in $\mathbb{Z}[\omega]$, ν and $\overline{\nu}$ are the two primes above n. Finally $\nu \overline{\nu}(P) = [n]P = 0$ implies either $\overline{\nu}(P) = 0$ or $\nu(P) = 0$. □

We have seen how to construct ν by the Cornacchia's algorithm in $\mathbb{Z}$. From the analysis in §4.1, $\mathfrak{n}'$ is the sub-$\mathbb{Z}[\omega]$-module of $\mathbb{Z}[\phi, \psi]$ or $\mathbb{Z}[\psi]$ generated by $(\nu, 0)$ and $(-\mu, 1)$ under the basis $\{1, \psi\}$ if $\psi^2 + r\psi + s = 0$ or $\psi^4 - \psi^2 + 1 = 0$. Similar to the GLV original paper [1], we can use the extended Euclidean algorithm to the pair (ν, μ) on $\mathbb{Z}[\omega]$ to get a short basis of $\mathfrak{n}'$.

For the Cornacchia's algorithm in $\mathbb{Z}[\omega]$, we also have three such sequences. In the j-th step with $r_j = q_{j+1} r_{j+1} + r_{j+2}$, positive quotient q_{j+1} and nonnegative remainder r_{j+2} are not available in $\mathbb{Z}[\omega]$. We will choose q_{j+1} as the closest integer to r_j / r_{j+1} denoted by $\lfloor r_j / r_{j+1} \rceil$ (see the following Lemma 3). Let us note that P4-P6 of Lemma 2 still hold and P1 holds in modulus (in particular, the algorithm terminates). Hence the (13), which plays a crucial role in the analysis of Cornacchia's algorithm in $\mathbb{Z}$, becomes invalid in $\mathbb{Z}[\omega]$. For controlling $\{|s_j|\}$, we give a neater and shorter argument (see the following Lemma 4), which is similar to the improved analysis in [8, Lemma 1]. By some deduction we obtain an

optimized terminal condition of the sequence $\{|r_j|\}$, which is an absolute constant independent of the curve.

We give the pseudo-code of Cornacchia's Algorithm in $\mathbb{Z}[\omega]$ in two forms, working with complex numbers (see Algorithm 2) and separating real and imaginary parts (see Algorithm 3 in **Appendi**x). The outputs of Algorithm 3 are a short basis of $\ker F$ as the rows in matrix (9) in §4.1. Note that the *imaginary* part in the Algorithm 3 denotes the coefficient of ω, i.e. the imaginary part of $a + b\omega$ is b. The running time of Algorithm 2, 3, similar to that of Cornacchia's Algorithm in $\mathbb{Z}[i]$, that is $O(\log^2 n)$. One may refer to [5].

Algorithm 2: The second part of the new algorithm—compact form

---

Input: ν prime dividing n rational prime, $1 < \mu < n$ such that $\mu^2 + r\mu + s \equiv 0 \mod n$.

Output: Two vectors in $\mathbb{Z}[\omega]^2$: υ_1, υ_2.

1. **initialize:**
   $r_0 \leftarrow \mu$, $r_1 \leftarrow \nu$, $r_2 \leftarrow n$,
   $s_0 \leftarrow 1$, $s_1 \leftarrow 0$, $s_2 \leftarrow 0$, $q \leftarrow 0$.
2. **main loop:**
   while $2|r_1|^2 \geq (3+\sqrt{3})n^{1/2}$ do
   $q \leftarrow \lfloor r_0/r_1 \rceil$,
   $r_2 \leftarrow r_0 - qr_1$, $r_0 \leftarrow r_1, r_1 \leftarrow r_2$,
   $s_2 \leftarrow s_0 - qs_1$, $s_0 \leftarrow s_1, s_1 \leftarrow s_2$.
3. **compute:**
   $q \leftarrow \lfloor r_0/r_1 \rceil$, $r_2 \leftarrow r_0 - qr_1$, $s_2 \leftarrow s_0 - qs_1$.
4. **return**: $\upsilon_1 = (r_1, -s_1)$,
   $\upsilon_2 = (r_0, -s_0)$ if $\max\{|r_0|, |s_0|\} \leq \max\{|r_2|, |s_2|\}$
   $= (r_2, -s_2)$ otherwise.

4.3 Proof of the upper bound

Theorem 7. *The two vectors υ_1, υ_2 output by Algorithm 2 are $\mathbb{Z}[\omega]$-linearly independent. They belong to $\mathfrak{n}'$ and satisfy* $|\upsilon_1|_\infty \leq \sqrt{\frac{3+\sqrt{3}}{2}} n^{\frac{1}{4}}, |\upsilon_2|_\infty \leq \frac{3+\sqrt{3}}{2}(\sqrt{1+|r|+|s|})n^{\frac{1}{4}}$.

Before proving the Theorem 7, we need the following lemmas. Since in the Algorithm 2, $q_{j+1} \in \mathbb{Z}[\omega]$ is the closest integer to r_j/r_{j+1}. Here, we define a lattice diamond that a diamond of side length one with vertices in $\mathbb{Z}[\omega]$, also a fundamental regin of the lattice $\mathbb{Z}[\omega]$. We single out an lattice diamond with a vertex of modulus 1 (such as, ± 1 or $\pm\omega$) but not containing the origin as a vertex (since $q_{j+1} \neq 0$). First, we discuss a property of the closest point in the lattice $\mathbb{Z}[\omega]$.

