Generation of “independent” points on elliptic curves by means of Mordell–Weil lattices

Dmitrii Koshelev

Computer sciences and networks department, Télécom Paris, France

https://www.telecom-paris.fr
dimitri.koshelev@gmail.com

Abstract. This article develops a novel method of generating “independent” points on an ordinary elliptic curve $E$ over a finite field. Such points are actively used in the Pedersen vector commitment scheme and its modifications. In particular, the new approach is relevant for Pasta curves (of $j$-invariant 0), which are very popular in the given type of elliptic cryptography. These curves are defined over highly 2-adic fields, hence successive generation of points via a hash function to $E$ is an expensive solution. Our method also satisfies the NUMS (Nothing Up My Sleeve) principle, but it works faster on average. More precisely, instead of finding each point separately in constant time, we suggest to sample several points at once with some probability.

Keywords: elliptic curves · generation of “independent” points · isotrivial elliptic surfaces · Mordell–Weil lattices · Pedersen hash · superelliptic curves · vector commitment schemes

1 Introduction

A commitment scheme is a cryptographic primitive that allows one party to commit to a chosen value while keeping it hidden to others, with the ability to reveal the committed value later. Commitment schemes are designed so that the party cannot change the value after they have committed to it. They have important applications in a number of cryptographic protocols including secure coin flipping and zero-knowledge proofs.

There is the classic Pedersen commitment scheme [31, Section 3]. It works in any cyclic group with the hard discrete logarithm problem (DLP). However, throughout the article we will deal only with (a large subgroup $G$ of) the $\mathbb{F}_q$-point group $E(\mathbb{F}_q)$ of an elliptic curve $E$ over a finite field $\mathbb{F}_q$. As is well known, today ordinary (i.e., non-supersingular) curves over fields of large characteristic $p$ are considered the safest. And every cryptographer understands perfectly that the order $\ell := \#G$ must be prime.

We can use a variant of the original Pedersen commitment (for $n = 1$) to commit to multiple values $(m_1, \cdots, m_n) \in \mathbb{F}_q^n$ at once (so-called vector commitment). We have to sample a vector of public points $(P_1, \cdots, P_n) \in G^n$, along with a fixed
generator $P_0 \in \mathbb{G}$. Then the commitment is just the sum $m_0 P_0 + \sum_{i=1}^n m_i P_i$, where $m_0 \in \mathbb{F}$ is an auxiliary value to ensure the security of the scheme.

Of course, we can simply commit to each $m_i$ individually, but this solution is much less efficient in terms of memory and computing resources. Indeed, the full multi-scalar multiplication can be performed much more rapidly than each one $r_1 P_0 + m_1 P_1$ alone. Here $(r_1, \ldots, r_n) \in \mathbb{F}_p^n$ is another random vector playing the role of $m_0$. Besides, vector commitments provide a way to store or transmit only one element of the group $\mathbb{G}$ instead of a vector from $\mathbb{G}^n$. In real-world cryptography it happens that $n$ reaches huge numbers such as $\approx 2^{30}$ as indicated, e.g., in \cite{10}.

The aforementioned primitive is also known as the Pedersen hash $\mathbb{F}_p^n \rightarrow \mathbb{G}$ (see, e.g., \cite{5}). It is provably secure, because its resistance is based on the multi-dimensional DLP. According to cryptanalysis performed in \cite{18}, \cite{19} the given problem does not seem to be simpler in general than the classical DLP. Another advantage of the Pedersen hash is in its additive homomorphic property. All this positively distinguishes it from (Merkle hash tree \cite{30} using) faster standard hash functions such as SHA-3 (Keccak).

Certainly, the Pedersen scheme is resistant only if the points $P_i$ are “independent”, that is nobody knows a non-trivial linear relation between them. In other words, it is hard to find values $(k_1, \ldots, k_n) \in \mathbb{F}_p^n$ such that $k_0 P_0 = \sum_{i=1}^n k_i P_i$ and at least one $k_i \neq 0$. Therefore, every point $P_i$ must be generated in a transparent way. Be careful that, from the mathematical point of view, conversely, any two points depend on each other, since the group $\mathbb{G}$ is prime.

Over time, a malicious user may find some relation between the points $P_i$ through a kind of brute-force attack. We have no guarantee that this cannot happen for concrete points, even though the multi-dimensional DLP is intractable in the general case. The fact is that for the large $n$ there is the huge number of linear relations. At the same time, it is enough to find just one to break the Pedersen scheme. That is why it is desirable for security to periodically change the points.

The author of \cite{16} prefers the word “basis” and he admits that “updating the basis at every round is inefficient”. Let’s assume the opposite situation when the points $P_i$ remain the same for a long time. Even in this situation, the task of their rapid generation is still important. First, the storage (resp. transmission) of the points requires a lot of memory (resp. bandwidth). And second, there is ground for a potential fault attack, because it is enough for an adversary to replace just one point.

As is known, the points $P_i$ can be obtained by means of a hash function $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{G}$, for example as $P_i = \mathcal{H}(\text{seed}||i)$ (cf. \cite{5}, Section 5.1]). This approach forces to evaluate $\mathcal{H}$ exactly $n$ times. The fastest constructed hash functions to elliptic curves extract one radical $\sqrt[m]{\cdot}$ in $\mathbb{F}_p$ for some $m \in \mathbb{N}$. Their actual classification is given in \cite{25}, Tables 1-2 (cf. \cite{15}). And the existence of $\mathcal{H}$ without radicals at all is highly unlikely. There is plenty of material devoted to extracting $\sqrt[m]{\cdot}$, starting with the seminal work of Adleman, Manders, and Miller.
But despite this, \( \sqrt{\cdot} \) continues to be a much more expensive operation than the arithmetic ones in \( \mathbb{F}_q \), namely +, −, *, and even /.

It is also worth noting the Kate–Zaverucha–Goldberg (KZG) commitment scheme (or just the Kate commitment) \[23\] based on pairings of elliptic curves. At the moment, this scheme is recognized by the cryptographic society as one of the best from the computational point of view. However, to deploy it we need a trusted setup. More concretely, the scheme substantially uses the points \( s^i P_0 \) (with a secret \( s \in \mathbb{F}_\ell \)) rather than arbitrary “independent” points. By the way, such points can be equally utilized in the Pedersen scheme.

