Application of Mordell–Weil lattices with large kissing numbers to acceleration of multi-scalar multiplication on elliptic curves

Dmitrii Koshelev[0000−0002−4796−8989] *
dimitri.koshelev@gmail.com

Parallel Computation Laboratory, École Normale Supérieure de Lyon, France
http://www.ens-lyon.fr

Abstract. This article aims to speed up (the precomputation stage of) multi-scalar multiplication (MSM) on ordinary elliptic curves of j-invariant 0 with respect to specific "independent" (a.k.a. "basis") points. For this purpose, so-called Mordell–Weil lattices (up to rank 8) with large kissing numbers (up to 240) are employed. In a nutshell, the new approach consists in obtaining more efficiently a considerable number (up to 240) of certain elementary linear combinations of the "independent" points. By scaling the point (re)generation process, it is thus possible to get a significant performance gain. As usual, the resulting curve points can be then regularly used in the main stage of an MSM algorithm to avoid repeating computations. Seemingly, this is the first usage of lattices with large kissing numbers in cryptography, while such lattices have already found numerous applications in other mathematical domains. Without exaggeration, the article results can strongly affect performance of today's real-world elliptic cryptography, since MSM is a widespread primitive (often the unique bottleneck) in modern protocols. Moreover, the new (re)generation technique is prone to further improvements by considering Mordell–Weil lattices with even greater kissing numbers.

Keywords: elliptic curves of j-invariant 0 · kissing number · minimal points · Mordell–Weil lattices · multi-scalar multiplication.

1 Introduction

It is not a secret that elliptic curves E over finite fields $\mathbb{F}_q$ of huge characteristics p are actively used in discrete logarithm cryptography. Multi-scalar multiplication (MSM) in the $\mathbb{F}_q$-point group $E(\mathbb{F}_q)$ is widely recognized as a very slow operation. To be more precise, it is about computing the sum $\sum_{i=1}^{N} n_i P_i$ for given $N \in \mathbb{N}$ "basis" points $P_i \in E(\mathbb{F}_q)$ and integers $n_i \in \mathbb{Z}$. At the same time, MSM is actually a ubiquitous primitive in advanced protocols of elliptic cryptography. Therefore, there is a vital need among implementers to speed up the given primitive.

* The author was supported by Ethereum Foundation.

As a confirmation of these words, one can mention the relatively recent ZPRIZE 2022 competition [1] (see also ZPRIZE 2023 [2]). Among its objectives was accelerating MSM on certain elliptic $\mathbb{F}_q$-curves $E_b : y^2 = x^3 + b$ (of j-invariant 0). The money rewards of this competition were quite tempting (the total prize was \$4,415,000), which indicates the importance of the topic. As is well known, $j = 0$ curves are the most attractive in pairing-based cryptography. Furthermore, they enjoy the most efficient group operation (at least among prime-order curves). That is why curves E_b are a popular choice for implementation of discrete logarithm-based protocols, even if they do not deal with pairings.

There are numerous algorithms of MSM (see, e.g., [3,4,6] and references therein). All of them in one way or another are reduced to precomputing auxiliary points of the form $P_v := \sum_{i=1}^N v_i P_i$ with various integer vectors $v = (v_i)_{i=1}^N$. The points P_v are then utilised (depending on the concrete n_i) in the main part of an MSM algorithm, allowing to avoid a lot of repeating elliptic curve additions. By the way, $P_i = P_{e_i}$, where $e_i = (0, \cdots, 0, 1, 0, \cdots, 0)$ are the standard basis vectors of the lattice $\mathbb{Z}^N$.

In fact, the points P_v become less useful whenever the vectors v are long with respect to a certain norm on $\mathbb{Z}^N$. In this situation, P_v seem to be too redundant points in the sense that we cannot often apply them during multi-scalar multiplication. The author decided to work with the 1-norm $|v|_1 = \sum_{i=1}^N |v_i|$ to stay with little naturals. Besides, it is the most suitable to reflect "complexity" of the points P_v. Indeed, if $|v_i| \leqslant 2$ and more frequently $|v_i| \leqslant 1$ (as it turns out in this paper), then the 1-norm almost coincides with the minimal number of additions on E necessary for computing P_v given v_i and P_i. Thus, it is sufficient to focus on vectors $v \in \mathbb{Z}^N$ that lie in the ball of some small radius $R \in \mathbb{N}$, i.e., $|v|_1 \leqslant R$. In particular, they have to possess maximum R non-zero coordinates.

For elliptic curves having an $\mathbb{F}_q$-endomorphism τ of degree close to 1, the famous GLV (Gallant–Lambert–Vanstone) decomposition can be applied in addition to accelerate MSM even more. As a consequence, MSM algorithms exploiting GLV are based rather on the auxiliary points

$$P_{(v,u)} := P_v + \tau(P_u) = \sum_{i=1}^N v_i P_i + u_i \tau(P_i)$$

with coefficients $u_i \in \mathbb{Z}$ that equally constitute the short vector $u := (u_i)_{i=1}^N$. By abuse of notation, instead of $P_{(v,u)}$ let's write just P_v with $v \in \mathbb{Z}^{2N}$ such that $v_{N+i} = u_i$.

Of course, having a huge amount of available memory or a wide communication channel, the desired points P_v can be found once and for all to regularly restore them from the given memory or channel. However, this solution is vulnerable to the constant danger that a malicious entity will perform a fault attack, somehow replacing one or several points in such a way that this breaks a cryptosystem. On the other hand, it is much easier to protect only basic information storing in a small piece of memory (or establish it over a reliable, but slow channel) from which every point P_v can be safely (re)generated. It is clear that the described strategy, applied directly to the points, is too expensive in any sense of the word.

The recent works [13,14] are devoted to the problem of generating efficiently the "basis" points P_i. In them it is suggested to express $N = (N \text{ div } n)n + (N \bmod n)$ for a little $n \in \mathbb{N}$. Besides, we are given n linearly independent points $P_i(t)$ from the *Mordell–Weil (MW) group* $\mathcal{E}(F)$ of a certain non-trivial twist $\mathcal{E}$ of E over the function field $F := \mathbb{F}_q(t)$. In the literature $\mathcal{E}$ is often called *isotrivial elliptic surface*. Then, n "basis" points can be obtained at once as the specialization of $P_i(t)$ at an element $t \in \mathbb{F}_q$. Transparently changing $t \in \mathbb{F}_q$, nothing prevents from applying the same procedure N div n (plus one if $n \nmid N$) times to obtain N points. In fact, $\mathcal{E}(F)$ has the structure of a Euclidean lattice modulo the torsion subgroup $\mathcal{E}(F)_{tor}$. The corresponding (positive definite) quadratic form $\widehat{h}\colon \mathcal{E}(F) \to \mathbb{Q}_{\geqslant 0}$ is said to be *canonical height*. However, this lattice structure previously played only a minor role in the cryptographic context under consideration.

The present work extends the above generation method to a considerable proportion of the points P_v, not exclusively P_i. It is proposed to pick MW lattices (of rank r) with large *kissing* (a.k.a. *Newton*) *number* k. By definition, it is the number of *the shortest* (i.e., *minimal*) *lattice points*. The norm of the F-point $P_v(t) := \sum_{i=1}^{r} v_i P_i(t)$, where $v = (v_i)_{i=1}^{r} \in \mathbb{Z}^r$, is an indicator of how quickly $P_v(t)$ can be evaluated at elements of $\mathbb{F}_q$. Indeed, the degrees of the point coordinates are proportional to the norm. And the more minimal points we have, the greater performance gain takes place. That is why we are interested in large k with respect to r, that is, in maximizing the quantity $\delta := \log_2(k)/r$. It can be seen that the generation of P_i from [13,14] corresponds to the case when $\mathcal{E}(F)$ is realized as the trivial lattice $\mathbb{Z}^r$, because e_i are its unique minimal vectors up to sign.