Lemma 3. *For any point P of a lattice diamond, different from the vertices, there exists a vertex V_1 which is the closest vertex to P, and satisfy $V_1P \leq \frac{\sqrt{3}}{2}$.*

Proof. This is one case where a picture is worth one thousand words. Refer to Fig. 1, we can easily give an explanation of why the distance works. The dashed circle arcs are centered on the vertices and have radius $\frac{\sqrt{3}}{2}$. Since the dashed disks cover everything, for any point P, by choosing the closest vertex V_1 to P, we have $V_1P \leq \frac{\sqrt{3}}{2}$. □

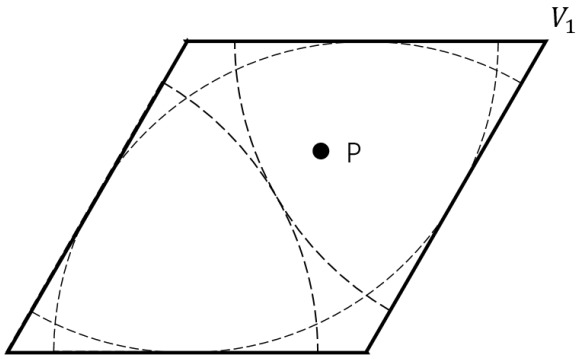

Figure 1: An lattice diamond in $\mathbb{Z}[\omega]$

Let $V_1 := q_{j+1}$ corresponds to the vertice of the lattice diamond, which is the one closest to the point P of affix r_j/r_{j+1} lies in the lattice diamond. When applying Lemma 3, it is essential that we be able to choose from the set of all vertices of the lattice diamond which one is the adequate V_1. Since $q_j \neq 0$, it means that we must be careful to avoid all four diamonds which have the origin as a vertex. So, at all steps $j \geq 0$ we always have $|r_j/r_{j+1}| \geq \sqrt{3}$.

Lemma 4. *If $|\frac{s_j}{s_{j+1}}| < 1$, then we have*

$$|s_{j+1}r_j| \leq \frac{3+\sqrt{3}}{2}|\nu|, \quad |s_jr_{j+1}| \leq \frac{5+\sqrt{3}}{2}|\nu|.$$

Proof. First we have $s_{j+1}r_j - s_jr_{j+1} = (-1)^{j+1}\nu$. If the condition $|\frac{s_j}{s_{j+1}}| < 1$ holds, and noticing that $|r_j/r_{j+1}| \geq \sqrt{3}$, then $|\frac{s_j}{s_{j+1}} \cdot \frac{r_{j+1}}{r_j}| < \frac{1}{\sqrt{3}}$. We can get

$$\left|1 - \frac{s_jr_{j+1}}{s_{j+1}r_j}\right| \geq 1 - \left|\frac{s_jr_{j+1}}{s_{j+1}r_j}\right| \geq 1 - \frac{1}{\sqrt{3}}$$

Together with $s_{j+1}r_j - s_j r_{j+1} = (-1)^{j+1}\nu$ we have

$$|\nu| = |s_{j+1}r_j - s_j r_{j+1}| > \left(1 - \frac{1}{\sqrt{3}}\right)|s_{j+1}r_j|,$$

which implies

$$|s_{j+1}r_j| \leq \frac{1}{1-\frac{1}{\sqrt{3}}}|\nu| = \frac{3+\sqrt{3}}{2}|\nu|.$$

By $|s_j r_{j+1}| = |s_{j+1}r_j + (-1)^j\nu|$, then $|s_j r_{j+1}| \leq \dfrac{5+\sqrt{3}}{2}|\nu|$. □

Lemma 5. *For any nonzero* $(v_1, v_2) \in \mathfrak{n}' \subset \mathbb{Z}[\omega]^2$, *we have*

$$\max(|v_1|, |v_2|) \geq \frac{\sqrt{|\nu|}}{\sqrt{1+|r|+|s|}}.$$

Proof. If $(0,0) \neq (v_1, v_2) \in \mathfrak{n}'$, then $v_1 + \mu v_2 \equiv 0 \mod \nu$. If μ' is the other root of $x^2 + rx + s \mod n$, we get that

$$v_1^2 - r v_1 v_2 + s v_2^2 \equiv (v_1 + \mu v_2)(v_1 + \mu' v_2) \equiv 0 \mod \nu$$

Since x^2+rx+s is irreducible in $\mathbb{Q}(\omega)$ because the two quadratic fields are linearly disjoint, we therefore have $|v_1^2 - r v_1 v_2 + s v_2^2| \geq |\nu|$. On the other hand, if

$$\max(|v_1|, |v_2|) < \frac{\sqrt{|\nu|}}{\sqrt{1+|r|+|s|}},$$

then

$$|v_1^2 - r v_1 v_2 + s v_2^2| \leq |v_1|^2 + |r||v_1||v_2| + s|v_2|^2| < |\nu|,$$

a contradiction. This proof uses an argument already appearing in the proof of the original GLV algorithm [9]. □

Proof. (Proof of Theorem 7). According to the property P4: $s_{j+1}r_j - s_j r_{j+1} = (-1)^{j+1}\nu$ and the property P6: $(r_j, -s_j) = t_j(\nu, 0) + (-s_j)(-\mu, 1)$, the vectors v_1, v_2 belong to $\ker F$.

We denote the output $\{r, s\}$ of the j-th step in the loop of Algorithm 2 by $\{r_{j+1}, s_{j+1}\}$, and assume Algorithm 2 stops at the m-th step. Then $v_1 = (r_{m+1}, -s_{m+1})$ and $|r_m| \geq \sqrt{\frac{3+\sqrt{3}}{2}}n^{\frac{1}{4}}$ and $|r_{m+1}| < \sqrt{\frac{3+\sqrt{3}}{2}}n^{\frac{1}{4}}$. We need to consider two cases. For brevity, we denote two constants $\sqrt{1+|r|+|s|}$, $\sqrt{\frac{3+\sqrt{3}}{2}}$ by c_1, c_2 respectively.

