General 4-GLV Lattice Reduction Algorithms

Bei Wang*, Xianhong Xie†, Songsong Li‡, Yi Ouyang† and Honggang Hu*
*Key Laboratory of Electromagnetic Space Information, CAS
University of Science and Technology of China
Email: wangbei@mail.ustc.edu.cn, hghu2005@ustc.edu.cn.
†CAS Wu Wen-Tsun Key Laboratory of Mathematics,
School of Mathematical Sciences,
University of Science and Technology of China
‡School of Cyber Science and Engineering
Shanghai Jiao Tong University

***Abstract*—With two $\mathbb{Z}$-linear independence endomorphisms Φ and Ψ satisfying $\Phi^2 + r\Phi + s = 0$ and $\Psi^2 - t_\Psi \Psi + n_\Psi = 0$, we construct general 4-GLV lattice reduction algorithms with $\mathbb{Z}[\Psi]$ principal maximal orders of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$. The algorithms can be used to calculate short bases for 4-GLV decompositions on elliptic curves (or Jacobians of genus 2 curves). Our algorithms have a theoretic upper bound of output $Cn^{1/4}$, where**

$$C = \begin{cases} \frac{4+2\sqrt{d+1}}{3-d}(\sqrt{1+|r|+|s|}), & \textbf{if } \mathbb{Z}[\Psi] = \mathbb{Z}[\sqrt{-d}], \\ \frac{4\sqrt{d}}{4\sqrt{d}-(d+1)}(\sqrt{1+|r|+|s|}), & \textbf{if } \mathbb{Z}[\Psi] = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]. \end{cases}$$

Especially, our algorithms cover the case $\mathbb{Z}[\Psi] = \mathbb{Z}[\sqrt{-1}]$ of Yi et al. (SAC 2017) and the case $\mathbb{Z}[\Psi] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ of Wang et al. (AMC 2021).

***Keywords*-Elliptic curves; Endomorphisms; 4-GLV lattice reduction algorithms; Short bases; Upper bounds;**

I. Introduction

Scalar multiplication is the fundamental operation in elliptic curve cryptography. It is important to accelerate this operation and numerous methods have been extensively discussed in the literature; for a good survey, see [1]. Longa and Sica [2] combined GLV [3] and GLS [4] method to construct a 4-GLV decomposition of scalar multiplication and constructed an efficient algorithm—the twofold Cornacchia-type algorithm. The basic idea can be explained as follows.

Let $p > 3$ be a prime and E an elliptic curve defined over $\mathbb{F}_p$. Let $E'/\mathbb{F}_{p^2}$ be a quadratic twist of $E(\mathbb{F}_{p^2})$ and $\mathcal{G} \subset E'(\mathbb{F}_{p^2})$ be a cyclic subgroup of large prime order n. The two endomorphisms Φ and Ψ satisfy $\Phi^2(P)+r\Phi(P)+sP = \mathcal{O}_{E'}$ and $\Psi^2(P) + P = \mathcal{O}_{E'}$ respectively. They are defined over $\mathbb{F}_{p^2}$ on E' with the assumpation that Φ and Ψ are $\mathbb{Z}$-linearly independent. Let λ_Φ and λ_Ψ be the eigenvalues of Φ and Ψ on $\mathcal{G}$, respectively. Longa and Sica [2] showed how to get a 4-GLV decomposition for $E'(\mathbb{F}_{p^2})$. For any scalar $k \in [1, n-1]$, we obtain that

$$[k]P = [k_1]P + [k_2]\Phi(P) + [k_3]\Psi(P) + [k_4]\Phi\Psi(P), \quad (1)$$

Corresponding Author: Honggang Hu

with $\max_i(|k_i|) < 2Cn^{1/4}$. To compute decomposition coefficients k_1, k_2, k_3, k_4, one can construct a map F:

$$F : \mathbb{Z}^4 \to \mathbb{Z}/n\mathbb{Z},$$
$$(x_1, x_2, x_3, x_4) \mapsto x_1 + x_2\lambda_\Phi + x_3\lambda_\Psi + x_4\lambda_\Phi\lambda_\Psi \bmod n. \quad (2)$$

