

On the discrete logarithm problem in elliptic curves II

Claus Diem

July 26, 2011

Abstract

We continue our study on the elliptic curve discrete logarithm problem over finite extension fields. We show, among other results, the following two results:

For sequences of prime powers $(q_i)_{i \in \mathbb{N}}$ and natural numbers $(n_i)_{i \in \mathbb{N}}$ with $n_i \rightarrow \infty$ and $\frac{n_i}{\log(q_i)^2} \rightarrow 0$ for $i \rightarrow \infty$, the discrete logarithm problem in the groups of rational points of elliptic curves over the fields $\mathbb{F}_{q_i}^{n_i}$ can be solved in subexponential expected time $(q_i^{n_i})^{o(1)}$.

Let $a, b > 0$ be fixed. Then the problem over fields \mathbb{F}_{q^n} , where q is a prime power and n a natural number with $a \cdot \log(q)^{1/3} \leq n \leq b \cdot \log(q)$, can be solved in an expected time of $e^{\mathcal{O}(\log(q^n)^{3/4})}$.

1 Introduction

In our previous work [Die11], we have derived the following theorem.

Theorem 1 *The discrete logarithm problem in the groups of rational points of elliptic curves over finite fields \mathbb{F}_{q^n} can be solved in an expected time of*

$$e^{\mathcal{O}(\max(\log(q), n^2))}.$$

Here and in the following, q is always a prime power and n a natural number.

It follows from this theorem that for any two sequences $(q_i)_{i \in \mathbb{N}}$ and $(n_i)_{i \in \mathbb{N}}$ of prime powers and natural numbers respectively with $n_i \rightarrow \infty$ and $\frac{n_i}{\log(q_i)} \rightarrow 0$ for $i \rightarrow \infty$, the discrete logarithm problem in the groups of rational points of elliptic curves over the fields $\mathbb{F}_{q_i}^{n_i}$ can be solved in an expected time of $(q_i^{n_i})^{o(1)}$.

In this work, we prove the following stronger result:

Theorem 2 *The discrete logarithm problem in the groups of rational points of elliptic curves over finite fields \mathbb{F}_{q^n} can be solved in an expected time of*

$$e^{\mathcal{O}(\max(\log(q), n \cdot \log(q)^{1/2}, n^{3/2}))}.$$

Furthermore, under the condition that q is even, the problem can be solved in an expected time of

$$e^{\mathcal{O}(\max(\log(q), n \cdot \log(q)^{1/2}, n \cdot \log(n)^{1/2}))} .$$

Note here that

$$\max(\log(q), n \cdot (\log(q))^{1/2}, n^{3/2}) = \begin{cases} \log(q) & \text{for } n \leq \log(q)^{1/2} \\ n \cdot (\log(q))^{1/2} & \text{for } \log(q)^{1/2} \leq n \leq \log(q) \\ n^{3/2} & \text{for } \log(q) \leq n \end{cases}$$

and similarly

$$\max(\log(q), n \cdot (\log(q))^{1/2}, n \cdot \log(n)^{1/2}) = \begin{cases} \log(q) & \text{for } n \leq \log(q)^{1/2} \\ n \cdot (\log(q))^{1/2} & \text{for } \log(q)^{1/2} \leq n \leq q \\ n \cdot \log(n)^{1/2} & \text{for } q \leq n \end{cases} .$$

Theorem 2 gives the following results.

1. Let sequences of prime powers $(q_i)_{i \in \mathbb{N}}$ and natural numbers $(n_i)_{i \in \mathbb{N}}$ with $q_i \rightarrow \infty$ and $n_i \rightarrow \infty$ for $i \rightarrow \infty$ be given. Under the additional condition that

- i) $\frac{n_i}{\log(q_i)^2} \rightarrow 0$ for $i \rightarrow \infty$

or

- ii) q_i is even for all i and $\frac{n_i}{q_i^2} \rightarrow 0$ for $i \rightarrow \infty$,

the discrete logarithm problem in the groups of rational points of elliptic curves over the fields $\mathbb{F}_{q_i^{n_i}}$ can be solved in an expected time of

$$(q_i^{n_i})^{o(1)} .$$

2. Let $\beta \geq \frac{1}{2}$ and $a, b > 0$ be fixed. Let

$$\alpha := \frac{1}{2\beta + 1} \quad \text{and} \quad \gamma := 1 - \frac{1}{2} \frac{1}{\beta + 1} = \frac{\beta + \frac{1}{2}}{\beta + 1} .$$

Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields \mathbb{F}_{q^n} with *even* q and

$$a \cdot \log(q)^\alpha \leq n \leq b \cdot \log(q)^\beta \tag{1}$$

can be solved in an expected time of

$$e^{\mathcal{O}(\log(q^n)^\gamma)} .$$

If furthermore $\beta \leq 1$, the same holds over *all* finite fields \mathbb{F}_{q^n} such that (1) is satisfied.