In comparison with the Pedersen protocol, KZG one is in fact a polynomial commitment. By definition, it allows a prover to commit to a polynomial \( f = \sum_{i=0}^{n-1} m_i+1 x^i \), with the property that the prover can later convince a verifier of the equality \( f(\alpha) = \beta \), given \( \alpha, \beta \in \mathbb{F}_\ell \). In addition, until \( n \) points of the form \( (\alpha, f(\alpha)) \) are revealed, the polynomial \( f \) remains hidden, as should be clear.

It turns out that the Pedersen vector commitment can be supplemented to give rise to a polynomial commitment without a trusted setup (see, e.g., [9, Section 3], [14, Section 4.5]). Incidentally, those sources are dedicated to a protocol of so-called recursive proof composition using an amicable pair \[37\] of prime-order elliptic curves. More precisely, the latter are non-pairing-friendly curves \( y^2 = x^3 + 5 \) of \( j \)-invariant 0 under the name Pasta curves (Pallas and Vesta) \[20\] (cf. \[21\]).

These curves (and many others \[2\]) are defined over highly 2-adic fields, i.e., \( 2^e | q - 1 \) for a fairly large \( e \in \mathbb{N} \). Such fields allow to utilize the fast Fourier transform (FFT) \[14, Section 4.2\] to speed up the polynomial arithmetic in numerous modern protocols. The downside is that one cannot express a square root in \( \mathbb{F}_q \) via one exponentiation in \( \mathbb{F}_q \). We can always resort to the Tonelli–Shanks algorithm \[13, Algorithm 5.14\], but it is substantially slower than the exponentiation operation. That is why we should avoid square roots as far as possible.

2 Underlying mathematical preliminaries

Consider a finite field \( \mathbb{F}_q \) of characteristic \( p > 3 \). The notion of an elliptic surface \[32, Section 5\], \[35, Chapter III\] over \( \mathbb{F}_q \) is key for us. Without loss of generality, we can confine to a short Weierstrass form

\[
E : y^2 = x^3 + a(t)x + b(t) \quad \subset \mathbb{A}^3_{(x,y,t)}
\]

with polynomial coefficients \( a(t), b(t) \in \mathbb{F}_q[t] \). As usual, \( E \) is interpreted as an elliptic curve over the function field \( F := \mathbb{F}_q(t) \) in one variable. From time to time, we will equally need the field \( F' := \overline{\mathbb{F}_q}(t) \) over the algebraic closure \( \overline{\mathbb{F}_q} \).

Recall that the Mordell–Weil group of \( E \) is the abelian group \( E(\mathbb{F}) \) of all \( \mathbb{F} \)-points on \( E \). Due to a special case of the Mordell–Weil theorem \[32, Section 3.3\] the group \( E(\mathbb{F}) \) is finitely generated. Its rank \( r \) is called the Mordell–Weil rank of \( E \). As always, we denote by \( E(\mathbb{F})_{\text{tor}} \) the (finite) torsion subgroup of \( E(\mathbb{F}) \). The quotient \( E(\mathbb{F})/E(\mathbb{F})_{\text{tor}} \simeq \mathbb{Z}^r \) enjoys a positive-definite quadratic form \( \tilde{h} \) under
elliptic curves are still relevant even though trivial twist of trivial surfaces are excluded from our consideration. By definition, elliptic surfaces (s.t. \( E \)) throughout the article we assume the coincidence of the 6.5]).

As is customary, we are given an ordinary elliptic \( E_q \)-curve \( E: y^2 = x^3 + ax + b \). Throughout the article we assume the coincidence of the \( j \)-invariants: \( j(E) = j(E) \). Such a surface \( E \) is said to be isotrivial. Note that \( r = 0 \) for trivial (constant) elliptic surfaces (s.t. \( E \cong F \)), because elliptic curves are not rational. Hence trivial surfaces are excluded from our consideration. By definition, \( E \) is a non-trivial twist of \( E \). Since \( p > 3 \), the results of [36 Section X.5] about twisting elliptic curves are still relevant even though \( F \) is not a perfect field.

Let’s define the function

\[
e(t) := \begin{cases} \frac{a(t)b(t)}{ab} & \text{if } ab \neq 0, \text{ i.e., } j(E) \notin \{0, 1728\}, \\ \frac{a(t)}{a} & \text{if } b = 0, \text{ i.e., } j(E) = 1728, \\ \frac{b(t)}{b} & \text{if } a = 0, \text{ i.e., } j(E) = 0. \end{cases}
\]

Let \( d \in \{2, 4, 6\} \) be the order of the cyclic group Aut(\( E \)) and \( s := \sqrt[d]{c(t)} \). The curves \( E, \mathcal{E} \) are isomorphic precisely over the Kummer extension \( F(s)/F \) of degree \( d \). It is the function field of the superelliptic curve \( C: s^d = c(t) \subset k_4^{2(t,s)} \). The corresponding isomorphism (from the proof of [36 Proposition III.1.4.(b)]) has the form

\[
\varphi : \mathcal{E} \rightarrow E \quad (x, y) \mapsto \left( \frac{x}{z^2}, \frac{y}{z^3} \right),
\]

where

\[
z := \begin{cases} \frac{as}{a(t)} = \frac{b(t)}{bs} & \text{if } ab \neq 0, \text{ i.e., } j(E) \notin \{0, 1728\}, \\ s & \text{otherwise.} \end{cases}
\]

It is worth saying that points from \( \mathcal{E}(F) \) are nothing but \( F_q \)-sections \( h_1^t \rightarrow \mathcal{E} \) of the projection \( pr_t \) to the variable \( t \). Below \( \mathcal{E}_t \) stands for its fiber over \( t \in F_q \). Similarly, \( \varphi_1 : \mathcal{E}_t \rightarrow E \) denotes the specialization of \( \varphi \). There is only a finite number of degenerate fibers, namely those for which the discriminant \( \Delta(\mathcal{E}_t) = -16(4a^3(t) + 27b^2(t)) \) vanishes. Clearly, this happens exactly when \( \varphi_1 \) is meaningless. In this situation, \( \varphi_t(x, y) = \infty \) is a convenient notation (for any map). Finally, given \( t \in F_q \), the condition \( \mathcal{E}_t \cong \mathcal{F}_q \) occurs iff \( \varphi_t \) is defined over \( F_q \) iff \( s \in \mathbb{F}_q^* \).

