# A New Twofold Cornacchia-Type Algorithm

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

[1]Key Laboratory of Electromagnetic Space Information, CAS
University of Science and Technology of China
Email: hghu2005@ustc.edu.cn,wangbei@mail.ustc.edu.cn

[2]CAS Wu Wen-Tsun Key Laboratory of Mathematics,
School of Mathematical Sciences,
University of Science and Technology of China
Email: yiouyang@ustc.edu.cn

[3]School of Cyber Science and Engineering
Shanghai Jiao Tong University
Email: songsli@mail.ustc.edu.cn

**Abstract**

We focus on exploring more potential of Longa and Sica's algorithm (ASIACRYPT 2012), 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. Besides, we give some applications of our new algotithm in some cuvres not considered in Longa and Sica's algorithm.

**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. 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. 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 $\phi$ and $\psi$ can be constructed on the GLS curve $E'/\mathbb{F}_{p^2}$. Let $G \subset E'(\mathbb{F}_{p^2})$ be a cyclic subgroup of large prime order $n$. The two 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 integers $k_i$ bounded by $n^{1/4}$, and any $P \in G$. 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] 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 $\mathbb{Z}[i]$.

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 the ring of integers $\mathbb{Z}[\omega] = \mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ of $\mathbb{Q}(\sqrt{-3})$. 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].

This paper is organized as follows. In §2, we give an overview of previous work on the GLV decomposition. §3 contains the main work of this paper, the construction of the new twofold Cornacchia-type algorithm. In §4 we give applications of our new twofold Cornacchia-type algorithm. In §5, we give some examples and experimental results. Finally, in §6 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 $\rho$ 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 $\lambda$ 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 $\mathcal{K} := \{(i, j) \mid i + \lambda j = 0 \mod n\}$ 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 $\upsilon_1, \upsilon_2$ 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 $\beta_i$ 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 $\phi$ 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 $\frac{1+\sqrt{-11}}{2}$ ($j = -32768$). 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 $\pi_0$ be the $p$-power Frobenius map on $E$ and $t_{\pi_0}$ the trace of $\pi_0$. 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 $\psi$ 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 $\mu \equiv t_{\pi_0}^{-1}(p-1) \mod n$.*

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 $\psi$ 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

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

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 $\psi$ 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 $\psi$ 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 $\psi$ 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 $\rho$ be the GLV endomorphism coming with the definition of a GLV curve. Then $\rho$ 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 $\phi$ and $\psi$ 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

$$[k]P = [k_1]P + [k_2]\phi(P) + [k_3]\psi(P) + [k_4]\phi\psi(P) \quad \text{with} \quad \max_i(|k_i|) < 2Cn^{1/4} \tag{3}$$

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 $\phi$ and $\psi$ are $\mathbb{Z}$-linearly independent. Review the implementation of the algorithm: the "restricted" endomorphism $\psi$ 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.

# 3 A new twofold Cornacchia-type algorithm

## 3.1 Analysis of the new twofold algorithm

First, we consider a curve which has two fast endomorphisms $\phi, \psi$ with minimal polynomials $x^2 + x + 1$ and $x^2 + rx + s$ respectively. Let $\lambda$ and $\mu$ be the eigenvalues of $\phi$ and $\psi$ on a cyclic subgroup of order $n$, respectively, $\lambda, \mu \in [0, n-1]$. Viewing $\phi$ and $\psi$ as algebraic integers, then $\mathbb{Q}(\phi) = \mathbb{Q}(\sqrt{-3})$. Moreover, Changing $\phi$ to $-\phi$ if necessary, then we may identify $\phi$ 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 $\lambda$ and $\mu$ 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 $F$:

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

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 §3.2 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.,

$$\mathfrak{n}' = \nu\mathbb{Z}[\omega] + (\psi - \mu)\mathbb{Z}[\omega]. \tag{5}$$

We now use the second Cornacchia's algorithm in $\mathbb{Z}[\omega]$ to find a short $\mathbb{Z}[\omega]$-basis $\{\upsilon_1, \upsilon_2\}$ of $\mathfrak{n}'$ (see §4.2 Algorithm 2) with $\max_i(|\upsilon_i|) \leq Cn^{1/4}$ for some constant $C > 0$. Thus we get a short $\mathbb{Z}$-basis $\{\upsilon_1, \upsilon_1\omega, \upsilon_2, \upsilon_2\omega\}$ of $\mathfrak{n}'$. Moreover, write $\upsilon_1 = (a_1 + b_1\omega) + (c_1 + d_1\omega)\psi$ and $\upsilon_2 = (a_2 + b_2\omega) + (c_2 + d_2\omega)\psi$, then

$$\mathfrak{n}' = (a_1 + b_1\omega + (c_1 + d_1\omega)\psi)\mathbb{Z}[\omega] + (a_2 + b_2\omega + (c_2 + d_2\omega)\psi)\mathbb{Z}[\omega]. \tag{6}$$