Note that $\alpha \leq \frac{1}{2}$ (with equality if $\beta = \frac{1}{2}$), and γ is maximal if $\alpha = \beta = \frac{1}{2}$, and then it is equal to $\frac{2}{3}$.

As a special case we obtain that for $a, b > 0$ the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields \mathbb{F}_{q^n} with

$$a \cdot \log(q)^{1/3} \leq n \leq b \cdot \log(q)$$

can be solved in an expected time of $e^{\mathcal{O}(\log(q^n)^{3/4})}$.

3. Let $\beta \in [1, 2)$ and $a, b > 0$ be fixed. Let

$$\alpha := \frac{2 - \beta}{3\beta} \text{ and } \gamma := \frac{3}{2} \cdot \frac{\beta}{1 + \beta}.$$

Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields \mathbb{F}_{q^n} with

$$a \cdot \log(q)^\alpha \leq n \leq b \cdot \log(q)^\beta$$

can be solved in an expected time of

$$e^{\mathcal{O}(\log(q^n)^\gamma)}.$$

The first statement follows immediately from Theorem 2.

The derivation of the second statement from Theorem 2 is as follows:

Note first that $n \leq q$ for nearly all instances.

We have $\beta = \frac{\gamma - \frac{1}{2}}{1 - \gamma}$ and $\alpha = \frac{1}{\gamma} - 1$.

The first inequality in (1) is equivalent to $n \geq a \cdot \log(q)^{\frac{1}{\gamma} - 1}$, and this is equivalent to $\frac{1}{a^\gamma} \cdot (n \log(q))^\gamma \geq \log(q)$.

The second inequality is equivalent to $b^{1-\gamma} \cdot \log(q)^{\gamma - \frac{1}{2}} \geq n^{1-\gamma}$, and this is equivalent to $b^{1-\gamma} \cdot (n \log(q))^\gamma \geq n \cdot \log(q)^{1/2}$.

The results now follow with Theorem 2.

We now show how the third statement follows from Theorem 2. We have $\beta = \frac{2\gamma}{3-2\gamma}$ and – as above – $\alpha = \frac{1}{\gamma} - 1$.

For the range $a \cdot \log(q)^\alpha \leq n \leq \log(q)$, the result follows from the second point, so we consider the range $\log(q) \leq n \leq b \cdot \log(q)^\beta$. We have $n \leq b \cdot \log(q)^{\frac{2\gamma}{3-2\gamma}}$, that is, $n^{\frac{3}{2}-\gamma} \leq b^{\frac{3}{2}-\gamma} \cdot \log(q)^\gamma$. With other words: $n^{\frac{3}{2}} \leq b^{\frac{3}{2}-\gamma} \cdot (n \cdot \log(q))^\gamma$. \square

Outline

Throughout this work, we assume that the reader is familiar with our previous work [Die11], possibly excluding the final subsection 4.5. In particular, we use the same notations as in our previous work. We also assume that the reader is familiar with toric geometry.

It follows an outline over of this article.

The algorithm for Theorem 2 is again based on the index calculus method, and also just as in [Die11], we use multivariate polynomial systems over \mathbb{F}_q to obtain relations. The main conceptual difference between the new algorithm and the previous algorithm is that we enlarge the factor base. This enlargement causes some difficulties in the analysis of the algorithm, and in order to complete the analysis we further modify the definition of the factor base. We also employ a new algorithm to find decompositions. The other steps of the index calculus algorithm in [Die11] are not changed.

We will focus on the parts of the index algorithm which need to be changed. Explicitly, these are Steps 4 and 5 for the constructions surrounding the definition of the factor base and the way relations are obtained in Step 6 of the algorithm presented in subsection 2.3 of [Die11].

Below we outline a preliminary algorithm, and on the basis of this algorithm, we discuss under various heuristic assumptions why one should be able to obtain an expected running time of $e^{\mathcal{O}(\max(\log(q), n \cdot \log(q)^{1/2}))}$. In the course of this work, we will change the algorithm in various ways. Unfortunately, even with a modified algorithm we cannot prove that one can obtain the expected running time one might expect by heuristic considerations. Indeed, in odd characteristic we can only complete the analysis under the condition that $c^n \leq q$ for a suitable constant $c > 0$ and in even characteristic we can only complete the analysis if $n^c \leq q$ for a suitable constant $c > 0$.

The two results in Theorem 2 then follow by applying the index calculus algorithm over a suitable extension field. This is completely analogous to the proof of Theorem 1 from Proposition 2.11 in [Die11].

In the next section, we give the new algorithm for the constructions leading to the definition of the factor base. In Section 3 we formulate a decomposition problem adapted to the new situation and give an algorithm to solve the problem. In the last section, we prove that under suitable conditions on n and q the probability that a uniformly randomly distributed point $P \in E(\mathbb{F}_{q^n})$ leads to a relation between P and factor base elements is large enough. In the last part of this section, we indicate how Theorem 2 can be obtained.