We need certain results about the endomorphism rings of elliptic curves, which can be found in any classical source like [36 Sections III.9, V.3]. Since \( E \) is an ordinary \( F_q \)-curve, new endomorphisms on it are not added when extending \( F_q \). It is also readily shown by exploiting \( \varphi \) that the coefficients of \( F(s) \)-endomorphisms on \( \mathcal{E} \) in fact belong to \( F \). Eventually, we have:

\[
\text{End}(E/F_q) = \text{End}(E/F) = \text{End}(E/F(s)) \cong \text{End}(\mathcal{E}/F(s)) = \text{End}(\mathcal{E}/F).
\]
By abuse of notation, we will identify all these rings by means of the single symbol \( \mathcal{O} \).

As is well known, \( \mathcal{O} \) is an order in the imaginary quadratic field \( \mathbb{Q}(\sqrt{D}) \), where \( D := t_q^2 - 4q \) and \( t_q \) is the trace (of the Frobenius) of \( E/F_q \). Furthermore, \( \mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\phi \) for some endomorphism \( \phi \) (with the dual one \( \hat{\phi} \)). Recall that its characteristic (and at the same time minimal) polynomial equals

\[
\chi_\phi = x^2 - \text{tr}(\phi)x + \deg(\phi), \quad \text{where} \quad \text{tr}(\phi) := \phi + \hat{\phi}, \quad \deg(\phi) := \phi \cdot \hat{\phi}.
\]

As explained in [4, Appendix A], original Schoof’s algorithm (see, e.g., [13, Algorithm 2.4]) for computing \( t_q \) is easily modified to compute \( \text{tr}(\phi) \) whenever \( \phi \) is the composition of a bounded number of small-degree isogenies.

There is a natural action of the group \( \mu_d \simeq \mathbb{Z}/d \) on the curve \( C \) and hence on its Jacobian \( J_C \). Let’s introduce the number

\[
k := \max \{ k' \in \mathbb{N} \mid \text{exists a surjective } \mu_d\text{-equivariant } \mathbb{F}_q\text{-morphism } J_C \to E^{k'} \},
\]

where \( \mu_d \) acts diagonally on \( E^{k'} \). Evidently, \( k \) does not exceed the geometric genus of \( C \). And when \( k \) attains the genus, \( J_C \) is said to be a \( \rho \)-maximal (or singular) abelian variety [6, Proposition 3].

By virtue of [27] (cf. [24, Sections 6, 7]) we have the sequence of homomorphisms of \( \mathcal{O} \)-modules

\[
\mathcal{E}(F) \simeq \text{Mor}_{\mu_d}(C, E) \to \text{Hom}_{\mu_d}(J_C, E) \simeq \text{Hom}(E^{k}, E) \simeq \text{End}(E)^k. \quad (1)
\]

The first homomorphism maps \( P \mapsto \varphi_P \) through \( \varphi \) in a clear way. The kernel of the second one consists of constant morphisms, which implies the equality \( r = 2k \). At last, the third one is not in any way a canonical isomorphism.

Likewise, we possess the sequence starting from

\[
\mathcal{E}(F(s)) \simeq E(F(s)) \simeq \text{Mor}(C, E).
\]

Looking ahead, this \( \mathcal{O} \)-module gives an advantage over \( \mathcal{E}(F) \) whenever the rank of the former is greater than that of the latter. Indeed, in Algorithm 1 one can evaluate any (not necessarily \( \mu_d \)-equivariant) covers \( \psi_1, \ldots, \psi_n : C \to E \) that are independent over \( \mathcal{O} \). However, \( \mathcal{E}(F(s)) \) is an awkward object that is more difficult to analyze than \( \mathcal{E}(F) \). In Section 5.1 we carry out such an analysis in a simple example.

### 3 New generation method and its running time

Let us keep the notation of the previous section. At the same time, consider an arbitrary cyclic \( \mathbb{F}_q \)-cover \( \chi : C \to \mathbb{P}^1 \) of degree \( m \mid q - 1 \). In other words, the curve can be represented in the form \( C : v^m = f(u) \in k_7^2(u,v) \) for some \( f \in \mathbb{F}_q[u] \) without roots of multiplicity \( \geq m \). In particular, the earlier coordinates \( t, s \) are expressed via rational \( \mathbb{F}_q \)-functions in \( u, v \) and vice versa: \((t, s) = \tau(u, v) \) and
(u, v) = τ^{-1}(t, s). When m = d, for our purposes, it will be sufficient to take f = c(t) (or, equivalently, χ = pr_t) and τ = id.

Pick any points P_1, ⋯, P_n ∈ E(F) \ E(F)_{tor} linearly independent over 𝒪. Given u ∈ 𝕂_q, the condition 𝒮_i ≃ E_i E evidently amounts to the fact that v = \sqrt{f(u)} ∈ 𝕂_q, unless τ(u, v) is meaningless or 𝒮_i is singular. If actually v ∈ 𝕂_q, we obtain the n points P_i(t) ∈ 𝒮_i(𝕂_q) ≃ E(𝕂_q) at least for integral P_i. Since in discrete logarithm cryptography the group E(𝕂_q) is (almost) prime, the specialized points (very often) become dependent for n > 1. However, we do not see a non-trivial relation between them. Finally, whenever 𝒢 ⊆ E(𝕂_q), it remains to clear the cofactor to definitely fall into 𝒢, but the resulting points are still “independent”.