It is easy to know that

$$\ker F = \{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 | x_1 + x_2\lambda_\Phi + x_3\lambda_\Psi + x_4\lambda_\Phi\lambda_\Psi \equiv 0 \bmod n\} \quad (3)$$

is a full sublattice of $\mathbb{Z}^4$. The set of decompositions of any k in $\mathbb{Z}/n\mathbb{Z}$ is then the lattice coset $F^{-1}(k) = (k, 0, 0, 0) + \ker F$. To find a short decomposition of k, we can subtract a nearby vector in $\ker F$ from $(k, 0, 0, 0)$. If $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$ is a basis for $\ker F$, then we let $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ be the (unique) solution in $\mathbb{Q}^4$ to the linear system $(k, 0, 0, 0) = \sum_{i=1}^4 \alpha_i \mathbf{v}_i$ and set

$$(k_1, k_2, k_3, k_4) = (k, 0, 0, 0) - \sum_{i=1}^4 \lfloor \alpha_i \rceil \mathbf{v}_i,$$

then (k_1, k_2, k_3, k_4) is a 4-dimensional decomposition of k. Since $(k_1, k_2, k_3, k_4) = \sum_{i=1}^4 (\alpha_i - \lfloor \alpha_i \rceil) \mathbf{v}_i$ and $|x - \lfloor x \rceil| \le 1/2$ for any x in $\mathbb{Q}$, we have $\|(k_1, k_2, k_3, k_4)\|_\infty \le 2\max_i \|\mathbf{v}_i\|_\infty$.

It is clear that finding short decompositions depends on finding a short basis for $\ker F$, as a result the LLL algorithm [9] is used. Longa and Sica [2] constructed an easy-to-implement algorithm–the twofold Cornacchia-type algorithm, which is an elaborate iterated Cornacchia algorithm that can compute short bases for $\ker F$. 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 $\mathbb{Z}[i]$. The twofold algorithm is efficient, but more importantly, it gives a better and uniform upper bound $\max_i \|\mathbf{v}_i\|_\infty \le Cn^{1/4}$ with $C = 51.5\sqrt{1+|r|+|s|}$. Recently, Yi et al. [6] obtained an improved twofold Cornacchia-type algorithm and showed that it possesses a better theoretic bound of output $Cn^{1/4}$ with $C = (2+\sqrt{2})\sqrt{1+|r|+|s|}$. In particular, their proof is much simpler than Longa and Sica's.

978-1-6654-9489-2/21/$31.00 ©2021 IEEE
DOI 10.1109/CIS54983.2021.00095

Wang et al. [8] constructed a new twofold Cornacchia-type algorithm, one in $\mathbb{Z}$ and the other one in $\mathbb{Z}[\omega]$, where $\omega = \frac{1+\sqrt{-3}}{2}$. It can be used to compute some 4-GLV decompositions on curves with two $\mathbb{Z}$-linear independenly endomorphisms Φ and Ψ satisfying $\Phi^2 + r\Phi + s = 0$ and $\Psi^2+\Psi+1 = 0$. The new algorithm gives a new and unified method to compute all 4-GLV decompositions on j-invariant 0 elliptic curves over $\mathbb{F}_{p^2}$, which is different from the Hu et al.'s algorithm [5]. It can also be used to compute the 4-GLV decomposition on the Jacobian of the hyperelliptic curve defined as $\mathcal{C}/\mathbb{F}_p : y^2 = x^6 + ax^3 + b$.

Our contribution. We construct general 4-GLV lattice reduction algorithms on general cases that $\mathbb{Z}[\Psi]$ are principal maximal orders of imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$, under the assumpution Φ and Ψ are $\mathbb{Z}$-linear independence. We also give the proof that the upper bound of output is $C \cdot n^{1/4}$ in our algorithms, where $C = \frac{4+2\sqrt{d+1}}{3-d}(\sqrt{1+|r|+|s|})$ for $\mathbb{Z}[\Psi] = \mathbb{Z}[\sqrt{-d}]$ and $C = \frac{4\sqrt{d}}{4\sqrt{d}-(d+1)}(\sqrt{1+|r|+|s|})$ for $\mathbb{Z}[\Psi] = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$. Our algorithm contain the case $\mathbb{Z}[\Psi] = \mathbb{Z}[i]$ of Yi et al. [6] which the refinement of Longa and Sica [2] and the case $\mathbb{Z}[\Psi] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ of Wang et al. [8].

The article is organized as follows. II gives the notations and the general 4-GLV decompositions. In III we give general 4-GLV lattice reduction algorithms. IV gives the proof of the upper bound of our algorithms and the value of C. Finally, V makes a conclusion.

