Analysis of the Gallant-Lambert-Vanstone Method based on Efficient Endomorphisms: Elliptic and Hyperelliptic Curves

Francesco Sica*, Mathieu Ciet*, and Jean-Jacques Quisquater

UCL Crypto Group
Place du Levant, 3. B-1348 Louvain-la-Neuve. Belgium
{sica, ciet, jjq}@dice.ucl.ac.be – http://www.dice.ucl.ac.be/crypto/

Abstract. In this work we analyse the GLV method of Gallant, Lambert and Vanstone (CRYPTO 2001) which uses a fast endomorphism Φ with minimal polynomial $X^2 + rX + s$ to compute any multiple kP of a point P of order n lying on an elliptic curve.
First we fill in a gap in the proof of the bound of the kernel $\mathcal{K}$ vectors of the reduction map $f\colon (i,j) \mapsto i + \lambda j \pmod{n}$. In particular, we prove the GLV decomposition with explicit constant

$$kP = k_1 P + k_2 \Phi(P), \quad \text{with } \max\{|k_1|, |k_2|\} \leq \sqrt{1 + |r| + s}\sqrt{n} \ .$$

Next we improve on this bound and give the best constant in the given examples for the quantity $\sup_{k,n} \max\{|k_1|, |k_2|\}/\sqrt{n}$. Independently Park, Jeong, Kim, and Lim (PKC 2002) have given similar but slightly weaker bounds.
Finally we provide the first explicit bounds for the GLV method generalised to hyperelliptic curves as described in Park, Jeong and Lim (EUROCRYPT 2002).

Keywords. *Elliptic curve cryptography, fast performance, efficiently-computable endomorphisms, algebraic number fields.*

1 Introduction

Since elliptic curves made their entrance into cryptography in 1985 [8, 13], it has become of vital importance to secure the same performance on the elliptic cryptosystems as on the traditional asymmetric ones such as RSA.

* The work described in this paper has been supported [in part] by the Commission of the European Communities through the IST Programme under Contract IST-1999-12324, http://www.cryptonessie.org/. The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. The views expressed are those of the authors and do not represent an official view/position of the NESSIE project (as a whole).

For this, a key step is to be able to compute a scalar multiple kP of an elliptic curve point P of large prime order n (see [1, 12] for background on elliptic curve cryptography). Various methods have been devised to this end [6], most of them adopting a binary setting (elliptic curves E over finite fields of characteristic 2). A group of methods cleverly employs a distinguished endomorphism $\Phi \in \mathrm{End}(E)$ to split a large computation into a sequence of cheaper ones so that the overall computational cost is lowered [17].

Recently, Gallant, Lambert and Vanstone [5] used such a technique, which, contrary to previous ones, also applies to curves defined over large prime fields. Their method uses an efficiently computable endomorphism $\Phi \in \mathrm{End}(E)$ to rewrite kP as

$$kP = k_1 P + k_2 \Phi(P), \quad \text{with } \max\{|k_1|, |k_2|\} = O(\sqrt{n}) \ . \tag{1}$$

Their key point is an algorithm (henceforth called the GLV algorithm) which inputs integers n and $0 < \lambda < n$ and produces for any $k \pmod n$, two residues $k_1, k_2 \pmod n$ such that

$$k \equiv k_1 + \lambda k_2 \pmod n \ .$$

However they fail to provide an upper bound on $\max\{|k_1|, |k_2|\}$ but only give a heuristic estimate that this should be $O(\sqrt{n})$ (but again no estimation of the involved constant appears in their paper). An upper bound was first demonstrated in [15] using an apparently different method.

In this work we first supply a proof that the original GLV algorithm works by producing a required upper bound and then we give the value for $\sup_{k,n} \max\{|k_1|, |k_2|\}/\sqrt{n}$ in the case where n is the norm of an element of $\mathbb{Z}[\Phi]$, which is the case in the examples given in [5, 15]. This allows us to show that the class of elliptic curves susceptible to the GLV speedup is exceptional.

At the conference, we became aware of another contribution to the GLV method [7] where a necessary condition is developed to insure that in (1) the constant in $O(\sqrt{n})$ is 1. An algorithm alternative to the GLV algorithm is then presented.

A way to improve the GLV algorithm would be to find a decomposition

$$kP = k_1 P + k_2 \Phi(P) + \cdots + k_d \Phi^{d-1}(P), \quad \text{with } \max_{1 \le i \le d} |k_i| = O(n^{1/d}) \ .$$

This is not possible in general using the GLV paradigm, since the powers Φ^i are independent (over $\mathbb{Z}$) only when $i < 2$. However, in [14], a class of Φ's for which such a decomposition exists is found. Nevertheless this does

not apply to our analysis since it is supposed that the norm of Φ is not too small (compared to n), whereas in our work it is fixed (denoted by s below).

On the other hand the previous decomposition can be applied to the generalisation of the GLV algorithm to hyperelliptic curves of genus at least $d/2$ as described in [16]: in this context we provide an explicit upper bound, of the same nature as (1).

2 Bridging the Logical Gaps of the GLV Algorithm

In this part, we will briefly summarize the Gallant-Lambert-Vanstone (GLV for short) computation method [5]. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and P be a point of this curve with order n such that the cofactor $h = \#E(\mathbb{F}_q)/n$ is small, say $h \leq 4$. Let us consider Φ a non trivial endomorphism defined over $\mathbb{F}_q$ and $X^2 + rX + s$ its characteristic polynomial. In all the examples r and s are actually small fixed integers and q is varying in some family. By the Hasse bound, since n is large, $\Phi(P) = \lambda P$ for some $\lambda \in [0, n-1]$. Indeed, there is only one copy of $\mathbb{Z}/n$ inside $E(\mathbb{F}_q)$ and $\Phi(P)$ has also order dividing n. We can easily exclude the case where $\lambda = 0$ which is exceptional (for instance in the examples we have $n \nmid s$, by the Hasse bound). In all cases, λ is obtained as a root of $X^2 + rX + s$ modulo n.

