Endomorphisms for Faster Cryptography on Elliptic Curves of Moderate CM Discriminants

Dimitri Koshelev[1]* and Antonio Sanso[2]

[1] University of Lleida, Department of Mathematics, Catalonia, Spain
dimitri.koshelev@gmail.com
[2] Ethereum Foundation
antonio.sanso@ethereum.org

Abstract. This article generalizes the widely-used GLV decomposition for scalar multiplication to a broader range of elliptic curves with moderate CM discriminant $D < 0$ (up to a few thousand in absolute value). Previously, it was commonly believed that this technique could only be applied efficiently for small D values (e.g., up to 100). In practice, curves with j-invariant 0 are most frequently employed, as they have the smallest possible $D = -3$. This article participates in the decade-long development of numerous real-world curves with moderate D in the context of ZK-SNARKs. Such curves are typically derived from others, which limits the ability to generate them while controlling the magnitude of D. The most notable example is so-called "lollipop" curves demanded, among others, in the Mina protocol.

Additionally, the new results are relevant to one of the "classical" curves (with $D = -619$) from the Russian ECC standard. This curve was likely found using the CM method (with overwhelming probability), though this is not explicitly stated in the standard. Its developers seemingly sought to avoid curves with small D values, aiming to mitigate potential DLP attacks on such curves, and hoped these attacks would not extend effectively to $D = -619$. One goal of the present article is to address the perceived disparity between the $D = -3$ curves and the Russian curve. Specifically, the Russian curve should either be excluded from the standard for potential security reasons or local software should begin leveraging the advantages of the GLV decomposition.

Keywords: binary quadratic forms · elliptic curve cryptography · GLV · ideal class groups · isogeny loops · scalar multiplication

* https://www.researchgate.net/profile/dimitri-koshelev
This paper is part of the project "Avances en criptografía post-cuántica aplicados al desarrollo de un sistema de cupones", financed by "European Union NextGeneration–UE, the Recovery Plan, Transformation and Resilience, through INCIBE". The paper is also part of the R&D+i project PID2021-124613OB-I00 funded by MICIU/AEI/10.13039/501100011033 and FEDER, EU.

1 Introduction

Throughout the article, E will stand for an elliptic curve over a finite field $\mathbb{F}_q$ of large characteristic (for simplicity). The *GLV (Gallant–Lambert–Vanstone) technique*, as described in [18], is a well-known method for accelerating a scalar multiplication on E. Specifically, it applies to curves having an efficient $\mathbb{F}_q$-endomorphism $\phi \in \mathrm{End}(E)$. The method is especially advantageous for curves with j-invariant $j = 0$ (or $j = 1728$), as it enables to take on the role of ϕ a non-trivial automorphism with only a single modular multiplication. Additionally, the GLV approach is easily extended to curves for which the endomorphism requires somewhat more computational effort, that is, the degree $d := \deg(\phi)$ is slightly greater than 1. The most famous instance is the *Bandersnatch curve* [22] admitting $d = 2$.

As is typical in DLP-based cryptography, the $\mathbb{F}_q$-point group $E(\mathbb{F}_q)$ contains a subgroup $\mathbb{G}$ of huge prime order r. For compactness, let's put $\ell := \lceil \log_2(r) \rceil$ and $\ell' := \lceil \ell/2 \rceil$. Assume that an entity of a cryptographic protocol wants to compute the scalar multiplication $Q := nP$ for $P \in \mathbb{G}$ and $n \in \mathbb{Z}/r$. Evidently, Q can be determined by means of one of the general exponentiation methods, such as the schoolbook double-add method, requiring ℓ doublings and at worst $\approx \ell$ additions on E.

In practice, the embedding degree of $\mathbb{G}$ is > 1, that is, $\mathbb{G} = E(\mathbb{F}_q)[r]$. Consequently, any endomorphism ϕ acts on $\mathbb{G}$ as the multiplication by some scalar $\lambda \in \mathbb{Z}/r$. The eigenvalue λ is one of the two roots in $\mathbb{Z}/r$ of the characteristic polynomial $(x - \phi)(x - \widehat{\phi}) = x^2 - ax + d$ considered over $\mathbb{Z}/r$, where $\widehat{\phi}$ is the dual endomorphism and $a \in \mathbb{Z}$ is the trace of ϕ. The latter can be determined via *Schoof's like algorithm* [4, Appendix A] whenever the degree d is sufficiently smooth (as in the setting of this article).