II. General 4-GLV decompositions

A. Notation

Let $\mathcal{A}/\mathbb{F}_q$ be an elliptic curve or a hyperelliptic curve defined over the finite field $\mathbb{F}_q$ with infinity point denoted by $\mathcal{O}$. $\mathcal{A}/\mathbb{F}_q$ has two endomorphisms Φ and Ψ satisfying $\Phi^2+r\Phi+s = 0$ and $\Psi^2 - t_\Psi\Psi + n_\Psi = 0$ respectively with $r, s, t_\Psi, n_\Psi \in \mathbb{Z}$. Suppose that $\Delta = t_\Psi^2 - 4n_\Psi = -dk^2 < 0$ be the discriminant of Ψ with d non-square positive integer. Let $K := \mathbb{Q}(\Psi) = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-d})$. Let $\mathcal{G} \subset \mathcal{A}(\mathbb{F}_q)$ be a cyclic subgroup of order n and P be a point in the group $\mathcal{G}$. λ_Φ and λ_Ψ are the eigenvalues of Φ and Ψ on $\mathcal{G}$, which satisfy $\lambda_\Phi^2 + r\lambda_\Phi + s \equiv 0 \bmod n$ and $\lambda_\Psi^2 - t_\Psi\lambda_\Psi + n_\Psi \equiv 0 \bmod n$ respectively. The rectangle norm of $(b_1, \cdots, b_t)$ is denoted by $\| (b_1, \ldots, b_t) \|_\infty = \max_i |b_i|$, for $i = 1, \cdots, t$, $t \in \mathbb{N}_+$. Let $L := \mathbb{Q}(\Phi, \Psi)$ be a biquadratic field and O_L be the maximal order of L. In this paper, we assume that Φ and Ψ are $\mathbb{Z}$-linear independence. This assumption is often achievable on elliptic curves or hyperelliptic curves, see some examples in [2], [8].

B. Analysis

With respect to $\{1, \Phi, \Psi, \Phi\Psi\}$, we can obtain a 4-GLV decomposition as the eq. (1) and construct a map F as the eq. (2). Consider the sequence of group homomorphisms:

$$\mathbb{Z}^4 \xrightarrow[\cong]{f} \mathbb{Z}[\Phi, \Psi] \xrightarrow[\bmod \mathfrak{n}\cap\mathbb{Z}[\Phi,\Psi]]{g} \mathbb{Z}/n\mathbb{Z}$$

Under the assumpution $\mathbb{Q}(\Phi)$ and $\mathbb{Q}(\Psi)$ are disjoint, let $\mathfrak{n}$ is a specific prime lying above n in the biquadratic field $\mathbb{Q}(\Phi, \Psi)$. We have $\mathbb{Z}[\Phi, \Psi] \subseteq O_L$. Since the degrees of Φ and Ψ are much smaller than n, the prime n is unramified in K, and the existence of λ and μ above means that n splits in $\mathbb{Q}(\Phi)$ and $\mathbb{Q}(\Psi)$, namely that n splits completely in K. There exists therefore a prime ideal $\mathfrak{n}$ of $\mathfrak{o}_K$ dividing $n\mathfrak{o}_K$, such that its norm is n. We can also suppose that $\mathfrak{n}' = \mathfrak{n} \cap \mathbb{Z}[\Phi, \Psi]$ and $\mathfrak{n}'' = \mathfrak{n} \cap \mathbb{Z}[\Psi]$. The inclusions $\mathbb{Z} \hookrightarrow \mathbb{Z}[\Psi] \hookrightarrow \mathbb{Z}[\Phi, \Psi] \hookrightarrow O_L$ induce isomorphisms $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}[\Psi]/\mathfrak{n}'' \cong \mathbb{Z}[\Phi, \Psi]/\mathfrak{n}' \cong O_L/\mathfrak{n}$. In particular we can suppose $\Phi \equiv \lambda_\Phi \mod \mathfrak{n}'$ and $\Psi \equiv \lambda_\Psi \mod \mathfrak{n}'$. Moreover, since the reduction map g is surjective, the composition of the two homomorphisms f and g gives (for the appropriate $\mathfrak{n}$) the 4-dimensional GLV map F:

$$\begin{aligned} F : \mathbb{Z}^4 &\to \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}[\Phi, \Psi]/\mathfrak{n}', \\ (x_1, x_2, x_3, x_4) &\mapsto x_1 + x_2\lambda_\Phi + x_3\lambda_\Psi + x_4\lambda_\Phi\lambda_\Psi \bmod n, \end{aligned} \tag{4}$$

which says that the index of $\mathfrak{n}'$ inside $\mathbb{Z}[\Phi, \Psi]$ is n. Since the first map f is an isomorphism, we get that $\ker F = f^{-1}(\mathfrak{n}')$ and $\ker F$ has index $[\mathbb{Z}^4 : \ker F] = n$ inside $\mathbb{Z}^4$. The key of finding a short basis of $\ker F$ is to find a short $\mathbb{Z}$-basis of $\mathfrak{n}'$. In the following, we give general 4-GLV lattice reduction algorithms to compute a short basis of $\ker F$.