Case 1: $\left|\frac{s_m}{s_{m+1}}\right| < 1$. Using Lemma 4 we have $|s_{m+1}| \le c_2\sqrt{|\nu|}$, together with $|r_{m+1}| < c_2\sqrt{|\nu|}$ we can easily deduce

$$|\upsilon_1|_\infty \le c_2 n^{\frac{1}{4}}.$$

Moreover, if $|r_{m+1}| < \frac{\sqrt{|\nu|}}{c_1}$, by Lemma 5 we have a lower bound $|s_{m+1}| \ge \frac{\sqrt{|\nu|}}{c_1}$ which implies $|r_m| \le c_1\frac{3+\sqrt{3}}{2}\sqrt{|\nu|}$ using again Lemma 4. Together with the restricted condition $|s_m| < |s_{m+1}| \le c_2\sqrt{|\nu|} < c_1\frac{3+\sqrt{3}}{2}\sqrt{|\nu|}$ we can obtain

$$|(r_m, -s_m)|_\infty \le c_1\frac{3+\sqrt{3}}{2}n^{\frac{1}{4}}.$$

If $|r_{m+1}| \ge \frac{\sqrt{|\nu|}}{c_1}$, when $|s_{m+1}| \ge |s_{m+2}|$ we have $|s_{m+2}| \le c_2\sqrt{|\nu|}$, $|r_{m+2}| \le |r_{m+1}| < c_2\sqrt{|\nu|}$. When $|s_{m+1}| < |s_{m+2}|$, by the Lemma 4 we can deduce $|s_{m+2}| \le c_1\frac{3+\sqrt{3}}{2}\sqrt{|\nu|}$. Hence in both cases we have

$$|(r_{m+2}, -s_{m+2})|_\infty \le c_1\frac{3+\sqrt{3}}{2}n^{\frac{1}{4}}.$$

Finally by the definition of v_2 we always have

$$|\upsilon_2|_\infty \le c_1\frac{3+\sqrt{3}}{2}n^{\frac{1}{4}}.$$

Case 2: $\left|\frac{s_m}{s_{m+1}}\right| \ge 1$. Let $k \le m$ be the index satisfying

$$|s_k| \ge |s_{k+1}| \ge \cdots \ge |s_m| \ge |s_{m+1}| \text{ and } |s_{k-1}| < |s_k|.$$

Applying Lemma 4 to the $(k-1)$-th step we have $|s_k r_{k-1}| \le \frac{3+\sqrt{3}}{2}\sqrt{|\nu|}$. Since $|r_{k-1}| \ge |r_k| \ge \cdots \ge |r_m| \ge c_2\sqrt{|\nu|}$ we can easily deduce $|s_k| \le c_2\sqrt{|\nu|}$ and then $|s_{m+1}| \le |s_k| \le c_2\sqrt{|\nu|}$. Together with $|r_{m+1}| < c_2\sqrt{|\nu|}$ we obtain

$$|\upsilon_1|_\infty \le c_2 n^{\frac{1}{4}}.$$

Similarly, if $|r_{m+1}| < \frac{\sqrt{|\nu|}}{c_1}$ we have $|s_{m+1}| \ge \frac{\sqrt{|\nu|}}{c_1}$ by Lemma 5. which implies $|s_k| \ge \frac{\sqrt{|\nu|}}{c_1}$ and then $|r_{k-1}| \le c_1\frac{3+\sqrt{3}}{2}\sqrt{|\nu|}$ by Lemma 4. Hence $|r_m| \le c_1\frac{3+\sqrt{3}}{2}\sqrt{|\nu|}$. Together with $|s_m| \le |s_k| \le c_2\sqrt{|\nu|} < c_1\frac{3+\sqrt{3}}{2}n^{\frac{1}{4}}$ we have

$$|(r_m, -s_m)|_\infty \le c_1\frac{3+\sqrt{3}}{2}n^{\frac{1}{4}}.$$

On the other hand, if $|r_{m+1}| \geq \frac{\sqrt{|\nu|}}{c_1}$, following the same argument described in the case $|s_m| < |s_{m+1}|$ we also have

$$|(r_{m+2}, -s_{m+2})|_\infty \leq c_1 \frac{3+\sqrt{3}}{2} n^{\frac{1}{4}}.$$

Therefore,

$$|\upsilon_2|_\infty \leq c_1 \frac{3+\sqrt{3}}{2} n^{\frac{1}{4}}.$$

□

Following Theorem 7 and the argument in §4.1, we can easily obtain the conclusion.

Theorem 8. *In the 4-dimensional GLV scalar multiplication using the combination of GLV and GLS, the new twofold Cornacchia-type algorithm will result in a decomposition of any scalar $k \in [1, n)$ into integers k_1, k_2, k_3, k_4 such that*

$$[k]P = [k_1]P + [k_2]\phi(P) + [k_3]\psi(P) + [k_4]\phi\psi(P),$$

with $k_i \in \mathbb{Z}$ bounded by $4.74(\sqrt{1+|r|+|s|})n^{1/4}$.

Remark 5. *Note that $\max_i(|k_i|)$ was bound by the form $2C(\sqrt{1+|r|+s})n^{1/4}$ in the original paper [5, 8], since the endomorphism ϕ is always separable with $s = \deg(\phi)$. However, in this paper, we use a "restricted" endomorphism satisfying $x^2 + rx + s = 0$ with s may negative, see the example: the 4-GLV decomposition (15) on Curve 4 in §6. This change doesn't affect the proof. The new twofold Cornacchia-type algorithm possesses a upper bound of decomposition coefficients $4.74(\sqrt{1+|r|+|s|})n^{1/4}$, which is very close to Hu et al.'s [7] and better than Longa and Sica's [5] and Yi et al.'s [8].*