The task of constructing arbitrary lattices having large kissing numbers is one of the most classical tasks in mathematics. It has been carefully studied for several centuries. Established lower and upper bounds on k in the first dimensions can be found in any lattice database like [7,17]. In turn, asymptotic results as $r \to \infty$ are well surveyed, e.g., in [31]. In that article Vlăduţ constructs a *k-asymptotically good family* of lattices for which the kissing number grows exponentially, that is, $\limsup_{r\to\infty} \delta > 0$. Unfortunately, this inequality probably does not hold for families of MW lattices, making them always *k-asymptotically bad*.

The last drawback is slightly mitigated for supersingular elliptic surfaces $\mathcal{E}$, because for them, δ decreases more slowly. In a series of articles [10,11,12] Elkies thoroughly studies MW lattices of such surfaces in characteristic 2. For moderate ranks, he (re)discovers lattices with the greatest known kissing numbers. Among the obtained lattices there is in particular the 24-dimensional *Leech lattice* Λ_{24} whose $k = 196560$, the optimal kissing number for $r = 24$. Regarding an odd characteristic p, it is worth mentioning Shioda's remarkable article [19] about certain supersingular surfaces $\mathcal{E}_{p+1}$ of j-invariant 0. Their MW lattices have the non-constant parameters $r = \Theta(p)$ and $k = \Omega(p^2)$. Therefore, for p of a cryptographic size, k is an order of magnitude greater than r. However, we cannot employ the given results in discrete logarithm cryptography, because supersingular elliptic curves E are known to be weaker than ordinary ones, especially for little p.

Fortunately, at least for even ranks $r \leqslant 8$, it is still possible to achieve the optimal kissing numbers through the MW lattices of ordinary elliptic surfaces, although we are forced to restrict ourselves to $j = 0$. By the way, in the extreme case $r = 8$, the largest $k = 240$. It is about the classical *root lattice* E_8, which is wonderful (in many senses) to the same extent as Λ_{24}. For other constant ordinary j-invariants, the author does not find in the literature examples of elliptic surfaces whose MW lattices enjoy quite large kissing numbers, not to mention the optimal ones. The situation when k is not substantially greater than r does not merit separate attention. As a consequence, we do not lose much, dealing hereafter only with curves E_b.

2 Preliminaries

We will freely use the basic notions and facts on Mordell–Weil lattices recalled in [13,14], because it is assumed that the reader is aware of those articles, especially of the first. In turn, abstract lattices have already become paramount objects of (post-quantum) cryptography, so they do not need any special introduction. Nonetheless, there may be some aspects of lattice theory that are not in widespread use by the cryptography society. If necessary, such knowledge gaps can be filled with the help of the manual book [8].

The notation $k(r)$ will stand for the maximal kissing number among all (not necessarily MW) lattices of rank r. For convenience, Table 1 exhibits lower and upper bounds on $k(r)$ for the first four even values r. Odd ranks are out of our interest, because MW ranks of isotrivial elliptic surfaces over finite fields are always even.

r	$\leqslant k(r)$	$k(r) \leqslant$
2	6	
4	24	
6	72	78
8	240	

Table 1. Bounds on the optimal kissing numbers in small even dimensions

For the sake of simplicity, elliptic $\mathbb{F}_q$-curves $y^2 = x^3 + b$ (of j-invariant 0) will be referred to just as E, i.e., without the index b. For the role of τ in the GLV decomposition on such curves, one usually chooses the order 3 automorphism

$[\omega](x, y) = (\omega x, y)$, where $\omega^2 + \omega + 1 = 0$. Recall that $\omega \in \mathbb{F}_p$ whenever 0 is an ordinary j-invariant as in the article context.

As well as in [13, Sections 4, 5], we will work exclusively with the (rational) elliptic surfaces

$$\mathcal{E}_m \colon y^2 = x^3 + t^m + c,$$

where $2 \leqslant m \leqslant 6$ and $c \in \mathbb{F}_q^*$ is a certain constant depending on m. We will suppose everywhere without reminders that $m \mid q - 1$. This condition guarantees that $\mathbb{F}_q$ is the splitting field of $\mathcal{E}_m$, i.e., $\mathcal{E}_m(F) = \mathcal{E}_m(\overline{\mathbb{F}_q}(t))$, where $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$. In principle, it is possible to consider alternative $j = 0$ elliptic surfaces. Attractive candidates are briefly discussed in Section 5.2. They will be perhaps considered during further research, but the surfaces $\mathcal{E}_m$ are quite enough to demonstrate the power of the article idea.

It is convenient that $\mathcal{E}_m(F)$ does not contain non-zero torsion points, that is, $\mathcal{E}_m(F) \simeq \mathbb{Z}^r$ as a group. We will refer to $\mathcal{E}_m(F)$ by means of L_m if it is necessary to stress the lattice structure. The fact is that L_m is never the trivial lattice $\mathbb{Z}^r$. As is conventional in lattice theory, the minimal norm of L_m is denoted by $\lambda_1 \in \mathbb{Q}_{>0}$. As it turns out, each minimal point $P \in L_m$ (i.e., such that $\widehat{h}(P) = \lambda_1$) is integral, i.e., $P = (x(t), y(t))$ is a pair of polynomial coordinates, not just rational ones. Some useful information on the lattices L_m is collected in Table 2 (cf. [13, Table 1]). Be careful, the symbol $\simeq$ here stands for the congruence (a.k.a. isometry) relation rather than the equivalence one as in [8].

m	L_m	k	$k/6$	λ_1	$\deg(x)$	$\deg(y)$
2	$\mathrm{A}_2^* \simeq$	6	1	$2/3$	0	1
3	$\mathrm{D}_4^* \simeq$	24	4	1	1	
4	$\mathrm{E}_6^* \simeq$	54	9	$4/3$		2
	$\mathrm{E}_6 \hookrightarrow$	72	12	2	2	3
5	$\mathrm{E}_8 \simeq$	240	40			
6						

Table 2. Some parameters of the Mordell–Weil lattices $L_m = \mathcal{E}_m(F)$

Note that $\mathrm{A}_2^* \simeq L_2$ and $\mathrm{D}_4^* \simeq L_3$ (along with their root sublattices A_2, D_4) possess the maximal kissing numbers in their dimensions. The situation is different for the case $m = 4$, because the value k of the lattice $\mathrm{E}_6^* \simeq L_4$ (in contrast to E_6) is not maximal for $r = 6$. That is why the sublattice E_6 is represented in a separate row of the table. Of course, we can likewise realise A_2, D_4 as sublattices of L_2, L_3, respectively. However, the minimal norm of the former is slightly greater (namely $\lambda_1 = 2$), which negatively influences the coordinate degrees of minimal points. Unlike E_6, the lattices A_2, D_4 thus do not provide any advantage in our context. Finally, $\mathrm{E}_8 \simeq L_5 \simeq L_6$ is simply a self-dual (a.k.a. unimodular) lattice.