It is worth avoiding torsion points P_i, because they and hence P_i(t) have tiny orders with respect to ℓ. We also emphasize that the points must be independent precisely over 𝒪, and not just over ℤ. Although 1, φ are linearly independent endomorphisms, their restrictions on 𝒢 are not. Indeed, from 𝒢 ≃ ℤ/ℓ it follows that End(𝒢) ≃ ℂ_ℓ. On the other hand, in practice 𝒢 = E(𝕂_q)[ℓ]. As a consequence, there exists λ ∈ ℂ_ℓ such that φ(P) = λP for all P ∈ 𝒢. In other terms, λ is a root of the characteristic polynomial χ_φ ∈ ℂ_ℓ[x], i.e., λ is an eigenvalue of φ|E[ℓ]. Eventually, knowing χ_φ, we can determine λ with 50-percent confidence (100-percent one when φ is easy to evaluate).

Realizing φ as an abstract element of ℚ(√D), we immediately get χ_φ, because ̂φ is the complex conjugate of φ. In turn, the latter can be found via randomized Bisson–Sutherland’s algorithm [17] (resp. deterministic Kohel’s one [17] Section 25.4.2). While in the worst case its running time is sub-exponential (resp. exponential), the curve E is usually generated once and for all by a certain regulator. It is not ruled out that φ is in its sleeve. That is why we should not rely on the hardness of finding φ. In addition, implementors of elliptic cryptosystems often choose E for which, conversely, φ is a small-degree endomorphism known to all. This is done in order to enjoy the GLV (Galbraith–Lambert–Vanstone) scalar multiplication method [17] Section 11.3.3]

Fix a hash function η : {0, 1}^* → ℂ_ℓ. We need to change u = η(seed||i), where i ∈ ℤ, while the desired requirement \sqrt{f(u)} ∈ ℂ_ℓ is not met. So the new generation method (formalized in Algorithm [17] is a priori non-constant-time. Nevertheless, this is not dangerous as regards timing attacks, because seed||i is public information. Frankly speaking, we have to continue sampling u when we encounter one of the degenerate situations τ(u, v) = ∞, ϕ_t(x, y) = ∞, or P_i(t) = ∞. They arise with negligible probability, so we do not pay attention to them anymore, with the permission of the reader.

We have the power residue symbol \left(\frac{z}{q}\right)_m := z^{(q-1)/m} generalizing the Legendre symbol (for m = 2). It is obviously a surjective homomorphism ℂ_q^* → ℤ_m to the group of all m-th roots of unity. As is well known, to determine whether f(u) is an m-th residue in ℂ_q it is sufficient to check the equality \left(\frac{f(u)}{q}\right)_m = 1. It turns out that for m ≤ 11 computing the residue symbol is a much cheaper operation due to [22] than extracting any root in ℂ_q. Thus, unlike the generation method
Generation of “independent” points by means of Mordell–Weil lattices

with a hash function $H : \{0, 1\}^* \to E(\mathbb{F}_q)$, we obtain a set of “independent” \( \mathbb{F}_q \)-points on \( E \) by extracting only one root in \( \mathbb{F}_q \) (of degree \( m \)).

The same thought occurs in [41, Section 3] to speed up (de)compression in the post-quantum protocol SIDH (Supersingular Isogeny Diffie–Hellman). Instead of applying a constant-time encoding (essentially $H$) to an elliptic curve, the authors of that article prefer to “subvert” it to produce at once two independent (in the strict sense) points with high probability. They agree with us that a randomized algorithm with one square root (and several Legendre symbols) is faster on average than a deterministic one with two square roots in the same field. This is especially relevant for SIDH, since the given protocol is deployed over a highly 2-adic field.

Algorithm 1: New generation method

**Data:** a seed $\in \{0, 1\}^*$ and a hash function $\eta : \{0, 1\}^* \to \mathbb{F}_q$,

an elliptic $\mathbb{F}_q$-curve $E$ and an elliptic $\mathbb{F}_q$-surface $\mathcal{E}$ of the same $j$-invariant,

points $P_1, \ldots, P_n \in E(\mathbb{F}_q) \setminus E(\mathbb{F}_q)_{tor}$ independent over $\mathcal{O}$,

a superelliptic curve $C : v^m = f(u)$ (where $m \mid q - 1$ and $f \in \mathbb{F}_q[u]$) such that $E \cong \mathcal{E}$ over the function field $\mathbb{F}_q(C)$.

**Result:** $n$ “independent” points in $E(\mathbb{F}_q)$.

```
begin
  i := 0;
  u := \eta(seed) || i;
  while $\left(\frac{f(u)}{N} \right)^m \neq 1$ do
    i := i + 1;
    u := \eta(seed) || i;
  end
  v := \sqrt{f(u)};
  (t, s) := \tau(u, v);
  return $\varphi_{P_1}(t, s), \ldots, \varphi_{P_n}(t, s)$.
end
```

We do not claim the authorship of the following lemma, but we prove it for the sake of completeness.

**Lemma 1.** Let $m \mid q - 1$ and $f \in \mathbb{F}_q[u]$ be a polynomial without roots of multiplicity $\geq m$. Given a random $u \in \mathbb{F}_q$, the probability that $\sqrt{f(u)} \in \mathbb{F}_q$ equals

$$\rho := \frac{N}{q} = \frac{1}{m} + O\left(\frac{1}{\sqrt{q}}\right),$$

where $N := \#\{u \in \mathbb{F}_q \mid \sqrt{f(u)} \in \mathbb{F}_q\}$,

$m, f$ are fixed, but $q \to +\infty$.

**Proof.** We are going to extend the reasoning of [13, Section 8.2.1] from the case $m = 2$. As is customary, $p_a \in \mathbb{N}$ stands for the arithmetic genus of $C : v^m = f(u)$.

Let $n_0$ be the number of $\mathbb{F}_q$-points on $C$ of the form $(u, 0)$ and $n_{\infty}$ be the number
of those at infinity. Trivially, \( p_a, n_0, n_\infty = O(1) \). Since \( C \) is known to be an absolutely irreducible curve, we have the Weil–Aubry–Perret inequality

\[
|\#C(\mathbb{F}_q) - (q + 1)| \leq 2p_a\sqrt{q}
\]

Corollary 2.4],

where \( n_\infty \) is taken into account in \( \#C(\mathbb{F}_q) \). Therefore, \( \#C(\mathbb{F}_q) - q = O(\sqrt{q}) \).