5 Applications of the new twofold Cornacchia-type algorithm

5.1 Computing all 4-GLV decompositions on j-invariant 0 curves over $\mathbb{F}_{p^2}$

We consider the class of elliptic curves over $\mathbb{F}_{p^2}$ which are twists of j-invariant 0 curves over $\mathbb{F}_p$. Recall there are two 4-GLV decompositions on this class of curves. The first one is described as (3) with the "restricted" endomorphism ψ_1 satisfying $\psi_1^4 - \psi_1^2 + 1 = 0$ in §2.2, the second one is described as (4) with the "restricted" endomorphisms ϕ, ψ_2 satisfying $\phi^2 + \phi + 1 = 0$ and $\psi_2^2 + 1 = 0$ in §2.3. So far, there are three methods to compute them: Hu et al.'s method[7], Longa and Sica's method[5] and Smith's method [17]. However, each method can only compute the 4-GLV decomposition under certain conditions. The method in [7] is only applicable to curves which are twists of degree 6 with a "restricted" endomorphism

ψ_1 satisfying $\psi_1^4 - \psi_1^2 + 1 = 0$. The methods in [5] and [17] are only applicable to curves which are twists of degree 2 with a "restricted" endomorphism ψ_2 satisfying $\psi_2^2 + 1 = 0$.

Note the "restricted" endomorphism $-\psi_1^2$ satisfies the equation $x^2 + x + 1 = 0$, as same as ϕ. Let $\phi := -\psi_1^2$ in the first 4-GLV decomposition. Therefore, for each of the 4-GLV decompositions, we exploit the facts that this class of curves must have an endomorphism ϕ with the ring $\mathbb{Z}[\phi] = \mathbb{Z}[\omega]$. Then, the new twofold Cornacchia-type algorithm in §4.2 can be used to compute all 4-GLV decompositions on curves over $\mathbb{F}_{p^2}$ with j-invariant 0. Different from previous algorithms, we propose a new and unified algorithm to compute all 4-GLV decompositions on this class of curves.

Remark 6. *For the class of quadratic twisted curves defined over $\mathbb{F}_{p^3}$, based on the existence of ψ satisfying $\psi^2 - \psi + 1 = 0$ when restricted to points defined over $\mathbb{F}_{p^3}$ (see the case $m = 3$ in [3, Corollary 2]), again we have $\mathbb{Z}[\psi] = \mathbb{Z}[\omega]$ and our new twofold algorithm can be used to compute the 4-GLV decomposition on this class of curves. However, curves defined over $\mathbb{F}_{p^3}$ are not really a good option in cryptography, their order is never a prime. Therefore, we will not elaborate too much here.*

5.2 Computing 4-GLV decompositions on Jacobians of a class of hyperellitic curves

Now, we consider a class of hyperelliptic curves which is the form $\mathcal{C} : y^2 = x^6 + ax^3 + b,\ a, b \in \mathbb{F}_p$. The Jacobian of $\mathcal{C}$ is $(2,2)$-isogenous to $E_c \times E_c$, which E_c is defined as $y^2 = x^3 + 3(2c-5)x + c^2 - 14c + 22$ with $c \in \mathbb{F}_{p^2}/\mathbb{F}_p,\ c^2 \in \mathbb{F}_p$.

The Jacobian of $\mathcal{C}$ was proposed for use in cryptography by Freeman and Satoh [21], who showed that it is isogenous over $\mathbb{F}_p$ to the Weil restriction of a curve of the form E_c. This property is exploited to derive fast point counting algorithms and pairing-friendly constructions [21, 22]. Guillevic and Ionica [6] investigated efficient scalar multiplication via the GLV technique on the Jacobian, they gave 4-GLV decompositions on $J_{\mathcal{C}}$ but didn't give examples or algorithms to compute them. In this paper, we give an example and use our algorithm to compute 4-GLV decompositions on $J_{\mathcal{C}}$.

Guillevic and Vergnaud [22, Theorem 2] showed that the complex multiplication discriminant $-D$ of E_c is of the form $-D = -3D'$, for some $D' \in \mathbb{N}_+$. Let t_{p^2} be the trace of $E_c(\mathbb{F}_{p^2})$. The equation of the complex multiplication is then $(t_{p^2})^2 - 4p^2 = -3D'\gamma^2$, for some $\gamma \in \mathbb{Z}$. Guillevic and Ionica [6] proved that there is an endomorphism on E_c whose degree of separability D', see the following.

Theorem 9. *[6, Theorem 2] There are integers m and n such that if $p \equiv 1 \mod 3$, then $t_{p^2} + 2p = D'm^2$ and $t_{p^2} - 2p = -3n^2$, and if $p \equiv 2 \mod 3$, then $t_{p^2} + 2p = 3n^2$ and $t_{p^2} - 2p = -D'm^2$. Let E_c be an elliptic curve defined as above. There is an endomorphism $\psi_{D'}$ of E_c with degree of separability D'. The characteristic equation of this endomorphism is*

$$\psi_{D'}^2 + D'm\psi_{D'} + D'p\mathrm{Id} = 0.$$

Now, reviewing the 4-GLV decomposition on $J_{\mathcal{C}}$ in [6, §5]. The first endomorphism ϕ on $J_{\mathcal{C}}$ is induced by the curve automorphism $(x, y) \to (\zeta^3 x, y)$, where ζ is a 3-th root of unity. Its characteristic equation is $\phi^2 + \phi + 1 = 0$. The second endomorphism is constructed as $\psi = \hat{I}(\psi_{D'}, \psi_{D'})I$, where $\psi_{D'}$ is the elliptic curve endomorphism constructed in Theorem 9 and the definition of $I, \hat{I}$ can refer [6, §2]. In order to compute the characteristic equation for ψ, similar to Theorem 3 in [6], we reproduce the result for $J_{\mathcal{C}}$.