To explain the GLV method, we lack the rank-2 lattice $L := s^{-1}(0) \subset \mathbb{Z}^2$, where $s(v, v') := v + \lambda v' \in \mathbb{Z}/r$, generated by the (long) vectors $(r, 0)$, $(\lambda, -1)$. It is suggested to introduce new numbers m, $m' \in \mathbb{Z}/r$ (to be specified later) such that $Q = mP + m'P'$, where $P' := \phi(P) = \lambda P$. The difference $(v_0, v_0') := (n, 0) - (m, m') = (n - m, -m')$ evidently lies in L. Note that $(m, m') = (n, 0) - (v_0, v_0') = (n - v_0, -v_0')$. The aim is to obtain the vector (m, m') shorter than $(n, 0)$ in the infinity norm $|| \cdot ||_\infty$, i.e., the vector (v_0, v_0') closer to $(n, 0)$ than the origin $(0, 0)$. This can be done, e.g., via one of quick *Babai's algorithms* [16, Sections 18.1 and 18.2]. As it turns out, one can expect the bit lengths $\log_2(|m|)$, $\log_2(|m'|) \approx \ell'$. For this, it is necessary to prepare in advance (e.g., via *(Lagrange–)Gauss' reduction* [16, Section 17.1]) a short basis of the lattice L whose two vectors are also of bit lengths $\approx \ell'$. To find Q, it remains to employ any double-scalar multiplication algorithm. For instance, *(Shamir–)Straus' trick* [26] costs ℓ' doublings and at most $\approx \ell'$ additions on E.

The endomorphism ϕ for the GLV decomposition has to be different from scalar endomorphisms on E. The point is that it is impossible to evaluate almost for free $[\lambda] \in \mathrm{End}(E)$ (of degree λ^2) for a huge number $\lambda \in \mathbb{Z}/r$. Meanwhile, for the other λ, the numbers m, m' simultaneously do not have (on average) half bit lengths. In turn, the eigenvalue λ of the non-scalar ϕ is most likely enormous as needed. In fact, there is a folklore trick (see, e.g., [14]) when $\phi = [2^{\ell'}]$, i.e., $\lambda = 2^{\ell'}$ and m, m' are respectively the remainder and quotient for the division of n by $2^{\ell'}$. The overall running time of this non-authentic GLV method amounts to ℓ doublings (ℓ' ones if the point P, i.e., P' is fixed) and at worst $\approx \ell'$ additions.

It is also worth mentioning the fake GLV approach [15] resembling the idea of [3] for faster verification of ECDSA signatures. The given GLV variation takes place even if an elliptic curve does not enjoy an appropriate endomorphism. In the scenario under consideration an entity simply desires to check the equality $Q = nP$ with the a priori known point Q. More precisely, the corresponding testing has the form $kQ + k'P = \mathcal{O}$, where $k, k' \in \mathbb{Z}/r$ are still some numbers of half bit lengths and $\mathcal{O} := (0 : 1 : 0)$ is the infinity (i.e., zero) point on E.

In 99.9...% of cases, the modern landscape of discrete logarithm problem (DLP) elliptic curve cryptography (ECC) is founded on ordinary (i.e., non-supersingular) elliptic curves. The only exceptions are supersingular curves involved in 2-cycles of pairing-friendly abelian varieties [10,11]. Since the result of the present article is irrelevant to supersingular curves, we can neglect them to avoid confusion. The endomorphism ring of each ordinary curve $E/\mathbb{F}_q$ is independent of the base field and isomorphic to a rank-2 order $\mathcal{O}_D$ (of some complex multiplication discriminant $D < 0$) in the imaginary quadratic field $F := \mathbb{Q}(\sqrt{t^2 - 4q})$, where t is the Frobenius trace of E. For instance, $D = -8$ for the Bandersnatch curve.

For the sake of simplicity, we will deal solely with fundamental CM discriminants, i.e., those for which $\mathcal{O}_D$ is the integer ring of F. Recall that such D are square free up to 4 in their structure. From the cryptographic point of view, generality is not lost under the given assumption. Indeed, an elliptic $\mathbb{F}_q$-curve of non-fundamental CM discriminant is $\mathbb{F}_q$-isogenous to that of fundamental one. Clearly, $\mathbb{F}_q$-isogenous curves are almost always equivalent concerning the hardness of the DLP. The opposite theoretical but impractical scenario (where $p^2 \mid D$ for a large prime p) is discussed in [16, Section 25.6] and [17]. On the other hand, curves with a predefined D are constructed exclusively via the *CM method* (see, e.g., [27]). This method becomes infeasible for large CM discriminants, specifically when $-D > 10^{17}$, given current computational capabilities. Consequently, there is no efficient way to generate an $\mathbb{F}_q$-curve that admits an ascending $\mathbb{F}_q$-isogeny of a very large prime degree p.

