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 (multi-)scalar multiplication to a much broader range of elliptic curves with moderate CM discriminant $D < 0$. Previously, it was commonly believed that this technique can only be applied efficiently for small values of D (e.g., up to 100). In practice, curves with j-invariant 0 are most frequently employed, as they have the smallest possible $D = -3$. However, $j = 0$ curves are either too suspicious for conservative government regulators (e.g., for Russian ones, which prefer $D = -619$) or unavailable under imposed extra restrictions in a series of cryptographic settings. The article thus participates in the decade-long development of numerous 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.

Keywords: binary quadratic forms · elliptic curve cryptography · ideal class groups · isogeny loops · relation lattices · (multi-)scalar multiplication · short vectors · weighted norms

1 Introduction

In 2025, *ECC (elliptic curve cryptography)* celebrates 40 glorious years of its development, which is a sufficient term to be sure in its reliability and efficiency. An excellent recent survey of ECC is given in the treatise [12] updating and extending its older web version [11]. The most important operation in this kind of cryptography is *scalar multiplication*. Sometimes, it can be sped up by the *GLV (Gallant–Lambert–Vanstone) technique* [27]. Furthermore, it is inherently

* https://www.researchgate.net/profile/dimitri-koshelev
This research is a result of the strategic project "Avances en criptografía post-cuántica aplicados al desarrollo de un sistema de cupones" (C039/24), resulting from an agreement between the National Cybersecurity Institute (INCIBE) and University of Lleida. This initiative is carried out in the scope of the funds from the Recovery, Transformation and Resilience Plan, funded by the European Union (Next Generation). The paper is also a part of the R&D+i project PID2021-124613OB-I00 funded by MICIU/AEI/10.13039/501100011033 and FEDER, EU.

extended to *MSM (multi-scalar multiplication)* with N "basis" curve points instead of a unique one. However, the GLV method remains useful whenever the number N is moderate, that is, its benefit fades as $N \to \infty$ as justified in [38, Section 4.2].

Throughout the article, E will stand for an elliptic curve over a finite field $\mathbb{F}_q$ of large characteristic (for simplicity). The (original) GLV technique 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 0 or 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* [38] 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* [25, 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* [25, 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* [49] 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., [22]) 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 [23] 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 $99.9\ldots\%$ 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 [18,19]. 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 [25, Section 25.6] and [26]. On the other hand, curves with a predefined D are constructed exclusively via the *CM method* (see, e.g., [50]). 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* [25, 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 [10], [32, 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 [25, 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 [25, 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 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 [20], [25, 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 $w := d_i$ among the non-zero values of $\mathrm{N}' = \deg$ on $I \simeq \mathrm{Hom}(E_i, E_{i+1})$. The most reasonable choice for w is perhaps the minimal (often prime) value, that is, the norm n. Once m is odd, w is not a perfect square, and m, w are both pretty small, we come to the desired non-scalar endomorphism ϕ on E of degree $d = w^m$. In the new notation, ϕ can be sequentially evaluated at the price of $\approx cmw$ multiplications in $\mathbb{F}_q$ instead of $\approx cw^m$ ones. We will see on practical examples that the theory under consideration actually works. Afterwards, in the second part of the paper, the described approach will be logically extended to serve much greater magnitudes of D provided that the group order r (equivalently, ℓ or ℓ') also grows accordingly.

For instance, some 2-*cycle* [5] of *pairing-friendly MNT curves* [40] (with $-D \approx 100{,}000{,}000$, i.e., $\log_2(-D) \approx 26.5$) is suitable for our contribution. The given 2-cycle was generated at one time by Guillevic [29] to provide ≈ 128 security bits, hence it was close to application in the real world. Another more performant MNT 2-cycle (with slightly smaller security level, but with much larger D) was really employed in the *protocol Coda* [44] (now *Mina* [42]) until zero-knowledge proof systems on significantly faster pairing-free (or half-pairing) 2-cycles were invented. It is also shown that many "lollipop" curves, recently proposed by Costello and Korpal [19] to replace MNT ones, are now covered by the GLV technique.

Additionally, the new result is relevant to one of the "classical" curves (with $D = -619$) from the Russian ECC standard [2, Appendices B, E], [48]. This curve was most likely found using the CM method, though this is not explicitly stated in the standard. Its developers seemingly sought to avoid curves with too small values of D, aiming to mitigate potential DLP attacks on such curves, and hoped these attacks would not extend effectively to $D = -619$. One of the goals of the present article is consequently to address the perceived disparity between the $D = -3$ curves and the Russian curve. Specifically, this curve should either be excluded from the standard for potential security reasons or local software should begin leveraging the advantages of the GLV decomposition.