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

$$\begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ -b_1 & a_1 - b_1 & -d_1 & c_1 - d_1 \\ a_2 & b_2 & c_2 & d_2 \\ -b_2 & a_2 - b_2 & -d_2 & c_2 - d_2 \end{pmatrix}. \tag{7}$$

Let $\{\widetilde{\upsilon}_1, \widetilde{\upsilon}_2, \widetilde{\upsilon}_3, \widetilde{\upsilon}_4\}$ be the row vectors of the matrix (7) with $\max_i(|\widetilde{\upsilon}_i|) \leq Cn^{1/4}$. For any $k \in [1, n-1]$, write $(k, 0, 0, 0) = \sum_{j=0}^{4} \beta_j \widetilde{\upsilon}_j$ with $\beta_j \in \mathbb{Q}$. Then $\upsilon := \sum_{j=0}^{4} \lfloor \beta_j \rceil \widetilde{\upsilon}_j \in \ker F$. Let $\kappa = (k_1, k_2, k_3, k_4) = (k, 0, 0, 0) - \upsilon$. By the triangle inequality, $|\kappa| = |\sum_{i=1}^{4} (\lfloor \beta_i \rceil - \beta_i)\widetilde{\upsilon}_i| \leq 4 \times \frac{1}{2} \max_i(|\widetilde{\upsilon}_i|) \leq 2Cn^{1/4}$. 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 $\psi$ satisfing $\psi^4 - \psi^2 + 1 = 0$. Hence the 4-GLV decomposition can be implemented on the curve as described as in (2). View $\psi$ 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 $\psi$ is a primitive 12-th root of unity, then $K/\mathbb{Q}$ is a Galois extension and $O_K = \mathbb{Z}[\psi]$. Let $\mu$ be the eigenvalue of $\psi$ 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

$$F : \mathbb{Z}^4 \to \mathbb{Z}/n\mathbb{Z} \cong O_K/\mathfrak{n}', \quad (x_1, x_2, x_3, x_4) \mapsto x_1 + x_2\mu + x_3\mu^2 + x_4\mu^3 \mod n. \tag{8}$$

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 $n, \lambda$, 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 $\nu, \mu$ to find a short $\mathbb{Z}[\omega]$-basis $\{\upsilon_1, \upsilon_2\}$ of $\mathfrak{n}'$. Moreover, in this case, the new twofold Cornacchia-type algorithm can be used for scalar decomposition as well.

**Remark 3.** *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 $\mathbb{Z}[i]$.*

### 3.2 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 $\nu$ 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 $n$.

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 1.** *Algorithm 1 is valid and the output $\nu = r_1 - \omega t_1$ is really lying over $n$.*

*Proof.* Let $\lambda \in [1, n-1]$ such that $\lambda \equiv \omega \mod n$, with $\omega$ being defined by $\phi(P) = \omega P$. To compute the g.c.d of $n$ and $\lambda$, 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

$$\begin{pmatrix} r_{j+2} & s_{j+2} & t_{j+2} \\ r_{j+1} & s_{j+1} & t_{j+1} \end{pmatrix} = \begin{pmatrix} -q_{j+1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{j+1} & s_{j+1} & t_{j+1} \\ r_j & s_j & t_j \end{pmatrix}, \tag{9}$$

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

$$\begin{pmatrix} r_1 & s_1 & t_1 \\ r_0 & s_0 & t_0 \end{pmatrix} = \begin{pmatrix} \lambda & 0 & 1 \\ n & 1 & 0 \end{pmatrix}. \tag{10}$$

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 $n s_j + \lambda t_j = r_j$.

P4 and P5 can be reformulated as

$$|s_{j+1} r_j| + |s_j r_{j+1}| = \lambda \text{ and } |t_{j+1} r_j| + |t_j r_{j+1}| = n. \tag{11}$$

The algorithm stops at $m$ when $r_m \geq \sqrt{n}$ and $r_{m+1} < \sqrt{n}$. For $j = m$ in (11), 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 $\nu = r_{m+1} - \omega t_{m+1}$, $\nu \overline{\nu} = n$. □

We have seen how to construct $\nu$ by the Cornacchia's algorithm in $\mathbb{Z}$. From the analysis in §3.1, $\mathfrak{n}'$ 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 $(\nu, \mu)$ 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 2). Let us note that P4-P6 of Lemma 1 still hold and P1 holds in modulus (in particular, the algorithm terminates). Hence the (11), 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 3), 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 (7) in §3.1. Note that the *imaginary* part in the Algorithm 3 denotes the coefficient of $\omega$, 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:** $\nu \in \mathbb{Z}[\omega]$ prime dividing $n$ rational prime, $1 < \mu < n$ such that $\mu^2 + r\mu + s \equiv 0 \mod n$.