Theorem 10. *Let $\mathcal{C} : y^2 = x^6 + ax^3 + b$ (with $a, b \neq 0 \in \mathbb{F}_p$, b not a square in $\mathbb{F}_p$) be a hyperelliptic curve defined over $\mathbb{F}_p$ with ordinary Jacobian and let r a prime number such that $r \parallel \#J_{\mathcal{C}}(\mathbb{F}_p)$. Let $I : J_{\mathcal{C}} \to E_c \times E_c$ the $(2,2)$-isogeny and assume I is defined over an extension field of degree $k > 1$. We define $\psi = \hat{I}(\psi_{D'}, \psi_{D'})I$, which is defined over $\mathbb{F}_p$. Then*

1. *For $\mathcal{D} \in J_{\mathcal{C}}[r](\mathbb{F}_p)$, we have $\psi(\mathcal{D}) = [\mu]\mathcal{D}$, with $\mu \in \mathbb{Z}$.*
2. *The characteristic equation of ψ is $\psi^2 + 2D'm\psi + 4D'p = 0$.*

Note that $\mathbb{Z}[\phi] = \mathbb{Z}[\omega]$, we can use the new twofold algorithm described in §4.2 to compute the 4-GLV decompositions on Jacobians of this class of curves.

6 Experimental results

In the following, we mainly describe the implementation of our methods. By the way, we verify that Smith's method is also valid for 4-GLV decompositions on high degree twisted curves. The objective is to verify that the new twofold Cornacchia-type algorithm can be used to compute all 4-GLV decompositions on GLS curves with j-invariant 0 and on Jacobians of a family of hyperelliptic curves defined over $\mathbb{F}_p$.

We describe an efficient parameter selection, carry out the corresponding operation count when computing scalar multiplications at the 128-bit security level on representative x86-64 processors. If computing endomorphisms is more expensive than point addition then we use precomputation. For the remainder, we use M and S, to denote the cost of multiplication and squaring over field $\mathbb{F}_{p^2}$, respectively, and m and s represent the same operations over $\mathbb{F}_p$. In order to give global estimates, we will assume that $m \sim s$ and that $M \sim 3m$ and $S \sim 3s$. For all implementations using the curves following, we just apply the width-ω non-adjacent form (ω-NAF) method [15, Alg. 3.36] for the case $\omega = 2$ to perform the scalar multiplication with dimension 4.

Curve 1. $E_1/\mathbb{F}_{p_1^2} : y^2 = x^3 + 6u^4x$, $p_1 = 2^{127} - 11791$. $\#E_1(\mathbb{F}_{p_1^2}) = 2n_1$, where n_1 is a 253-bit prime. We use $\mathbb{F}_{p_1^2} = \mathbb{F}_{p_1}[X]/(X^2 - 7)$ and $u^4 = \sqrt{7} \in \mathbb{F}_{p_1^2}$. E_1 is the quartic twist of the curve $y^2 = x^3 + 9$. $\phi_1(x, y) = [\lambda_1]P = (-x, iy)$ and $\psi_1(x, y) = [\mu_1]P = (u^{2(1-p_1)}x^{p_1}, u^{3(1-p_1)}y^{p_1})$. We

have that $\phi_1^2+1=0$ and $\psi_1^4+1=0$.

$n_1 = 144740111546645244279463731260859864755928153594046897167184762288081355232 97$.

Curve 2. $E_2/\mathbb{F}_{p_2^2} : y^2 = x^3+8u^6$, $p_2 = 2^{128}-40557$. $\#E_2(\mathbb{F}_{p_2^2}) = n_2$, where n_2 is a 256-bit prime. We use $\mathbb{F}_{p_2^2} = \mathbb{F}_{p_2}[X]/(X^2+1)$ and $u^6 = 3+\sqrt{-1} \in \mathbb{F}_{p_2^2}, u \in \mathbb{F}_{p_2^{12}}$. We have that $p_2 = a^2+ab+b^2$, with $a = -532813233214206943$ and $b = 18707378648059847118$, where $a \equiv 2 \mod 3, b \equiv 0 \mod 3$. E_2 is the sextic twist of the curve $y^2 = x^3+8$. $\psi_2(x,y) = [\mu_2]P = (u^{2(1-p_2)}x^{p_2}, u^{3(1-p_2)}y^{p_2})$. We have that $\psi_2^4-\psi_2^2+1=0$.

$n_2 = 115792089237316195423570985008687880252285787304655451067586303088174318594253$.

Curve 3. $E_3/\mathbb{F}_{p_3^2} : y^2 = x^3+9u^6$, $p_3 = 2^{127}-58309$. $\#E_3(\mathbb{F}_{p_3^2}) = n_3$, where n_3 is a 254-bit prime. We use $\mathbb{F}_{p_3^2} = \mathbb{F}_{p_3}[X]/(X^2+1)$ and $u^6 = 1+\sqrt{-1} \in \mathbb{F}_{p_3^2}$. E_3 is the quadratic twist of the curve $y^2 = x^3+9$. $\phi_3(x,y) = [\lambda_3]P = (\xi x, y)$ ($\xi^3 = 1 \mod p_3$) and $\psi_3(x,y) = [\mu_3]P = (u^{2(1-p_3)}x^{p_3}, u^{3(1-p_3)}y^{p_3})$. We have that $\phi_3^2+\phi_3+1=0$ and $\psi_3^2+1=0$.

$n_3 = 289480223093290488558927462521719571221154468803425622050225870260093170926 13$.

