Endomorphisms for Faster Cryptography on Elliptic Curves of Moderate CM Discriminants, II

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. The present article is a natural extension of the previous one [17] about the GLV method of accelerating a (multi-)scalar multiplication on elliptic curves of moderate CM discriminants $D < 0$. In comparison with the first article, much greater magnitudes of D (in absolute value) are achieved, although the base finite fields of the curves have to be pretty large. This becomes feasible by resorting to quite powerful algorithmic tools developed primarily in the context of lattice-based and isogeny-based cryptography. Curiously, pre-quantum cryptography borrows research outcomes obtained when seeking conversely quantum-resistant solutions or attacks on them.

For instance, some 2-cycle of pairing-friendly MNT curves (with $-D \approx$ 100,000,000, i.e., $\log_2(-D) \approx 26.5$) is relevant for the result of the current article (as opposed to [17]). The given 2-cycle was generated at one time by Guillevic to provide ≈ 128 security bits, hence it was close to application in real-world zk-SNARKs. Another more performant MNT 2-cycle (with slightly smaller security level, but with much larger D) was really employed in the protocol Coda (now Mina) until zero-knowledge proof systems on significantly faster pairing-free (or half-pairing) 2-cycles were invented. It is also shown in the given work that more lollipop curves, recently proposed by Costello and Korpal to replace MNT ones, are now covered by the GLV technique.

Keywords: binary quadratic forms · GLV · ideal class groups · isogeny loops · pairing-friendly curves · relation lattices · short vectors · weighted norms

* 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.

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 [7] updating and extending its older web version [6]. 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* [12]. To avoid repetitions, let's omit here its standard explanation. The only additional comment is that the GLV method is inherently extended to *MSM (multi-scalar multiplication)* with N "basis" curve points instead of a unique one. However, the method in fact remains useful whenever the number N is moderate, that is, its benefit fades as $N \to \infty$ as justified in [22, Section 4.2].

This article is essentially founded on the first one [17], hence with the reader's permission, we will stick to the majority of its notions and notation. The most basic of them will be nonetheless repeated where appropriate. As a consequence, we immediately proceed to technical description of the given work. Its 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 [17] 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 [17] 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 article 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 article, 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 [17], 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.

2 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*

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

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_w^1 is actually a norm in the strict sense of [20, Section XII.2], but it is not a quadratic form on $\mathbb{Z}^n$. The "closest" one to ℓ_w^1 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* $\ell_w^2(v) := \sqrt{Q_w(v)}$. 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 $\ell_w^1(v) = \ell^1(Wv)$.

The norms ℓ^1, ℓ^2 are known to be equivalent. By virtue of [23, 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_w^1, ℓ_w^2 (and so between ℓ_w^1, Q_w).

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

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

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 $\approx 7.5 w_i$ as explained in [17, 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 [25].

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)* [21, 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.

3 Examples

It is time to illustrate the article idea in several elliptic curves $E/\mathbb{F}_q$ of moderate fundamental CM discriminants D from the cryptographic literature. Table 1 (cf. [17, 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 [18]. Besides, it stores Magma code allowing to instantly verify the tables of this section.

Tables 2, 3 (cf. [17, Table 2]) demonstrate all (up to inversion in Cl) the reduced binary quadratic forms f_i of prime norms < 150 and < 50 (apart from

Curve	Reference	e	ℓ	D	$\lceil\log_2(-D)\rceil$	Cl
MNT curves	[14]	753		-331787862733683	49	$\mathbb{Z}/2 \times \mathbb{Z}/1335648$
		992		-95718723	27	$\mathbb{Z}/2 \times \mathbb{Z}/784$
lollipop curve	[10, Section 5]	956	451	-160807944	28	$(\mathbb{Z}/2)^3 \times \mathbb{Z}/632$

Table 1. Certain curves (remarkable for ECC) of moderate fundamental CM discriminants D and their derived parameters

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.

Denote by $\{u_i\}_{i=1}^n$ the standard basis of $\mathbb{Z}^n$. Tables 2, 3 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 [8, 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.

Table 4 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, the 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

№	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 2. 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

№	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 3. The reduced binary quadratic forms $f_i \in \mathrm{Cl}$ (up to the sign) of prime norms $w_i < 50$

if the reader (like the authors) does not dispose the paid Magma version, but only the free online one.

Curve	Short vector	Form	$\ell_w^1(s)$	$Q_w(s)$	σ
MNT curves	$(1,0,1,1,0,0,-1,0,0,-6,2,0,0,0,0,0)$	$\frac{f_1f_3f_4f_{11}^2}{f_7f_{10}^6}$	430	1442	207280768
	$(1,1,-1,1,0,-3,0)$	$\frac{f_1f_2f_4}{f_3f_6^3}$	123	201	1095
lollipop curve	$(0,0,0,0,0,0,7,2,-1,0)$	$\frac{f_7^7f_8^2}{f_9}$	72	296	32094

Table 4. Certain short vectors $s \in L$ and their derived parameters (apart from σ)

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 5 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. Among other things, we lack a symbol for the sum $\sigma := \sum_{i=1}^{N} p_i k_i$ playing 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 6 (cf. [17, Table 3]) one can see the estimated numbers of multiplications in $\mathbb{F}_q$ for evaluating the endomorphisms $[2^{\ell'}]$, $\phi_{\min}$, 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 5. The prime factorizations for the degrees of the endomorphisms $\phi_{\min}$, ϕ