III. General 4-GLV lattice reduction algorithms

A. The First Part in $\mathbb{Z}$

We identify $\mathbb{Z}[\Phi, \Psi]$ with the free $\mathbb{Z}[\Psi]$-module of rank 2 with basis $\{e_1, e_2\} = \{1, \Phi\}$. To find a short $\mathbb{Z}$-basis of $\mathfrak{n}'$, we first need to find a generator $\nu = a + b\Psi$ of $\mathfrak{n}''$ in the order $\mathbb{Z}[\Psi]$. This can be achieved by using the first Cornacchia's algorithm in $\mathbb{Z}$, see the Algorithm 1.

Algorithm 1: The first part in $\mathbb{Z}$

Input: n, $1 < \lambda_\Psi < n$.
Output: $\nu = a + b\Psi$ dividing n.

1. **initialize**
   $r_0 \leftarrow n$, $r_1 \leftarrow \lambda_\Psi, r_2 \leftarrow n$,
   $t_0 \leftarrow 0$, $t_1 \leftarrow 1, t_2 \leftarrow 0$,
   $q \leftarrow 0$.
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: $\nu = r_1 - \Psi t_1,\ a = r_1,\ b = -t_1$

Now, we prove that the Algorithm 1 is feasible, i.e., there exists an element $\nu = a + b\Psi \in \mathbb{Z}[\Psi]$ with $|a|, |b| < \sqrt{n}$

such that the norm

$$N_{\mathbb{Z}[\Psi]/\mathbb{Z}}(\nu) = b_n n, \quad \nu(P) = \mathcal{O} \tag{5}$$

for some positive integer b_n, which is relatively small to n.

Recall that Algorithm 1 makes use of the extended Euclidean algorithm applied to n, λ_Ψ to produce a sequence of relations

$$s_i n + t_i \lambda_\Psi = r_i, \qquad \text{for } i = 0, 1, 2, \ldots \tag{6}$$

where $|s_i| < |s_{i+1}|$ for $i \geq 1, |t_i| < |t_{i+1}|$ and $r_i > r_{i+1} \geq 0$ for $i \geq 0$. Also, we have

$$|s_{j+1} r_j| + |s_j r_{j+1}| = \lambda_\Psi \text{ and } |t_{j+1} r_j| + |t_j r_{j+1}| = n, \tag{7}$$

for all $i \geq 0$. The Algorithm 1 defines the index m as the largest integer for which $r_m > \sqrt{n}$. Then the equation (7) with $i = m$ gives that $|t_{m+1}| < \sqrt{n}$, so that the vector $(r_{m+1}, -t_{m+1})$ has rectangle norm bounded by $\sqrt{n}$. Now, the existence of such ν is guaranteed from the following.

Lemma 3.1 ([10]): There exists an element $\nu \in \mathbb{Z}[\Psi]$ satisfying (5) for some positive integer $b_n \leq 3n_\Psi$. Moreover, $b_n = 1$ when $\mathbb{Z}[\Psi]$ is a principal maximal order and n splits in $\mathbb{Q}(\Psi)/\mathbb{Q}$.

Proof: Let $\upsilon_1 = (r_{m+1}, -t_{m+1})$ be a short vector constructed in Algorithm 1 such that $r_{m+1} - t_{m+1}\lambda_\Psi \equiv 0 \bmod n$ by equation (6), it is clear that $(r_{m+1} - t_{m+1}\Psi)P = \mathcal{O}$. Put $a := r_{m+1}, b := -t_{m+1}$ and $\nu = a + b\Psi$, let $n' = N_{\mathbb{Z}[\Psi]/\mathbb{Z}}(a + b\Psi) \in \mathbb{Z}$. Then we have $N_{\mathbb{Z}[\Psi]/\mathbb{Z}}(\nu) = (a+b\bar{\Psi})(a+b\Psi) = n'$, so $n'P = (a+b\bar{\Psi})(a+b\Psi)P = \mathcal{O}$. It implies that $n' \equiv 0 \mod n$ and $n' = b_n n$ for some integer b_n. Since $a, b \leq \sqrt{n}$ in Algorithm 1 and $|t_\Psi| < 2\sqrt{n_\Psi}$ by Ψ is in general not a rational integer, we have

$$\begin{aligned} b_n n &= a^2 + abt_\Psi + b^2 n_\Psi \leq a^2 + |abt_\Psi| + b^2 n_\Psi \\ &\leq n_\Psi \left(a^2 + |ab| + b^2\right) \leq 3n_\Psi n. \end{aligned}$$

The first assertion is proven.