Isogeny loops are ubiquitous in isogeny-based cryptography. For instance, they are related to collisions in seminal *Charles–Lauter–Goren's hash function* [17]. 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., [46]). The action of the ideal class group of an imaginary quadratic field also plays an important role [21] in the given post-quantum cryptography, although supersingular curves in this context are more preferable [16] than ordinary ones. Finally, the hard DLP in the group Cl gives rise to yet another type of (pre-quantum) cryptography starting with [14]. It is appropriate for developing more specific mechanisms such as *verifiable delay functions (VDF)* [52], 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 moderate 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., [20]. For detailed information on the latter, refer to [25, 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 [25, 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 [33]. 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 cardinally different evaluation strategy from [9] (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 CM discriminants up to a few thousands

This section is dedicated to a few practical elliptic curves of moderate (as earlier, fundamental) CM discriminants D. For credibility, it is accompanied by the code [34] written in the computer algebra systems Magma and 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	$d_{\min}$	$h = m$	$n = w$	$d = w^m$
Russian curve	[2, Appendices B, E]	256	-619	$5 \cdot 31$	5	5	3125
Lollipop curves	[19, Section 5]	201	-547	137	3	11	1331
		261	-3019	$5 \cdot 151$	7	5	78125

Table 1. Certain curves (remarkable for ECC) of moderate fundamental CM discriminants D and their derived parameters. In every case, $\mathrm{Cl} \simeq \mathbb{Z}/h$.

Russian curve	$(1, 1, 155)$, $(5, \pm 1, 31)$, $(7, \pm 5, 23)$
Lollipop curves	$(1, 1, 137)$, $(11, \pm 5, 13)$
	$(1, 1, 755)$, $(5, \pm 1, 151)$, $(13, \pm 7, 59)$, $(25, \pm 9, 31)$

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

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 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 $d = w^m$.

Generally speaking, $d_{\min} = \prod_{i=1}^{N} p_i^{k_i}$, where p_i are pairwise distinct primes and $N, k_i \in \mathbb{N}$. We lack a symbol for the sum $\sigma := \sum_{i=1}^{N} p_i k_i$. 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 $\lceil 7.5mw \rceil$, 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 a prime-order Weierstrass curve $E\colon y^2 = x^3 - 3x + a_6$ 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* [48, Table 2]. 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 point is that Russian civilian cryptography is intuitively less matured than in the West, so local private companies (almost) never utilize elliptic curves of small CM discriminants (such as $D = -3$), produced by their own R&D departments.

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 [47, 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 [19, 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 considered only a few lollipops to illustrate the main idea of the article. Perhaps, it is extended to several others generated by Costello and Korpal. More precisely, the instances with bit lengths $\ell = 201$ (i.e., *Lollipop-489-201*) and $\ell = 261$ (i.e., *Lollipop-574-261*) were selected, as they offer satisfactory security levels ≈ 100. For reference, the common Barreto–Naehrig curve BN254 [51] has approximately the same resistance. This curve was endorsed (e.g., for the Ethereum ecosystem) in the period when its security was falsely estimated as ≈ 128 bits. Despite the discovered weakness, BN254 is still actively employed in the real world for compatibility.

4 CM discriminants up to one hundred millions

The present long section contains a natural extension of the previous material. In comparison with the latter, much greater magnitudes of CM discriminants (in absolute value) are achieved below, although the base finite fields of elliptic curves have to be pretty large. With the reader's permission, we will stick to the majority of notions and notation already encountered. The most basic of them will be nonetheless repeated where appropriate. Our objective is to systemize the anterior result. As it will be shown, the new insight enables to efficiently implement the GLV approach on certain elliptic curves for which Section 3 in its original form does not cope with.

As usual, let $E\colon y^2 = x^3 + a_4x + a_6$ be an ordinary (i.e., non-supersingular) Weierstrass curve over a finite field $\mathbb{F}_q$ of large characteristic. Recall that the GLV method needs a quick non-scalar $\mathbb{F}_q$-endomorphism ϕ on E. In a nutshell, the approach of Section 3 suggests for the role of ϕ the composition of m isogenies $\phi_j : E_j \to E_{j+1}$ (where $E = E_1 = E_{m+1}$) also defined over $\mathbb{F}_q$ and of the same (prime) degree w. Thereby, ϕ is evaluated at points of E via the sequential application of ϕ_j. The obstacle is that for the huge m, the isogeny loop becomes too long and hence ϕ is no longer a cheap endomorphism even if w is itself small. As a generalization, the present section aims to establish shorter isogeny loops admitting the variable degrees $\deg(\phi_j)$ that still do not exceed some modest bound.

As well as in the previous section, we will deal exclusively with elliptic curves E of fundamental CM (complex multiplication) discriminants $D < 0$ to circumvent redundant complications. The set of all such curves constitutes the so-called crater (or surface). The central instrument for us is the ideal (or form) class group Cl of finite order h and its regular action on the crater. The elements of Cl can be either full ideal (form) equivalence classes or their canonical representatives, namely reduced ideals (binary quadratic forms) of discriminant D. To be definite, let's operate with reduced forms. In Section 3, the isogenies ϕ_j are derived with the help of the successive action by such an m-order form $f = (w, w', w'') = wx^2 + w'xy + w''y^2$, where $D = (w')^2 - 4ww''$, starting with E. In this language, w is nothing but the norm of (the ideal associated with) f.

Unfortunately, for the sufficiently big D, the group Cl may not have an element such that its parameters m, w are both little and the resulting endomorphism ϕ is non-scalar. To mitigate this situation, it is logical to pick in Cl a few distinct reduced forms of bounded norms, eliminating (severe) conditions on their orders. We will find out how to choose the forms (and in what quantities) more optimally given D. In a nutshell, it is proposed to resolve a specific instance of the small-dimensional *SVP (shortest vector problem)* approximated in a satisfactory manner. By the way, the GLV method is itself founded on solving the approximated *CVP (closest vector problem)* in another 2-rank lattice.