Let us represent E in (weighted) projective coordinates to avoid the computationally expensive inversion operation in $\mathbb{F}_q^*$. As explained in Section 2.2, classical *Vélu's formulas* [16, Section 25.1.1] for evaluating $\phi \in \mathrm{End}(E)$ require at most $\approx cd$ multiplications in $\mathbb{F}_q$ with the constant $c = 7.5$. Meanwhile, one doubling [2] on E (according to [6], [19, Annex A.10.4]) costs $c' \in \{8, 9, 10\}$ field multiplications for the short Weierstrass form $y^2 = x^3 + a_4x + a_6$. The concrete choice for c' depends on the magnitude of the coefficient a_4 (inter alia, $c' = 8$ if $a_4 = -3$). Looking ahead, we will not encounter in this paper any curves admitting commonly used composite-order forms [16, Section 9.12], for which c' would need to be slightly smaller. As we see, $c'\ell'$ multiplications are the total overhead of $[2^{\ell'}]$. Therefore, the GLV technique with respect to ϕ is a faster solution than the aforementioned folklore trick only if d is quite small, or rather d is less than $\approx c'\ell'/c$.

It is known that the minimal degree $d_{\min}$ of a non-scalar endomorphism on E is equal to $-D/4$ or $(1-D)/4$, depending on whether $D \mod 4$ is 0 or 1, respectively. However, $d_{\min}$ is often not smooth enough to allow the successful application of [16, Theorem 25.1.2], i.e., to decompose the associated endomorphism $\phi_{\min}$ into small-degree $\mathbb{F}_q$-isogenies. Consequently, it was widely believed in the past that scalar multiplication on the majority of curves is not subject to extra acceleration.

1.1 New contribution

The idea of the current work is elementary, but powerful. To the authors' knowledge, it has not yet occurred in the public literature. Not looking at $d_{\min}$, it is suggested to originally take a loop (cycle) of $m \in \mathbb{N}$ non-backtracking $\mathbb{F}_q$-isogenies $\phi_i : E_i \to E_{i+1}$ (where $E = E_1 = E_{m+1}$) of little prime degrees d_i. "Non-backtracking" means that ϕ_{i+1} differs from the dual isogeny $\widehat{\phi_i} : E_{i+1} \to E_i$, hence the loop cannot be shortened. Every isogeny ϕ_i itself is not an endomorphism (except for $m = 1$), but so is their entire composition $\phi = \phi_m \circ \cdots \circ \phi_1$ of degree $d = d_1 \cdots d_m$. Thereby, the overall running time of evaluating $\phi \in \mathrm{End}(E)$ is obviously reduced to $\approx c(d_1 + \cdots + d_m)$ multiplications in $\mathbb{F}_q$ instead of $\approx cd$ ones. Of course, it is necessary to verify that the endomorphism ϕ is non-scalar. In particular, this is the case whenever $\sqrt{d} \notin \mathbb{Z}$. Curiously, d may be much greater than the lower bound $d_{\min} \approx -D/4$, despite the better performance of ϕ rather than $\phi_{\min}$.

Let's bring into play the *(ideal) class group* Cl of the ring $\mathcal{O}_D$ (i.e., of the field F). It will not hurt to briefly overview main concepts and results connected with Cl. They (or at least most of them) can be encountered, e.g., in [12], [16, Sections 25.3.1 and 25.4.1]. First, Cl is a finite abelian group. Its order $h := \#\mathrm{Cl}$ is called *(ideal) class number* and behaves approximately like $\sqrt{-D}$ as $D \to -\infty$. The group Cl acts regularly on the crater (surface), i.e., on the set of all elliptic $\mathbb{F}_q$-curves of the same trace t and with the endomorphism ring $\simeq \mathcal{O}_D$. In other words, an ideal class $[I] \in \mathrm{Cl}$ maps such a curve E to some horizontally $\mathbb{F}_q$-isogenous one E'.

By definition, the cardinality, i.e., index $n := \#(\mathcal{O}_D/I) = (\mathcal{O}_D : I)$ is the (numerical) norm of I. Do not confuse this concept with the norm map $\mathrm{N} : F \to \mathbb{Q}$, for which $\mathrm{N}(\mathcal{O}_D) \subset \mathbb{Z}$. The ideal I, being the unique integral reduced one in $[I]$, coincides, as a lattice (up to homothety by $\sqrt{n}$), with the rank-2 lattice $\mathrm{Hom}(E, E')$ of all ($\mathbb{F}_q$)-isogenies between E and E'. The corresponding integral positive definite quadratic forms on I and $\mathrm{Hom}(E, E')$ are the tweaked norm $\mathrm{N}' := \mathrm{N}/n$ and the degree deg, respectively. The map $[I] \mapsto \mathrm{N}'$ defines an isomorphism of Cl onto the group (also denoted Cl) of all reduced binary quadratic forms of discriminant D, endowed with *Gauss'* (also known as *Dirichlet's* or *Legendre's*) *composition law*.