A preliminary algorithm

The algorithm follows the usual “index calculus” strategy: We fix a so-called factor base, generate relations between input elements and factor base elements and finally solve the discrete logarithm problem via linear algebra.

Just as in [Die11], the factor base is defined in an algebraic way, and the relations are obtained by solving systems of multivariate polynomial equations over \mathbb{F}_q .

Let some instance of the problem with a prime power q , a natural number $n \geq 2$ and an elliptic curve E/\mathbb{F}_{q^n} be given, where E is (as usual) given by an affine Weierstraß equation in x and y with neutral element the point at infinity.

Let m be some natural number $\leq n$, which will be optimized later, and let $d := \lceil \frac{n}{m} \rceil$ and $\delta := dm - n$.

Now we choose some d -dimensional vector subspace U of the \mathbb{F}_q -vector space \mathbb{F}_{q^n} and define the factor base by

$$\mathcal{F} := \{P \in E(\mathbb{F}_{q^n}) \mid x(P) \in U\}.$$

Furthermore, if n is not divisible by m (that is, $\delta \neq 0$), we choose a $d - 1$ -dimensional vector subspace U' of U and set

$$\mathcal{F}' := \{P \in E(\mathbb{F}_{q^n}) \mid x(P) \in U'\}.$$

Given some element $P \in E(\mathbb{F}_{q^n})$, we want to find a relation

$$P_1 + \dots + P_m = P$$

with $P_i \in \mathcal{F}'$ for $i = 1, \dots, \delta$ and $P_i \in \mathcal{F}$ for $i = \delta + 1, \dots, m$. The key idea is again to find such relations by solving systems of polynomial equations over \mathbb{F}_q . One possibility to obtain such a system is as follows:

We use the $(m + 1)^{\text{th}}$ affine summation polynomial, the dehomogenization of the $(m + 1)^{\text{th}}$ homogeneous summation polynomial with respect to Y_1, \dots, Y_{m+1} . Let $s_{m+1} \in \mathbb{F}_{q^n}[x_1, \dots, x_{m+1}]$ be this polynomial. We expand the polynomial $s_{m+1}(x_1, \dots, x_m, x(P))$ over \mathbb{F}_q and restrict the coordinates to U' respectively U . This gives a system of n polynomials in n variables. As $s_{m+1}(x_1, \dots, x_m, x(P))$ has degree 2^{m-1} in each variable and therefore total degree $\leq m \cdot 2^{m-1}$, the system has degree $\leq m \cdot 2^{m-1}$.

Now a list of solutions over \mathbb{F}_q of such a system containing all isolated solutions over \mathbb{F}_q (that is, the \mathbb{F}_q -rational isolated points of the algebraic subspace defined by the system), can be determined in an expected time of $\text{Poly}(e^{nm} \cdot \log(q))$ with an algorithm by M. Rojas ([Roj99]). Let us assume that for varying P , most solutions over \mathbb{F}_q of these systems are indeed isolated.

It is reasonable to estimate the size of \mathcal{F} as roughly q^d and the size of \mathcal{F}' as roughly q^{d-1} . This indicates that the expected value of relations obtained per try is in $\mathcal{O}(\frac{1}{m!})$.

Disregarding the possibility that some of the relations generated might be linearly dependent, we need roughly q^d relations. This indicates an expected running time of

$$\mathcal{Poly}(m! \cdot e^{nm+\log(q)\cdot d}) = \mathcal{Poly}(e^{nm+\log(q)\cdot \frac{n}{m}}).$$

for the relation generation part. The expected running time for the linear algebra part is merely $\mathcal{Poly}(e^{\log(q)\cdot d})$.

Now for $m := \min(\lceil \sqrt{\log(q)} \rceil, n)$, we obtain, again on the basis of the above heuristic arguments, a total expected running time of

$$\mathcal{Poly}(e^{\max(\log(q), n \cdot \sqrt{\log(q)})}).$$

We stress again that we have used various heuristic assumptions. The goal of the rest of this work is to modify the algorithm in such a way that we can indeed prove the claimed expected running time for large input classes. As already stated, we are however not able to establish the desired expected running time for all instances of the problem.

Tangent spaces and ramification

We make frequent use of homomorphisms between tangent spaces to address if morphisms of schemes over fields are unramified at rational points. For the convenience of the reader and because we could not find a suitable reference, we make some general remarks here.

Let k be a field.