4.1 Relation lattices and weighted norms

Fix n pairwise-different reduced forms $f_i \in \mathrm{Cl}$ of norms $w_i \in \mathbb{N}$. To be definite, suppose that the forms generate Cl, albeit they should be dependent as far as possible. Otherwise, the material of this section becomes degenerated and hence meaningless for our goals. Consider the group homomorphism

$$\mathbb{Z}^n \to \mathrm{Cl} \qquad v = (v_i)_{i=1}^n \mapsto \prod_{i=1}^n f_i^{v_i}.$$

Its kernel L is known as *relation (or period) lattice*. Since $\mathbb{Z}^n/L \simeq \mathrm{Cl}$, we deal with a full-rank sublattice of index $(\mathbb{Z}^n : L) = h$. It is appropriate to say that the identity of the group Cl is the form $f_0 = (1, w_0', d_{\min})$ for which $w_0' \in \{0, 1\}$.

Let's introduce the *weighted* 1-*norm*

$$\ell^1_w \colon \mathbb{Z}^n \to \mathbb{N} \qquad v \mapsto \sum_{i=1}^{n} w_i |v_i|,$$

where the weight vector $w := (w_i)_{i=1}^n$. It is a logical generalization of the classical 1-norm ℓ^1 when w is the unit vector, i.e., all $w_i = 1$. The function ℓ^1_w is actually a norm in the strict sense of [36, Section XII.2], but it is not a quadratic form on $\mathbb{Z}^n$. The "closest" one to ℓ^1_w is the *weighted form*

$$Q_w \colon \mathbb{Z}^n \to \mathbb{N} \qquad v \mapsto \sum_{i=1}^{n} w_i v_i^2.$$

To complete the picture, we lack the *weighted* 2-*norm* $\ell^2_w(v) := \sqrt{Q_w(v)}$. Notice that Q_w is the standard quadratic form Q when all $w_i = 1$ and thereby $\ell^2(v) := \sqrt{Q(v)}$ is the usual 2-norm. The Gram matrix of the form Q_w is the diagonal matrix W with the vector w on the main diagonal. In particular, the Gram matrix of Q is the unit matrix I_n. Besides, we see that $\ell^1_w(v) = \ell^1(Wv)$.

The norms ℓ^1, ℓ^2 are known to be equivalent. By virtue of [39, Theorem 2.14.2.1], the same statement holds for the general w. Even though we will not leverage this statement directly, it will not hurt to formulate it as the next lemma to better perceive the relationship between ℓ^1_w, ℓ^2_w (and so between ℓ^1_w, Q_w).

Lemma 1. *For every $v \in \mathbb{Z}^n$, we have the inequality sequence*

$$\frac{\ell^1_w(v)}{\sqrt{c}} \leqslant \ell^2_w(v) \leqslant \ell^1_w(v) \leqslant \sqrt{c} \cdot \ell^2_w(v),$$

that is,

$$\frac{\ell^1_w(v)^2}{c} \leqslant Q_w(v) \leqslant \ell^1_w(v)^2 \leqslant c \cdot Q_w(v),$$

where $c := \ell^1(w)$. Thus, the norms ℓ^1_w, ℓ^2_w are equivalent regardless of $w \in \mathbb{N}^n$.

Let $v = (v_i)_{i=1}^n \in \mathbb{Z}^n$ and $j = \sum_{i'=1}^{i-1} |v_{i'}| + j'$, where $1 \leqslant j' \leqslant |v_i|$. Denote by $\phi_j \colon E_j \to E_{j+1}$ the $\mathbb{F}_q$-isogeny derived from the action of the form f_i on the elliptic curve E_j, starting with $E_1 = E$. Note that $m := \ell^1(v)$ is the length of the isogeny chain. By definition of L, the vector $v \in L$ if and only if $\prod_{i=1}^n f_i^{v_i} = f_0$. In turn, this condition is necessary and sufficient for $\phi := \phi_m \circ \ldots \circ \phi_1$ to be an endomorphism on E or, equivalently, $E_{m+1} = E$ as we want. In addition, it is needed to guarantee that $\phi \in \mathrm{End}(E)$ is non-scalar. In particular, this holds whenever $d := \deg(\phi) = \prod_{i=1}^n w_i^{|v_i|}$ is not a square in $\mathbb{Z}$, which is often met.

Hereafter, the norms w_i are assumed to be little primes, although nothing is required for the orders of f_i. The shortest vectors (with respect to ℓ^1_w) of the lattice L precisely correspond to the fastest isogeny loops of the curve E, at least if solely the forms f_i are at our disposal. Indeed, the number of multiplications in $\mathbb{F}_q$ for evaluating (in projective coordinates) any isogeny obtained by f_i amounts to $\approx 7.5w_i$ as explained in Section 2.2. Consequently, the cost of ϕ is equal to $\approx 7.5 \cdot \ell^1_w(v)$ field multiplications. By the way, in a similar context the norm ℓ^1_w is already encountered in [41].