As is well known, the automorphism group of both E, $\mathcal{E}_m$ is generated by the order 6 automorphism $[-\omega] = -[\omega]$ of the form $[-\omega](x,y) = (\omega x, -y)$. Given a point P on E or $\mathcal{E}_m$, we lack the notation $\overline{P} := \big\{[-\omega]^i P\big\}_{i=0}^5$ for the orbit of P with respect to $[-\omega]$. As should be clear, the norm of $P \in \mathcal{E}_m(F)$ is invariant under $[-\omega]$. Therefore, the automorphisms also act on the set of minimal points. This action is free, since the non-zero fixed points of $[-\omega]^i$ (for which $xy = 0$) are obviously outside $\mathcal{E}_m(F)$ regardless of $i \in \mathbb{Z}/6$ and m. Thereby, $\#\overline{P} = 6$ unless P is the infinity point $(0:1:0)$. In particular, always $6 \mid k$.

Like in [13, Section 5], everywhere below a basis of $\mathcal{E}_m(F)$ will be taken in the form $P_1, \cdots, P_{r/2}$, $[\omega]P_1, \cdots, [\omega]P_{r/2}$ and, moreover, all its points will be minimal. After identifying $\mathcal{E}_m(F) \simeq \mathbb{Z}^r$ with respect to such a basis, we obtain the following action of $[-\omega]$ induced on $\mathbb{Z}^r$:

$$[-\omega](v_1, \cdots, v_r) = (v_{r/2+1}, \cdots, v_r,\ v_{r/2+1} - v_1, \cdots, v_r - v_{r/2}).$$

Here, the equality $\omega^2 = -\omega - 1$ is utilised. Similarly, denote by $\overline{v}$ the orbit of $v \in \mathbb{Z}^r$ under the given action. Evidently, for the point

$$P_v := \sum_{i=1}^{r/2} v_i P_i + v_{r/2+i}[\omega]P_i,$$

its orbit $\overline{P_v} = \{P_u\}_{u \in \overline{v}}$.

The coordinates x, y of the six orbit representatives P_u coincide up to multiplication by ω, -1, respectively. Consequently, for computing all the points $P_u \in \overline{P_v}$, it is essentially sufficient to determine only one of them. To simplify this process as much as possible, it is necessary to define the "lightest" point P_u in a sense. One of the reasonable ways (adopted in the next section) is to take a vector $u \in \overline{v}$ with the smallest 1-norm $|u|_1 = \sum_{i=1}^r |u_i|$. We will equally call this number the 1-norm of P_u, which has nothing to do with the other norm $\widehat{h}(P_u)$. As an example, the basis points P_i, $[\omega]P_i$ are actually the "lightest", because they (along with their inverse ones) are of 1-norm 1.

3 Minimal points of the lattices L_m

This section is heavily based on [13, Section 5]. From there we will borrow the concrete bases P_i, $[\omega]P_i$ depending on m. Be careful, the below points $P_{r/2+i} \neq [\omega]P_i$ in contrast to the previous article. We will tacitly resort to the computer algebra system Magma. The corresponding code is loaded on the web page [15]. We will consider step by step the remaining minimal points $P_i \in L_m$, where $r/2 < i \leqslant k/6$. For compactness, their explicit formulas are omitted in the text (except for the degenerate case $m = 2$), but they are momentarily obtained by launching the Magma code.

3.1 The case $m = 2$

Without loss of generality, one can choose the coefficient $c = 1$. Then, the point $P_1 := (-1, t)$ generates $\mathcal{E}_2(F)$ over the ring $\mathbb{Z}[\omega]$. Furthermore, the set of all minimal points is nothing but the orbit of P_1, since $k = 6$ for the lattice L_2.

3.2 The case $m = 3$

In addition to the basis points P_1, P_2 from [13, Section 5.2], orbit representatives among the remaining minimal points in the lattice L_3 are the points

$$P_3 := [\omega]P_2(\omega t) = [\omega]P_1 + P_2, \qquad P_4 := P_2(\omega^2 t) = [\omega]P_2 - P_1$$

of the smallest 1-norm 2.

3.3 The case $m = 4$

The subcase $\mathbf{E}_6^* \simeq \boldsymbol{L_4}$. In addition to the basis points P_1, P_2, P_3 from [13, Section 5.3], orbit representatives (of the smallest 1-norm) among the remaining minimal points in the lattice L_4 are:

Points of 1*-norm* 2:

$$P_4 := P_1 + P_2, \qquad P_5 := P_1 + P_3, \qquad P_6 := [\omega]P_2 + P_3;$$

Points of 1*-norm* 3:

$$P_7 := P_1 + P_2 - [\omega]P_3, \qquad P_8 := [\omega]P_1 - P_2 + [\omega]P_3;$$

Points of 1*-norm* 4:

$$P_9 := [1 + \omega]P_1 + [\omega]P_2 + P_3.$$

Moreover, the points of 1-norm $n \geqslant 3$ are expressed via the points of 1-norm $< n$ as follows:

$$P_7 = P_4 - [\omega]P_3, \qquad P_8 = [\omega]P_5 - P_2, \qquad P_9 = [\omega]P_4 + P_5.$$

The subcase $\mathbf{E}_6 \hookrightarrow \boldsymbol{L_4}$. The lattice L_4 contains the sublattice L_4' generated over $\mathbb{Z}[\omega]$ by the points

$$P_1' := P_1 - [\omega]P_2, \qquad P_2' := P_1 - [\omega]P_3, \qquad P_3' := P_2 - [\omega]P_3.$$

The Gram matrix of $\widehat{h}$ with respect to the order P_1', P_2', P_3', $[\omega]P_1'$, $[\omega]P_2'$, $[\omega]P_3'$ has the form

$$\begin{pmatrix} 2 & 1 & 0 & -1 & 0 & -1 \\ 1 & 2 & 0 & -1 & -1 & -1 \\ 0 & 0 & 2 & 1 & 1 & -1 \\ -1 & -1 & 1 & 2 & 1 & 0 \\ 0 & -1 & 1 & 1 & 2 & 0 \\ -1 & -1 & -1 & 0 & 0 & 2 \end{pmatrix}.$$

Its determinant and minimal norm are equal to $\varDelta = 3$ and $\lambda_1 = 2$, respectively. Recall that $\delta = \lambda_1^{r/2}/(2^r\sqrt{\varDelta})$ is the *center density* (see, e.g., [8, Section 1.1]) of an arbitrary r-dimensional lattice. Therefore, the center density of our lattice L_4' is equal to $\delta = 1/(8\sqrt{3})$ as well as for E_6. At the same time, as stated in [8, Section 4.8.3], there is the unique (up to an isometry) lattice of rank 6 with the given value δ. Consequently, $L_4' \simeq \mathrm{E}_6$ as we wanted.