Denote by m the order of the ideal class $[I]$ in the group Cl. Consequently, the m successive actions of $[I]$ (beginning with E) produce an isogeny loop

$E_i \to E_{i+1}$ of length $m \mid h$. It is sufficient to choose at each step an isogeny ϕ_i of the same degree $\delta := d_i$ among the non-zero values of $\mathrm{N}' = \deg$ on $I \simeq \mathrm{Hom}(E_i, E_{i+1})$. The most reasonable choice for δ is perhaps the minimal (often prime) value, that is, the norm n. Once m is odd, δ is not a perfect square, and m, δ are both pretty small, we come to the desired non-scalar endomorphism ϕ on E of degree $d = \delta^m$. In the new notation, ϕ can be sequentially evaluated at the price of $\approx cm\delta$ multiplications in $\mathbb{F}_q$ instead of $\approx c\delta^m$ ones. We will see on practical examples that the theory under consideration actually works.

By the way, isogeny loops are ubiquitous in isogeny-based cryptography. For instance, they are related to collisions in seminal *Charles–Lauter–Goren's hash function* [9]. Moreover, "smoothing" isogenies of large prime degrees (by increasing the dimension) has become a popular technique in the field of isogeny-based cryptography (see, e.g., [23]). The action of the ideal class group of an imaginary quadratic field also plays an important role [13] in the given post-quantum cryptography, although supersingular curves in this context are more preferable [8] than ordinary ones. Finally, the hard DLP in the group Cl gives rise to yet another type of (pre-quantum) cryptography starting with [7]. It is appropriate for developing more specific mechanisms such as *verifiable delay functions (VDF)* [28], which cannot be achieved on elliptic curves due to Schoof's point counting algorithm. It is worth stressing that, in the cryptographic domains mentioned, CM discriminants are of exponential size, unlike the small values of D considered in the present paper.

2 Preliminaries

2.1 Binary quadratic forms in connection with isogenies

For convenience of the reader, in this section we briefly remind basic notions and properties related to binary quadratic forms and their relationship with elliptic curve isogenies. For comprehensive details on the former, see, e.g., [12]. For detailed information on the latter, refer to [16, Sections 9, 25] for example.

An integral *binary quadratic form* is a homogeneous $\mathbb{Z}$-polynomial of the type $f(x,y) = ax^2 + bxy + cy^2$ traditionally denoted by (a,b,c) for laconicity. As always, the *discriminant* of f is the number $D := b^2 - 4ac \equiv 0, 1 \pmod 4$. It is said to be *fundamental* if either $D \equiv 1 \pmod 4$ and D is square-free, or so is $D/4 \in \mathbb{Z}$ and $D/4 \equiv 2, 3 \pmod 4$. If the form f is *non-degenerate* (i.e., $D \neq 0$) and returns exclusively positive values (except for $x = y = 0$), then f is referred to as *positive definite*. This holds if and only if $D < 0$, but $a > 0$. We will assume everywhere that our forms are integral, positive definite, and with fundamental discriminant. Finally, such a form f is *reduced* whenever $|b| \leqslant a \leqslant c$ and $b \geqslant 0$ if $a = c$. It is easily proved that under these conditions, $a = f(1,0)$ is the minimal non-zero value of f on $\mathbb{Z}^2$.

We say that two binary quadratic forms are *(properly) equivalent* if they differ by a matrix from the special linear group $\mathrm{SL}_2(\mathbb{Z})$. Suppose that $\gcd(a_1, a_2, (b_1 + b_2)/2) = 1$ given two forms $f_i = (a_i, b_i, c_i)$ of the same discriminant D (with

$i \in \{1, 2\}$). Their *(Dirichlet) composition* is $f_1 \cdot f_2 := (a_1a_2, B, \frac{B^2-D}{4a_1a_2})$, where B is the unique integer modulo $2a_1a_2$ such that $B \equiv b_i \pmod{2a_i}$ and $B^2 \equiv D \pmod{4a_1a_2}$. It turns out that this operation is well-defined on equivalence classes and it produces a finite abelian group Cl under the name *class group*. If $D \equiv 0 \pmod 4$, then the identity element of this group is $(1, 0, -D/4)$. In turn, if $D \equiv 1 \pmod 4$, then it is $(1, 1, (1-D)/4)$. Furthermore, the form inverse to f_i is nothing but $f_i^{-1} = (a_i, -b_i, c_i)$. Even though there are quick reduction algorithms, the forms $f_1 \cdot f_2$ and f_i^{-1} themselves are not necessarily reduced even if f_1, f_2 are initially so.