When $\mathbb{Z}[\Psi]$ is a principal maximal order and n splits in $\mathbb{Q}(\Psi)/\mathbb{Q}$, it is obvious that $N_{\mathbb{Z}[\Psi]/\mathbb{Z}}(a+b\Psi) = n$, i.e. $b_n = 1$. ■

In this paper, we consider the cases of principle maximal orders $\mathbb{Z}[\Psi]$ to construct a short basis of determinant n of $\ker F$. By $\mathbb{Q}(\Psi) = \mathbb{Q}(\sqrt{-d})$ and $\mathbb{Z}[\Psi]$ is the maximal order of $\mathbb{Q}(\Psi)$, then $\mathbb{Z}[\Psi] = \mathbb{Z}[\sqrt{-d}]$ for $d \equiv 1, 2 \mod 4$ and $\mathbb{Z}[\Psi] = \mathbb{Z}[(1 + \sqrt{-d})/2]$ for $d \equiv 3 \mod 4$. Moreover, if $\mathbb{Z}[\Psi]$ is a principle maximal order, then $d = 1, 2, 3, 7, 11$ or 19 et al..

B. The Second Part in $\mathbb{Z}[\Psi]$

We have seen how to construct $\nu \in \mathbb{Z}[\Psi]$ with $\nu(P) = \mathcal{O}$ in III-A. By identifying $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ with $(z_1, z_2) = (x_1 + \Psi x_3, x_2 + \Psi x_4) \in \mathbb{Z}[\Psi]^2$, we can rewrite the 4-GLV reduction map F in (4) as (using the same letter F by abuse of notation)

$$\begin{aligned} F : \mathbb{Z}[\Psi]^2 &\to \mathbb{Z}[\Psi]/\nu \cong \mathbb{Z}/n\mathbb{Z} \\ (z_1, z_2) &\mapsto z_1 + \lambda_\Phi z_2 (\mathrm{mod}\nu). \end{aligned} \tag{8}$$

From the output ν with $N_{\mathbb{Z}[\Psi]/\mathbb{Z}}(\nu) = n$ in the Algorithm 1 and λ_Φ, we can apply the extended Euclidean algorithm with integer divisions occurring in $\mathbb{Z}[\Psi]$, see the Algorithm 2.

Suppose we have used the Algorithm 2 to find a short $\mathbb{Z}[\Psi]$-basis $\{\upsilon_1, \upsilon_2\}$ of $\mathfrak{n}'$ with $\max_i(|\upsilon_i|) \leq Cn^{1/4}$ for some constant $C > 0$. Thus we get a short $\mathbb{Z}$-basis $\{\upsilon_1, \upsilon_1\Psi, \upsilon_2, \upsilon_2\Psi\}$ of $\mathfrak{n}'$. Moreover, write $\upsilon_1 = (a_1+b_1\Psi)+(c_1 + d_1\Psi)\Phi$ and $\upsilon_2 = (a_2 + b_2\Psi) + (c_2 + d_2\Psi)\Phi$, then

$$\mathfrak{n}' = (a_1 + b_1\Psi + (c_1 + d_1\Psi)\Phi)\mathbb{Z}[\Psi] \tag{9}$$
$$+ (a_2 + b_2\Psi + (c_2 + d_2\Psi)\Phi)\mathbb{Z}[\Psi]. \tag{10}$$

By $\ker F = f^{-1}(\mathfrak{n}')$, we get a short basis $\{\widetilde{\upsilon}_1, \widetilde{\upsilon}_2, \widetilde{\upsilon}_3, \widetilde{\upsilon}_4\}$ of $\ker F$, which are the rows of the following matrix with Ψ satistying the quadratic equation $\Psi^2 - t_\Psi\Psi + n_\Psi = 0$.

$$\begin{pmatrix} a_1 & c_1 & b_1 & d_1 \\ -n_\Psi b_1 & -n_\Psi d_1 & a_1 + t_\Psi b_1 & c_1 - n_\Psi d_1 \\ a_2 & c_2 & b_2 & d_2 \\ -n_\Psi b_2 & -n_\Psi d_2 & a_2 + t_\Psi b_2 & c_2 - n_\Psi d_2 \end{pmatrix} \tag{11}$$

Algorithm 2: The second part in $\mathbb{Z}[\Psi]$

Input: ν prime dividing n rational prime,
$1 < \lambda_\Phi < n$, such that $\lambda_\Phi^2 + r\lambda_\Phi + s \equiv 0 \bmod n$.
Output: Two vectors in $\mathbb{Z}[\Psi]^2$: υ_1, υ_2.
1. **initialize:**
   $r_0 \leftarrow \lambda_\Phi$, $r_1 \leftarrow \nu$, $r_2 \leftarrow n$,
   $s_0 \leftarrow 1$, $s_1 \leftarrow 0$, $s_2 \leftarrow 0$, $q \leftarrow 0$.
2. **main loop:**
   while $|r_1| \geq Cn^{1/4}$ 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**: $\upsilon_1 = (r_1, -s_1)$,
   if $\max\{|r_0|, |s_0|\} \leq \max\{|r_2|, |s_2|\}$
   $\upsilon_2 = (r_0, -s_0)$
   else $\upsilon_2 = (r_2, -s_2)$.