A crucial role of the GLV method lies in the definition of the group homomorphism

$$\begin{aligned} f \colon \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Z}/n \\ (i, j) &\mapsto i + \lambda j \pmod{n} \ . \end{aligned}$$

Let $\mathcal{K} = \ker f$. It is clearly a sublattice of $\mathbb{Z} \times \mathbb{Z}$. Let v_1, v_2 be two linearly independent vectors of $\mathcal{K}$ satisfying $\max\{ \mid v_1 \mid , \mid v_2 \mid \} < M$ for some $M > 0$, where $\mid \cdot \mid$ denotes any metric norm. Express

$$(k, 0) = \beta_1 v_1 + \beta_2 v_2 \ ,$$

where $\beta_i \in \mathbb{Q}$. Then round β_i to the nearest integer $b_i = \lfloor \beta_i \rceil = \lfloor \beta_i + 1/2 \rfloor$ and let $v = b_1 v_1 + b_2 v_2$. Note that $v \in \mathcal{K}$ and that $u \stackrel{\text{def}}{=} (k, 0) - v$ is short. Indeed by the triangle inequality we have that

$$\mid u \mid \ \leq \ \left| \frac{v_1 + v_2}{2} \right| < M \ .$$

If we set $(k_1, k_2) = u$, then we get $k = k_1 + k_2 \lambda$ or equivalently $kP = k_1 P + k_2 \Phi(P)$, with $\mid (k_1, k_2) \mid \ < M$. Thus it is essential in the GLV

method that M be as small as possible, keeping in mind that by a simple counting argument we must have $M \geq \sqrt{n}/2$.

Gallant, Lambert and Vanstone then claim without proof that in fact $M \leq \Bbbk\sqrt{n}$, for some constant $\Bbbk$.[1]

We overcome this omission in the next section.

2.1 A Value for $\Bbbk$

Recall that the GLV algorithm makes use of the extended Euclidean algorithm applied to n, λ to produce a sequence of relations

$$s_i n + t_i \lambda = r_i, \quad \text{for } i = 0, 1, 2, \ldots \ , \tag{2}$$

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 (cf. [5, Lemma 1(iv)])

$$r_i|t_{i+1}| + r_{i+1}|t_i| = n \quad \text{for all } i \geq 0 \ . \tag{3}$$

The GLV algorithm defines the index m as the largest integer for which $r_m > \sqrt{n}$. Then (3) with $i = m$ gives that $|t_{m+1}| < \sqrt{n}$, so that the kernel vector $v_1 = (r_{m+1}, -t_{m+1})$ has rectangle norm[2] bounded by $\sqrt{n}$. The GLV algorithm then sets v_2 to be the shorter between $(r_m, -t_m)$ and $(r_{m+2}, -t_{m+2})$ but does not give any estimate on the size of v_2. In fact, Gallant, Lambert and Vanstone claim that

$$\min\left(|(r_m, -t_m)|, |(r_{m+2}, -t_{m+2})|\right) \leq \Bbbk\sqrt{n} \ ,$$

which is what we will now show, with an explicit value of $\Bbbk$.

Let $\lambda, \mu \in [1, n-1]$ be the zeros of $X^2 + rX + s \pmod n$. For any $(x, y) \in \mathcal{K} - \{(0, 0)\}$, we have

$$0 \equiv (x + \lambda y)(x + \mu y) \equiv x^2 - rxy + sy^2 \pmod n \ ,$$

hence since $X^2 + rX + s$ is irreducible in $\mathbb{Z}[X]$ we must have $x^2 - rxy + sy^2 \geq n$. This certainly implies that

$$\max(|x|, |y|) \geq \sqrt{\frac{n}{1 + |r| + s}} \ .$$

In particular, $|(r_{m+1}, -t_{m+1})| \geq \sqrt{n}/\sqrt{1 + |r| + s}$.

[1] They actually also assume $\Bbbk = 1$ which is true in their examples from Corollary 1, but cannot be true in general, by our analysis on the optimal bound.

[2] The rectangle norm of (x, y) is by definition $\max(|x|, |y|)$. We denote it by $|(x, y)|$.

Case 1: $|t_{m+1}| \geq \sqrt{n}/\sqrt{1+|r|+s}$. Then (3) with $i = m$ implies that $r_m < \sqrt{1+|r|+s}\sqrt{n}$, hence

$$|(r_m, -t_m)| < \sqrt{1+|r|+s}\sqrt{n} \ . \tag{4}$$

Case 2: $r_{m+1} \geq \sqrt{n}/\sqrt{1+|r|+s}$. The same (3) with $i = m+1$ implies that $|t_{m+2}| < \sqrt{1+|r|+s}\sqrt{n}$, hence

$$|(r_{m+2}, -t_{m+2})| < \sqrt{1+|r|+s}\sqrt{n} \ . \tag{5}$$

We have thus proved the following

Theorem 1. *An admissible value for* $\mathbb{k}$ *is*

$$\mathbb{k} = \sqrt{1+|r|+s} \ .$$

In particular any multiple kP *can be decomposed as* $kP = k_1 P + k_2 \Phi(P)$ *with* $\max\{|k_1|, |k_2|\} < \sqrt{1+|r|+s}\sqrt{n}$.

We next revisit the GLV map f, following an idea already present in [15]. This will lead us to an improvement for $\mathbb{k}$ and in some instances, to the best possible constant.

3 An Algebraic Interpretation of the GLV Method

Let Φ be a non trivial endomorphism defined over $\mathbb{F}_q$, as in the GLV method, satisfying $\Phi^2 + r\Phi + s = 0$.