We come to a famous lattice problem of computing a fairly short vector. Nonetheless, it is not expected to be one of the shortest vectors in L, because the latter may give rise to scalar endomorphisms on E. The rank n will be small in the further examples, so we can benefit from widespread (but exponential-time in n) lattice algorithms such as *LLL (Lenstra–Lenstra–Lovász)* [37, Section 1]. On the one hand, the computer algebra systems Magma and Sage, preferred by the authors, apparently do not enable to return a short vector with respect to a norm unlike a quadratic form. On the other hand, Magma provides the functionality in selecting a more desirable form than the standard one Q. As an approximation, it is thus reasonable for us to operate with the function Q_w less exact than ℓ^1_w, but more exact than Q.

4.2 Examples

It is time to illustrate the above idea in several elliptic curves $E/\mathbb{F}_q$ of moderate fundamental CM discriminants D from the cryptographic literature. Table 4 (cf. Table 1) contains main parameters associated with E as well as with D and interesting for us. Inter alia, $e := \lceil \log_2(q) \rceil$ and $\ell := \lceil \log_2(r) \rceil$, where r is the order of a cryptographically strong subgroup $\mathbb{G} \subset E(\mathbb{F}_q)$. Each curve will be separately discussed below. As a supplementary source, they (along with suitable $\mathbb{F}_q$-isogenous curves) are implemented in Sage on the web page [34]. Besides, it stores Magma code allowing to instantly verify all the tables of this paper.

Curve	Reference	e	ℓ	D	$\lceil \log_2(-D) \rceil$	Cl
MNT curves	[29]	753		-331787862733683	49	$\mathbb{Z}/2 \times \mathbb{Z}/1335648$
		992		-95718723	27	$\mathbb{Z}/2 \times \mathbb{Z}/784$
Lollipop curve	[19, Section 5]	956	451	-160807944	28	$(\mathbb{Z}/2)^3 \times \mathbb{Z}/632$

Table 4. Certain curves (remarkable for ECC) of moderate fundamental CM discriminants D and their derived parameters.

Tables 5, 6 (cf. Table 2) demonstrate all (up to inversion in Cl) the reduced binary quadratic forms f_i of prime norms < 150 and < 50 (apart from the identity f_0) for the curves MNT-753 and MNT-992, Lollipop-956-451, respectively. The bounds 150 and 50 were chosen manually as round numbers. If desired, the reader can play by choosing the other bounds. The authors tried 200 and 100 as an alternative, but this led to nothing new, that is, the next tables remained unchanged.

№	Form	Order	=
0	$(1, 1, 82946965683421)$	1	1
1	$(3, 3, 27648988561141)$	2	f_{10}^{667824}
2	$(131, 131, 633182944181)$		f_2
3	$(43, 13, 1928999201941)$	83478	f_{10}^{185168}
4	$(109, 41, 760981336549)$	222608	f_{10}^{349554}
5	$(149, 33, 556691044857)$	333912	$f_2 f_{10}^{845740}$
6	$(139, 117, 596740760337)$	445216	$f_{10}^{1189197}$
7	$(7, 1, 11849566526203)$	667824	$f_{10}^{1027390}$
8	$(47, 41, 1764829057103)$		$f_2 f_{10}^{656686}$
9	$(137, 89, 605452304273)$		$f_2 f_{10}^{639566}$
10	$(31, 3, 2675708570433)$	1335648	f_{10}
11	$(41, 29, 2023096723991)$		$f_2 f_{10}^{1248073}$
12	$(53, 11, 1565037088367)$		$f_2 f_{10}^{767525}$
13	$(103, 3, 805310346441)$		$f_{10}^{1102297}$
14	$(107, 5, 775205286761)$		$f_2 f_{10}^{1070359}$
15	$(113, 67, 734043944111)$		$f_2 f_{10}^{275059}$
16	$(127, 65, 653125714051)$		f_{10}^{955363}

Table 5. The reduced binary quadratic forms $f_i \in \mathrm{Cl}$ (up to the sign) of prime norms $w_i < 150$ in the case of MNT-753.

Denote by $\{u_i\}_{i=1}^n$ the standard basis of $\mathbb{Z}^n$. Tables 5, 6 help to construct the relation lattice L, namely one $\{b_i\}_{i=1}^n$ of its long bases. To be definite, let's explain this in the case of MNT-753. For the others, there is no principal difference, hence the details are omitted. As is seen in the table, the forms f_2, f_{10} (of orders 2 and $h_{10} := h/2$, respectively) are picked as a basis of the group Cl. By definition, the remaining forms are uniquely expressed via them. If $f_i = f_2^{e_2} f_{10}^{e_{10}}$, where $e_2 \in \mathbb{Z}/2$ and $e_{10} \in \mathbb{Z}/h_{10}$, then the corresponding vector $b_i := u_i + e_2 u_2 - e_{10} u_{10}$ for $i \notin \{0, 2, 10\}$. In turn, $b_2 := 2u_2$ and $b_{10} := h_{10} u_{10}$. It is worth saying that Magma automatically returns an LLL-reduced basis of L once $\{b_i\}_{i=1}^n$ is inputted. Curiously, in [13, Section 3] the class group structure (for the CSIDH-512 parameter set) is conversely found through establishing a lot of non-trivial relations in the 74-rank relation lattice. Note that $\lceil \log_2(h) \rceil = 256$ in this situation, being the largest determined class group of fundamental discriminant to the authors' knowledge.