**Output:** Two vectors in $\mathbb{Z}[\omega]^2$: $\upsilon_1, \upsilon_2$.

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.

## 3.3 Proof of the upper bound

**Theorem 3.** *The two vectors $\upsilon_1, \upsilon_2$ 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 3, 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 a lattice diamond with a vertex of modulus 1 (such as, $\pm 1$ or $\pm\omega$) but not containing the origin as a vertex (since $q_{j+1} \neq 0$).

First, we discuss a property that the closest lattice point to a point in the fundamental parallelogram of the lattice $\mathbb{Z}[\omega]$ .

**Lemma 2.** *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 $V_1P \leq \frac{\sqrt{3}}{2}$. □

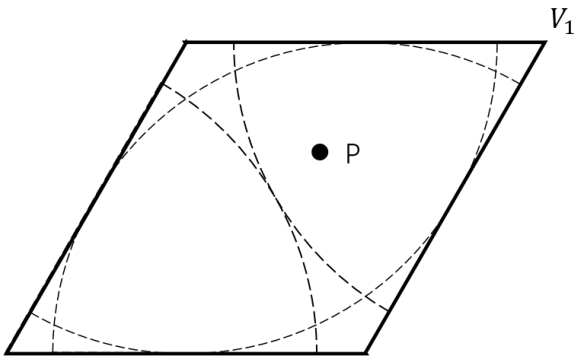


Figure 1: An lattice diamond in $\mathbb{Z}[\omega]$

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 2, 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 3.** *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

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

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 $|s_j r_{j+1}| \leq \frac{5+\sqrt{3}}{2}|\nu|$. □

**Lemma 4.** *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 $\mu'$ 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 3). 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 3 we have $|s_{m+1}| \leq c_2\sqrt{|\nu|}$, together with $|r_{m+1}| < c_2\sqrt{|\nu|}$ we can easily deduce

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

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

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

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

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

Finally by the definition of $v_2$ we always have

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

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

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

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

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

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

$c_1\frac{3+\sqrt{3}}{2}n^{\frac{1}{4}}$ we have

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

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 3 and the argument in §3.1, we can easily obtain the conclusion.

**Theorem 4.** *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 4.** *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 $\phi$ 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 (13) on Curve 3 in §5. 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].*

# 4 Experimental results

In the following, we mainly describe the implementation of our methods. Note that our new 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, the count of corresponding operation 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-$\omega$ non-adjacent form ($\omega$-NAF) method [15, Alg. 3.36] for the case $\omega = 2$ to perform the scalar multiplication with dimension 4.

**Curve 1.** $E_1/\mathbb{F}_{p_1^2} : y^2 = x^3 + 9u^6$, $p_1 = 2^{127} - 58309$. $\#E_1(\mathbb{F}_{p_1^2}) = n_1$, where $n_1$ is a 254-bit prime. We use $\mathbb{F}_{p_1^2} = \mathbb{F}_{p_1}[X]/(X^2+1)$ and $u^6 = 1 + \sqrt{-1} \in \mathbb{F}_{p_1^2}$. $E_1$ is the quadratic twist of the curve $y^2 = x^3 + 9$. $\phi_1(x,y) = [\lambda_1]P = (\xi x, y)$ ($\xi^3 = 1 \mod p_1$) 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 $\phi_1^2 + \phi_1 + 1 = 0$ and $\psi_1^2 + 1 = 0$.
$n_3 = 28948022309329048855892746252171957122115446880342562205022587026009317092613$.