Consider the sequence of group homomorphisms:

$$\begin{array}{ccccc} \mathbb{Z}\times\mathbb{Z} & \xrightarrow[\varphi]{\cong} & \mathbb{Z}[\Phi] & \xrightarrow[\text{mod } \mathfrak{n}\cap\mathbb{Z}[\Phi]]{\text{reduction}} & \mathbb{Z}/n \\ (i,j) & \longmapsto & i+j\Phi & \longmapsto & i+\lambda j \pmod n \ . \end{array}$$

Here $\mathfrak{n}$ is a specific prime lying above n in the quadratic field $\mathbb{Q}(\Phi)$ (remember that n splits in $\mathbb{Q}(\Phi)$). The composition of the two homomorphisms gives (for the appropriate $\mathfrak{n}$) the Gallant-Lambert-Vanstone map $f : (i,j) \mapsto i + \lambda j \pmod n$. We henceforth assume we made this choice of $\mathfrak{n}$.

Note that $\mathbb{Z}[\Phi]$ is actually a normed ring with norm

$$N_{\mathbb{Z}[\Phi]/\mathbb{Z}}(i + j\Phi) = i^2 + sj^2 - rij \ .$$

When embedding $\mathbb{Z}[\Phi]$ into $\mathbb{C}$, this norm actually becomes the square of the usual complex Euclidean norm. Therefore under the (group) isomorphism φ, we can define the *number theoretic norm* $\langle\langle (i,j)\rangle\rangle$ of $(i,j) \in \mathbb{Z} \times \mathbb{Z}$ to be

$$\langle\langle (i,j)\rangle\rangle = \sqrt{i^2 + sj^2 - rij} \ ,$$

different from (but equivalent to) the *rectangle norm* on $\mathbb{Z} \times \mathbb{Z}$, denoted by

$$|(i,j)| = \max(|i|, |j|) \ .$$

We will denote v_1 and v_2 two linearly independent vectors in the kernel $\mathcal{K}$ of the map f. We also require that v_1 and v_2 have rectangle norm $O(\sqrt{n})$.

We say a vector $v \in \mathbb{Z} \times \mathbb{Z}$ is the *shortest* if it has the smallest rectangle norm and that it is the *smallest* when it has the smallest number theoretic norm.

4 Examples

We quote here four examples, dubbed E_1, E_2, E_3 and E_4, appearing already in [5, 15]. Note that in all these examples, $\mathbb{Z}[\Phi]$ is the maximal order and it is principal.

Example 1. Let $p \equiv 1 \pmod 4$ be a prime. Define an elliptic curve E_1 over $\mathbb{F}_p$ by

$$y^2 = x^3 + ax \ .$$

If β is an element of order 4, then the map Φ defined in the affine plane by

$$\Phi(x,y) = (-x, \beta y) \ ,$$

is an endomorphism of E_1 defined over $\mathbb{F}_p$ with $\mathbb{Z}[\Phi] = \mathbb{Z}[\sqrt{-1}]$. Moreover Φ satisfies the equation

$$\Phi^2 + 1 = 0 \ .$$

Example 2. Let $p \equiv 1 \pmod 3$ be a prime. Define an elliptic curve E_2 over $\mathbb{F}_p$ by

$$y^2 = x^3 + b \ .$$

If γ is an element of order 3, then the map Φ defined in the affine plane by

$$\Phi(x,y) = (\gamma x, y) \ ,$$

is an endomorphism of E_2 defined over $\mathbb{F}_p$ with $\mathbb{Z}[\Phi] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. Moreover Φ satisfies the equation

$$\Phi^2 + \Phi + 1 = 0 \ .$$

Example 3. Let $p > 3$ be a prime such that -7 is a quadratic residue modulo p. Define an elliptic curve E_3 over $\mathbb{F}_p$ by

$$y^2 = x^3 - \frac{3}{4}x^2 - 2x - 1 \ .$$

If $\xi = (1 + \sqrt{-7})/2$ and $a = (\xi - 3)/4$, then the map Φ defined in the affine plane by

$$\Phi(x, y) = \left(\frac{x^2 - \xi}{\xi^2(x - a)}, \frac{y(x^2 - 2ax + \xi)}{\xi^3(x - a)^2} \right) \ ,$$

is an endomorphism of E_3 defined over $\mathbb{F}_p$ with $\mathbb{Z}[\Phi] = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Moreover Φ satisfies the equation

$$\Phi^2 - \Phi + 2 = 0 \ .$$

Example 4. Let $p > 3$ be a prime such that -2 is a quadratic residue modulo p. Define an elliptic curve E_4 over $\mathbb{F}_p$ by

$$y^2 = 4x^3 - 30x - 28 \ .$$

The map Φ defined in the affine plane by

$$\Phi(x, y) = \left(-\frac{2x^2 + 4x + 9}{4(x + 2)}, -\frac{2x^2 + 8x - 1}{4\sqrt{-2}(x + 2)^2} \right) \ ,$$

is an endomorphism of E_4 defined over $\mathbb{F}_p$ with $\mathbb{Z}[\Phi] = \mathbb{Z}[\sqrt{-2}]$. Moreover Φ satisfies the equation

$$\Phi^2 + 2 = 0 \ .$$

In the next section, we will investigate an alternative way to construct the GLV vectors v_1 and v_2. We will then give an optimal result on smallest decompositions.

5 The GLV Method Revisited

Let $\Delta = r^2 - 4s < 0$ be the discriminant of the minimal polynomial of Φ and $\epsilon_r = (1-(-1)^r)/2$. In order to find v_1 and v_2, the most natural method to use is Gaussian reduction,[3] which gives an optimal reduced basis v_1 and v_2 meaning:

$$\langle v_1 \rangle = \min_{v \in \mathcal{K} - \{(0,0)\}} \langle v \rangle \leq \frac{\sqrt{3|\Delta|}}{2} \sqrt{n} \ ,$$
$$\langle v_2 \rangle = \min_{v \in \mathcal{K} - \{\mathbb{Z} v_1\}} \langle v \rangle \leq \frac{\sqrt{\epsilon_r - \Delta}}{2} \langle v_1 \rangle \ .$$

The first inequality arises from Theorem 1, while the second comes from taking the norm of $\varphi(v_1)\Phi'$, with $\Phi' = \Phi - [\Re\Phi] = (\epsilon_r + \sqrt{\Delta})/2 \in \mathbb{Z}[\Phi]$.