In addition to the basis points P_1', P_2', P_3', orbit representatives (of the smallest 1-norm) among the remaining minimal points in the lattice L_4' are:

Points of 1*-norm* 2:

$$P_4' := P_1' - P_2', \qquad P_5' := [\omega]P_1' - P_3', \qquad P_6' := [\omega]P_2' - P_3',$$
$$P_7' := [\omega]P_1' + P_2', \qquad P_8' := P_1' + [\omega]P_3', \qquad P_9' := P_2' + [\omega]P_3';$$

Points of 1*-norm* 3:

$$P_{10}' := [\omega]P_1' + P_2' - P_3', \qquad P_{11}' := [\omega]P_1' + P_2' + [\omega]P_3';$$

Points of 1*-norm* 4:

$$P_{12}' := [1+\omega]P_1' + P_2' + [\omega]P_3'.$$

Moreover, the points of 1-norm $n \geqslant 3$ are expressed via the points of 1-norm $< n$ as follows:

$$P_{10}' = P_7' - P_3', \qquad P_{11}' = [\omega]P_3' + P_7', \qquad P_{12}' = P_1' + P_{11}'.$$

3.4 The case $m = 5$

In addition to the basis points P_1, P_2, P_3, P_4 from [13, Section 5.4], orbit representatives (of the smallest 1-norm) among the remaining minimal points in the lattice L_5 are:

Points of 1*-norm* 2:

$$P_5 := P_1 + P_2, \qquad P_6 := P_2 + P_3, \qquad P_7 := P_3 + P_4,$$
$$P_8 := P_1 - [\omega]P_2, \qquad P_9 := P_2 - [\omega]P_3, \qquad P_{10} := P_3 - [\omega]P_4;$$

Points of 1*-norm* 3:

$$P_{11} := P_1 + P_2 + P_3, \qquad P_{12} := P_2 + P_3 + P_4, \qquad P_{13} := P_1 + P_2 - [\omega]P_3,$$
$$P_{14} := P_2 + P_3 - [\omega]P_4, \qquad P_{15} := P_1 - [\omega]P_2 - [\omega]P_3, \qquad P_{16} := P_2 - [\omega]P_3 - [\omega]P_4;$$

Points of 1*-norm* 4:

$$\begin{aligned} P_{17} &:= P_1 + P_2 + P_3 + P_4, & P_{18} &:= P_1 + P_2 + P_3 - [\omega]P_4, \\ P_{19} &:= P_1 + P_2 - [\omega]P_3 - [\omega]P_4, & P_{20} &:= P_1 - [\omega]P_2 - [\omega]P_3 - [\omega]P_4, \\ P_{21} &:= P_1 + [1-\omega]P_2 - [\omega]P_3, & P_{22} &:= [\omega]P_1 + [1+\omega]P_2 + P_3, \\ P_{23} &:= P_2 + [1-\omega]P_3 - [\omega]P_4, & P_{24} &:= [\omega]P_2 + [1+\omega]P_3 + P_4; \end{aligned}$$

Points of 1*-norm* 5:

$$\begin{aligned} P_{25} &:= P_1 + P_2 + [1-\omega]P_3 - [\omega]P_4, & P_{26} &:= P_1 - [\omega]P_2 - [1+\omega]P_3 - P_4, \\ P_{27} &:= P_1 + [1-\omega]P_2 - [\omega]P_3 - [\omega]P_4, & P_{28} &:= [1+\omega]P_1 + P_2 + P_3 - [\omega]P_4, \\ P_{29} &:= [\omega]P_1 + [1+\omega]P_2 + P_3 + P_4, & P_{30} &:= [\omega]P_1 + [\omega]P_2 + [1+\omega]P_3 + P_4; \end{aligned}$$

Points of 1*-norm* 6:

$$\begin{aligned} P_{31} &:= P_1 + [2]P_2 + [1-\omega]P_3 - [\omega]P_4, \\ P_{32} &:= P_1 + [1-\omega]P_2 - [2\omega]P_3 - [\omega]P_4, \\ P_{33} &:= P_1 + [1-\omega]P_2 + [1-\omega]P_3 - [\omega]P_4, \\ P_{34} &:= P_1 + [1-\omega]P_2 - [\omega]P_3 - [1+\omega]P_4, \\ P_{35} &:= [1+\omega]P_1 + P_2 + [1-\omega]P_3 - [\omega]P_4; \end{aligned}$$

Points of 1*-norm* 7:

$$\begin{aligned} P_{36} &:= P_1 + [1-\omega]P_2 - [2\omega]P_3 - [1+\omega]P_4, \\ P_{37} &:= [1+\omega]P_1 + [2]P_2 + [1-\omega]P_3 - [\omega]P_4; \end{aligned}$$

Points of 1*-norm* 8:

$$\begin{aligned} P_{38} &:= P_1 + [1-\omega]P_2 - [2\omega]P_3 - [1+2\omega]P_4, \\ P_{39} &:= [\omega]P_1 + [1+2\omega]P_2 + [2+\omega]P_3 + P_4, \\ P_{40} &:= [2+\omega]P_1 + [2]P_2 + [1-\omega]P_3 - [\omega]P_4. \end{aligned}$$

Moreover, the points of 1-norm $n \geqslant 3$ are expressed via the points of 1-norm $< n$ as follows:

Points of 1*-norm* 3:

$$\begin{aligned} P_{11} &= P_3 + P_5, & P_{12} &= P_4 + P_6, & P_{13} &= P_1 + P_9, \\ P_{14} &= P_2 + P_{10}, & P_{15} &= P_8 - [\omega]P_3, & P_{16} &= P_9 - [\omega]P_4; \end{aligned}$$

Points of 1*-norm* 4:

$$P_{17} = P_5 + P_7, \qquad P_{18} = P_5 + P_{10}, \qquad P_{19} = P_1 + P_{16},$$
$$P_{20} = P_{15} - [\omega]P_4, \qquad P_{21} = P_2 + P_{15}, \qquad P_{22} = [\omega]P_5 + P_6,$$
$$P_{23} = P_3 + P_{16}, \qquad P_{24} = [\omega]P_6 + P_7;$$

Points of 1*-norm* 5:

$$P_{25} = P_3 + P_{19}, \qquad P_{26} = P_{15} - P_7, \qquad P_{27} = P_2 + P_{20},$$
$$P_{28} = [\omega]P_1 + P_{18}, \qquad P_{29} = P_4 + P_{22}, \qquad P_{30} = P_7 + [\omega]P_{11};$$

Points of 1*-norm* 6:

$$P_{31} = P_{11} + P_{16}, \qquad P_{32} = P_{15} + P_{16}, \qquad P_{33} = P_{11} - [\omega]P_{12},$$
$$P_{34} = P_{27} - P_4, \qquad P_{35} = P_{28} - [\omega]P_3;$$

Points of 1*-norm* 7:

$$P_{36} = P_{34} - [\omega]P_3, \qquad P_{37} = P_2 + P_{35};$$

Points of 1*-norm* 8:

$$P_{38} = P_{36} - [\omega]P_4, \qquad P_{39} = [\omega]P_9 + P_{29}, \qquad P_{40} = P_1 + P_{37}.$$

3.5 The case $m = 6$

This case is similar to the previous one because of the isometry $L_5 \simeq L_6$. Indeed, the above linear relations remain the same if a basis $P_i, [\omega]P_i$ of L_6, where $i \leqslant 4$, has the Gram matrix exactly as in [13, Section 5.4]. Clearly, this can be ensured with the help of an appropriate coordinate change. The main difference consists in other formulas of the minimal points P_i, where $i \leqslant 40$. In [13] formulas of the basis points P_i are not derived when $m = 6$, because in the context of that article (unlike the current one) the L_6-based generation method is not faster than the L_3-based one.

By our assumption, $m \mid q - 1$. The condition $5 \mid q - 1$ sometimes may not hold. In turn, $6 \mid q - 1$ or, equivalently, $3 \mid q - 1$ automatically for all ordinary curves of j-invariant 0. Therefore, it is actually useful to possess formulas for the points $P_i \in L_6$. Nevertheless, derivating such formulas is a much less ambitious task than the research project from Section 5.2 whose outcomes promise to substantially outperform the case under consideration. That is why the author decided not to dwell on it (at least now). Besides, as explained in the next section, the L_5-based generation method (when applicable) is still a little bit more efficient on average than the L_6-based one. Thus, the case $m = 5$ does not completely lose relevance at the moment.