№	Form	Order	=
0	$(1,1,23929681)$	1	1
1	$(3,3,7976561)$	2	f_1
2	$(41,41,583661)$		$f_1 f_6^{392}$
3	$(23,3,1040421)$	112	$f_1 f_6^{91}$
4	$(17,7,1407629)$	392	$f_1 f_6^{486}$
5	$(31,15,771927)$		f_6^{130}
6	$(13,11,1840747)$	784	f_6
7	$(19,3,1259457)$		f_6^{333}

The case of MNT-992

№	Form	Order	=
0	$(1,0,40201986)$	1	1
1	$(2,0,20100993)$	2	f_1
2	$(3,0,13400662)$		f_2
3	$(11,0,3654726)$		f_3
4	$(19,0,2115894)$		$f_1 f_2 f_3 f_7^{316}$
5	$(41,40,980546)$	158	$f_1 f_7^{344}$
6	$(43,4,934930)$		$f_1 f_2 f_3 f_7^{24}$
7	$(5,4,8040398)$	632	f_7
8	$(7,2,5743141)$		$f_1 f_2 f_7^{179}$
9	$(23,12,1747914)$		f_7^{365}
10	$(47,26,855365)$		f_7^{517}

The case of Lollipop-956-451

Table 6. The reduced binary quadratic forms $f_i \in \mathrm{Cl}$ (up to the sign) of prime norms $w_i < 50$.

Table 7 exhibits fairly short vectors $s = (s_i)_{i=1}^n \in L$ (and the related forms in Cl) with respect to the weighted norm ℓ_w^1. For comparison, values of the weighted quadratic form Q_w are equally included in the given table. The vectors s are obtained by brute force over the ball $B := \{v \in L \mid Q_w(v) \leqslant R\}$ for some round radius $R \in \mathbb{N}$. Once again, Magma (as well as Sage) does not possess an intrinsic outputting a vector short in terms of ℓ_w^1 rather than Q_w. Meanwhile, the inequalities from Lemma 1 do not seem to be tight enough to reasonably reduce the search. And in general, it is probably difficult to deduce (much) tighter inequalities between ℓ_w^1, Q_w. Nevertheless, since we deal with lattices of little ranks, the brute force promptly yields quite good results. Importantly, if we made use of another quadratic form (for example Q) as a measure on L, the ball B would be less adequate (or R should have be greater) and thereby the resulting vectors (or their search time) might be longer. This is especially wise if the reader (like the authors) does not dispose the paid Magma version, but only the free online one.

Recall that $d_{\min}$ (the third coefficient of f_0) coincides with the minimal possible degree of non-scalar endomorphisms on E, whereas $\phi_{\min}$ stands here for one of them. Table 8 shows the prime factorizations $d_{\min} = \prod_{i=1}^N p_i^{k_i}$ and $d = \prod_{i=1}^n w_i^{|s_i|}$ for the degrees of $\phi_{\min}$, ϕ. Note that the sum $\sigma := \sum_{i=1}^N p_i k_i$ plays the same role as $\ell_w^1(s)$. To better reflect a big gap between these quantities, they are simultaneously represented in the previous table. Finally, in Table 9 (cf. Table 3) one can see the estimated numbers of multiplications in $\mathbb{F}_q$ for evaluating the endo-

Curve	Short vector	Form	$\ell_w^1(s)$	$Q_w(s)$	σ
MNT curves	$(1,0,1,1,0,0,-1,0,0,-6,2,0,0,0,0,0)$	$\frac{f_1 f_3 f_4 f_{11}^2}{f_7 f_{10}^6}$	430	1442	207280768
	$(1,1,-1,1,0,-3,0)$	$\frac{f_1 f_2 f_4}{f_3 f_6^3}$	123	201	1095
Lollipop curve	$(0,0,0,0,0,0,7,2,-1,0)$	$\frac{f_7^7 f_8^2}{f_9}$	72	296	32094

Table 7. Certain short vectors $s \in L$ and their derived parameters (apart from σ).

morphisms $[2^{\ell'}]$, $\phi_{\min}$, and ϕ, where $\ell' := \lceil \ell/2 \rceil$. In other words, the columns mean the values $8\ell'$, $\lceil 7.5\sigma \rceil$, and $\lceil 7.5 \cdot \ell_w^1(s) \rceil$, respectively.

Curve	$d_{\min}$	d
MNT curves	$7^2 \cdot 8167 \cdot 207272587$	$3 \cdot 7 \cdot 31^6 \cdot 41^2 \cdot 43 \cdot 109$
	$103 \cdot 379 \cdot 613$	$3 \cdot 13^3 \cdot 17 \cdot 23 \cdot 41$
Lollipop curve	$2 \cdot 3 \cdot 11 \cdot 19 \cdot 32059$	$5^7 \cdot 7^2 \cdot 23$

Table 8. The prime factorizations for the degrees of the endomorphisms $\phi_{\min}$, ϕ.

Curve	$[2^{\ell'}]$	$\phi_{\min}$	ϕ
MNT curves	3016	1554605760	3225
	3968	8213	923
Lollipop curve	1808	240705	540

Table 9. Approximate numbers of field multiplications for evaluating the endomorphisms $[2^{\ell'}]$, $\phi_{\min}$, and ϕ.