Binary quadratic forms of discriminant D, ideals in the integer ring (i.e., the maximal order) $\mathcal{O}_D$ of the imaginary quadratic field $F = \mathbb{Q}(\sqrt{D})$, and isogenies between elliptic curves of CM discriminant D are intimately interwoven. More precisely, a reduced form $f = (a, b, c)$ corresponds to the integral *reduced ideal* $I := a\mathbb{Z} + b'\mathbb{Z}$, where $b' := (b + \sqrt{D})/2$. Moreover, this correspondence yields an isomorphism of the group Cl to the group of (fractional) ideals of $\mathcal{O}_D$ modulo principal ideals. It is important to remember that there exists a unique reduced form (or, alternatively, reduced ideal) in every equivalence class, hence in practice all the work is carried out with the given representatives. It can be shown that a is the numerical norm of I and $\mathrm{N}(ax + b'y) = af(x, y)$ regardless of $x, y \in \mathbb{Z}$ for the norm map $\mathrm{N}\colon \mathcal{O}_D \to \mathbb{Z}$.

In addition, for any elliptic curve E admitting a ring isomorphism $\iota\colon \mathcal{O}_D \simeq \mathrm{End}(E)$, the reduced ideal I defines the horizontal isogeny $E \to E/K$ (of degree a) with the cyclic kernel $K := E[a] \cap \ker(\iota(b'))$. To put it in another way, the group Cl regularly (i.e., transitively and freely) acts on the crater of the isogeny volcano.

2.2 Evaluating isogenies in projective coordinates

Let E, E' be two short Weierstrass $\mathbb{F}_q$-curves on the projective plane $\mathbb{P}^2_{(x:y:z)}$. By virtue of [16, Lemma 9.6.12 and Corollary 25.1.8], any $\mathbb{F}_q$-isogeny $\psi\colon E \to E'$ of odd degree $d > 1$ relatively prime to q can be expressed as follows:

$$\psi(x : y : z) = \Big((\psi_1\psi_3)(x, z) : y\psi_2(x, z)z^{d'-d_2-1} : \psi_3^3(x, z)z\Big),$$

where ψ_i are binary homogeneous $\mathbb{F}_q$-polynomials of degrees $d_i := \deg(\psi_i)$, namely

$$d_1 = d, \qquad d_2 \leqslant 3\frac{d-1}{2}, \qquad d_3 = \frac{d-1}{2}, \qquad \text{and} \qquad d' := d_1 + d_3 = \frac{3d-1}{2}.$$

The last number d' is nothing but the same degree of the resulting coordinates of ψ. At worst, $d_2 = d'-1 = 3(d-1)/2$. For our purposes, it will be sufficient to work under this less favorable condition in order to eliminate d_2 as an independent variable.

By definition, $\psi_i = \sum_{j=0}^{d_i} c_{i,j} x^j z^{d_i-j}$ with coefficients $c_{i,j} \in \mathbb{F}_q$. The homogeneous version of *Horner's scheme* has the form

$$\psi_i(x, z) = c_{i,0}z^{d_i} + x(c_{i,1}z^{d_i-1} + x(c_{i,2}z^{d_i-2} + \cdots + c_{i,d_i})\cdots).$$

Separately, each polynomial ψ_i can be evaluated at a point $P \in E(\mathbb{F}_q)$ at the price of $\approx 3d_i$ multiplications in $\mathbb{F}_q$. Truly, $\approx d_i$ ones are needed for all the powers z^j, for the multiplications by x, and finally the same amount when multiplying by $c_{i,j}$. However, it is enough to determine z^j solely in the case of the largest degree d_2. Consequently, computing $\psi(P)$ requires $\approx 2d' + 3d_2 \approx 7.5d$ multiplications in total.

In the given quantity we do not take into account the fact that the coefficients $c_{i,j}$ may be repeated or little (even zero) for the concrete isogeny ψ. Hence, its real cost may be (drastically) less. One more further optimization (when d is not small) consists in determining $\psi_i(P)$ through the algorithm described in [20]. It has the better asymptotic complexity $2d_i + \Theta(\log(d_i))$, which implies the overall one $6d + \Theta(\log(d))$. Lastly, it is worth saying about the fundamentally different evaluation strategy from [5] (so-called *square-root Vélu's formulas* or just $\sqrt{\text{é}}$lu), which reduces the complexity to $\widetilde{O}(\sqrt{d})$. Of course, the actual running time is decreased only for the pretty big d. An attempt to find this borderline is done in [1].