Let X be a k -scheme of finite type and P a k -rational point of X . The k -vector spaces $\Omega_{X,P} \otimes_{\mathcal{O}_{X,P}} \kappa(P)$ and $\mathfrak{m}_P/\mathfrak{m}_P^2$ are canonically isomorphic; see [Har77, II, Proposition 8.7]. Either one of these spaces is called the *cotangent space* at P . The *Zariski tangent space* or simply *tangent space* of P in S is $T_P(X) := \text{Hom}_k(\mathfrak{m}_P/\mathfrak{m}_P^2, k)$. The formation of the tangent spaces behaves well under base change via a field extension over k . Let us note here that it is important that P is a k -rational point.

Let now X be a smooth k -scheme. Then the *tangent sheaf* of X is $\mathcal{T}_X := \Omega_X^\vee = \mathcal{H}om_{\mathcal{O}_X}(\Omega_X, \mathcal{O}_X)$. Let P be a k -rational point of X . The canonical homomorphism $\mathcal{T}_{X,P} \simeq \text{Hom}_{\mathcal{O}_{X,P}}(\Omega_{X,P}, \mathcal{O}_{X,P}) \longrightarrow \text{Hom}_{\mathcal{O}_{X,P}}(\Omega_{X,P}, \kappa(P)) \simeq \text{Hom}_k(\Omega_{X,P} \otimes_{\mathcal{O}_{X,P}} \kappa(P), \kappa(P)) \simeq T_P(X)$ induces a homomorphism of k -vector spaces

$$\mathcal{T}_{X,P} \otimes_k \kappa(P) \longrightarrow T_P(X).$$

As $\Omega_{X,P}$ is (by assumption) a free $\mathcal{O}_{X,P}$ -module, this homomorphism is an isomorphism. We denote the image of $t \in \mathcal{T}_{X,P}$ in $T_P(X)$ by $t(P)$.

Now let X and Y be arbitrary k -schemes of finite type, let $f : X \rightarrow Y$ be a morphism of k -schemes and let $P \in X$. Then the local ring of P in its fiber over $f(P)$ is $\mathcal{O}_{P,X}/f^\#(\mathfrak{m}_{Y,f(P)})\mathcal{O}_{X,P}$, and f is said to be *unramified* at P if this local ring is a finite and separable $\kappa(f(P))$ -algebra. If f is unramified at P then it is in particular quasi-finite at P , that is, P is isolated in its fiber.

Let now P be a k -rational point of X . Then f is unramified at P if and only if $f^\#(\mathfrak{m}_{Y,f(P)})$ generates the maximal ideal of $\mathcal{O}_{X,P}$. By Nakayama, this is the case if and only if the induced homomorphism between cotangent vector spaces $f^* : \mathfrak{m}_{f(P)}/\mathfrak{m}_{f(P)}^2 \rightarrow \mathfrak{m}_P/\mathfrak{m}_P^2$ is surjective. Therefore, f is unramified at P if and only if the induced homomorphism between tangent spaces $f_* : T_P(X) \rightarrow T_{f(P)}(Y)$ is injective.

2 The factor base

2.1 Some general thoughts

In [Die11] we first described the algorithm, which is rather elementary, and later presented the geometric background, involving in particular the role of the Weil restriction of the elliptic curve with respect to $\mathbb{F}_{q^n}|\mathbb{F}_q$.

This approach would also be possible here. However, we now present the geometric background together with the description of the algorithm. The main reason for this is that the conditions required for the definition of the factor base are quite involved but closely related to geometric considerations.

We first make some remarks on the definition of the factor base in [Die11].

Let an instance with a non-trivial extension of finite fields $\mathbb{F}_{q^n}|\mathbb{F}_q$ and an elliptic curve E over \mathbb{F}_{q^n} be given, where an affine part of E is given by a Weierstraß equation in x and y with degree 2 in x . Let $k := \mathbb{F}_q$ and $K := \mathbb{F}_{q^n}$.

Then in [Die11], the factor base is defined as follows:

We fix a covering $\varphi : E \rightarrow \mathbb{P}_K^1$ of degree 2 with $\varphi \circ [-1] = \varphi$ satisfying a certain condition (Condition 2.7 in [Die11]). Then the factor base \mathcal{F} is the set

$$\{P \in E(K) \mid \varphi(P) \in \mathbb{P}^1(k)\}. \quad (2)$$

Now there exists a unique automorphism α of \mathbb{P}_k^1 with $\varphi = \alpha \circ x|_E$. The factor base is then equal to

$$\{P \in E(K) \mid x|_E(P) \in \alpha^{-1}(\mathbb{P}^1(k))\}. \quad (3)$$

A geometric description of the definition of the factor base in (2) is as follows: We define V by the diagram

$$\begin{array}{ccc} V \hookrightarrow & \text{Res}_k^K(E) & \\ \downarrow & & \downarrow \text{Res}_k^K(\varphi) \\ \mathbb{P}_k^1 \hookrightarrow & \xrightarrow{\iota} & \text{Res}_k^K(\mathbb{P}_k^1). \end{array} \quad (4)$$

being Cartesian, where $\iota = \text{id}_{\odot}$. Then under the canonical isomorphism $E(K) \simeq \text{Res}_k^K(E)(k)$, the factor base \mathcal{F} corresponds to $V(k)$. Recall here that as the morphism $\varphi : E \rightarrow \mathbb{P}_K^1$ is a flat covering of degree 2, the morphism $\text{Res}_k^K(\varphi) : \text{Res}_k^K(E) \rightarrow \text{Res}_k^K(\mathbb{P}_K^1)$ and the induced morphism $V \rightarrow \mathbb{P}_k^1$ are flat coverings of degree 2^n .