Perhaps, explicit formulas of $P_i \in L_6$ are not represented anywhere in the literature for the abstract coefficient c from the equation of $\mathcal{E}_6$. The author succeeded to find only the paper [21] handling the special case $c = -1$, although its reasoning is in parallel with [20] dealing with the general c when $m \in \{4, 5\}$. Recall that the latter paper underlies [13, Sections 5.3, 5.4]. Therefore, the former paper appears to be generalized to the other values $c \in \mathbb{F}_q^*$. In particular, for an appropriately chosen c, the splitting field of $\mathcal{E}_6$ probably can be reduced from $\mathbb{F}_q(\sqrt[12]{1}, \sqrt[3]{2})$ (when $c = -1$) to the expected field $\mathbb{F}_q(\sqrt[6]{1})$, that is, to $\mathbb{F}_q$ in our setting.

4 Generating the minimal points

Assume that $t \in \mathbb{F}_q$ is a known element such that the reduction (a.k.a. specialization) $\mathcal{E}_{m,t}$ of the surface $\mathcal{E}_m$ at t is $\mathbb{F}_q$-isomorphic to the original curve E. As explained in [13, Section 3], we are able to obtain such an element as some m-th root $t = \sqrt[m]{\cdot}$ when it is extracted over $\mathbb{F}_q$, that is, approximately with the probability $1/m$. The associated isomorphism has the form

$$\varphi_t \colon \mathcal{E}_{m,t} \to E \qquad (x, y) \mapsto (c_x x, c_y y),$$

where the coefficients c_x, $c_y \in \mathbb{F}_q$ depend on t.

To this moment, we are given (formulas of) the minimal points $P_i \in L_m$ from Section 3. All of the following is equally true in the case of the points $P_i' \in L_4'$. Therefore, this case will not be mentioned further to avoid sitting on two chairs. Throughout the section, we will assume that the "basis" points $\varphi_t(P_i(t)) \in E(\mathbb{F}_q)$, where $i \leqslant r/2$, have already been generated by [13, Algorithm 1] with respect to $t \in \mathbb{F}_q$. Our purpose is to generate as fast as possible the remaining "minimal" points $\varphi_t(P_i(t))$, where $i \leqslant k/6$. By abuse of notation, we will refer to these points simply by P_i as well as for the initial lattice points. Let's suppose for simplicity that multiplications by ω, -1 (apart from additions in $\mathbb{F}_q$) are not taken into account in the below estimations of running time. Thereby, once a "minimal" point P_i is determined, so is its full orbit $\overline{P_i}$ of 6 conjugates.

A naive method of finding $P_i \in E(\mathbb{F}_q)$ consists in performing successive curve additions of the form $P_i = P_{i_1} + P_{i_2}$ (up to the automorphisms of E) such that i_1, i_2, $r/2 < i$. As shown in Section 3, such a minimal addition chain takes place regardless of m. Thus, the total number of additions on E is equal to $A := k/6 - r/2$. According to [5], [9, Section 6.4.1], the general addition operation on an arbitrary curve $E : y^2 = x^3 + bz^6$ (in Jacobian coordinates) costs no less than 16 multiplications in $\mathbb{F}_q$. Sometimes, E can be transformed into other forms enjoying faster addition formulas. The most efficient among them is widely recognized to be the twisted Edwards form (in extended coordinates) on which + requires 10 multiplications. To sum up, the overall running time of the naive generation method lies between $10A$ and $16A$ field multiplications.

From the geometric point of view, the minimal points are no different from the basis ones. As a result, we have another Algorithm 1 of generating all the "minimal" $\mathbb{F}_q$-points on E, which supplements [13, Algorithm 1] in a natural way. Formally speaking, the corresponding vectors $v \in \mathbb{Z}^r$ (i.e., such that $P_i = P_v$) have to be returned in the new algorithm in parallel with the points. Otherwise, the latter are useless for subsequent MSM algorithms. Note that reducing $P_i(t)$ amounts to two Horner's schemes applied to the coordinate polynomials $x = x(P_i)$ and $y = y(P_i)$. In turn, each application of φ_t costs 2 multiplications in $\mathbb{F}_q$ (by c_x, c_y). As a consequence, to obtain one "minimal" point it is enough to perform $M := \deg(x) + \deg(y) + 2$ field multiplications. Therefore, MA is the total number of multiplications in the new generation method.

```
Algorithm 1: New method of generating all the "minimal" points
  Data: finite field $\mathbb{F}_q$ of characteristic 7 or greater,
  ordinary elliptic $\mathbb{F}_q$-curve $E$ of $j$-invariant 0,
  natural $m$ such that $2 \leqslant m \leqslant 6$ and $m \mid q - 1$,
  element $t \in \mathbb{F}_q$ such that $\mathcal{E}_{m,t} \simeq_{\mathbb{F}_q} E$ and the $\mathbb{F}_q$-isomorphism $\varphi_t\colon \mathcal{E}_{m,t} \to E$,
  coordinate formulas for representatives $P_1, \cdots, P_{k/6} \in \mathcal{E}_m(F)$ of the orbits of
  minimal points;
  Result: $k$ "minimal" points in $E(\mathbb{F}_q)$;
  begin
      for $i := 1$ to $k/6$ do
          $P_i := \varphi_t(P_i(t))$;
      end
      return $\overline{P_1}, \cdots, \overline{P_{k/6}}$.
  end
```

We see that the new approach is faster than the naive one whenever the cost of one addition on E is greater than M. Interestingly, this is always the case, because $M \leqslant 7$, that is, $10 - M \geqslant 3$ and $16 - M \geqslant 9$. Table 3 demonstrates the exact numbers of multiplications (checked in Magma [15]) for all the cases $2 \leqslant m \leqslant 6$. As expected, the performance gain (namely, the last two columns) increases when m does. In particular, we do not get any benefit for $m = 2$ and the best result occurs for $m \in \{5, 6\}$. Curiously, there is one exception: the value $(10 - M)A$ is equal to 30 for the lattice L_4, but 27 for its sublattice L_4'. Nevertheless, the situation is opposite ($66 < 81$) if the curve E is in the short Weierstrass form.

It is impossible not to mention that the entries of Table 3 should be slightly recalculated under a deeper complexity analysis. Indeed, there are several minor optimization possibilities not taken into account before, but explained in the next paragraphs. For simplicity, such a detailed analysis is omitted in the present paper, because it is more mathematical in nature than engineering. Undoubtedly, the table tendencies will remain after recalculation. In other words, supremacy of the new generation method over the naive one is beyond question.

Lattice	A	M	$10-M$	$16-M$	$10A$	$16A$	MA	$(10-M)A$	$(16-M)A$
L_2	0	3	7	13	0				
L_3	2	4	6	12	20	32	8	12	24
L_4	6	5	5	11	60	96	30	30	66
L'_4	9	7	3	9	90	144	63	27	81
L_5	36				360	576	252	108	324
L_6									

Table 3. Comparison (in terms of the numbers of multiplications in $\mathbb{F}_q$) of the naive and new methods of generating all the "minimal" $\mathbb{F}_q$-points on E

Ideally, the optimization tricks under consideration have to be used in the process of programming Algorithm 1 (or some of its versions) in one of low-level languages. Nonetheless, in view of Section 5.2, it is more logical at the beginning to conduct further research on the topic prior to proceeding with an optimized implementation.