Curve 4. $E_4/\mathbb{F}_{p_4^2} : y^2 = x^3+4u^6$, $p_4 = 2^{127}-10711$. $\#E_4(\mathbb{F}_{p_4^2}) = n_4$, where n_4 is a 254-bit prime. We use $\mathbb{F}_{p_4^2} = \mathbb{F}_{p_4}[X]/(X^2-5)$ and $u^6 = \sqrt{5} \in \mathbb{F}_{p_4^2}$, $u \in \mathbb{F}_{p_4^{12}}$. E_4 is the sextic twist of the curve $y^2 = x^3+4$. $\phi_4(x,y) = [\lambda_4]P = (\xi x, y)$ with $\xi^3 = 1 \mod p_4$, $\psi_3(x,y) = [\mu_4]P = (u^{2(1-p_4)}x^{p_4}, u^{3(1-p_4)}y^{p_4})$ and $\widetilde{\phi}_4(x,y) = [\nu_4]P = \left(\frac{1}{3}\left(x^{p_4}+\frac{16u^6}{x^{2p_4}}\right), \frac{y^{p_4}}{3\sqrt{3}}\left(1+\frac{32u^6}{x^{3p_4}}\right)\right)$ for all points in $E_4(\mathbb{F}_{p_4^2})$. We have that $\phi_4^2+\phi_4+1=0$, $\psi_4^4-\psi_4^2+1=0$ and $\widetilde{\phi}_4^2-3=0$.

$n_4 = 289480223093290488558927462521719733184006554073723478116493094650134118608 97$.

Hyperellitic Curve. $\mathcal{C}/\mathbb{F}_p : y^2 = x^6-3x^3-92$ with $b=-92$ which is neither a square nor a cube, $p = 2^{127}-1$. Let $\mathbb{F}_{p^2} = \mathbb{F}_p[x]/(x^2+1) = \mathbb{F}_p[i]$, $c = \frac{a}{\sqrt{b}} \in \mathbb{F}_{p^2}/\mathbb{F}_p$ and $E_c/\mathbb{F}_{p^2} : y^2 = x^3+3(2c-5)x+c^2-14c+22$. A few second computation gives us $t_{p^2} = \texttt{0x6089c0341e5414a24bef1a1a93c54fd2}$ and $2p-t_{p^2} = 3n^2$ as expected with $n = \pm\texttt{0x74a69cde5282dbb6}$ and $2p+t_{p^2} = m^2D'$ with $m=4$, $D' = \texttt{0x16089c0341e5414a24bef1a1a93c54fd}$. Hence $\#J_{\mathcal{C}}(\mathbb{F}_p) = p^2+p+1+3n(p+1)+3n^2$. Using few random points on the Jacobian, we find $n<0$ and that $\#J_{\mathcal{C}}(\mathbb{F}_p)$ has a 250-bit prime factor: $r = \texttt{0x25ed097b425ed0974c75619931ea7f1271757b237c3ff3c5c00a037e7906557}$.

Two endomorphisms ϕ and ψ on $J_{\mathcal{C}}$ satisfy $\phi^2+\phi+1=0$ and $\psi^2+2D'm\psi+4D'p=0$.

Remark 7. *The endomorphism $\widetilde{\phi}_4$ satisfies $\widetilde{\phi}_4 = I_3 \circ \pi_p$, where I_3 is an isogeny with degree 3 and constructed by Vélu's formula [13, 14] with kernel $H = \{\mathcal{O}, (0,2u^3), (0,-2u^3)\}$. More details can be found in [6]. From the endomorphisms of curve E_4, we can get $[\mathbb{Q}(\psi_4):\mathbb{Q}] = [\mathbb{Q}(\widetilde{\phi}_4, \phi_4):\mathbb{Q}] = 4$. For*

$P \in E_4(\mathbb{F}_{p_4^2})[n_4]$ and any integer $k \in [1, n_4 - 1]$, two 4-GLV decompositions are constructed as follows:

$$[k]P = [k_1]P + [k_2]\psi_4(P) + [k_3]\psi_4^2(P) + [k_4]\psi_4^3(P); \quad (14)$$

$$= [k_1]P + [k_2]\phi_4(P) + [k_3]\widetilde{\phi}_4(P) + [k_4]\phi_4\widetilde{\phi}_4(P). \quad (15)$$

In Table 1, we give operation counts for 4-GLV decompositions on these curves. For the curves E_1 with j-invariant 1728 we use projective coordinates, a doubling costs $4M + 3S$ and an addition costs $7M + 1S$. For the curves E_2, E_3 and E_4 with j-invariant 0 we use Jacobian coordinates. A state-of-the-art formulas can be found in [16, formula (6.7)], which a doubling costs $3M + 4S$ and an addition costs $12M + 4S$. For genus 2 arithmetic on curves of the form $y^2 = x^6 + ax^3 + b$, we used formulæ given by Costello and Lauter [23] in projective coordinates. An addition costs $43M + 4S$ and a doubling costs $30M + 9S$.

Table 1. Total cost of scalar multiplication at a 128-bit security level.

Curve	Method	Operation counts	Global estimation
$E_1(\mathbb{F}_{p_1^2})$	4-GLV(Algorithm in [5, 8]) Smith's method (Theorem 5)	$718M + 326S$	$3132m$
$E_2(\mathbb{F}_{p_2^2})$	4-GLV(Algorithm in [7]) Smith's method (Theorem 6) 4-GLV(Our algorithm)	$816M + 548S$	$4092m$
$E_3(\mathbb{F}_{p_3^2})$	4-GLV(Algorithm in [5, 8]) Smith's method (Theorem 4) 4-GLV (Our algorithm)	$885M + 580S$	$4395m$
$E_4(\mathbb{F}_{p_4^2}) - (14)$	4-GLV(Algorithm in [7]) Smith's method (Theorem 6) 4-GLV (Our algorithm)	$834M + 560S$	$4182m$
$E_4(\mathbb{F}_{p_4^2}) - (15)$	Smith's method (Theorem 6 in [17]) 4-GLV (Our algorithm)	$834M + 556S$	$4170m$
$J_{\mathcal{C}}(\mathbb{F}_p)$	4-GLV(Our algorithm)	$1623m + 300s$	$1923m$