Note that when n is the norm of *an element* of $\mathbb{Z}[\Phi]$, one has

$$\langle v_1 \rangle = \sqrt{n} \qquad \text{and} \qquad \varphi(v_2) = \varphi(v_1)\Phi' \Longrightarrow \langle v_2 \rangle = \frac{\sqrt{\epsilon_r - \Delta}}{2} \sqrt{n} \ .$$

This is the case in the examples of the preceding section, because $\mathbb{Z}[\Phi]$ is maximal and principal (we already know that n is the norm of the ideal $\mathfrak{n}$). One can also easily prove the following geometric lemma.

Lemma 1. *The rectangle and number theoretic norms are related by the following optimal inequality: for any vector $u \in \mathbb{Z} \times \mathbb{Z}$ one has*

$$|u| \leq \frac{2\sqrt{s}}{\sqrt{|\Delta|}} \langle u \rangle \ .$$

Hence we deduce

Theorem 2. *Assume n is the norm of an element of $\mathbb{Z}[\Phi]$ then one can take*

$$\Bbbk = \frac{\sqrt{s}\sqrt{\epsilon_r - \Delta}}{\sqrt{|\Delta|}} \ .$$

This is already better than the first bound (Theorem 1) on the examples, although on the same assumptions one can improve on this.

[3] The standard Gaussian algorithm is sufficient here. It is deterministic and runs in average constant time, better than the Euclidean algorithm and with same order of magnitude for the worst case. We refer to [3] for all these facts and for the description of the algorithm. However in the examples we do not need this algorithm as Cornacchia's algorithm [2, Section 1.5.2] to find ν such that $N_{\mathbb{Z}[\Phi]/\mathbb{Z}}(\nu) = n$ gives us automatically $(\nu, \nu\Phi')$ as a reduced basis of $\mathcal{K}$ (see Section 7).

6 An Optimal Improvement

The idea, which already appears in [15], consists in working directly in the (Euclidean) space $\mathbb{C}$ where we have embedded $\mathbb{Z}[\Phi]$. We will denote $\mathcal{T}$ the triangle whose vertices are 0, 1 and Φ' and $\mathcal{P}$ the fundamental parallelogram with vertices 0, 1, Φ' and $\Phi' + 1$. The heart of our main result lies in the following lemma.

Lemma 2. *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 $R \stackrel{def}{=} f(O) = \max_{P \in \overline{ABC}} f(P)$. In other terms, O is the farthest point from any vertex. Then

1. *if ABC is acutangle, $O = \mathcal{O}$ 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 $R = AB/(2\cos\widehat{CBA})$.*

Proof. Let $\mathcal{O}$ be the center of the circumscribed circle.

1. (See Figure 1). In the first case, since the triangle is acutangle, $\mathcal{O} \in \overline{ABC}$. Therefore ABC can be partitioned into three isosceles subtriangles $\mathcal{O}AB$, $\mathcal{O}BC$ and $\mathcal{O}CA$. Also, each of these three triangles can be subdivided into two symmetric right triangles, for instance, $\mathcal{O}CA$ is made up of $\mathcal{O}CB'$ and $\mathcal{O}B'A$, where B' is the midpoint of the segment $[AC]$ and similarly for the other two subtriangles.
   Suppose by absurd $O \neq \mathcal{O}$. Without loss of generality, we can suppose $O \in \overline{\mathcal{O}B'A}$. Since the triangle is right-angled, $\mathcal{O}A$ is its diameter, which is unique,[4] therefore $OA < \mathcal{O}A = f(\mathcal{O})$. Hence $f(O) < f(\mathcal{O})$, contradicting the definition of O and $O = \mathcal{O}$.

[4] The diameter of a set Σ is by definition $\sup_{P,P' \in \Sigma} PP'$. We will say the diameter is unique if the sup is attained for exactly one pair $\{P, P'\}$.

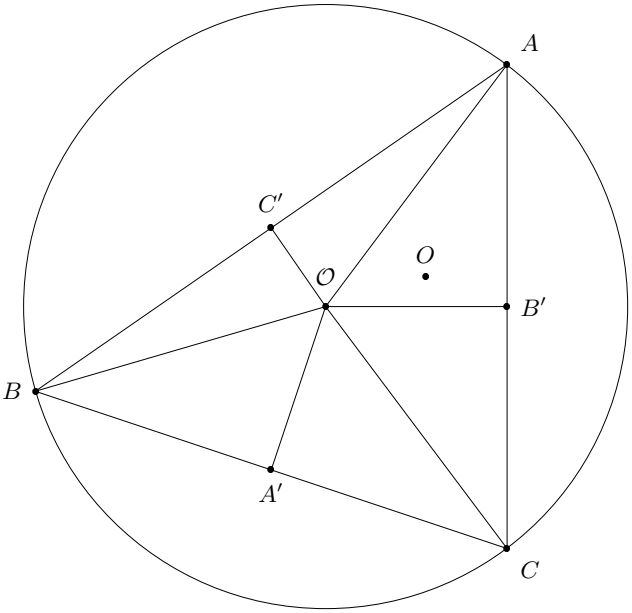

Fig. 1. Case 1 of Lemma 2

2. (See Figure 2). In this case $\mathcal{O} \notin \overline{ABC}$, so we have to look for another point O. Let O be the point constructed as in the statement of the lemma, and let O' be the intersection of the axis of $[AC]$ with $[BC]$. Then ABC is partitioned into ABO, AOO' and $AO'C$, the first and the last being isosceles, since $AO = BO$ and $AO' = CO'$. We claim that $AB \geq AC$ is equivalent to $AO \geq AO'$, with equality holding simultaneously. By an argument of symmetry, it suffices to show that $AB > AC$ implies $AO > AO'$. We have

$$\begin{cases} BO &= \dfrac{AB}{2\cos\widehat{CBA}} \ , \\ CO' &= \dfrac{AC}{2\cos\widehat{ACB}} \ . \end{cases} \tag{6}$$