First, the constant $\omega \in \mathbb{F}_p$ may be quite large (in absolute value) in contrast to -1. Hence, multiplication by ω may not be completely free. Second, formulas of the minimal points $P_i \in L_m$ may sometimes have small or repeating coefficients, at least for different indices i. As a result, with the same input argument $t \in \mathbb{F}_q$, evaluating $P_i(t)$ together (i.e., for all $i \leqslant k/6$) may cost considerably less separately. On the contrary, repeating field multiplications are seemingly rare in the addition chains $P_i = P_{i_1} + P_{i_2}$ and the majority of these multiplications are general (i.e., not by a constant). The fact is that addition chains are inherently computed successively (not in parallel as $P_i(t)$), hence there is limited room for their optimization.

The operation $+$ on E does not keep affine coordinates unless the inverse operation in $\mathbb{F}_q^*$ is used. Since the latter is recognized to be much more expensive than multiplication, $+$ must return (weighted) projective coordinates. In particular, most instances of $+$ in our addition chains are forced to receive such burdensome input coordinates. As an exception, the points P_i of 1-norm 2 (unlike those of larger 1-norms) are the sums of two basis points, which are usually given on the affine plane. Therefore, the 1-norm 2 points require fewer multiplications than 10 and 16, respectively. However, the proportion of these points decreases with growth of m. For the cases $m \in \{5, 6\}$ the most interesting for us, there are solely 6 such points among 36 non-basis minimal points. By the way, all the minimal points $P_i \in L_m$ are integral, hence reducing them always avoids inverting in $\mathbb{F}_q^*$. This circumstance no doubt leads to a slight acceleration of MSM algorithms based on P_i.

It has not yet been clearly justified for which value m the L_m-based generation method (let's denote it by M_m) is the best. So far, we have just made sure that this method is better than the naive one with the same m. Evidently, the smaller the given parameter, the more performant Algorithm 1, but at the price of fewer returning points. It is important to remember that this algorithm is always preceded by much slower [13, Algorithm 1]. Recall that its complexity on average amounts to $m\big(\frac{\cdot}{q}\big)_m + \sqrt[m]{\cdot}$ (apart from several more multiplications), where $\big(\frac{\cdot}{q}\big)_m$ is the m-th power residue symbol and $\sqrt[m]{\cdot}$ is the m-th root in the field $\mathbb{F}_q$.

Specialists know well that the symbol $\big(\frac{\cdot}{q}\big)_m$ can be determined (at least for $m \leqslant 6$) by means of Euclidean-type algorithms. With proper implementation, their execution times are close to that of several dozen multiplications. Thus, extracting $\sqrt[m]{\cdot}$ is an order of magnitude more laborious operation (even for $m = 2$) than the others in $\mathbb{F}_q$ that we encountered. Concrete complexity estimates heavily depend on m and q. At best, $\sqrt[m]{\cdot}$ is expressed via one exponentiation in $\mathbb{F}_q$, which costs no less than $\ell := \lceil \log_2(q) \rceil$ field multiplications. As an example, for the conventional 128-bit security level, $\ell \gtrsim 256$ and this lower bound on ℓ is known to be even higher for pairing-friendly curves E.

Let's compare, e.g., the methods M_5, M_6 with the degenerate one M_2. The following reasoning is mutatis mutandis transformed for the cases $m \in \{3, 4\}$. The methods M_5, M_6 both give $k/6 = 40$ points in $E(\mathbb{F}_q)$ at the cost of one radical, of ≈ 5, 6 residue symbols, respectively, and of ≈ 250 multiplications according to Table 3. In turn, M_2 generates only one "basis" point (apart from its conjugates by $[-\omega]$) after computing ≈ 2 Legendre symbols and one square root (and a few auxiliary multiplications). Therefore, the latter needs to be launched 40 times (with different elements $t \in \mathbb{F}_q$) to obtain the identical number of points. At least when $\sqrt{\cdot}$, $\sqrt[5]{\cdot}$, $\sqrt[6]{\cdot}$ are all represented by exponentiations in $\mathbb{F}_q$, the 40-time method M_2 is without doubt substantially slower than the one-time M_5, M_6.

Besides, M_2 does not return "dependent" points unlike M_5, M_6. This means that the total number of $\mathbb{F}_q$-points on E generated by the multiple method M_2 is still smaller. As in the introduction, let N stand for the number of all "basis" points, which must be generated in any case. We see that M_2 generates exactly N ("basis") points with the same number of launches against $40N/4 = 10N$ points returned by M_5, M_6 after $N/4$ launches, where $4 \mid N$ for simplicity. Of course, a concrete MSM algorithm may not need certain "dependent" points (e.g., those of higher 1-norms), hence for it, the efficiency of M_5, M_6 may be too exaggerated. Nevertheless, in general (i.e., abstracting from MSM algorithms), the methods M_5, M_6 are justified to be the best among all the state-of-the-art generation methods. This is also consistent with the conclusions of [13, Section 4], where "basis" points are the only resulting ones.

Finally, it remains to choose the winner between M_5 and M_6. As already said in Section 3.5, the first method (unlike the second) suffers from an applicability restriction (of the form $5 \mid q - 1$). However, if both methods are available, then M_5 is a little more preferable than M_6, because on average the first has one residue symbol less than the second. Certainly, we are under the pretty natural heuristic assumption that $\big(\frac{\cdot}{q}\big)_5$ (resp., $\sqrt[5]{\cdot}$) is implemented not slower than $\big(\frac{\cdot}{q}\big)_6$ (resp., $\sqrt[6]{\cdot}$).

5 Final remarks

5.1 Hybrid point generation

Special attention should be paid to the generation technique combined from the minimal points $P_i \in L_4$ and $P_i' \in L_4'$ simultaneously, that is, with one element $t \in \mathbb{F}_q$ such that $\mathcal{E}_{4,t} \simeq_{\mathbb{F}_q} E$. This technique allows to obtain at once more $\mathbb{F}_q$-points on E. A minor comment is that P_1', P_2', P_3' are no longer considered as basis points, but as points of 1-norm 2 with respect to P_1, P_2, P_3 and their counterparts $[\omega]P_i$. Therefore, none of the induced points $P_i' \in E(\mathbb{F}_q)$ are given in advance and hence they all need to be computed. It is also worth bearing in mind that the 1-norm becomes greater for all the points P_i'.

To continue we lack the notion of so-called *everywhere integral points* (in the sense of Shioda [22,25,26]) in the MW lattice of an elliptic $\mathbb{F}_q$-surface $\mathcal{E}$. By one of definitions, these are integral points $P = (x, y) \in \mathcal{E}(F)$ for which $\widehat{h}(P) \leqslant 2\chi$ or, equivalently, $\deg(x) \leqslant 2\chi$ and $\deg(y) \leqslant 3\chi$, where $\chi \in \mathbb{N}$ is the *arithmetic genus* of $\mathcal{E}$. No worries, χ is nothing but 1 whenever $\mathcal{E}$ is a rational surface, which is the case for $\mathcal{E}_m$ with $m \leqslant 6$. Be careful, in some sources (but not here) such points are called just integral, while arbitrary points with polynomial coordinates x, y are called ∞-*integral* or $\mathbb{F}_q[t]$-*integral*. For convenience, let e be the (finite) number of all everywhere integral points in $\mathcal{E}(F)$.