3 Examples

This section is dedicated to a few practical elliptic curves of moderate (as earlier, fundamental) CM discriminants D. It is accompanied by the code [21] written in the computer algebra system Sage. In particular, the reader can find there the parameters of the curves and the coefficients of isogenies forming loops. We will keep the notation of the introduction. Table 1 contains the basic information on the curves and on the ideal class groups Cl for the given D. In turn, Table 2 exhaustively lists the elements of Cl, namely the reduced binary quadratic forms of discriminants D.

Curve	Reference	ℓ	D	$d_{\min}$	$h = m$	$n = \delta$	$d = \delta^m$
Russian curve	[2, Appendices B, E]	256	-619	$5 \cdot 31$	5	5	3125
Lollipop curves	[11, Section 5]	201	-547	137	3	11	1331
		261	-3019	$5 \cdot 151$	7	5	78125

Table 1. Some real-world curves of moderate CM discriminants D and their derived parameters. In every case, $\mathrm{Cl} \simeq \mathbb{Z}/h$.

All the curves $E : y^2 = x^3 + a_4x + a_6$ under consideration are of prime order, although not all of them have the Weierstrass form $E' : y^2 = x^3 - 3x + a_6'$ over $\mathbb{F}_q$. Alternatively, the fraction $-3/a_4$ may not have any quartic roots in $\mathbb{F}_q$, as can be easily checked. Recall that one doubling on E' amounts to $c' = 8$ multiplications in $\mathbb{F}_q$ rather than 9 or 10 ones in general. Nonetheless, let's always suppose for uniformity that the constant $c' = 8$. One cannot rule out that the

Russian curve	$(1,1,155)$,	$(5,\pm1,31)$,	$(7,\pm5,23)$	
Lollipop curves	$(1,1,137)$,	$(11,\pm5,13)$		
	$(1,1,755)$,	$(5,\pm1,151)$,	$(13,\pm7,59)$,	$(25,\pm9,31)$

Table 2. The reduced binary quadratic forms of discriminants D. The first one in each row is the neutral element in Cl.

curves E enjoy small-degree $\mathbb{F}_q$-isogenies to (from) $\mathbb{F}_q$-curves E' of the desired form, enabling to accomplish a scalar multiplication on E' instead of E. Hence, it is fairer to assume that [2] costs as few as possible and to demonstrate that even in this hypothetical case, the doubling-free GLV approach is still better.

To justify the contribution of this article, it is sufficient to leverage the simple evaluation method from Section 2.2, as we are primarily interested in loops of small-degree isogenies. As noted in that section, large-degree isogenies in the decomposition of the "minimal" endomorphism $\phi_{\min}$ could benefit from additional optimizations. Nevertheless, it is highly unlikely that $\phi_{\min}$ would (noticeably) outperform the "looped" endomorphism ϕ. The authors chose not to derive the absolutely fair cost for $\phi_{\min}$, as doing so would significantly complicate the text. The primary objective is to compare ϕ with the scalar endomorphism $[2^{\ell'}]$. It is generally believed that $\phi_{\min}$ is unlikely to be (much) faster than $[2^{\ell'}]$, except when the degree $d_{\min}$ is extremely smooth, such as $d = \delta^m$.

Generally speaking, $d_{\min} = \prod_{i=1}^{k} p_i^{e_i}$, where p_i are pairwise distinct primes, and $k, e_i \in \mathbb{N}$. We lack a symbol for the sum $\sigma := \sum_{i=1}^{k} e_i p_i$. According to Table 3, the endomorphism ϕ outperforms the others in speed on the curves E (or E') listed below. For each curve, the columns $[2^{\ell'}]$, $\phi_{\min}$, and ϕ in this table correspond to the values $8\ell'$, $\lceil 7.5\sigma \rceil$, and $\lceil 7.5 m\delta \rceil$, respectively.

Curve	$[2^{\ell'}]$	$\phi_{\min}$	ϕ
Russian curve	1024	270	188
Lollipop curves	808	1028	248
	1048	1170	263

Table 3. Approximate numbers of field multiplications for evaluating the endomorphisms $[2^{\ell'}]$, $\phi_{\min}$, and ϕ.

The executing time of inverting in $\mathbb{F}_q^*$ weakly correlates with that of multiplying in the field. Therefore, we abstract from the former, working entirely in projective coordinates. As a downside, this greatly increases the number of multiplications compared to affine coordinates. As is customary, the given approach is anyway worthwhile for evaluating $[2^{\ell'}]$, otherwise ℓ' non-batchable inversions must be carried out. However, the loop for the endomorphism ϕ (not to mention $\phi_{\min}$) consists of the non-considerable number m of isogenies. Thus, evaluating them in affine coordinates may be in reality a (much) more rapid solution. For clarity of comparison, it is nevertheless suggested to operate in the idealized computational model not admitting the inversion operation. The authentic cost of ϕ (as opposed to $[2^{\ell'}]$) can only get better than reported in Table 3.