Indeed working in the right-angled triangle $OC'B$, where C' is the midpoint of $[AB]$, we have that $\cos\widehat{CBA} = BC'/BO = AB/(2BO)$

and similarly for the other equality. Notice that the well-known fact

$$\sin \widehat{CBA}/AC = \sin \widehat{ACB}/AB \tag{7}$$

together with $AB > AC$ implies that $\widehat{CBA} < \widehat{ACB}$ (we are measuring angles in $[0, \pi]$). Hence $\widehat{CBA} < \pi/4$. Using (7) in (6) we get

$$\begin{cases} BO\dfrac{AC}{\sin \widehat{CBA}} &= \dfrac{AB\,AC}{2\cos \widehat{CBA} \sin \widehat{CBA}} = \dfrac{AB\,AC}{\sin 2\widehat{CBA}} \\ CO'\dfrac{AB}{\sin \widehat{ACB}} &= \dfrac{AC\,AB}{2\cos \widehat{ACB} \sin \widehat{ACB}} = \dfrac{AB\,AC}{\sin 2\widehat{ACB}} \end{cases},$$

Hence

$$\frac{AO}{AO'} = \frac{\sin 2\widehat{ACB}}{\sin 2\widehat{CBA}} .$$

Notice that $\widehat{CBA} = x - \widehat{ACB}$ for some $0 < x < \pi/2$. Hence $2\widehat{CBA} = 2x - 2\widehat{ACB} = \pi - \theta$ with $\theta > 2\widehat{ACB}$. Finally, we have that $\sin 2\widehat{CBA} = \sin \theta < \sin 2\widehat{ACB}$, because $2\widehat{CBA} < 2\widehat{ACB} < \theta$ and $2\widehat{CBA} < \pi/2$. This proves the claim.

Any point $\Omega \neq O$ in $\overline{ABO}$ satisfies $\min\{\Omega A, \Omega B\} < OA = OB$ by the same kind of arguments (splitting into two right-angled triangles) used in Case 1. In that case, $f(\Omega) < f(O)$.

Similarly if $\Omega \in \overline{AOO'}$, then by the claim we have $A\Omega < AO$, except when $\Omega = O'$ and $AO = AO'$. Hence in this case $f(\Omega) < f(O)$ except when $AB = AC$ and $\Omega = O'$.

The remaining case $\Omega \in AO'C$ can be treated like the case $\Omega \in \overline{ABO}$ and in this case $f(\Omega) < f(O') \leq f(O)$. □

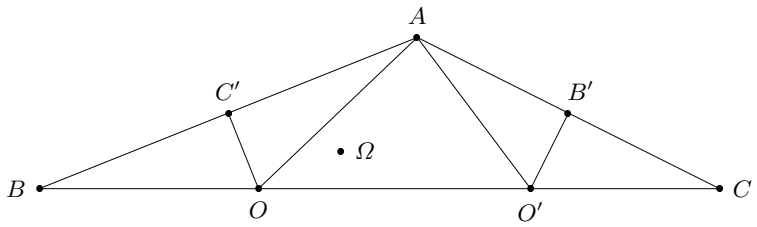

Fig. 2. Case 2 of Lemma 2

This lemma shows that any point lying inside $\mathcal{T}$ (or $\mathcal{P}$) will be at a distance $\leq R$ from one of the vertices, and that this R is optimal. Determining it is easy and we write here the final result.

$$R = \begin{cases} \dfrac{\sqrt{6 - \Delta - \Delta^{-1}}}{4}, & \text{if } r \text{ is odd,} \\ \dfrac{\sqrt{4 - \Delta}}{4}, & \text{if } r \text{ is even.} \end{cases} \tag{8}$$

Thus we get

Theorem 3. *In the above-defined notations, given a vector $(k, 0) \in \mathbb{Z} \times \mathbb{Z}$, there exists a vector $v = b_1 v_1 + b_2 v_2 \in \mathcal{K}$ such that the vector $u \stackrel{def}{=} (k, 0) - v$ has number theoretic norm bounded by*

$$\langle u \rangle \leq R\sqrt{n} \ ,$$

with R given by (8). Such a vector v is obtained as the closest vertex of the copy of $\varphi^{-1}(\nu\mathcal{P})$ (or $\varphi^{-1}(\nu\mathcal{T})$) inside which $(k, 0)$ lies.

Hence the main difference with previous methods is that b_i is not defined as $\lfloor \beta_i \rceil$ anymore when r is odd, but rather as either $\lfloor \beta_i \rfloor$ or $\lceil \beta_i \rceil$. In general one has to test three possible values but for each endomorphism ring there are shortcuts (conditions) that can be checked, so to avoid this probabilistic check. For even values of r Theorem 3 gives the same bound as [15].

Applying Lemma 1, one immediately gets

Theorem 4. *Assume n is the norm of an element of $\mathbb{Z}[\Phi]$ then one can take*

$$\Bbbk = \frac{2\sqrt{s}R}{\sqrt{|\Delta|}} \ ,$$

where R is given by (8). Furthermore, this constant cannot be improved.

Applying this theorem to Examples E_1 to E_4 we get:

Corollary 1. *In Examples E_1 to E_4, the optimal bounds for $|k_1|, |k_2|$ are:*

$$\max\{|k_1|, |k_2|\} \leq \begin{cases} \sqrt{n}/\sqrt{2}, & \textit{for } E_1, \\ \sqrt{7\,n}/3, & \textit{for } E_2, \\ \sqrt{46\,n}/7, & \textit{for } E_3, \\ \sqrt{3\,n}/2, & \textit{for } E_4. \end{cases}$$

This result ought to be compared to [15], where we improve $\Bbbk$ in the case when $r \neq 0$, that is in Examples 2 and 3.

7 On the Optimality of Theorems 3 and 4

We now discuss the optimality of this method. The first step is to show that the inequality in Theorem 3 is best possible, that is we have

$$R = \sup_{k,n} \langle (k_1, k_2) \rangle / \sqrt{n} \ . \tag{9}$$

We begin with a number theoretic lemma.