4.2.1 MNT curves

MNT (Miyaji–Nakabayashi–Takano) curves [40] are historically the first ordinary *pairing-friendly curves* of prime orders r. Their embedding degrees k are 3, 4, or 6. Afterwards, other such curves appeared, namely Freeman and BN (Barreto–Naehrig) ones enjoying the greater k equal to 10 and 12, respectively. So, MNT curves lost their practical significance for a while. By the way, the requirement on r to be prime is redundant, since uselessly increases the Miller loop during pairing computation. That is why the most optimal curves (at least for the 128-bit security level) appropriate for pairings are widely recognized to be BLS12 (Barreto–Lynn–Scott) ones with $k = 12$ and value $\rho \approx 1.5$. More information on pairing-friendly families can be found, e.g., in [24, Section 4].

The situation is flipped on its head if we are talking about (2-)*cycles* of pairing-friendly curves. At the moment, the humanity does not know examples of such cycles (with bigger k) different from MNT ones. This is an open academic problem (see details in [5]). If it was resolved, one could fully benefit, e.g., from *Groth16* [28], a very famous *zk-SNARK (succinct non-interactive argument of knowledge)*. Nowadays, the problem nevertheless has nothing to do with real-world cryptography, since some time ago people managed to deploy zk-SNARKs (e.g., *Nova* [35]) by means of (semi-)plain 2-cycles such as *Pasta curves* [30] or *Pluto/Eris* [31]. In other words, the pairing-friendly property eventually became superfluous for cycles. It is worth stressing that this concept is essentially the unique known way in overall cryptography to bring to life **succinct** zero-knowledge proofs of unrestricted recursion. And vice versa, this niche is in essence the only pertinent cryptographic application of cycles.

The most prominent pairing-friendly 2-cycle is perhaps *MNT-753* [29]. Experts in the area are equally aware of the 2-cycles *MNT-298* [7, Section 3.2] and *MNT-992* [29]. Each mentioned 2-cycle consists of one curve with $k = 4$ and of another with $k = 6$. Both curves possess the identical D, as their Frobenius discriminants are described by the function $s(q, r) := (q + 1 - r)^2 - 4q$ symmetric in q, r. [3] Furthermore, the number in every name means ℓ and obviously coincides with e. In the past, the MNT-753 cycle was employed in *Coda* [44] (after rebranding, *Mina* [42]) *protocol*, although it now also gives the preference to Pasta curves as follows from [43]. In accordance with Guillevic, the given MNT cycle provides 113 security bits, while MNT-298, MNT-992 correspond to 77 and 126 bits, respectively. MNT-298 is a too weak cycle, hence it has never been leveraged in practice to the authors' knowledge. It was generated at one time exclusively as a demonstration. In turn, MNT-992 is even slower than MNT-753. Indeed, the fields $\mathbb{F}_q$, $\mathbb{F}_r$ of the former (unlike the latter) are not highly 2-adic (not to mention the larger bit length): $q - 1$ and $r - 1$ are not divided by sufficient powers of 2. The point is that highly 2-adic fields are the most suitable

[3] In fact, the CM discriminant D' indicated in [29] for the MNT-753 curves E' is not fundamental for unexplained reasons, namely $D' = 27^2 D$ for the fundamental one D (from Table 4). Put another way, elliptic curves related to D' are not located on the crater, although the CM method is (usually) launched for fundamental CM discriminants. Since D is large and the authors do not possess necessary computational resources, they did not manage to determine the true CM discriminant for the MNT-753 curves to which Guillevic refers. Fortunately, it is easily verified that D is the square-free part of the Frobenius discriminant $s(q, r)$. Even if the curves E' have the CM discriminant D' rather than D, there are in this case uniquely defined crater curves E and vertical $\mathbb{F}_q$-isogenies $E \to E'$ (as well as their duals $E' \to E$) of the modest degree 27. So, we can actually work on the crater without any remorse.

for implementing FFT (fast Fourier transform), which dramatically speeds up execution of zk-SNARKs.

In 2019, the *Coda–Dekrypt challenge* [45] was held with the purpose to exhaustively accelerate the MNT-753 cycle (including MSM optimization). The authors did not hear about fundamental advances in the challenge except for the invention of *lollipops* [19]. According to Table 9, the technique of the present article does not improve upon $[2^{\ell'}]$ (so far) on the cycle in question. Nevertheless, in the running-time estimation of the new endomorphism ϕ, we do not take in account that the higher-degree isogenies ϕ_j defining ϕ (let's say when $w_i > 40$) may be evaluated more rapidly than in Section 2.2, e.g., via *square-root Vélu's formulas* [9]. For conciseness, we leave this subtle work for the future in the hope to attract attention of experienced developers to the given computational task. Despite the fact that the Coda–Dekrypt challenge expired many years ago, any noteworthy progress in solving its concerns should be fascinating and (potentially) useful in diverse branches of ECC. On the other hand, there is apparently no room for optimizing $[2^{\ell'}]$.