Note that L_4' is an instance of what is known as the *narrow Mordell–Weil lattice* $L_m' := \mathcal{E}_m(F)^\circ$ whose definition is given, e.g., in [19, Section 2]. By virtue of [19, Remark 3.5], the lattices L_m' are root ones we have previously encountered (not only for $m = 4$). It turns out (cf. [26, Section 3.1]) that the minimal points of L_m and those of L_m' (a.k.a. *roots*) together constitute the set of all everywhere integral points in $\mathcal{E}_m(F)$. For $m \in \{2, 3\}$, the number $e = 2k \in \{12, 48\}$, since the kissing numbers of A_2, A_2^* coincide and this is equally true for D_4, D_4^*. Finally, $\mathrm{E}_8 = \mathrm{E}_8^*$, which implies the equality $e = k$ $(= 240)$ in the last cases $m \in \{5, 6\}$. For clarity, these facts are translated into Table 4 supplementing Table 2. Among other things, the column "ind" contains the indices $[L_m : L_m']$.

m	L_m'	*ind*	e	$e/6$
2	A_2	3	12	2
3	D_4	4	48	8
4	E_6	3	126	21
5	E_8	1	240	40
6				

Table 4. Some parameters of the narrow sublattices $L_m' \subset L_m$

The aforementioned hybrid generation is naturally generalized to the other cases $m \neq 4$ by exploiting likewise all everywhere integral points in $\mathcal{E}_m(F)$.

However, the maximal number $e = 240$ occurs for $m \in \{5, 6\}$, hence the original methods M_5, M_6 remain the best. Moreover, there is the fact [25, Theorem 2.1] that none of rational elliptic surfaces $\mathcal{E}$ enjoys $e > 240$. Certainly, nothing prevents us from using other points from $\mathcal{E}(F)$. Nevertheless, it is desirable to keep the integrality property to be able to return affine points in $E(\mathbb{F}_q)$ without inverting in $\mathbb{F}_q^*$. Extra integral points in $\mathcal{E}_m(F)$ (of canonical height > 2) are succinctly surveyed in [23, Section 8]. There are only an insignificant number of such "sporadic" points, not to mention that $\deg(x) > 2$ or $\deg(y) > 3$ for them. Therefore, it is not expected that the efficiency of the generation process including these points is so impressive to dwell on it.

5.2 Mordell–Weil lattices of higher kissing numbers

This section briefly outlines a promising research direction on the topic. It is reasonable to wonder about extending the article idea to MW lattices (of isotrivial ordinary elliptic surfaces) with kissing numbers $k > 240$. Intuitively, they should provide a more impressive performance gain during point generation than the lattices previously considered. As before, there is hope to identify desired lattices only for the j-invariant 0. Unfortunately, all rational elliptic surfaces necessarily have the MW ranks $r \leqslant 8$ (see, e.g., [18]), which is somewhat demotivating in view of Table 1. Therefore, we are forced to resort to elliptic surfaces of greater arithmetic genus $\chi > 1$. The next case $\chi = 2$ corresponds to so-called *K3 surfaces*. Already in this case, the theory of MW lattices is significantly complicated.

In a series of works [27,28,29,30] Usui establishes the full classification (i.e., for all $m \in \mathbb{N}$) of the lattices L_m over the algebraic closure $\overline{\mathbb{F}_q}$. As explained in [13, Section 3], for each $m \geqslant 6$, the cost of finding a necessary element $t \in \mathbb{F}_q$ is permanent and amounts just to $6\left(\frac{\cdot}{q}\right)_6 + \sqrt[6]{\cdot}$. Thereby, the kissing number or rather $\delta := k/r$ is actually the main indicator for running time of the L_m-based generation methods. The minimal norm λ_1 (crucial for the speed of point reduction) also plays a role, but appears to be secondary as we will see in the next noteworthy examples ($\lambda_1 = 4$ for all of them).

According to [30, Main Theorem], solely the lattice L_{12} merits attention, because it is easily seen that L_{12} enjoys the largest value $\delta = 115.5$ among all the lattices L_m. More precisely, L_{12} possesses the parameters $r = 16$, $\lambda_1 = 4$, and $k = 1848$. Although the last value is pretty small compared to $4320 \leqslant k(16) \leqslant 7320$, it is much greater than the kissing number $2 \cdot 240 = 480$ of the 16-dimensional direct squares L_5^2, L_6^2. The latter essentially underlie the methods M_5, M_6 applied twice, that is, with two different seeds $t \in \mathbb{F}_q$.

Recall that at the moment the maximal (in characteristic 0) MW rank $r = 68$, which is attained by the lattice L_{360}. For it, $\lambda_1 = 120 \gg 4$ and $k = 2472$ and hence $\delta \approx 36.353 \ll 115.5$. The inequalities $\gg$, $\ll$ confirm that L_{360} (like the other lattices L_m for $m \neq 12$) loses to L_{12} based on a combination of factors. This opinion is opposite to [13, Section 3], because for generating only "independent" points, the MW rank is the unique important indicator.

In addition to the surfaces $\mathcal{E}_m$, separate consideration deserve the K3 surfaces

$$\mathcal{F}_m\colon y^2 = x^3 + c_1 t^m + \frac{c_1'}{t^m} + c_0,$$

where similarly $m \leqslant 6$ and c_1, $c_1' \neq 0$. Over arbitrary fields (including $\mathbb{F}_q$) the MW lattices Λ_m of these surfaces are thoroughly studied in [16]. In particular, over $\overline{\mathbb{F}_q}$ one can put $c_1 = c_1' = 1$ without loss of generality. The coefficient c_0 conversely matters even over $\overline{\mathbb{F}_q}$ (unlike c in the equation of $\mathcal{E}_m$), hence it is more correct to indicate c_0 as follows: $\mathcal{F}_m(c_0)$, $\Lambda_m(c_0)$.

Obviously, if $c_1 = 1$, $c_1' = c$, then $\mathcal{E}_{12} \simeq_{\mathbb{F}_q} \mathcal{F}_6(0)$ and hence $L_{12} \simeq \Lambda_6(0)$. In turn, $\Lambda_5(0)$ has the even better parameters $r = 16$, $\lambda_1 = 4$, and $k = 2640$ (i.e., $\delta = 165$) by virtue of [30, Section 3]. The cases $m \leqslant 4$ are less remarkable, since the value δ of the lattice $\Lambda_m(0)$ diminishes by analogy with L_m. Thus, the family $\mathcal{F}_m(0)$ remotely resembles $\mathcal{E}_m$. Finally, little is known about $\Lambda_m(0)$ for $m > 6$.

It must be understood that, generally speaking, minimal and everywhere integral points are not at all the same thing. In this connection, there is an independent task of maximizing the number e instead of k. As stated in [26, Section 4], the record is $e = 5820$, at least in 2010 when that article was published. This record is due to the MW lattice of the surface $\mathcal{E}\colon y^2 = x^3 + t^5 - t^{-5} - 11$ from [24] isomorphic to $\mathcal{F}_5(11\sqrt{-1})$ as usual over $\overline{\mathbb{F}_q}$. For this lattice, $\lambda_1 = 4$, $r = 18$, and so $e/r = 323.(3) \gg 165$. By the way, 18 is the maximal possible MW rank for ordinary elliptic K3 surfaces (see, e.g., [16, Section 8]). In the literature such surfaces are said to be *singular*.