For compactness, we use the auxiliary notation

\[
\alpha(u) := \sum_{i=0}^{m-1} \left( \frac{f_i(u)}{q} \right)_m, \quad A := \sum_{u \in \mathbb{F}_q} \alpha(u).
\]

From the equality \( (x^m - 1)/(x - 1) = \sum_{i=0}^{m-1} x^i \) it follows that

\[
\alpha(u) = \begin{cases} 
  m & \text{if } \sqrt[m]{f(u)} \in \mathbb{F}_q^*, \\
  1 & \text{if } f(u) = 0, \\
  0 & \text{otherwise}. 
\end{cases}
\]

Consequently,

\[
\#C(\mathbb{F}_q) = A + n_\infty, \quad N = \frac{A + n_0(m - 1)}{m}.
\]

Eventually,

\[
\rho - \frac{1}{m} = \frac{A - q + n_0(m - 1)}{mq} = \frac{\#C(\mathbb{F}_q) - n_\infty - q + n_0(m - 1)}{mq} = \frac{O(\sqrt{q}) - n_\infty + n_0(m - 1)}{mq} = O\left(\frac{1}{\sqrt{q}}\right).
\]

Lemma 2. The average-case complexity of Algorithm \( 1 \) is that of computing \( m \) symbols \( \left( \frac{\cdot}{q} \right)_m \) and one radical \( \sqrt[m]{\cdot} \) in \( \mathbb{F}_q \).

Proof. We suggest to consider the probability \( \rho_k \) that for \( k \in \mathbb{N} \) random independent elements \( u_i \in \mathbb{F}_q \) the root \( \sqrt[m]{f(u_i)} \notin \mathbb{F}_q \) and for the \( (k + 1)\)-th one, conversely, \( \sqrt[m]{f(u_{k+1})} \in \mathbb{F}_q \). By virtue of Lemma 1 we get:

\[
\rho_k = x^k \cdot \frac{1}{m} = \frac{(m - 1)^k}{m^{k+1}}, \quad \text{where} \quad x := \frac{m - 1}{m}.
\]

Denote by \( X \) the random variable returning \( k + 1 \) with the probability \( \rho_k \). It corresponds to the number of symbols \( \left( \frac{\cdot}{q} \right)_m \) arising during the work of our algorithm.

By definition of average-case complexity, we need to compute the expected value

\[
\mathbb{E}[X] = \sum_{k=0}^{\infty} (k + 1)\rho_k = \frac{1}{m} \sum_{k=0}^{\infty} (k + 1)x^k
\]
It is a classical fact that under the condition $|x| < 1$ (fulfilled for $m \in \mathbb{N}$) the geometric series $\sum_{k=0}^{\infty} x^k = 1/(1-x)$, hence

$$E[X] = \frac{1}{m} \left( \sum_{k=0}^{\infty} x^{k+1} \right)' = \frac{1}{m} \left( \frac{x}{1-x} \right)' = \frac{1}{m(1-x)^2} = m.$$ 

Bearing in mind the final $m$-th root extraction, the lemma is proved.

Due to (1) the number $n = r/2 \in \mathbb{N}$ is the most optimal in Algorithm 1. Besides, the smaller number $m$, simpler methods exist (over a general field $\mathbb{F}_q$) for finding $\sqrt[2m]{\cdot} \mathbb{F}_q$ and $m\sqrt{\cdot}$, not to mention Lemma 2. The minimal possible $m$ is the cyclic analogue

$$\gamma_c := \min \{ \deg(\chi) \mid \chi: C \to \mathbb{P}^1 \text{ is a cyclic (i.e., Kummer) } \mathbb{F}_q\text{-cover} \}$$

of the gonality $\gamma$ [23 Section 6.5.3] of the curve $C$. Trivially, $2 \leq \gamma \leq \gamma_c \leq d \leq 6$.

Thus, we see that our generation method works more productively if the fraction $\delta := r/\gamma_c$ is greater. It is natural to call it the relative Mordell–Weil rank $r$. Of course, this notion is useless when $j(E) \notin \{0, 1728\}$, that is $d = 2$.

In the opposite case, it seems quite difficult to determine the exact value $\gamma_c$, so it is reasonable to also define $\delta(\chi) := r/\deg(\chi)$. Then $\delta = \max_{\chi} \{\delta(\chi)\}$.

The problem of maximizing $\delta$ has much in common with a classic one of pure mathematics about how big the conventional Mordell–Weil rank $r$ can theoretically be for elliptic surfaces. Over an algebraically closed field of zero characteristic (or just $\mathbb{C}$) the current record equals 68 for the surfaces $E_m: y^2 = x^3 + t^m + 1$ such that $360 \mid m$ (see [32 Section 13.2]). Be careful, there is a discrepancy with our previous notation $E_t$ of a fiber.

Circumstances are drastically different in a prime characteristic $p$. There is no upper bound on $r$ in the class of non-isotrivial surfaces [39], whose $j$-invariants are always ordinary. The same is true for (isotrivial) surfaces of supersingular $j$-invariants [35]. In fact, among those it is enough to confine to $E_{p^e+1}$ (where $e \in \mathbb{N}$) as shown in [33]. Surprisingly, in accordance with the articles [8], [12] the rank $r$ can be made arbitrarily large even in the class of isotrivial surfaces of ordinary $j$-invariants. However, it is not clear how constructive the results established in those articles.

### 4 The case of $j$-invariant 0

Hereafter we focus on elliptic curves of $j$-invariant 0, that is $a = a(t) = 0$, because they are popular in practice. Since we deal only with ordinary curves, $3 \mid q - 1$ or, equivalently, a primitive cubic root $\omega = (-1 + \sqrt{-3})/2$ of unity lies in $\mathbb{F}_q$ (see [36 Example V.4.4]). There is on $E$, $E$ the automorphism $[\omega](x, y) = (\omega x, y)$ of order 3 and moreover $\mathcal{O} = \mathbb{Z}[\omega]$.