Lemma 3. *In the notations of Section 3 the index* $(\mathbb{Z} \times \mathbb{Z} \colon \mathcal{K})$ *of* $\mathcal{K}$ *inside* $\mathbb{Z} \times \mathbb{Z}$ *is* n*. Furthermore, under the assumption that* n *is the norm of an element* $\nu \in \mathbb{Z}[\Phi]$*, we have* $\mathcal{K} = \varphi^{-1}\big(\nu\mathbb{Z}[\Phi]\big)$*. In particular, a reduced fundamental domain of* $\mathcal{K}$ *is* $\varphi^{-1}(\nu\mathcal{P})$*, where* $\mathcal{P}$ *is the fundamental parallelogram described at the beginning of the last section.*

Proof. By the third isomorphism theorem of algebra and the group isomorphism given by φ we have

$$\big(\mathbb{Z} \times \mathbb{Z}\big)/\mathcal{K} \cong \mathbb{Z}[\Phi]/\big(\mathfrak{n} \cap \mathbb{Z}[\Phi]\big) \cong \big(\mathbb{Z}[\Phi] + \mathfrak{n}\big)/\mathfrak{n} \ . \tag{10}$$

Since $\mathbb{Z}[\Phi] + \mathfrak{n}$ is contained in the ring of integers $\mathfrak{I}$ of $\mathbb{Q}(\Phi)$, the right-most quotient group is a subgroup of $\mathfrak{I}/\mathfrak{n} \cong \mathbb{Z}/n$. Hence its cardinality is 1 or n. But if it were 1, then $\mathbb{Z}[\Phi] \subset \mathfrak{n}$, hence $1 \in \mathfrak{n}$ which is impossible. The cardinality must therefore be n and the same is true for the left-most group, whose cardinality is $(\mathbb{Z} \times \mathbb{Z} \colon \mathcal{K})$. Notice that

$$\mathbb{Z}[\Phi] \supset \mathfrak{n} \cap \mathbb{Z}[\Phi] \supset \nu\mathbb{Z}[\Phi] \tag{11a}$$

or equivalently

$$\mathbb{Z} \times \mathbb{Z} \supset \mathcal{K} \supset \varphi^{-1}\big(\nu\mathbb{Z}[\Phi]\big) \ . \tag{11b}$$

Therefore, in order to prove the second statement, we have to prove that the right-most inclusions in Equations (11) are actually equalities, and it suffices to do so for the first one.

In view of (10), it suffice to prove $\big(\mathbb{Z}[\Phi] \colon \nu\mathbb{Z}[\Phi]\big) = n$. Note that $N_{\mathfrak{I}/\mathbb{Z}}(\nu) = n$ can be viewed as the determinant of the multiplication by ν map when viewed as a linear endomorphism of $\mathfrak{I}$. This determinant does not change under a linear change of variables with *rational* coefficients, hence n is also the determinant of multiplication by ν when viewed as a linear endomorphism of $\mathbb{Z}[\Phi]$. But the geometric interpretation of the determinant gives that this is also the index of $\nu\mathbb{Z}[\Phi]$ inside $\mathbb{Z}[\Phi]$.

The third statement is an immediate consequence of the second. □

Notice that the lemma tells us something more than we already knew from the last section, namely that $\varphi^{-1}(\nu\mathcal{P})$ is a fundamental domain for $\mathcal{K}$. Moreover ν and $\nu\Phi'$ form a Gaussian reduced (in the sense of Section 5) basis of $\mathcal{K}$. Furthermore, the cosets $(k,0)$ modulo $\mathcal{K}$ for $0 \leq k \leq n-1$ represent all cosets of $\big(\mathbb{Z} \times \mathbb{Z}\big)/\mathcal{K}$. Their representatives (rather, their images under φ) are then uniformly spaced inside $\nu\mathcal{P}$.

This fact, coupled with the trivial remark that there are n such cosets and that the area in $\mathbb{C}$ of $\nu\mathcal{P}$ is $O(n)$, implies that any point in $\nu\mathcal{P}$ can be approximated by some $\varphi(k,0)$ with an error $O(1)$. Hence since there is a point of $\nu\mathcal{P}$ distant as far as $R\sqrt{n}$ from a vertex of $\nu\mathcal{P}$, there exists some $\varphi(k,0)$ which is at distance $R\sqrt{n}+O(1)$, implying (9).

To deduce that the constant in Theorem 4 is also optimal, we invoke the optimality of Lemma 1, together with the fact that any point in $\nu\mathcal{P}$ can be approximated by some $\varphi(k,0)$ in a given angular sector (cone) stemming from that point with an error $O(1)$ (here, the constant may depend on the angle of the sector). In other words, points $\varphi(k,0)$ tend to be distributed all around any point.

Theorem 4 implies in particular that $\Bbbk \geq \sqrt{-\Delta}/4$. A consequence of this fact is that one cannot hope to always get $\Bbbk \leq 1$ and that the GLV method is only effective for those exceptional elliptic curves that have complex multiplication by an order with small discriminant. We give a heuristic argument showing this: it is known by [18] that the number of elliptic curves E defined over $\mathbb{F}_p$ with Frobenius endomorphism σ_p of trace t is $H(t^2-4p)$, the Kronecker class number of t^2-4p. By Dirichlet's class number formula [4, p. 49], this is $O(\sqrt{4p-t^2})$. Hence there are few isomorphism classes with $4p-t^2$ small. But generally, the index $\big(\mathrm{End}(E)\colon \mathbb{Z}[\sigma_p]\big)$ is small [9, p. 41], so $4p-t^2$ is small if and only if the discriminant of $\mathrm{End}(E)$ is small. Thus there are few E's with $\mathrm{End}(E)$ of small discriminant. On the other hand, if $4p-t^2$ becomes large (say of order p), so does $-\Delta$, so that $\Bbbk \approx \sqrt{p} \approx \sqrt{n}$. But this implies that in the GLV decomposition we can only gain at most few bits, thus rendering the method ineffective.