3.1 Russian curve

It is about a prime-order Weierstrass curve $E : y^2 = x^3 - 3x + a_6$ over the prime field $\mathbb{F}_q$ of order $q = 2^{255} + 3225$. Its official name is *id-GostR3410-2001-CryptoPro-B-ParamSet* [2, Appendices B, E] or just *GC256C* [25]. As shown in Table 1, the degrees $d_{\min} = 5 \cdot 31$ and $d = 5^5$ for this curve. One 31-isogeny is not much slower to evaluate than four 5-isogenies (cf. Table 3). Our contribution is thereby not so interesting for the curve in question, although it is actually the state of the art. Moreover, it is unlikely that many Russian developers have heard about the GLV technique before and used it at least with the endomorphism $\phi_{\min}$.

The Russian ECC standard includes two more prime-order curves at the 128-bit security level, namely *GC256A* and *GC256B*. Interestingly, their values of D are significantly large, meaning they could not be generated using the CM method. This is one reason why GC256C appears to be less popular in Russia compared to its counterparts, although all these curves are maintained by Russian servers on an equal basis. However, the curves GC256A and GC256B are also not entirely pseudo-random, as noted in [24, Section 4.1], due to the fact that their coefficients a_6 are relatively small (while $a_4 = -3$).

3.2 Lollipop curves

In this section, we discuss the components of plain (i.e., non-pairing-friendly) 2-cycles that lie in the "sticks" of certain *pairing-friendly lollipops*, as described in [11, Section 5]. This complex construction has recently emerged as a response to the lack of known *pairing-friendly cycles* with suitable embedding degrees $\geqslant 12$. The existence of such cycles is one of the most important open problems in modern DLP-based ECC. Fortunately, lollipops allow the majority of operations to be performed in the optimized stick before irreversibly moving to the more time-consuming 2-cycle of supersingular pairing-friendly curves.

As seen in the tables above, the authors chose to consider only a few lollipops to illustrate the main idea of the article. Perhaps, it is extended to several others generated by Costello and Korpal. In particular, the instance with bit length $\ell = 261$ (i.e., *lollipop-574-261*) was selected, as it offers an almost optimal security level, in contrast to *lollipop-489-201*. Thus, the 261-bit lollipop may soon be deployed in real-world cryptographic applications.

4 Conclusion

This paper offers a fresh perspective on the classical GLV method, extending its applicability to a broader class of elliptic curves with moderate CM discriminants. These include, apart from one Russian standardized curve, the plain 2-cycles that form part of certain pairing-friendly lollipops. While the curves discussed in the paper are quite exotic, it is possible that other real-world curves affected by this result already exist or may emerge in the near future. Although the authors do not consider their contribution groundbreaking, it nonetheless opens a new chapter in accelerating elliptic curve cryptography.

Acknowledgements. The authors express their gratitude to Luca De Feo and Benjamin Smith for fruitful email correspondence regarding the techniques discussed in this article. They also thank Evgeny Alekseev and Vasily Nikolaev for their comments on the state of affairs in Russia concerning the curve GC256C, and Simon Masson for his help with Sage.

References

1. Adj, G., Chi-Domínguez, J.J., Rodríguez-Henríquez, F.: Karatsuba-based square-root Vélu's formulas applied to two isogeny-based protocols. Journal of Cryptographic Engineering **13**(1), 89–106 (2023)
2. Alekseev, E.K., Nikolaev, V.D., Smyshlyaev, S.V.: On the security properties of Russian standardized elliptic curves. Mathematical Aspects of Cryptography **9**(3), 5–32 (2018)
3. Antipa, A., Brown, D., Gallant, R., Lambert, R., Struik, R., Vanstone, S.: Accelerated verification of ECDSA signatures. In: Preneel, B., Tavares, S. (eds.) Selected Areas in Cryptography. SAC 2005. Lecture Notes in Computer Science, vol. 3897, pp. 307–318. Springer, Berlin, Heidelberg (2006)
4. Bank, E., Camacho-Navarro, C., Eisenträger, K., Morrison, T., Park, J.: Cycles in the supersingular ℓ-isogeny graph and corresponding endomorphisms. In: Balakrishnan, J., Folsom, A., Lalín, M., Manes, M. (eds.) Research Directions in Number Theory. Association for Women in Mathematics Series, vol. 19, pp. 41–66. Springer, Cham (2019)
5. Bernstein, D.J., De Feo, L., Leroux, A., Smith, B.: Faster computation of isogenies of large prime degree. In: Galbraith, S.D. (ed.) Algorithmic Number Theory Symposium. ANTS XIV. The Open Book Series, vol. 4, pp. 39–55. Mathematical Sciences Publishers, Berkeley (2020)
6. Bernstein, D.J., Lange, T.: Explicit-formulas database, `https://www.hyperelliptic.org/EFD/index.html`
7. Buchmann, J., Williams, H.C.: A key-exchange system based on imaginary quadratic fields. Journal of Cryptology **1**(2), 107–118 (1988)
8. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology – ASIACRYPT 2018. Lecture Notes in Computer Science, vol. 11274, pp. 395–427. Springer, Cham (2018)
9. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic hash functions from expander graphs. Journal of Cryptology **22**(1), 93–113 (2009)