For 4-GLV decompositions on these curve, we use all possible algorithms to compute them. From the experimental results in Table 1, we first show that our method is valid by comparing with previous methods on curves E_2, E_3 and E_4. Now, we focus on 4-GLV decompositions on GLS curves with j-invariant 0 and compare our method with two previous methods in [7, 5, 8]. We can see that the two previous methods can only compute 4-GLV decompositions under specific conditions. Hu et al.'s method [7] can only compute 4-GLV decomposition on GLS curves which are sextic twists, see curves E_2, Longa and Sica's method is only applicable to those curves with the "restricted" endomorphism ψ satisfying $\psi^2 + 1 = 0$, see curve E_3. Also, for these two 4-GLV decompositions on curve E_4, the method

in [7] can compute the decomposition (14) but not the decomposition (15), and the method in [5, 8] can not compute the decompositions either. Our method can compute all 4-GLV decompositions on GLS curves with j-invariant 0, it gives a new and unified method on this class of elliptic curves.

Secondly, we show that Smith's method (Theorem 6,7) can be used to compute 4-GLV decompositions on high degree twisted elliptic curves, such as curves E_1 and E_2 which are quartic twist and sextic twist, respectively. So, what we've done in §3 make Smith's method to adapt to more elliptic curves over $\mathbb{F}_{p^2}$. However, we note that Smith's method can not be used to calculate the 4-GLV decomposition on $J_{\mathcal{C}}(\mathbb{F}_p)$. In Table 1, our method is the only one that can be used to calculate all 4-GLV decompositions on these curves.

7 Conclusion

We have constructed a new twofold Cornacchia-type algorithm, the first part in $\mathbb{Z}$ and the second part in the Euclidean domain $\mathbb{Z}[\omega]$ ($\omega = \frac{-1+\sqrt{-3}}{2}$), with a theoretic upper bound of output $C \cdot n^{1/4}$, where $C = \frac{3+\sqrt{3}}{2}\sqrt{1+|r|+|s|}$ with r, s given by the curve. It is a variation of the twofold Cornacchia-type algorithm [5, 8]. Moreover, we observe that the second Cornacchia's algorithm can also implemented on imaginary quadratic orders which are Euclidean. The new twofold Cornacchia-type algorithm can compute the 4-GLV decompositions on two families of curves. It is a new and unified method to compute all 4-GLV decompositions on the family of GLS curves over $\mathbb{F}_{p^2}$ with j-invariant 0 and it can compute the 4-GLV decompositions on Jacobians of a family of hyperelliptic curves. The new twofold algorithm is as efficient as the original twofold algorithm but has broader applications. We also give supplements to Smith's method for 4-GLV decompositions on twisted elliptic curves with degree of twists 4 or 6, which make Smith's method to adapt to more curves. In the future, we will explore more and more applications about new twofold Cornacchia-type algorithms with the second Cornacchia's algorithm implemented on some orders of imaginary quadratic fields which are Euclidean except $\mathbb{Z}[i]$.

Appendix

Algorithm 3: The second part of the new algorithm—real & imaginary parts

Input: ν prime dividing n rational prime, $1 < \mu < n$ such that $\mu^2 + r\mu + s \equiv 0 \mod n$.

Output: A short basis of $\ker F \subset \mathbb{Z}^4$: $\widetilde{v}_1, \widetilde{v}_2, \widetilde{v}_3, \widetilde{v}_4$

1. **initialize:**

   $r_{0(R)} \leftarrow \mu$, $r_{0(I)} \leftarrow 0$, $r_{1(R)} \leftarrow a$, $r_{1(I)} \leftarrow b$, $r_{2(R)} \leftarrow n$, $r_{2(I)} \leftarrow 0$,

   $s_{0(R)} \leftarrow 1$, $s_{0(I)} \leftarrow 0$, $s_{1(R)} \leftarrow 0$, $s_{1(I)} \leftarrow 0$, $s_{2(R)} \leftarrow 0$, $s_{2(I)} \leftarrow 0$, $q_R \leftarrow 0$, $q_I \leftarrow 0$.

2. **main loop:**

   while $2(r_{1(R)}^2 - r_{1(R)}r_{1(I)} + r_{1(I)}^2) \geq (3+\sqrt{3})n^{1/2}$ do

   $q_R \leftarrow \lceil \frac{r_{0(R)}r_{1(R)} - r_{0(R)}r_{1(I)} + r_{0(I)}r_{1(I)}}{r_{1(R)}^2 - r_{1(R)}r_{1(I)} + r_{1(I)}^2} \rfloor$,

   $q_I \leftarrow \lceil \frac{r_{0(I)}r_{1(R)} - r_{0(R)}r_{1(I)}}{r_{1(R)}^2 - r_{1(R)}r_{1(I)} + r_{1(I)}^2} \rfloor$,

   $r_{2(R)} \leftarrow r_{0(R)} - (q_R r_{1(I)} - q_I r_{1(I)})$,

   $r_{2(I)} \leftarrow r_{0(I)} - (q_R r_{1(I)} + q_I r_{1(R)} - q_I r_{1(I)})$,

   $r_{0(R)} \leftarrow r_{1(R)}, r_{0(I)} \leftarrow r_{1(I)}, r_{1(R)} \leftarrow r_{2(R)}, r_{1(I)} \leftarrow r_{2(I)}$,

   $s_{2(R)} \leftarrow s_{0(R)} - (q_R s_{1(R)} - q_I s_{1(I)})$,

   $s_{2(I)} \leftarrow s_{0(I)} - (q_R s_{1(I)} + q_I s_{1(R)} - q_I s_{1(I)})$,

   $s_{0(R)} \leftarrow s_{1(R)}, s_{0(I)} \leftarrow s_{1(I)}, s_{1(R)} \leftarrow s_{2(R)}, s_{1(I)} \leftarrow s_{2(I)}$,