From a geometric point of view, the equivalence of the two descriptions of the factor base via (2) and (3) follows from the commutativity of the diagram

$$\begin{array}{ccc} V \hookrightarrow & \text{Res}_k^K(E) & \\ \downarrow & & \downarrow \text{Res}_k^K(x|_E) \\ \mathbb{P}_k^1 \hookrightarrow & \xrightarrow{(\alpha^{-1})_{\odot}} & \text{Res}_k^K(\mathbb{P}_K^1) \\ & \searrow \iota & \downarrow \text{Res}_k^K(\alpha) \\ & & \text{Res}_k^K(\mathbb{P}_K^1). \end{array} \quad \text{Res}_k^K(\varphi)$$

Note here that by the universal property of the Weil restriction of \mathbb{P}_K^1 with respect to $K|k$, the immersions $\mathbb{P}_k^1 \hookrightarrow \text{Res}_k^K(\mathbb{P}_K^1)$ correspond exactly to the automorphisms of \mathbb{P}_K^1 (via $\alpha \mapsto \alpha_{\odot}$). Thus instead of varying the covering $\varphi : E \rightarrow \mathbb{P}_K^1$ in the construction of the factor base, we could also have varied the immersion of \mathbb{P}_K^1 into $\text{Res}_k^K(\mathbb{P}_K^1)$.

2.2 The preliminary definition of the factor base

We now give some geometric background on the definition of the factor base in the preliminary algorithm outlined in the introduction. We conclude this subsection with a wish list on the geometric objects related to the definition of the factor base. This then leads to a modification of the construction of the factor base which is described in the next subsection.

Let E_a be the ‘‘affine part’’ of E , that is, $E_a := x|_E^{-1}(\mathbb{A}_K^1)$. Furthermore, as already mentioned above, let m be some natural number $\leq n$ and let $d := \lceil \frac{n}{m} \rceil$ and $\delta := dm - n$.

In the preliminary algorithm in the introduction we defined the factor base as follows: We fix a d -dimensional k -vector subspace U of K , and we set

$$\mathcal{F} := \{P \in E_a(K) \mid x(P) \in U\}.$$

From a geometric point of view, we can describe this as follows: Let us fix a k -basis b_1, \dots, b_n of K and let us consider the K -morphism $\mathbb{A}_K^n = \text{Spec}(K[x_1, \dots, x_n]) \rightarrow \mathbb{A}_k^1 = \text{Spec}(K[x])$ given by $x \mapsto b_1x_1 + \dots + b_nx_n$.

With this morphism as universal morphism, \mathbb{A}_k^n is the Weil restriction of \mathbb{A}_K^1 with respect to $K|k$. (Without fixing the universal morphism, \mathbb{A}_k^n is isomorphic to $\text{Res}_k^K(\mathbb{A}_K^1)$ but not in a canonical way.)

Now we have the commutative diagram of isomorphisms of k -vector spaces

$$\begin{array}{ccc} K & \longrightarrow & k^n \\ \downarrow & & \downarrow \\ \mathbb{A}^1(K) & \longrightarrow & \mathbb{A}^n(k), \end{array} \quad (5)$$

where the upper morphism is induced by b_1, \dots, b_n , the lower morphism is given by the universal property of the Weil restriction $\text{Res}_k^K(\mathbb{A}_K^1)$ and the vertical morphisms are the canonical morphisms.

Via the above diagram, U defines a k -vector subspace of $\mathbb{A}^n(k)$. Now, there exists a group subvariety A of \mathbb{A}_k^n with $A(k) = U$ in $\mathbb{A}^n(k)$ (with A being isomorphic to $\mathbb{A}_k^{\dim(U)}$).

Defining $V_a \subseteq \text{Res}_k^K(E)$ by the diagram

$$\begin{array}{ccc} V_a & \hookrightarrow & \text{Res}_k^K(E_a) \\ \downarrow & & \downarrow \text{Res}_k^K(x|_{E_a}) \\ A & \hookrightarrow & \mathbb{A}_k^n, \end{array} \quad (6)$$

being Cartesian, the factor base corresponds to $V_a(k)$.