10. Corte-Real Santos, M., Costello, C., Naehrig, M.: On cycles of pairing-friendly abelian varieties. In: Reyzin, L., Stebila, D. (eds.) Advances in Cryptology – CRYPTO 2024. Lecture Notes in Computer Science, vol. 14928, pp. 221–253. Springer, Cham (2024)
11. Costello, C., Korpal, G.: Lollipops of pairing-friendly elliptic curves for composition of proof systems (2024), https://eprint.iacr.org/2024/1627
12. Cox, D.A., with contributions by Lipsett, R.: Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication, AMS Chelsea Publishing, vol. 387. American Mathematical Society, Providence, 3 edn. (2022)
13. De Feo, L., Kieffer, J., Smith, B.: Towards practical key exchange from ordinary isogeny graphs. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology – ASIACRYPT 2018. Lecture Notes in Computer Science, vol. 11274, pp. 365–394. Springer, Cham (2018)
14. Dubois, R.: RIP-7696 : generic double scalar multiplication (DSM) for all curves (2024), https://ethereum-magicians.org/t/rip-7696-generic-double-scalar-multiplication-dsm-for-all-curves/19798
15. El Housni, Y.: Fake GLV: You don't need an efficient endomorphism to implement GLV-like scalar multiplication in SNARK circuits (2024), https://ethresear.ch/t/fake-glv-you-dont-need-an-efficient-endomorphism-to-implement-glv-like-scalar-multiplication-in-
20394
16. Galbraith, S.D.: Mathematics of public key cryptography. Cambridge University Press, New York (2012)
17. Galbraith, S.D.: Climbing and descending tall volcanos (2024), https://eprint.iacr.org/2024/924
18. Gallant, R.P., Lambert, R.J., Vanstone, S.A.: Faster point multiplication on elliptic curves with efficient endomorphisms. In: Kilian, J. (ed.) Advances in Cryptology – CRYPTO 2001. Lecture Notes in Computer Science, vol. 2139, pp. 190–200. Springer, Berlin, Heidelberg (2001)
19. Institute of Electrical and Electronics Engineers: IEEE standard specifications for public-key cryptography (IEEE Std 1363-2000) (2000), https://ieeexplore.ieee.org/document/891000
20. Koshelev, D., Jeřábek, E.: What is the fastest known algorithm for evaluating a homogeneous binary polynomial? (2024), https://mathoverflow.net/questions/482276/what-is-the-fastest-known-algorithm-for-evaluating-a-homogeneous-binary-polynomi
21. Koshelev, D., Sanso, A.: Sage code (2024), https://github.com/asanso/Endomorphisms-for-Faster-Cryptography-on-Elliptic-Curves-of-Moderate-CM-Discriminants
22. Masson, S., Sanso, A., Zhang, Z.: Bandersnatch: a fast elliptic curve built over the BLS12-381 scalar field. Designs, Codes and Cryptography **92**(12), 4131–4143 (2024)
23. Robert, D.: On the efficient representation of isogenies (a survey) (2024), https://eprint.iacr.org/2024/1071
24. Sedlacek, V., Suchanek, V., Dufka, A., Sys, M., Matyas, V.: DiSSECT: Distinguisher of standard and simulated elliptic curves via traits. In: Batina, L., Daemen, J. (eds.) Progress in Cryptology – AFRICACRYPT 2022. Lecture Notes in Computer Science, vol. 13503, pp. 493–517. Springer, Cham (2022)
25. Smyshlyaev, S.V., Belyavskiy, D.M., Alekseev, E.K.: GOST cipher suites for transport layer security (TLS) protocol version 1.2 (2022), https://datatracker.ietf.org/doc/rfc9189

26. Straus, E.G.: Addition chains of vectors (problem 5125). American Mathematical Monthly **71**(7), 806–808 (1964)
27. Sutherland, A.V.: Accelerating the CM method. LMS Journal of Computation and Mathematics **15**, 172–204 (2012)
28. Wesolowski, B.: Efficient verifiable delay functions. Journal of Cryptology **33**(4), 2113–2147 (2020)