3. **compute**:

   $q_R \leftarrow \lceil \frac{r_{0(R)}r_{1(R)} - r_{0(R)}r_{1(I)} + r_{0(I)}r_{1(I)}}{r_{1(R)}^2 - r_{1(R)}r_{1(I)} + r_{1(I)}^2} \rfloor$,

   $q_I \leftarrow \lceil \frac{r_{0(I)}r_{1(R)} - r_{0(R)}r_{1(I)}}{r_{1(R)}^2 - r_{1(R)}r_{1(I)} + r_{1(I)}^2} \rfloor$,

   $r_{2(R)} \leftarrow r_{0(R)} - (q_R r_{1(I)} - q_I r_{1(I)})$, $r_{2(I)} \leftarrow r_{0(I)} - (q_R r_{1(I)} + q_I r_{1(R)} - q_I r_{1(I)})$,

   $s_{2(R)} \leftarrow s_{0(R)} - (q_R s_{1(R)} - q_I s_{1(I)})$, $s_{2(I)} \leftarrow s_{0(I)} - (q_R s_{1(I)} + q_I s_{1(R)} - q_I s_{1(I)})$,

4. **return**:

   $\widetilde{v}_1 = (r_{1(R)}, r_{1(I)}, -s_{1(R)}, -s_{1(I)}), \widetilde{v}_2 = (-r_{1(I)}, r_{1(R)} - r_{1(I)}, s_{1(I)}, s_{1(I)} - s_{1(R)})$,

   $a := \max\left\{(r_{0(R)}^2 - r_{0(R)}r_{0(I)} + r_{0(I)}^2), (s_{0(R)}^2 - s_{0(R)}s_{0(I)} + s_{0(I)}^2)\right\}$

   $b := \max\left\{(r_{2(R)}^2 - r_{2(R)}r_{2(I)} + r_{2(I)}^2), (s_{2(R)}^2 - s_{2(R)}s_{2(I)} + s_{2(I)}^2)\right\}$

   If $a \leq b$ then

   $\widetilde{v}_3 = (r_{0(R)}, r_{0(I)}, -s_{0(R)}, -s_{0(I)}), \widetilde{v}_4 = (-r_{0(I)}, r_{0(R)} - r_{0(I)}, s_{0(I)}, s_{0(I)} - s_{0(R)})$.

   otherwise

   $\widetilde{v}_3 = (r_{2(R)}, r_{2(I)}, -s_{2(R)}, -s_{2(I)}), \widetilde{v}_4 = (-r_{2(I)}, r_{2(R)} - r_{2(I)}, s_{2(I)}, s_{2(I)} - s_{2(R)})$.

References

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

[2] Iijima T., Matsuo K., Chao J., et al.: Construction of Frobenius maps of twists elliptic curves and its application to elliptic scalar multiplication. In: Proc. of SCIS, pp. 699-702 (2002).

[3] 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).

[4] Zhou Z., Hu Z., Xu M., et al.: Efficient 3-dimensional GLV method for faster point multiplication on some GLS elliptic curves. Information Processing Letters. **110**(22), 1003-1006 (2010).

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

[6] 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).

[7] 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).

[8] Yi H., Zhu Y., Lin D.: Refinement of the Four-Dimensional GLV Method on Elliptic Curves. In: International Conference on Selected Areas in Cryptography. pp. 23-42. Springer, Cham (2017).

[9] Sica F., Ciet M., Quisquater J.J.: Analysis of the Gallant-Lambert-Vanstone method based on efficient endomorphisms: Elliptic and hyperelliptic curves. In: International Workshop on Selected Areas in Cryptography. pp. 21-36. Springer, Berlin, Heidelberg (2002).

[10] Bos J.W., Costello C., Hisil H., et al.: High-performance scalar multiplication using 8-dimensional GLV/GLS decomposition. In: International Workshop on Cryptographic Hardware and Embedded Systems. pp. 331-348. Springer, Berlin, Heidelberg (2013).

[11] Silverman J.H.: The arithmetic of elliptic curves. GTM 106. Springer, New York (2009).

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

[13] Miret J.M., Moreno Chiral R., Rio A.: Generalization of Vélu's formulae for isogenies between elliptic curves. Publicacions matemàtiques, **Extra**, 147-163 (2007).

[14] Vélu, J.: Isogenies entre courbes elliptiques. Comptes Rendus De lAcadémie Des Sciences Paris, Série IMath'ematique, Série A. **273**, 238-241 (1971).

[15] Hankerson D., Menezes A.J., Vanstone S.: Guide to Elliptic Curve Cryptography. Springer, Heidelberg (2004).

[16] Longa P.: High-speed elliptic curve and pairing-based cryptography. Ph.D Thesis, University of Waterloo (2011). http://hdl.handle.net/10012/5857.

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

[18] 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).

[19] 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).

[20] 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).

[21] Freeman, D.M., Satoh, T.: Constructing pairing-friendly hyperelliptic curves using Weil restriction. Journal of Number Theory 131(5), 959-983 (2011)

[22] Guillevic, A., Vergnaud, D.: Genus 2 Hyperelliptic Curve Families with Explicit Jacobian Order Evaluation and Pairing-Friendly Constructions. In: Abdalla, M., Lange, T. (eds.) Pairing-Based Cryptography-Pairing 2012. LNCS, vol. 7708, pp. 234-253. Springer (2013)

[23] Costello, C., Lauter, K.: Group Law Computations on Jacobians of Hyperelliptic Curves. In: Miri, A., Vaudenay, S. (eds.) Selected Areas in Cryptography. LNCS, vol. 7118, pp. 92-117. Springer (2011)

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

[25] A. Menezes, T. Okamoto, S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory 39, 1639–1646 (1993)

[26] G. Frey, H. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comput. 62, 865–874 (1994)