8 The GLV Method Carries Over to Hyperelliptic Curves

In [16] it is shown[5] how to generalise the construction of the GLV method to hyperelliptic curves in two ways. The first one is a straightforward generalisation of the Gallant-Lambert-Vanstone arguments, which involve

[5] However, we would like to stress that these ideas appear and have been extensively studied in Lange's PhD thesis [10].

only lattice theory, to a higher dimensional setting (namely $d \leq 2g$ instead of 2 in the case of elliptic curves). In particular, one has to resort to the LLL algorithm to find small vectors $v_1, \ldots, v_d$ in the lattice given by a prime $\mathfrak{n}$ lying above n in some degree d extension of the rationals. We recall here this method and give an upper bound on $\max |v_i|$, where $|v|$ denotes the rectangle norm of v.

Let X be a hyperelliptic curve defined over a finite field $\mathbb{F}_q$ and $\mathrm{Jac}(X)$ its Jacobian variety. Suppose $\#\,\mathrm{Jac}(X)(\mathbb{F}_q) = hn$ with h "small" (say less than 4, but strictly less than n would theoretically suffice) and n prime. Let Φ be an efficiently computable endomorphism of $\mathrm{Jac}(X)$ defined over $\mathbb{F}_q$ and let $X^d + a_1 X^{d-1} + \cdots + a_{d-1}X + a_d$ be its minimal polynomial. Let $D \in \mathrm{Jac}(X)$ be a divisor defined over $\mathbb{F}_q$ of order n and $\lambda \in [1, n-1]$ defined by $\Phi(D) = \lambda D$.

Consider the generalised GLV reduction map f_d by

$$\begin{aligned} f_d \colon \mathbb{Z}^d &\to \mathbb{Z}/n \\ (x_1, \ldots, x_d) &\mapsto \textstyle\sum_{j=1}^{d} x_j \lambda^{j-1} \pmod{n} \ . \end{aligned}$$

If we can find linearly independent vectors $v_1, \ldots, v_d$ inside $\ker f_d$, say with $\max_i |v_i| < M$ for some small $M > 0$, then for any $k \in [1, n-1]$ we can write

$$(k, 0, \ldots, 0) = \sum_{j=1}^{d} \beta_j v_j \ ,$$

with $\beta_j \in \mathbb{Q}$. As in the GLV method one sets $v = \sum_{j=1}^{d} \lfloor \beta_j \rceil v_j$ and

$$u = (k, 0, \ldots, 0) - v = (k_1, \ldots, k_d) \ .$$

We then get

$$kD = \sum_{j=1}^{d} k_j \Phi^{j-1}(D) \quad \text{with } \max_j |k_j| < M \ .$$

The generalisation of GLV is completed if we find M of the smallest possible order, namely around $n^{1/d}$. This is what we will do next.

Let $K = \mathbb{Q}(\Phi)$. Its degree over $\mathbb{Q}$ is d. The key point of [16] is that there is a prime ideal $\mathfrak{n}$ in K dividing n, such that $\mathbf{N}\mathfrak{n} = n$. This follows from the fact that λ is a root of the minimal polynomial of Φ modulo n, ensuring the existence of such a prime ideal $\mathfrak{n}$, generated as a $\mathbb{Z}$-algebra by n and $\Phi - \lambda$.

Thus again as previously, we can factor the GLV map f_d as

$$\begin{array}{ccccc} \mathbb{Z}^d & \xrightarrow{\ \varphi\ } & \mathbb{Z}[\Phi] & \xrightarrow[\text{mod } \mathfrak{n}\cap\mathbb{Z}[\Phi]]{\text{reduction}} & \mathbb{Z}/n \\ (x_1,\dots,x_d) & \longmapsto & \displaystyle\sum_{j=1}^{d} x_j\Phi^{j-1} & \longmapsto & \displaystyle\sum_{j=1}^{d} x_j\lambda^{j-1} \pmod n \ . \end{array}$$

Note that the index (hence the volume $\mathrm{Vol}(\mathcal{F})$ of a fundamental domain $\mathcal{F}$) of $\varphi^{-1}(\mathfrak{n}\cap\mathbb{Z}[\Phi])$ inside $\mathbb{Z}^d$ is certainly bounded by $\mathbf{N}\mathfrak{n}$. It is equal to $\mathbf{N}\mathfrak{n}$ if $\mathbb{Z}[\Phi]$ is the whole ring of integers of K.

The LLL algorithm [11] then finds, for a given basis $w_1,\dots,w_d$ of $\varphi^{-1}(\mathfrak{n}\cap\mathbb{Z}[\Phi])$, a reduced basis $v_1,\dots,v_d$ in polynomial time (in d and the size of the w_i's) such that (cf. [2, Theorem 2.6.2 p.85])

$$\mathrm{Vol}(\mathcal{F}) \le \prod_{i=1}^{d} \|v_i\| \le 2^{d(d-1)/4} n \ . \tag{12}$$

Lemma 4. *Let*

$$\begin{aligned} \mathcal{N}\colon \mathbb{Z}^d &\to \mathbb{Z} \\ (x_1,\dots,x_d) &\mapsto \sum_{\substack{i_1,\dots,i_d \\ i_1+\cdots+i_d=d}} b_{i_1,\dots,i_d} x_1^{i_1}\dots x_d^{i_d} \end{aligned}$$

be the norm of an element $\sum_{j=1}^{d} x_j\Phi^{j-1} \in \mathbb{Z}[\Phi]$, where the $b_{i_1,\dots,i_d}$'s lie in $\mathbb{Z}$. Then, for any nonzero $v_i \in \varphi^{-1}(\mathfrak{n}\cap\mathbb{Z}[\Phi])$, one has

$$|v_i| \ge \frac{n^{1/d}}{\Big(\displaystyle\sum_{\substack{i_1,\dots,i_d \\ i_1+\cdots+i_d=d}} |b_{i_1,\dots,i_d}|\Big)^{1/d}} \ . \tag{13}$$

Proof. This is a straightforward generalisation of the argument given in the proof of Theorem 1. Indeed for $v_i \in \varphi^{-1}(\mathfrak{n}\cap\mathbb{Z}[\Phi])$ we have $\mathcal{N}(v_i) \equiv 0 \pmod n$ and if $v_i \neq 0$ we must therefore have $|\mathcal{N}(v_i)| \ge n$. On the other hand, if we did not have (13), then every component of v_i would be strictly less than the right-hand side and plugging this upper bound in the definition of $\mathcal{N}(v_i)$ would yield a quantity $< n$, a contradiction. □

Let B be the denominator of the right-hand side of (13), then (12) and (13) imply that

$$|v_i| \le B^{d-1}\, 2^{d(d-1)/4}\, n^{1/d} \ .$$

Thus we have proved the following.