4.2.2 Lollipop curve

This section is dedicated to an ordinary pairing-friendly curve $E/\mathbb{F}_q$ of embedding degree $k = 4$ in the stick of *Lollipop-956-451* from [19, Section 5]. The field $\mathbb{F}_q$ is of the length $e = 956$, but the discrete logarithm problem is considered in the prime subgroup $\mathbb{G} \subset E(\mathbb{F}_q)$ of length $\ell = 451$. Thereby, the value $\rho > 2$, that is, $\mathbb{G}$ is more than two times smaller than the whole group $E(\mathbb{F}_q)$. Furthermore, the bit security of $\mathbb{G}$ itself is equal to $\ell' - 1 = 225$ (much greater than 128), while the true one (of the lollipop) is 142 bits because of the MOV (Menezes–Okamoto–Vanstone) attack through the multiplicative group $\mathbb{F}_{q^4}^*$. The example under consideration has the largest value ℓ (and hence ℓ') among all the ordinary pairing-friendly lollipop curves generated by Costello and Korpal: $\ell \leqslant 262 \ll 451$ for the others. Meanwhile, their CM discriminants are not an order of magnitude smaller than D. As a result, E seems to be the unique curve for which the endomorphism ϕ (noticeably) outperforms the conventional scalar one $[2^{\ell'}]$.

Recall that Section 3 analyzes a few curves constituting Lollipop-489-201 and Lollipop-574-261, but those are plain (i.e., non-pairing-friendly) and located in another part of the stick: more far than E from the corresponding supersingular 2-cycle. In particular, the CM discriminants of the plain lollipop curves are much more modest than that of E. The authors decided to take the curve E for diversity to tackle the cardinally new case. However, it is highly likely that the relation-lattice method of this section is relevant to all the plain lollipop curves from [19, Section 5].

Moreover, by using several prime-norm forms from Cl instead of the same one, it is apparently possible to construct slightly faster non-scalar endomorphisms ϕ on the curves addressed earlier (including GC256C). In other words, the numbers of multiplications in the last column of Table 3 may even be reduced. Nevertheless, these numbers are insignificant, since the values D from Table 1 are not as large as those from Table 4. Therefore, the further optimization of the first curves was sacrificed for simplicity of exposition. Otherwise, one would have to immediately involve the concepts of relation lattices and weighted norms, which would complicate understanding of the text.

5 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. Specifically, the relevance of the GLV method is justified for a series of curves arising in pairing-based recursive zk-SNARKs (apart from one Russian standardized curve). These include certain 2-cycles of MNT curves and ordinary curves participating in formation of lollipops. In theory, lollipops are intended to supersede MNT 2-cycles. However, it is unlikely that the GLV technique (even in view of the current work) is applicable to supersingular curves forming lollipop 2-cycles. Moreover, lollipops provide in a sense restricted recursion. Thus, MNT 2-cycles have some benefits over lollipops.

Advances in accelerating MSM on (pairing-friendly) 2-cycles/lollipops are partially able to increase interest to zero-knowledge proof systems based on ECC. It is not a secret that cryptographic hash functions (from [8,15]) are usable for implementing *zk-STARKs (zero-knowledge scalable transparent argument of knowledge)* [6]. Nevertheless, hash-based cryptography does not respect the succinctness property, which is often crucial for blockchain technology. So, the authors think that further investigations are necessary to better understand the full cryptographic capabilities of elliptic curves. Of course, this point of view is vital only if the probability of creating a multi-qubit quantum computer is not higher than that of finding a novel attack on (or a backdoor in) a used hash function.

To conclude, one more step is done in the given paper towards more rapid cryptography on elliptic curves. While the curves discussed are quite exotic, it is possible that other real-world curves affected by the paper 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. This definitely deserves attention of the scientific community, since the speed is frequently one of the main advantages of ECC versus trendy (presumably) PQC. The more efficient the former, the more tempting to keep it at least for the sake of niche time-critical scenarios (especially with short-term data) than to make the entire transition to the latter.

Acknowledgements. The authors express their gratitude to Luca De Feo and Benjamin Smith for fruitful email correspondence related to this article. They also thank Evgeny Alekseev and Vasily Nikolaev for their comments on the status of the curve GC256C in Russia, and Simon Masson for his help with Sage. In addition, the authors are grateful to Kobi Gurkan for telling them about the state of affairs with 2-cycles in Mina protocol. Finally, Dimitri Koshelev appreciates the aid of Sergi Simón Balcells and Josep Conde Colom in configuration of his work computer.