For any $m \mid q - 1$ and $c \in \mathbb{F}_q^*$ consider the twist $E_m: y^2 = x^3 + t^m + c$ of the aforementioned elliptic surface. Remarkably, the group $E_m(F)$ is torsion-free regardless of $m$. Further, for $E_m$ to be a rational surface it is necessary and
sufficient that \( m \leq 6 \). These and other details about the surfaces \( E_m \) can be found in [33]. And the general theory of rational elliptic surfaces is discussed, e.g., in [32, Chapter 7].

It is also natural to denote the curve \( C \) from the previous sections by \( C_m : bs^6 = t^m + c \). Its geometric genus \( g(C_m) \) can be computed via a formula from [28, Section 5.1]. In this article we decided to focus only on the case \( m \leq 6 \), because it is the simplest and investigated in the literature. For instance, \( C_6 \) is a twist of the Fermat sextic curve [6, Proposition 7], [27, Example 4.3]. We hope to study the opposite case \( m > 6 \) in the future articles. So from now on, we represent the curve in the form \( C_m : t^m = bs^6 - c \). In terms of Section 3 this means that \( f = bs^6 - c \), i.e., \( \chi = pr_a \) and \( (t, s) = (v, u) \).

Table 1 exhibits main information about the rational surfaces \( E_m \) over \( \mathbb{F}_q \).

<table>
<thead>
<tr>
<th>( m )</th>
<th>( E_m(\mathbb{F}_q) )</th>
<th>( \delta(\chi) )</th>
<th>( d_{\text{min}} )</th>
<th>( \text{disc} )</th>
<th>( g(C_m) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>( A^2_5 )</td>
<td>1</td>
<td>2/3</td>
<td>1/3</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>( D^2_4 )</td>
<td>4/3</td>
<td>1</td>
<td>1/4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>( E^5_6 )</td>
<td>3/2</td>
<td>4/3</td>
<td>1/3</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>( E_8 )</td>
<td>8/5</td>
<td>2</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>4/3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. The rational surfaces \( E_m / \mathbb{F}_q \)

Note that \( 0 < 1 < 4/3 < 3/2 < 8/5 \) for the values from the column \( \delta(\chi) \). For Algorithm 1 the surface \( E_6 \) does not provide any advantage with respect to \( E_3 \). That is why we do not consider it in detail. In turn, the surface \( E_5 \) is the best. Unfortunately, \( 5 \nmid q - 1 \) for Pasta curves, hence for them we have to be content with \( E_4 \). So we are able to generate 3 “independent” \( \mathbb{F}_q \)-points on \( E \) in such a way that the average running time coincides with that of computing 4 symbols \( \left( \frac{2}{q} \right)_4 \) and one quartic root in \( \mathbb{F}_q \). The latter can be obviously represented as 2 successive square roots. Alternatively, one can apply (a variation of) the Adleman–Manders–Miller algorithm in order to directly find \( \sqrt[4]{\cdot} \).

It is time to remind that Pasta curves were designed, taking into account the existence of \( \mathbb{F}_q \)-isogenies of small degree (namely 3) from auxiliary elliptic curves of \( j \)-invariants different from 0. As a result, the state-of-the-art hash function for Pasta curves is the Wahby–Boneh hash function \( H_{WB} \) [40] based on
the simplified SWU (Shallue–van de Woestijne–Ulas) one \[15\] Section 6.6.2. It requires to compute one square root in \(\mathbb{F}_q\) during the execution.

As we said before, \(\sqrt{\cdot}\) (as well as \(4\sqrt{\cdot}\)) is a laborious operation over highly 2-adic fields and Pasta curves are defined over such fields. Fortunately, their fields \(\mathbb{F}_q\) are not highly 3-adic (more concretely, \(27 \nmid q - 1\)). Therefore, the cubic root extraction in \(\mathbb{F}_q\) can be performed by one exponentiation by virtue of \[11\] Proposition 1. Thus, instead of \(\mathcal{E}_4\), it might be wise to use the surface \(\mathcal{E}_3\) to obtain 2 “independent” points at the price of 3 symbols \((\frac{\cdot}{q})_3\) and one cubic root in \(\mathbb{F}_q\).

Finally, the surface \(\mathcal{E}_2\) is useless, because we always have the opportunity to exploit the more advantageous surface \(\mathcal{E}_3\). Indeed, we are not aware of practical situations in which \(\mathbb{F}_q\) is a highly 3-adic field and at the same time \(4, 5 \nmid q - 1\). Even if this situation occurs (and \(\mathcal{H}_{WB}\) is not applicable), it is enough to use the universal SW hash function \[15\] Sections 8.3.4, 8.4.2 with the same running time as for the method built on \(\mathcal{E}_2\).

To sum up, methods of generating \(n\) “independent” \(\mathbb{F}_q\)-points on elliptic curves of \(j\)-invariant 0 are exhibited in Table 2. To justify its bottom row, in the next section we will demonstrate that for all \(m \leq 5\) there is \(c \in \mathbb{F}_q^*\) for which the Mordell–Weil lattices of \(\mathcal{E}_m/\mathbb{F}_q\) and \(\mathcal{E}_{m}/\mathbb{F}_q\) coincide. To be precise, we will explicitly construct \(r\) (resp. \(r/2\)) minimal points \(P_i \in \mathcal{E}_m(\mathbb{F})\) independent over \(\mathbb{Z}\) (resp. \(\mathbb{Z}[\omega]\)). We are guided by the fact that the size of point formulas is proportional to their canonical height. Furthermore, \(P_i\) form a basis (cf. \[29\]), although this property is not applied anywhere by us.