We can also give the direct form algorithm similar to the Algorithm 3 in [8], and the output of the algorithm is a short basis of $\ker F$ as the rows in matrix (11).

IV. The Value of C

For the algorithm in $\mathbb{Z}[\Psi]$, we also have three such sequences $\{r_j\}, \{s_j\}, \{q_j\}$ for $j \geq 0$. 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 $\mathbb{Z}[\Psi]$. We will choose q_{j+1} as the closest integer to r_j/r_{j+1} denoted by $\lfloor r_j/r_{j+1} \rceil$. Let us note that $r_i > r_{i+1} \geq 0$ for $i \geq 0$

holds in modulus (in particular, the algorithm terminates). However, a crucial role is played by the following equation

$$s_{j+1}r_j - s_j r_{j+1} = (-1)^{j+1}\nu, \tag{12}$$

which can derive a bound on $|s_{j+1}r_j|$ and $|s_j r_{j+1}|$.

Theorem 4.1: The two vectors υ_1, υ_2 output by Algorithm 2 are $\mathbb{Z}[\Psi]$-linearly independent. They belong to $\mathfrak{n}'$ and satisfy that if $\mathbb{Z}[\Psi] = \mathbb{Z}[\sqrt{-d}]$

$$\begin{cases} \|\upsilon_1\|_\infty \leq \sqrt{\dfrac{4+2\sqrt{d+1}}{3-d}} n^{\frac{1}{4}} \\ \|\upsilon_2\|_\infty \leq \dfrac{4+2\sqrt{d+1}}{3-d}(\sqrt{1+|r|+|s|})n^{\frac{1}{4}} \end{cases},$$

and if $\mathbb{Z}[\Psi] = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]$

$$\begin{cases} \|\upsilon_1\|_\infty \leq \sqrt{\dfrac{4\sqrt{d}}{4\sqrt{d}-(d+1)}} n^{\frac{1}{4}} \\ \|\upsilon_2\|_\infty \leq \dfrac{4\sqrt{d}}{4\sqrt{d}-(d+1)}(\sqrt{1+|r|+|s|})n^{\frac{1}{4}} \end{cases}.$$

Before proving Theorem 4.1, we need the following lemmas. In the Algorithm 2, $q_{j+1} \in \mathbb{Z}[\Psi]$ is the closest integer to r_j/r_{j+1}. Here, we define a fundamental regin of the lattice $\mathbb{Z}[\Psi]$. We single out a fundamental parallelogram but not containing the origin as a vertex (since $q_{j+1} \neq 0$). First, we quote the conclusion in [7, Lemma 2] to give a property that the closest lattice point to a point in the fundamental parallelogram of the lattice $\mathbb{Z}[\Psi]$, see the following.

Lemma 4.2 ([7]): Let ABC be any triangle in $\mathbb{R}^2$ with vertices A, B and C. For any two points P, P', let PP' denote their distance. Let O be any point inside the closure of ABC maximising

$$f(P) = \min\{PA, PB, PC\},$$

so that $R \overset{\text{def}}{=} f(O) = \max_{P \in \overline{ABC}} f(P)$. In other terms, O is the farthest point from any vertex. Then

1. if ABC is acutangle, O is the centre of the circumscribed circle and $R = r$ is its radius,
2. if $\widehat{BAC}$ (the angle abutting to A) has measure greater than $\pi/2$ radians, so that $[BC]$ is the largest side of the triangle, supposing that $[AC]$ is the smallest side, then O is obtained as the intersection of the axis of $[AB]$ with $[BC]$ (so that $OA = OB$) and $R = AB/(2\cos\widehat{CBA})$.

From the Lemma 4.2, it shows that any point lying inside a fundamental parallelogram will be at a distance $< R$ from one of the vertices. The R is optimal with the value:

$$R = \begin{cases} \dfrac{\sqrt{1+d}}{2}, & \text{if } \mathbb{Z}[\Psi] = \mathbb{Z}[\sqrt{-d}], \\ \dfrac{\sqrt{d}+\sqrt{d^{-1}}}{4}, & \text{if } \mathbb{Z}[\Psi] = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]. \end{cases} \tag{13}$$

By Lemma 4.2, we can choose from the set of all vertices of the fundamental parallelogram which one is the adequate. Let q_{j+1} corresponds to the vertice of the fundamental parallelogram, which is the one closest to the point r_j/r_{j+1} lies in the fundamental parallelogram. Since $q_j \neq 0$, it means that we must be careful to avoid all four diamonds which have the origin as a vertex. But this follows from the fact that at all steps $j \geq 0$ we always have $|r_j/r_{j+1}| \geq 1/R$.