In the preliminary algorithm, we also have a $d - 1$ -dimensional k -vector subspace U' of U , defining a subset \mathcal{F}' of \mathcal{F} . By the considerations above, U' corresponds to a group subvariety A' of A . Analogously to the above, we now define V'_a . Then \mathcal{F}' corresponds to $V'_a(k)$. As the maps $V_a \rightarrow A$ and $V'_a \rightarrow A'$ are finite flat, every irreducibility component of V_a has dimension m and every irreducibility component of V'_a has dimension $m - 1$; see [Har77, III, Corollary 9.6].

Now, we would like that the following conditions on V_a and V'_a are satisfied:

1. The addition morphism $(\text{Res}_k^K(E))^m \rightarrow \text{Res}_k^K(E)$ induces a dominant morphism from every irreducibility component of $(V'_a)^\delta \times V_a^{m-\delta}$ to $\text{Res}_k^K(E)$.
2. There exists an (absolute) constant $c > 0$ such that $V_a(k)$ contains at least $c \cdot q^d$ points and $V'_a(k)$ contains at least $c \cdot q^{d-1}$ points.

Note that $\dim((V'_a)^\delta \times V_a^{m-\delta}) = n$ and therefore the statement in the first item implies that the morphism $(V'_a)^\delta \times V_a^{m-\delta} \rightarrow \text{Res}_k^K(E)$ is generically quasi-finite.

With a randomized algorithm it is straightforward to construct in an efficient way U and U' such that the second item is satisfied.

For $d = 1$, the morphism $(V'_a)^\delta \times V_a^{m-\delta} \rightarrow \text{Res}_k^K(E)$ is surjective and therefore if V'_a and V_a are irreducible, the first item is satisfied; see [Die11, Remark 4.21]. However, for $d > 1$, we cannot even give an example for which we can prove that the first condition holds. For this reason, we modify the definition of the factor base.

2.3 The essential modification

We now discuss the modification of the construction of the factor base.

We impose the following condition.

Condition 2.1 $0 \in \mathbb{P}_K^1$ is not a branch point of $x|_E : E \rightarrow \mathbb{P}_K^1$ and its preimage in E consists of two K -rational points.

Note that for $q^n \geq 16$, there exist at least 5 K -rational points on E , so there exists a point in $E(K)$ which is not a ramification point. In the algorithm, we first pass to a projectively equivalent elliptic curve, also given in Weierstraß form with the point at infinity being the neutral element, such that the condition is satisfied.

In the algorithm, we fix k -vector subspaces U_i of K of dimension $d - 1$ for $i = 1, \dots, \delta$ and of dimension d for $i = \delta + 1, \dots, m$ such that we have a decomposition

$$K = \bigoplus_{i=1}^m U_i. \quad (7)$$

With

$$\mathcal{F}_i := \{P \in E_a(K) \mid x(P) \in U_i - \{0\}\}, \quad (8)$$

we define the factor base as

$$\mathcal{F} := \bigcup_{i=1}^m \mathcal{F}_i. \quad (9)$$

Later, for $P \in E(K)$, we search for a relation of the form

$$P_1 + \dots + P_m = P$$

with $P_i \in \mathcal{F}_i$.

We now apply the geometric considerations of the previous subsection here. We obtain that decomposition (7) corresponds to a direct sum decomposition

$$\mathbb{A}_k^n = \bigoplus_{i=1}^m A_i \quad (10)$$

in the category of k -group varieties. (Decomposition (7) is obtained from (10) by taking k -valued points and applying the canonical isomorphisms.)

Similarly to above, we define $V_i \subseteq \text{Res}_k^K(E_a)$ via the diagram

$$\begin{array}{ccc} V_i & \hookrightarrow & \text{Res}_k^K(E_a) \\ \downarrow & & \downarrow \\ A_i & \hookrightarrow & \mathbb{A}_k^n \end{array}$$

being Cartesian. Note that the morphism $\text{Res}_k^K(E_a) \rightarrow \mathbb{A}_k^n$ is a flat covering of degree 2^n which is unramified at $0 \in \mathbb{A}_k^n$. As flatness and unramifiedness are stable under base change, the morphism $V_i \rightarrow A_i$ is a flat covering of degree 2^n which is unramified at $0 \in A_i$ too.

Let

$$a_m : \text{Res}_k^K(E)^m \rightarrow \text{Res}_k^K(E) \quad (11)$$

be the m -fold addition morphism and

$$a'_m : V_1 \times \cdots \times V_m \rightarrow \text{Res}_k^K(E) \quad (12)$$

be the restriction of a_m to $V_1 \times \cdots \times V_m$. Let P_0 be one of the two points of $E(K)$ which are mapped to 0 by $x|_E$.

Note that $\text{Res}_k^K((P_0)_\circledast) = 0$. In particular, $(P_0)_\circledast$ is a k -rational point of all V_i .