**Curve 2.** $E_2/\mathbb{F}_{p_2^2} : y^2 = x^3 + 4u^6$, $p_2 = 2^{127} - 10711$. $\#E_2(\mathbb{F}_{p_2^2}) = n_2$, where $n_2$ is a 254-bit prime. We use $\mathbb{F}_{p_2^2} = \mathbb{F}_{p_2}[X]/(X^2-5)$ and $u^6 = \sqrt{5} \in \mathbb{F}_{p_2^2}$, $u \in \mathbb{F}_{p_2^{12}}$. $E_2$ is the sextic twist of the curve $y^2 = x^3 + 4$. $\phi_2(x,y) = [\lambda_2]P = (\xi x, y)$ with $\xi^3 = 1 \mod p_2$, $\psi_2(x,y) = [\mu_2]P = (u^{2(1-p_2)}x^{p_2}, u^{3(1-p_2)}y^{p_2})$ and $\widetilde{\phi}_2(x,y) = [\nu_2]P = \left(\frac{1}{3}\left(x^{p_2} + \frac{16u^6}{x^{2p_2}}\right), \frac{y^{p_2}}{3\sqrt{3}}\left(1 + \frac{32u^6}{x^{3p_2}}\right)\right)$ for all points in $E_2(\mathbb{F}_{p_2^2})$. We have that $\phi_2^2 + \phi_2 + 1 = 0$, $\psi_2^4 - \psi_2^2 + 1 = 0$ and $\widetilde{\phi}_2^2 - 3 = 0$.
$n_2 = 28948022309329048855892746252171973318400655407372347811649309465013411860897$.

**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 seconds computation gives us $t_{p^2} = \texttt{0x}6089c0341e5414a24bef1a1a93c54fd2$ and $2p - t_{p^2} = 3n^2$ as expected with $n = \pm\texttt{0x}74a69cde5282dbb6$ and $2p + t_{p^2} = m^2D'$ with $m = 4$, $D' = \texttt{0x}16089c0341e5414a24bef1a1a93c54fd$. 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: $r = \texttt{0x}25ed097b425ed0974c75619931ea7f1271757b237c3ff3c5c00a037e7906557$.
Two endomorphisms $\phi$ and $\psi$ on $J_{\mathcal{C}}$ satisfy $\phi^2 + \phi + 1 = 0$ and $\psi^2 + 2D'm\psi + 4D'p = 0$.

**Remark 5.** *The endomorphism $\widetilde{\phi}_2$ in Curve 2 satisfies $\widetilde{\phi}_2 = I_3 \circ \pi_p$, 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 $E_2$, we can get $[\mathbb{Q}(\psi_2) : \mathbb{Q}] = [\mathbb{Q}(\widetilde{\phi}_2, \phi_2) : \mathbb{Q}] = 4$. For $P \in E_2(\mathbb{F}_{p_2^2})[n_2]$ and any integer $k \in [1, n_2 - 1]$, two 4-GLV decompositions are constructed as follows:*

$$[k]P = [k_1]P + [k_2]\psi_4(P) + [k_3]\psi_4^2(P) + [k_4]\psi_4^3(P); \quad (12)$$

$$= [k_1]P + [k_2]\phi_4(P) + [k_3]\widetilde{\phi}_4(P) + [k_4]\phi_4\widetilde{\phi}_4(P). \quad (13)$$

In Table 1, we give operation counts for 4-GLV decompositions on these curves. For the curves $E_1$ and $E_2$ 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 formule given by Costello and Lauter [17] 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])<br>4-GLV (Our algorithm) | $885M + 580S$ | $4395m$ |
| $E_2(\mathbb{F}_{p_2^2}) - (12)$ | 4-GLV(Algorithm in [7])<br>4-GLV (Our algorithm) | $834M + 560S$ | $4182m$ |
| $E_2(\mathbb{F}_{p_2^2}) - (13)$ | 4-GLV (Our algorithm) | $834M + 556S$ | $4170m$ |
| $J_{\mathcal{C}}(\mathbb{F}_p)$ | 4-GLV(Our algorithm) | $1623m + 300s$ | $1923m$ |

First, we focus on 4-GLV decompositions on the curves $E_1$ and $E_2$ 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, Longa and Sica's method is only applicable to those curves with the "restricted" endomorphism $\psi$ satisfying $\psi^2 + 1 = 0$. Also, for these two 4-GLV decompositions on curve $E_2$, the method in [7] can compute the decomposition (12) but not the decomposition (13), and the method in [5, 8] can not compute the decompositions either. Secondly, our algorithm can be used to calculate the 4-GLV decomposition on $J_{\mathcal{C}}(\mathbb{F}_p)$, while the methods in [7, 5, 8] can not to do. In Table 1, our method is the only one that can be used to calculate all 4-GLV decompositions on these curves and gives a new and unified method for the 4-GLV on GLS curves with $j$-invariant 0.

# 5 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]. In the future, we will explore more twofold Cornacchia-type algorithms with the second Cornacchia's algorithm implemented on some orders of imaginary quadratic fields except $\mathbb{Z}[i]$.

# 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] 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)

# Appendix

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

**Input:** $\nu$ 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

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