Lemma 4.3: If $|\frac{s_j}{s_{j+1}}| < 1$, then we have

$$|s_{j+1}r_j| \leq \frac{1}{1-R}|\nu|, \quad |s_j r_{j+1}| \leq \frac{2-R}{1-R}|\nu|.$$

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

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

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

$$|\nu| = |s_{j+1}r_j - s_j r_{j+1}| > (1-R)|s_{j+1}r_j|,$$

which implies $|s_{j+1}r_j| \leq \frac{1}{1-R}|\nu|$. By $|s_j r_{j+1}| = |s_{j+1}r_j + (-1)^j\nu|$, then $|s_j r_{j+1}| \leq \frac{2-R}{1-R}|\nu|$. ■

Lemma 4.4 ([2], [8]): For any nonzero $(\upsilon_1, \upsilon_2) \in \mathfrak{n}' \subset \mathbb{Z}[\Psi]^2$, we have

$$\max(|\upsilon_1|, |\upsilon_2|) \geq \frac{\sqrt{|\nu|}}{\sqrt{1+|r|+|s|}}.$$

In particular, for any $j \geq 0$, we have

$$\max(|r_j|, |s_j|) \geq \frac{\sqrt{|\nu|}}{\sqrt{1+|r|+|s|}}$$

Proof: (Proof of Theorem 4.1). According to the eq. (6) and (7), it is easily to get that the vectors υ_1, υ_2 are $\mathbb{Z}[\Psi]$-linearly independent and belong to $\mathfrak{n}'$.

We assume that Algorithm 2 stops at the m-th step ($m \geq 1$). Then $\upsilon_1 = (r_{m+1}, -s_{m+1})$ and $|r_m| \geq \sqrt{\frac{1}{1-R}} n^{\frac{1}{4}}$ and $|r_{m+1}| < \sqrt{\frac{1}{1-R}} n^{\frac{1}{4}}$. Considering the two cases $\left|\frac{s_m}{s_{m+1}}\right| < 1$ and $|s_m| \geq |s_{m+1}|$, we can get

$$\|\upsilon_1\|_\infty \leq \sqrt{\frac{1}{1-R}} n^{\frac{1}{4}}, \quad \|\upsilon_2\|_\infty \leq \frac{1}{1-R}\sqrt{1+|r|+|s|} n^{\frac{1}{4}}.$$

These discussions are similar to the proof in [8], [6, Theorem 2], just pay attention to the difference in coefficients of $n^{1/4}$.

Here we just give the disscussion for the case $\left|\frac{s_m}{s_{m+1}}\right| < 1$, the other case $|s_m| \geq |s_{m+1}|$ is similar. Using Lemma 4.3 we get $|s_{m+1}| \leq \sqrt{\frac{1}{1-R}}\sqrt{|\nu|}$, with $|r_{m+1}| < \sqrt{\frac{1}{1-R}}\sqrt{|\nu|}$ we can easily deduce

$$\|\upsilon_1\|_\infty \leq \sqrt{\frac{1}{1-R}} n^{\frac{1}{4}}.$$

If $|r_{m+1}| < \frac{\sqrt{|\nu|}}{\sqrt{1+|r|+|s|}}$, by Lemma 4.4 we get a lower bound $|s_{m+1}| \geq \frac{\sqrt{|\nu|}}{\sqrt{1+|r|+|s|}}$ which implies $|r_m| \leq \frac{1}{1-R}\sqrt{1+|r|+|s|}\sqrt{|\nu|}$ using again Lemma 4.3. Together with the restricted condition $|s_m| < |s_{m+1}| \leq \sqrt{\frac{1}{1-R}}\sqrt{|\nu|} < \frac{1}{1-R}\sqrt{1+|r|+|s|}\sqrt{|\nu|}$ we can obtain

$$\|(r_m, -s_m)\|_\infty \leq \frac{1}{1-R}\sqrt{1+|r|+|s|}n^{\frac{1}{4}}.$$

If $|r_{m+1}| \geq \frac{\sqrt{|\nu|}}{\sqrt{1+|r|+|s|}}$, when $|s_{m+1}| \geq |s_{m+2}|$ we can get $|s_{m+2}| \leq \sqrt{\frac{1}{1-R}}\sqrt{|\nu|}$, $|r_{m+2}| \leq |r_{m+1}| < \sqrt{\frac{1}{1-R}}\sqrt{|\nu|}$. When $|s_{m+1}| < |s_{m+2}|$, by the Lemma 4.3 we can deduce $|s_{m+2}| \leq \frac{1}{1-R}\sqrt{1+|r|+|s|}\sqrt{|\nu|}$. Hence in both cases we have