Proposition 2.2 *The morphism a'_m is unramified at $((P_0)_\circledast, \dots, (P_0)_\circledast)$.*

Remark 2.3 As unramifiedness is an open property, we obtain: a'_m is unramified in an open neighborhood of $((P_0)_\circledast, \dots, (P_0)_\circledast)$. Every irreducibility component of $V_1 \times \cdots \times V_m$ has dimension n (because we have a flat covering of $V_1 \times \cdots \times V_m$ to \mathbb{A}_k^n). Thus the morphism a'_m is dominant. If furthermore V_1, \dots, V_m are irreducible, a'_m is generically unramified.

Proof of Proposition 2.2. We wish to show that

$$(a'_m)_* : T_{((P_0)_\circledast, \dots, (P_0)_\circledast)}(V_1 \times \cdots \times V_m) \rightarrow T_{m \cdot (P_0)_\circledast}(\text{Res}_k^K(E))$$

is an isomorphism.

As the morphism $\text{Res}_k^K(x|_E)$ is unramified at $(P_0)_\otimes$, it induces an isomorphism of tangent spaces

$$T_{(P_0)_\otimes}(\text{Res}_k^K(E_a)) \xrightarrow{\sim} T_0(\mathbb{A}_k^n). \quad (13)$$

We have the decomposition $T_0(\mathbb{A}_k^n) = \bigoplus_{i=1}^m T_0(A_i)$ (corresponding to $K = \bigoplus_{i=1}^n U_i$). Under isomorphism (13), $T_{(P_0)_\otimes}(V_i)$ corresponds to $T_0(A_i)$. Therefore, we have the decomposition

$$T_{(P_0)_\otimes}(\text{Res}_k^K(E_a)) = \bigoplus_{i=1}^m T_{(P_0)_\otimes}(V_i). \quad (14)$$

By the next lemma, we have the commutative diagram

$$\begin{array}{ccc} T_{((P_0)_\otimes, \dots, (P_0)_\otimes)}(V_1 \times \dots \times V_m) \hookrightarrow T_{((P_0)_\otimes, \dots, (P_0)_\otimes)}(\text{Res}_k^K(E)^m) \xrightarrow{(a_m)_*} T_{(P_0)_\otimes}(\text{Res}_k^K(E)) \\ \downarrow \qquad \qquad \qquad \downarrow ((p_1)_*, \dots, (p_m)_*) \qquad \qquad \qquad \uparrow (\tau_{(m-1) \cdot (P_0)_\otimes})_* \\ T_{(P_0)_\otimes}(V_1) \times \dots \times T_{(P_0)_\otimes}(V_m) \hookrightarrow (T_{(P_0)_\otimes}(\text{Res}_k^K(E)))^m \longrightarrow T_{(P_0)_\otimes}(\text{Res}_k^K(E)), \end{array}$$

where $p_i : \text{Res}_k^K(E)^m \rightarrow \text{Res}_k^K(E)$ is the projection to the i^{th} coordinate and the map $T_{(P_0)_\otimes}(\text{Res}_k^K(E)) \rightarrow T_{(P_0)_\otimes}(\text{Res}_k^K(E))$ is the addition of the k -vector space $T_{(P_0)_\otimes}(\text{Res}_k^K(E))$.

Now because of decomposition (14), under the addition, $T_{(P_0)_\otimes}(V_1) \times \dots \times T_{(P_0)_\otimes}(V_m)$ is mapped bijectively to $T_{(P_0)_\otimes}(\text{Res}_k^K(E))$. This gives the desired statement. \square

Lemma 2.4 *Let k be a field.*

- a) *Let X_1, X_2 be two k -schemes, and let $P_1 \in X_1(k)$, $P_2 \in X_2(k)$. Let us assume that X_1 is smooth at P_1 and X_2 is smooth at P_2 . The points P_i give rise to closed immersions $\iota_i : X_i \rightarrow X_1 \times_k X_2$. Let $p_i : X_1 \times X_2 \rightarrow X_i$ be the canonical projections. Then the maps $(\iota_1)_* + (\iota_2)_* : T_{P_1}(X_1) \times T_{P_2}(X_2) \rightarrow T_{(P_1, P_2)}(X_1 \times X_2)$ and $((p_1)_*, (p_2)_*) : T_{(P_1, P_2)}(X_1 \times X_2) \rightarrow T_{P_1}(X_1) \times T_{P_2}(X_2)$ are isomorphisms of k -vector spaces which are inverse with respect to each other.*
- b) *Let A be an abelian variety over k with addition morphism $a : A \times A \rightarrow A$ be the addition morphism and neutral element O . Let $\iota_i : A \rightarrow A \times A$ be the two canonical immersions. Then the map $a_* \circ ((\iota_1)_* + (\iota_2)_*) : T_O(A) \times T_O(A) \rightarrow T_O(A)$ is the addition on the k -vector space $T_O(A)$.*
- c) *Let A be an abelian variety over k and $P \in A(k)$. Then we have a*

commutative diagram

$$\begin{array}{ccc} T_P(A \times A) & \xrightarrow{a_*} & T_{2P}(A) \\ ((p_1)_*, (p_2)_*) \downarrow & & \uparrow (\tau_P)_* \\ T_P(A) \times T_P(A) & \longrightarrow & T_P(A), \end{array}$$

where the lower map $T_P(A) \times T_P(A) \longrightarrow T_P(A)$ is the addition morphism on the k -vector space $T_P(A)$.