Theorem 5. *Let Φ be an endomorphism of* $\mathrm{Jac}(X)$ *and let d be the degree of its minimal polynomial. The hyperelliptic GLV method yields a decomposition*

$$kD = \sum_{j=1}^{d} k_j \Phi^{j-1}(D) \quad \textit{with } \max_j |k_j| \leq B^{d-1}\, 2^{d(d-1)/4}\, n^{1/d} \ ,$$

where B is the denominator of the right-hand side of (13)*, that is a polynomial expression in the coefficients of the minimal polynomial of Φ.*

9 Examples

We quickly list some examples by producing the minimal polynomial $P(X)$ of Φ, which is all we need. For a complete description of the curves, we refer the reader to [16].

- In Example 2, we have $P(X) = X^2 + 1$. When $d = 2$, the discussion about elliptic curves applies (since it's not a matter of curves, but of rings $\mathbb{Z}[\Phi]$) and the first bound of Corollary 1 applies.
- In Examples 3 and 4, the minimal polynomial is of the form $P(X) = G(X^2)$, where $G(Y) = Y^2 + rY + s$ is the minimal polynomial of $\Psi = \Phi^2$. Then we have

$$\begin{aligned} B^d = 1 + r^2 + 9s^2 + \left|s^2(r-1)^2 + r^3 s\right| + 7s + 3r^2 s + 3rs + 3\,|r| \\ + 9\,|r|\,s + \left|2s(r-1) - r^3\right| + \left|4s - 2r^3\right| + \left|2s^2(r-1) + r^2 s\right| \\ + \left|4s^2(r-1) + 2r^2 s\right| \ . \end{aligned}$$

  In the case when $r = 0$, we get the simplified equation

$$B^d = 1 + 13s + 16s^2 \ .$$

10 Conclusion

This work does a careful analysis of the GLV method on fast scalar multiplication on elliptic curves. It improves on existing bounds [15] and produces in classical examples the best constants obtainable by this method. In particular we prove that the GLV method is not effective for a generic elliptic curve with complex multiplication by an order of large discriminant. This analysis can be generalised to the hyperelliptic variant of the GLV method [16] and we provide the first explicit bounds on the size of the decomposition, thus quantifying the effectiveness of the GLV method for higher genus curves.

11 Acknowledgements

The authors would like to thank Marc Joye, David Kohel and Takakazu Satoh for fruitful discussions and useful comments on preliminary versions of this paper. We are also grateful to the anonymous referees for their valuable remarks.

References

1. I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society*. Cambridge University Press, 2000.
2. H. Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer, 1996.
3. H. Daudé, P. Flajolet, and B. Vallée. An Average-case Analysis of the Gaussian Algorithm for Lattice Reduction. Technical Report 2798, INRIA, February 1996.
4. H. Davenport. *Multiplicative Number Theory*, volume 74 of *Graduate Texts in Mathematics*. Springer Verlag, 1980.
5. R. P. Gallant, J. L. Lambert, and S. A. Vanstone. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In J. Kilian, editor, *Advances in Cryptology - Proceedings of CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 190–200. Springer, 2001.
6. D. M. Gordon. A Survey of Fast Exponentiation Methods. *Journal of Algorithms*, 27(1):129–146, 1998.
7. D. Kim and S. Lim. Integer Decomposition for Fast Scalar Multiplication on Elliptic Curves. In Howard Heys and Kaisa Nyberg, editors, *Selected Areas in Cryptography, 9th Annual International Workshop, SAC 2002*, Lecture Notes in Computer Science. Springer, 2002. (this volume).
8. K. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.
9. D. Kohel. *Endomorphism Rings of Elliptic Curves over Finite Fields*. PhD thesis, UC Berkeley, 1996.
10. T. Lange. *Efficient Arithmetic on Hyperelliptic Koblitz Curves*. PhD thesis, University of Essen, 2001.
11. A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Ann.*, 261:513–534, 1982.
12. A.J. Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1995.
13. V. Miller. Use of Elliptic Curves in Cryptography. In A. M. Odlyzko, editor, *Advances in Cryptology - Proceedings of CRYPTO 1986*, volume 263 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1986.
14. V. Müller. Efficient Point Multiplication for Elliptic Curves over Special Optimal Extension Fields. In Walter de Gruyter, editor, *Public-Key Cryptography and Computational Number Theory*, pages 197–207, Warschau, Poland, September 11-15, 2000 (2001).
15. 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*, volume 2274 of *Lecture Notes in Computer Science*, pages 323–334. Springer, 2002.

16. Y-H. Park, S. Jeong, and J. Lim. Speeding Up Point Multiplication on Hyperelliptic Curves with Efficiently-computable Endomorphisms. In L. Knudsen, editor, *Advances in Cryptology - Proceedings of EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 197–208. Springer, 2002.
17. J. A. Solinas. An Improved Algorithm for Arithmetic on a Family of Elliptic Curves. In Burton S. Kaliski Jr., editor, *Advances in Cryptology - Proceedings of CRYPTO 1997*, volume 1294 of *Lecture Notes in Computer Science*, pages 357–371. Springer, 1997.
18. E. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 2:521–560, 1969.