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

By the definition of υ_2, it is easily to get

$$\|\upsilon_2\|_\infty \leq \frac{1}{1-R}\sqrt{1+|r|+|s|}n^{\frac{1}{4}}.$$

For the two cases of $\mathbb{Z}[\Psi] = \mathbb{Z}[\sqrt{-d}]$ or $\mathbb{Z}[(1+\sqrt{-d})/2]$ and the corresponding R in eq. (14), we can easily get the upper bound of the vectors υ_1, υ_2. ■

From the Theorem 4.1, the value of C in the Algorithm 2 is that

$$C = \begin{cases} \frac{4+2\sqrt{d+1}}{3-d}(\sqrt{1+|r|+|s|}), & \text{if } \mathbb{Z}[\Psi] = \mathbb{Z}[\sqrt{-d}], \\ \frac{4\sqrt{d}}{4\sqrt{d}-(d+1)}(\sqrt{1+|r|+|s|}), & \text{if } \mathbb{Z}[\Psi] = \mathbb{Z}[\frac{1+\sqrt{-d}}{2}]. \end{cases} \tag{14}$$

Morever, for general 4-GLV decompositions, we can obtain the conclusion.

Theorem 4.5: For general 4-GLV decmpositions with the two $\mathbb{Z}$-linearly independent endomorphisma Φ and Ψ, under the considition that $\mathbb{Z}[\Psi]$ is the principle maximal order, our general 4-GLV lattice algorithms 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 $2Cn^{1/4}$.

Remark 1: If $d = 1$ and $\mathbb{Z}[\Psi] = \mathbb{Z}[\sqrt{-1}]$, then $C = (2+\sqrt{2})\sqrt{1+|r|+|s|}$, which is the case of Yi et al. [6]. If $d = 3$ and $\mathbb{Z}[\Psi] = \mathbb{Z}[(1+\sqrt{-3})/2]$, then $C = \frac{(3+\sqrt{3})}{2}\sqrt{1+|r|+|s|}$, which is the case of Wang et al.[8].

V. Conclusion

We have constructed general 4-dimensional GLV lattice reduction algorithms under the assumpation that Φ and Ψ are $\mathbb{Z}$-linearly independence and $\mathbb{Z}[\Psi]$ is the principle maximal order of $\mathbb{Q}(\sqrt{-d})$. The general 4-dimensional GLV lattice reduction algorithms are twofold Cornacchia-type algorithms, the first part in $\mathbb{Z}$ and the second part in the domain $\mathbb{Z}[\Psi]$. Our algorithms cover the previous results in [6], [8].

Acknowledgements

The third author was supported by NSFC grant 1210010386. The fourth author was supported by Anhui Initiative in Quantum Information Technologies grant AHY150200, NSFC grant 11571328. The fifth author was supported by NSFC (grant 61972370 and 61632013), Fundamental Research Funds for Central Universities in China grant WK3480000007.

References

[1] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, CRC Press, Boca Raton (2005).

[2] P.Longa and F. Sica, “Four-Dimensional Gallant-Lambert-Vanstone Scalar Multiplication”,J. Cryptol, vol.27(2), 2014, pp. 248-283.

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

[4] S. Galbraith, X. Lin and M. Scott, “Endomorphisms for faster elliptic curve cryptography on a large class of curves”, In: Joux, A. (ed.) Advances in Cryptology-Eurocrypt 2009. LNCS, vol. 5479. Springer (2009).

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

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

[7] F. Sica, M. Ciet and J.J. Quisquater, “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).

[8] B. Wang, Y. Ouyang, S. Li and H G. Hu, “A New Twofold Cornacchia-Type Algorithm and Its Applications”, Advances in Mathematics of Communications, accepted, https://www.aimsciences.org/article/doi/10.3934/amc.2021026.

[9] H. Cohen, A Course in Computational Algebraic Number Theory, GTM 138, Springer, Heidelberg, 2000.

[10] Y H. Park, S. Jeong, C. Kim and J. Lim, “An Alternate Decomposition of an Integer for Faster Point Multiplication on Certain Elliptic Curves”, In D. Naccache and P. Paillier, editors, Advances in Cryptology - Proceedings of PKC 2002, vol: Lncs 2274, pp: 323–334. Springer, 2002.