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. Bellés-Muñoz, M., Urroz, J.J., Silva, J.: Revisiting cycles of pairing-friendly elliptic curves. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023. Lecture Notes in Computer Science, vol. 14082, pp. 3–37. Springer, Cham (2023)
6. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Scalable, transparent, and post-quantum secure computational integrity (2018), https://eprint.iacr.org/2018/46
7. Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M.: Scalable zero knowledge via cycles of elliptic curves. In: Garay, J.A., Gennaro, R. (eds.) Advances in Cryptology – CRYPTO 2014. Lecture Notes in Computer Science, vol. 8617, pp. 276–294. Springer, Berlin, Heidelberg (2014)
8. Ben-Sasson, E., Goldberg, L., Levit, D., with an appendix by Faugère, J.-C., Perret, L.: STARK friendly hash – survey and recommendation (2020), https://eprint.iacr.org/2020/948
9. 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)
10. Bernstein, D.J., Lange, T.: Explicit-formulas database, https://www.hyperelliptic.org/EFD/index.html
11. Bernstein, D.J., Lange, T.: Safe curves: choosing safe curves for elliptic-curve cryptography (2017), https://safecurves.cr.yp.to
12. Bernstein, D.J., Lange, T.: Safe curves for elliptic-curve cryptography (2024), https://eprint.iacr.org/2024/1265
13. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: efficient isogeny based signatures through class group computations. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019. Lecture Notes in Computer Science, vol. 11921, pp. 227–247. Springer, Cham (2019)
14. Buchmann, J., Williams, H.C.: A key-exchange system based on imaginary quadratic fields. Journal of Cryptology **1**(2), 107–118 (1988)
15. Canteaut, A., Beyne, T., Dinur, I., Eichlseder, M., Leander, G., Leurent, G., Naya-Plasencia, M., Perrin, L., Sasaki, Y., Todo, Y., Wiemer, F.: Report on the security of STARK-friendly hash functions (version 2.0) (2020), https://eips.ethereum.org/assets/eip-5988/papers/report_security_stark_friendly_hash.pdf

16. 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)
17. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic hash functions from expander graphs. Journal of Cryptology **22**(1), 93–113 (2009)
18. 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)
19. Costello, C., Korpal, G.: Lollipops of pairing-friendly elliptic curves for composition of proof systems (2024), `https://eprint.iacr.org/2024/1627`
20. 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)
21. 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)
22. 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`
23. 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-s 20394`
24. El Mrabet, N., Joye, M. (eds.): Guide to pairing-based cryptography. Cryptography and Network Security Series, Chapman and Hall/CRC, New York (2017)
25. Galbraith, S.D.: Mathematics of public key cryptography. Cambridge University Press, New York (2012)
26. Galbraith, S.D.: Climbing and descending tall volcanos (2024), `https://eprint.iacr.org/2024/924`
27. 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)
28. Groth, J.: On the size of pairing-based non-interactive arguments. In: Fischlin, M., Coron, J.S. (eds.) Advances in Cryptology – EUROCRYPT 2016. Lecture Notes in Computer Science, vol. 9665, pp. 305–326. Springer, Berlin, Heidelberg (2016)
29. Guillevic, A.: Pairing-friendly curves (2021), `https://members.loria.fr/AGuillevic/pairing-friendly-curves`
30. Hopwood, D.: The Pasta curves for Halo 2 and beyond (2020), `https://electriccoin.co/blog/the-pasta-curves-for-halo-2-and-beyond`
31. Hopwood, D.: Pluto/Eris supporting evidence (2021), `https://github.com/daira/pluto-eris`
32. Institute of Electrical and Electronics Engineers: IEEE standard specifications for public-key cryptography (IEEE Std 1363-2000) (2000), `https://ieeexplore.ieee.org/document/891000`

33. 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
34. Koshelev, D., Sanso, A.: Magma and Sage code (2025), https://github.com/asanso/Endomorphisms-for-Faster-Cryptography-on-Elliptic-Curves-of-Moderate-CM-Discriminants
35. Kothapalli, A., Setty, S., Tzialla, I.: Nova: recursive zero-knowledge arguments from folding schemes. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology – CRYPTO 2022. Lecture Notes in Computer Science, vol. 13510, pp. 359–388. Springer, Cham (2022)
36. Lang, S.: Algebra, Graduate Texts in Mathematics, vol. 211. Springer, New York, 3 edn. (2002)
37. Lenstra, A.K., Lenstra, Jr., H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen **261**(4), 515–534 (1982)
38. 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)
39. Mitrinović, D.S., in cooperation with Vasić, P.M.: Analytic inequalities, Grundlehren der mathematischen Wissenschaften, vol. 165. Springer, Berlin, Heidelberg (1970)
40. Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **E84-A**(5), 1234–1243 (2001)
41. Nakagawa, K., Onuki, H., Takayasu, A., Takagi, T.: L_1-norm ball for CSIDH: optimal strategy for choosing the secret key space. Discrete Applied Mathematics **328**, 70–88 (2023)
42. $O(1)$ Labs: Mina protocol, https://minaprotocol.com
43. $O(1)$ Labs: Pasta curves, https://o1-labs.github.io/proof-systems/specs/pasta.html#pasta-curves
44. $O(1)$ Labs: Coda protocol (2022), https://codaprotocol.com
45. $O(1)$ Labs, Dekrypt Capital: Coda + Dekrypt: the SNARK challenge (2019), https://coinlist.co/build/coda
46. Robert, D.: On the efficient representation of isogenies (a survey) (2024), https://eprint.iacr.org/2024/1071
47. 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)
48. 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
49. Straus, E.G.: Addition chains of vectors (problem 5125). American Mathematical Monthly **71**(7), 806–808 (1964)
50. Sutherland, A.V.: Accelerating the CM method. LMS Journal of Computation and Mathematics **15**, 172–204 (2012)
51. Wang, J.: BN254 for the rest of us (2024), https://hackmd.io/@jpw/bn254
52. Wesolowski, B.: Efficient verifiable delay functions. Journal of Cryptology **33**(4), 2113–2147 (2020)