<table>
<thead>
<tr>
<th>method</th>
<th>(n)</th>
<th>average complexity</th>
<th>conditions on (q)</th>
</tr>
</thead>
<tbody>
<tr>
<td>classical with (\mathcal{H}: {0,1}^* \rightarrow E(\mathbb{F}_q))</td>
<td>1</td>
<td>[25] Tables 1-2</td>
<td>((\sqrt{\cdot}) for (\mathcal{H}_{WB}))</td>
</tr>
<tr>
<td>new with (\mathcal{E}_m), where (2 \leq m \leq 5)</td>
<td>(m - 1)</td>
<td>(m(\frac{\cdot}{q})_m + \sqrt{\cdot})</td>
<td>(m \mid q - 1)</td>
</tr>
</tbody>
</table>

**Table 2.** Generation methods for elliptic \(\mathbb{F}_q\)-curves \(E\) of \(j\)-invariant 0

### 5 Linearly independent points in \(\mathcal{E}_m(\mathbb{F})\)

In the current section we tacitly resort to the computer algebra system Magma. The corresponding code is loaded on the web page \[26\]. Besides, we will regularly use a folklore result that, given a pair of lattices \(L' \subset L\) of the same rank, the squared index \([L : L']^2 = \text{disc}(L')/\text{disc}(L)\). In particular, \(L = L'\) if and only if \(\text{disc}(L) = \text{disc}(L')\).

#### 5.1 The case \(m = 2\)

Assume that \(\sqrt{\cdot} \in \mathbb{F}_q\). It is readily seen that the points \(P_i := (-\omega^{j-1} \sqrt{c}, t)\) belong to \(\mathcal{E}_2(\mathbb{F})\). Any two of them are clearly independent over \(\mathbb{Z}\) and dependent...
over \( \mathbb{Z}[\omega] \). The height pairing on the sublattice \( \langle P_1, P_2 \rangle \subset \mathcal{E}_2(F) \) is given by the Gram matrix

\[
M = \begin{pmatrix}
\frac{2}{3} & \frac{1}{3} \\
\frac{1}{3} & \frac{2}{3}
\end{pmatrix},
\]

where the \( i \)-th row and column correspond to \( P_i \). Since \( \det(M) = 1/3 = \text{disc}(A^2) \), the minimal points \( P_1, P_2 \) in fact constitute a \( \mathbb{Z} \)-basis of \( \mathcal{E}_2(F) = \mathcal{E}_2(F') \cong A^2 \). Consequently, \( P := P_1 \) is a generator over \( \mathbb{Z}[\omega] \).

In comparison with \( m > 2 \), the case under consideration is easier, hence let’s dwell on it in more detail. The curve \( C_2: t^2 = bs^6 - c \) is a famous hyperelliptic curve of geometric genus 2 (see, e.g., [6, Example 1]). There are two quadratic \( \mathbb{F}_q \)-covers

\[
\varphi_p: C_2 \to E \quad \text{and} \quad \varphi': C_2 \to E', \quad (s, t) \mapsto \left( \frac{-\sqrt{c}}{s^3}, \frac{t}{s^3} \right),
\]

where \( E: y^2 = x^3 + b, \)

\( E': y^2 = x^3 - b^2c. \)

Notice that \( \varphi_p \in \text{Mor}_{\mathbb{F}_q}(C_2, E) \) as always, but \( \varphi' \notin \text{Mor}_{\mathbb{F}_q}(C_2, E') \). This immediately implies independency of \( \varphi_p, \varphi' \) over \( \mathbb{Z}[\omega] \) after identifying the curves \( E, E' \) by an isomorphism, which exists at most over \( \mathbb{F}_q^\times \). In other words, \( J_{C_2} \sim_{\mathbb{F}_q} E \times E' \sim_{\mathbb{F}_q} E^2 \).

By analogy with the sequence [1], there are two \( \mathbb{F}_q \)-covers \( C_2 \to E \) independent over \( \mathbb{Z}[\omega] \) if and only if

\[
J_{C_2} \sim_{\mathbb{F}_q} E^2 \iff E \sim_{\mathbb{F}_q} E' \iff E \cong_{\mathbb{F}_q} E' \iff \sqrt{-bc} \in \mathbb{F}_q \iff \sqrt{-bc}, \sqrt{b} \in \mathbb{F}_q.
\]

The first \( \iff \) takes place according to uniqueness (up to an \( \mathbb{F}_q \)-isogeny) of the Jacobian decomposition into simple components. The second one follows from the fact that \( E, E' \) are ordinary twists of each other. The remaining ones are evident. The restriction \( \sqrt{-bc} \in \mathbb{F}_q \) is surmountable by picking \( c = -b^3 \). But despite this, for many curves \( E \) (including Pasta curves) \( \sqrt{b} \notin \mathbb{F}_q \).

### 5.2 The case \( m = 3 \)

From the proof of [83 Proposition 5.2] we know that the sought points in \( \mathcal{E}_3(F) \) have the form \( (x, y) = (a_1t + a_0, b_1t + b_0) \) for some \( a_i, b_i \in \mathbb{F}_q \). Substituting it into the equation of \( \mathcal{E}_3 \), we get the points

\[
P_1 := \left( -t, \frac{-3 \cdot u^3}{18} \right), \quad P_2 := \left( -t + \frac{u^2}{3}, ut - \frac{u^3}{6} \right),
\]

where \( u := \sqrt{108c} \), as well as \( P_3 := [\omega]P_1 \) and \( P_4 := [\omega]P_2 \). Note that \( u \in \mathbb{F}_q \) if and only if \( \sqrt{c}, \sqrt{4c} \in \mathbb{F}_q \). Of course, it is sufficient to just take \( c = -1/108 \) or, equivalently, \( u = \sqrt{1}. \)
The height pairing on the sublattice \((P_i)_{i=1}^4 \subset \mathcal{E}_3(F)\) is given by the Gram matrix

\[
M = \begin{pmatrix}
1 & 0 & -\frac{1}{2} & \frac{1}{2} \\
0 & 1 & -\frac{1}{2} & -\frac{1}{2} \\
-\frac{1}{2} & -\frac{1}{2} & 1 & 0 \\
\frac{1}{2} & -\frac{1}{2} & 0 & 1
\end{pmatrix}
\]

where the \(i\)-th row and column correspond to \(P_i\). Since \(\det(M) = 1/4 = \text{disc}(D_4^*)\), the minimal points \(P_i\) constitute a \(\mathbb{Z}\)-basis of \(\mathcal{E}_3(F) = \mathcal{E}_3(F') \simeq D_4^*\). As a result, \(P_1, P_2\) do a \(\mathbb{Z}[^{\omega}]\)-basis.