3.1 MNT curves

MNT (Miyaji–Nakabayashi–Takano) curves [24] are historically the first ordinary *pairing-friendly curves* of prime orders r. Their embedding degrees k are 3, 4, or

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

Table 6. Approximate numbers of field multiplications for evaluating the endomorphisms $[2^{\ell'}]$, $\phi_{\min}$, and ϕ

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 [11, 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 [1]). If it was resolved, one could fully benefit, e.g., from *Groth16* [13], 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* [19]) by means of (semi-)plain 2-cycles such as *Pasta curves* [15] or *Pluto/Eris* [16]. 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* [14]. Experts in the area are equally aware of the 2-cycles *MNT-298* [3, Section 3.2] and *MNT-992* [14]. 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

[3] In fact, the CM discriminant D' indicated in [14] for the MNT-753 curves E' is not fundamental for unexplained reasons, namely $D' = 27^2 D$ for the fundamental one D (from Table 1). 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

coincides with e. In the past, the MNT-753 cycle was employed in *Coda* [28] (after rebranding, *Mina* [26]) *protocol*, although it now also gives the preference to Pasta curves as follows from [27]. 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 for implementing FFT (fast Fourier transform), which dramatically speeds up execution of zk-SNARKs.

In 2019, the *Coda–Dekrypt challenge* [29] 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* [10]. According to Table 6, 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 [17, Section 2.2], e.g., via *square-root Vélu's formulas* [5]. 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 $[2^{\ell'}]$.

3.2 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 [10, 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 $\mathbb{F}_{q^4}^*$.

Recall that the anterior paper [17] 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

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.

supersingular 2-cycle. In particular, the CM discriminants of the plain lollipop curves are much more modest than that of E (denoted by D as earlier). 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 article is relevant to all the plain lollipop curves from [10, Section 5], not solely to those of [17].

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 $[2^{\ell'}]$.

4 Conclusion

This article justifies the relevance of the GLV method for a series of elliptic curves arising in pairing-based recursive zk-SNARKs. These include a certain 2-cycle of MNT curves and yet another ordinary pairing-friendly curve participating in formation of a lollipop. 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 may 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 [4,9]) are usable for implementing *zk-STARKs (zero-knowledge scalable transparent argument of knowledge)* [2]. 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. 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. Dimitri Koshelev expresses his gratitude to Sergi Simón Balcells and Josep Conde Colom for the aid in configuration of the author's work computer. In addition, the authors are grateful to Kobi Gurkan for telling them about the state of affairs with 2-cycles in Mina protocol.

References

1. 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)
2. Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M.: Scalable, transparent, and post-quantum secure computational integrity (2018), https://eprint.iacr.org/2018/46
3. 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)
4. 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
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.: Safe curves: choosing safe curves for elliptic-curve cryptography (2017), https://safecurves.cr.yp.to
7. Bernstein, D.J., Lange, T.: Safe curves for elliptic-curve cryptography (2024), https://eprint.iacr.org/2024/1265
8. 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)
9. 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
10. Costello, C., Korpal, G.: Lollipops of pairing-friendly elliptic curves for composition of proof systems (2024), https://eprint.iacr.org/2024/1627
11. El Mrabet, N., Joye, M. (eds.): Guide to pairing-based cryptography. Cryptography and Network Security Series, Chapman and Hall/CRC, New York (2017)
12. 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)
13. 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)
14. Guillevic, A.: Pairing-friendly curves (2021), https://members.loria.fr/AGuillevic/pairing-friendly-curves
15. Hopwood, D.: The Pasta curves for Halo 2 and beyond (2020), https://electriccoin.co/blog/the-pasta-curves-for-halo-2-and-beyond
16. Hopwood, D.: Pluto/Eris supporting evidence (2021), https://github.com/daira/pluto-eris

17. Koshelev, D., Sanso, A.: Endomorphisms for faster cryptography on elliptic curves of moderate CM discriminants (2024), `https://eprint.iacr.org/2024/1985`
18. Koshelev, D., Sanso, A.: Magma and Sage code (2025), `https://github.com/asanso/Endomorphisms-for-Faster-Cryptography-on-Elliptic-Curves-of-Moderate-CM-Discriminants-II`
19. 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)
20. Lang, S.: Algebra, Graduate Texts in Mathematics, vol. 211. Springer, New York, 3 edn. (2002)
21. Lenstra, A.K., Lenstra, Jr., H.W., Lovász, L.: Factoring polynomials with rational coefficients. Mathematische Annalen **261**(4), 515–534 (1982)
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. Mitrinović, D.S., in cooperation with Vasić, P.M.: Analytic inequalities, Grundlehren der mathematischen Wissenschaften, vol. 165. Springer, Berlin, Heidelberg (1970)
24. 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)
25. 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)
26. $O(1)$ Labs: Mina protocol, `https://minaprotocol.com`
27. $O(1)$ Labs: Pasta curves, `https://o1-labs.github.io/proof-systems/specs/pasta.html#pasta-curves`
28. $O(1)$ Labs: Coda protocol (2022), `https://codaprotocol.com`
29. $O(1)$ Labs, Dekrypt Capital: Coda + Dekrypt: the SNARK challenge (2019), `https://coinlist.co/build/coda`