It should be stressed that the splitting field of $\mathcal{E}$ is exactly $\mathbb{F}_q(\sqrt[5]{1}, \sqrt[3]{10})$. Probably, there is not yet an article dedicated to the twists of the surface $\mathcal{E}$, in contrast to $\mathcal{E}_m$, $\mathcal{F}_m(0)$ with $m \leqslant 6$. This subject is important if we want to try to ease the restrictions on $\mathbb{F}_q$ as much as possible. Currently, $\sqrt[5]{1}, \sqrt[3]{10} \subset \mathbb{F}_q$ seem quite severe conditions to be able to use $\mathcal{E}$ for generating $\mathbb{F}_q$-points on $j = 0$ elliptic curves. In other words, we are interested in coefficients $c_0, c_1, c_1' \in \mathbb{F}_q$ such that the surface $\mathcal{F}_5$ (with the given coefficients) is a twist of $\mathcal{E}$ whose MW lattice is full already over $\mathbb{F}_q$ under more mild conditions (e.g., without $\sqrt[3]{10} \subset \mathbb{F}_q$).

Acknowledgements. The author expresses his gratitude to Antonio Sanso and Justin Drake from Ethereum Foundation for motivation (and help in searching for financial support) they provided to complete this article. Besides, the author was contacted by Victor Miller with appreciation for the previous work [14], which also encouraged to continue research in this direction.

References

1. ZPRIZE 2022 competition, `https://github.com/z-prize`
2. ZPRIZE 2023 competition, `https://www.zprize.io`
3. Avanzi, R.M.: The complexity of certain multi-exponentiation techniques in cryptography. Journal of Cryptology **18**, 357–373 (2005)
4. Bernstein, D.J.: Pippenger's exponentiation algorithm (2002), `https://cr.yp.to/papers/pippenger-20020118-retypeset20220327.pdf`

5. Bernstein, D.J., Lange, T.: Explicit-formulas database, `https://www.hyperelliptic.org/EFD/index.html`
6. Botrel, G., El Housni, Y.: Faster Montgomery multiplication and multi-scalar-multiplication for SNARKs. Transactions on Cryptographic Hardware and Embedded Systems (TCHES) **2023**(3), 504–521 (2023)
7. Cohn, H.: Kissing numbers, `https://cohn.mit.edu/kissing-numbers`
8. Conway, J.H., Sloane, N.J.A.: Sphere packings, lattices and groups, Grundlehren der Mathematischen Wissenschaften, vol. 290. Springer, New York, 3 edn. (2013)
9. El Mrabet, N., Joye, M. (eds.): Guide to pairing-based cryptography. Cryptography and Network Security Series, Chapman and Hall/CRC, New York (2017)
10. Elkies, N.D.: Mordell–Weil lattices in characteristic 2, I: Construction and first properties. International Mathematics Research Notices **1994**(8), 343–361 (1994)
11. Elkies, N.D.: Mordell–Weil lattices in characteristic 2, II: The Leech lattice as a Mordell–Weil lattice. Inventiones Mathematicae **128**(1), 1–8 (1997)
12. Elkies, N.D.: Mordell–Weil lattices in characteristic 2, III: A Mordell–Weil lattice of rank 128. Experimental Mathematics **10**(3), 467–473 (2001)
13. Koshelev, D.: Generation of "independent" points on elliptic curves by means of Mordell–Weil lattices (2022), `https://eprint.iacr.org/2022/794`
14. Koshelev, D.: Generation of two "independent" points on an elliptic curve of j-invariant $\neq 0, 1728$ (2023), `https://eprint.iacr.org/2023/785`
15. Koshelev, D.: Magma code (2023), `https://github.com/dishport/Application-of-MW-lattices-with-large-kissing-numbers-to-acceleration-of-MSM-on-elliptic-curves`
16. Kumar, A., Kuwata, M.: Elliptic K3 surfaces associated with the product of two elliptic curves: Mordell–Weil lattices and their fields of definition. Nagoya Mathematical Journal **228**, 124–185 (2017)
17. Nebe, G., Sloane, N.: LATTICES, `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES`
18. Oguiso, K., Shioda, T.: The Mordell–Weil lattice of a rational elliptic surface. Commentarii Mathematici. Universitatis Sancti Pauli, Rikkyo Daigaku Sugaku Zasshi **40**(1), 83–99 (1991)
19. Shioda, T.: Mordell–Weil lattices and sphere packings. American Journal of Mathematics **113**(5), 931–948 (1991)
20. Shioda, T.: Cyclotomic analogue in the theory of algebraic equations of type E_6, E_7, E_8. In: Kim, M.H., Hsia, J.S., Kitaoka, Y., Schulze-Pillot, R. (eds.) Integral Quadratic Forms and Lattices. Contemporary Mathematics, vol. 249, pp. 87–96. American Mathematical Society, Providence (1999)
21. Shioda, T.: The splitting field of Mordell–Weil lattices. In: Pragacz, P., Szurek, M., Wiśniewski, J. (eds.) Algebraic Geometry: Hirzebruch 70. Contemporary Mathematics, vol. 241, pp. 297–303. American Mathematical Society, Providence (1999)
22. Shioda, T.: Integral points and Mordell–Weil lattices. In: Wüstholz, G. (ed.) A Panorama of Number Theory or The View from Baker's Garden. pp. 185–193. Cambridge University Press, Cambridge (2002)
23. Shioda, T.: Elliptic surfaces and Davenport–Stothers triples. Commentarii Mathematici. Universitatis Sancti Pauli, Rikkyo Daigaku Sugaku Zasshi **54**(1), 49–68 (2005)
24. Shioda, T.: The Mordell–Weil lattice of $y^2 = x^3 + t^5 - 1/t^5 - 11$. Commentarii Mathematici. Universitatis Sancti Pauli, Rikkyo Daigaku Sugaku Zasshi **56**(1), 45–70 (2007)
25. Shioda, T.: Gröbner basis, Mordell–Weil lattices and deformation of singularities, I. Proceedings of the Japan Academy. Series A, Mathematical Sciences **86**(2), 21–26 (2010)

26. Shioda, T.: Gröbner basis, Mordell–Weil lattices and deformation of singularities, II. Proceedings of the Japan Academy. Series A, Mathematical Sciences **86**(2), 27–32 (2010)
27. Usui, H.: On the Mordell–Weil lattice of the elliptic curve $y^2 = x^3 + t^m + 1$. I. Commentarii Mathematici. Universitatis Sancti Pauli, Rikkyo Daigaku Sugaku Zasshi **49**(1), 71–78 (2000)
28. Usui, H.: On the Mordell–Weil lattice of the elliptic curve $y^2 = x^3 + t^m + 1$. II. Commentarii Mathematici. Universitatis Sancti Pauli, Rikkyo Daigaku Sugaku Zasshi **50**(1), 65–87 (2001)
29. Usui, H.: On the Mordell–Weil lattice of the elliptic curve $y^2 = x^3 + t^m + 1$. III. Commentarii Mathematici. Universitatis Sancti Pauli, Rikkyo Daigaku Sugaku Zasshi **55**(2), 173–194 (2006)
30. Usui, H.: On the Mordell–Weil lattice of the elliptic curve $y^2 = x^3 + t^m + 1$. IV. Commentarii Mathematici. Universitatis Sancti Pauli, Rikkyo Daigaku Sugaku Zasshi **57**(1), 23–63 (2008)
31. Vlăduţ, S.: Lattices with exponentially large kissing numbers. Moscow Journal of Combinatorics and Number Theory **8**(2), 163–177 (2019)