### 5.3 The case \(m = 4\)

In this section, \(i := \sqrt{-1} \in \mathbb{F}_q\). Also, we need the values \(v := 26\sqrt{3} - 45\) and \(u := \sqrt{283}v\). The surface \(\mathcal{E}_4\) over a non-closed field is discussed in the article [34]. From there we know that one can search for the desired points from \(\mathcal{E}_4(F)\) in the form \((x, y) = (a_1t + a_0, t^2 + b_1t + b_0)\), substituting it into the equation of \(\mathcal{E}_4\). In addition to \(P_1 := (-\sqrt{c}, t^2)\), we find a point \(P_2\) with the coordinates

\[
x_2 := ut + \frac{\sqrt{3} + 3}{12}u^4, \quad y_2 := t^2 + \frac{u^3}{2}t + \frac{\sqrt{3} + 2}{8}u^6
\]

and \(P_3(t) := -P_2(it)\). Obviously, \(u \in \mathbb{F}_q\) if and only if \(\sqrt{283}v, \sqrt{3}v \in \mathbb{F}_q\). Inter alia, \(\sqrt{3}v \in \mathbb{F}_q\), because \(\sqrt{3}v = 2\sqrt{3} - 3\). Of course, it is enough to just pick \(c = 1/(2\sqrt{3}v)\) or, equivalently, \(u = \sqrt[3]{1}\).

As usual, there are equally the counterparts \(P_{3+j} := [\omega]P_j\), where \(1 \leq j \leq 3\). The height pairing on the sublattice \((P_k)_{k=1}^6 \subset \mathcal{E}_4(F)\) is given by the Gram matrix \(M\) such that

\[
3M = \begin{pmatrix}
4 & -2 & -2 & -2 & 1 & 1 \\
-2 & 4 & 1 & 1 & -2 & 1 \\
-2 & 1 & 4 & 1 & -2 & -2 \\
-2 & 1 & 1 & 4 & -2 & -2 \\
1 & -2 & -2 & 4 & 1 & 1 \\
1 & 1 & -2 & -2 & 1 & 4
\end{pmatrix}
\]

where the \(k\)-th row and column correspond to \(P_k\). Since \(\det(M) = 1/3 = \text{disc}(E_6^*)\), the minimal points \(P_k\) constitute a \(\mathbb{Z}\)-basis of \(\mathcal{E}_4(F) = \mathcal{E}_4(F') \simeq E_6^*\). As a result, \(P_j\) do a \(\mathbb{Z}[\omega]\)-basis.
5.4 The case $m = 5$

As well as $E_4$, the surface $E_5$ over a non-closed field is studied in article [34] on which we rely. First of all, possessing $\zeta := \sqrt[5]{1} \in \mathbb{F}_q$, $\zeta \neq 1$, we besides have the root $\sqrt[5]{5} = 2\zeta^3 + 2\zeta^2 + 1$. Also, we need the values

$$v := \sqrt{\frac{3(\sqrt[5]{5} + 5)}{2}} = \zeta^2(\zeta - 1)\sqrt{-3},$$

$$\theta := 564300 + 252495\sqrt[5]{5} + 170252v + 76074\sqrt[5]{5}v,$$

$$u := \sqrt[5]{60\cdot \theta c}.$$ 

Without further ado, one can just take $c = 1/(60\cdot \theta)$, that is $u = \sqrt[5]{60\cdot \theta}$.

It turns out to be enough to confine to points of the form

$$Q_u = \left(\frac{1}{u^2}t^2 + a_1t + a_0, \frac{1}{u^3}t^3 + b_2t^2 + b_1t + b_0\right).$$

As earlier, the substitution of $Q_u$ into the equation of $E_5$ gives rise to a polynomial system. After that, we find its solution

$$a_0 := -\frac{(8289\zeta^3 + 35113\zeta^2 + 43402\zeta + 21701)\omega + (26238\zeta^3 + 39650\zeta^2 + 21701\zeta - 2804)}{15}u^{10},$$

$$a_1 := -\frac{(58\zeta^3 + 246\zeta^2 + 304\zeta + 152)\omega + (184\zeta^3 + 278\zeta^2 + 152\zeta - 19)}{5}u^4,$$

$$b_0 := \frac{12a_0a_1 - a_3^2u^2 - 12a_0u^4 + 15a_1^2u^6 + 9a_1u^{10} + u^{14}}{16},$$

$$b_1 := \frac{12a_0 + 3a_1^2u^2 - 6a_1u^6 - u^{10}}{8u} - \frac{3a_1 + u^4}{2u}.$$ 

Consider the points $P_i := Q_{\zeta^{i-1}u}$ and $P_{i+4} := [\omega]P_i = Q_{\omega^{i-1}u}$, where $1 \leq i \leq 4$. The height pairing on the sublattice $\langle P_k \rangle_{k=1}^8 \subset E_5(F)$ is given by the Gram matrix

$$M = \begin{pmatrix}
2 & -1 & 0 & 0 & -1 & 1 & 0 & 0 \\
-1 & 2 & -1 & 0 & 0 & -1 & 1 & 0 \\
0 & -1 & 2 & -1 & 0 & 0 & -1 & 1 \\
0 & 0 & -1 & 2 & 0 & 0 & 0 & -1 \\
-1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\
1 & -1 & 0 & 0 & -1 & 2 & -1 & 0 \\
0 & 1 & -1 & 0 & 0 & -1 & 2 & -1 \\
0 & 0 & 1 & -1 & 0 & 0 & -1 & 2
\end{pmatrix},$$

where the $k$-th row and column correspond to $P_k$. Since $\det(M) = 1 = \text{disc}(E_8)$, the minimal points $P_k$ constitute a $\mathbb{Z}$-basis of $E_5(F) = E_5(F') \simeq E_8$. As a result, $P_i$ do a $\mathbb{Z}[\omega]$-basis.
Acknowledgements. The author expresses his gratitude to Alistair Stewart, Antonio Sanso, Geoffrey Couteau, Jeffrey Burdges, and Sergey Vasilyev for their useful comments on the role of generating “independent” points on elliptic curves in real-world vector commitment schemes.

References