Proof. a) The k -linear map

$$T_{P_1}(X_1) \times T_{P_2}(X_2) \xrightarrow{(\iota_{X_1})_* + (\iota_{X_2})_*} T_{(P_1, P_2)}(X_1 \times X_2) \xrightarrow{((p_1)_*, (p_2)_*)} T_{P_1}(X_1) \times T_{P_2}(X_2)$$

is obviously the identity. As the dimensions of these k -vector spaces are the same, the two maps in a) are both isomorphisms.

b) We only have to check that the k -linear map $a_* \circ ((\iota_1)_* + (\iota_2)_*) : T_O(A) \times T_O(A) \longrightarrow T_O(A)$ agrees with the addition (which is also k -linear) on the first and second factor. But restricted to factor i , $a_* \circ ((\iota_1)_* + (\iota_2)_*)$ becomes $a_* \circ \iota_i$, which is the identity, just as is the addition when restricted to one of the factors.

c) Let us consider A as an abelian variety with P as neutral element, and let a_P be the addition law. Then $a_P = \tau_{-P} \circ a$. The commutativity of the diagram then follows from b). \square

2.4 Irreducibility

If the characteristic is odd, in order to complete the analysis of the relation generation procedure, we need that the V_i are irreducible. In this subsection, we give some theoretical background for the algorithmic construction of the V_i such that they are indeed irreducible.

All the statements in this subsection are valid except in the case that the characteristic is 2 and the j -invariant of E is 0, or, in other words, except if E is a supersingular elliptic curve in characteristic 2. So let us assume that it does not hold that the characteristic is 2 and $j = 0$.

Lemma 2.5 *Let $A \subseteq \mathbb{A}_k^n$ be a group subscheme, and let V_a be defined as in (6). If A contains an irreducible scheme containing 0 whose preimage in V_a is irreducible, then V_a is irreducible. Likewise, if A contains a geometrically irreducible scheme containing 0 whose preimage in V_a is geometrically irreducible, then V_a is geometrically irreducible.*

Proof. Assume that V_a is not irreducible, and let $V_a^{(1)}$ and $V_a^{(2)}$ be two irreducibility components of V_a . Let $\mathcal{A} \subseteq A$ be the étale locus of the flat

covering $V_a \rightarrow A$ and \mathcal{V}_a its preimage on V_a . By base change to \bar{k} one sees that by the first part of Condition 2.1 every point over 0 is contained in \mathcal{V}_a and thus 0 is contained in \mathcal{A} . In particular, \mathcal{A} is non-empty and thus a non-empty open part of A .

For $i = 1, 2$, the map $V_a^{(i)} \rightarrow A$ is surjective. (As the map $V_a^{(i)} \rightarrow A$ is flat and finite, by [Har77, Corollary 9.6], $V_a^{(i)}$ has the same dimension as A . The dimension of $V_a^{(i)}$ is equal to the dimension of its image. Thus the dimension of the image is equal to A . Therefore the map is dominant. As the map is finite, it is in particular closed, and therefore the image is equal to A .) Therefore $V_a^{(i)}$ contains a preimage of 0. Let $\mathcal{V}_a^{(i)}$ be the preimage of \mathcal{A} in $V_a^{(i)}$. Then $\mathcal{V}_a^{(i)}$ is a non-empty open part of $V_a^{(i)}$ which contains a preimage of 0.

As A is smooth so is \mathcal{A} , and as furthermore $\mathcal{V} \rightarrow \mathcal{A}$ is étale, \mathcal{V} is also smooth. It follows that $\mathcal{V}_a^{(1)}$ and $\mathcal{V}_a^{(2)}$ are disjoint.

Let now S be an irreducible subscheme of A as in the first claim of the lemma. As $V_a \rightarrow A$ is unramified at 0 and $0 \in S$ by assumption, $S \cap \mathcal{A}$ is a non-empty open part of S . It follows that the preimage of $S \cap \mathcal{A}$ is a non-empty open part of the preimage of S and thus also irreducible. Therefore it is contained in either $\mathcal{V}_a^{(1)}$ or $\mathcal{V}_a^{(2)}$. On the other hand, as it contains all preimages of 0, it has non-trivial intersection with both $\mathcal{V}_a^{(1)}$ and $\mathcal{V}_a^{(2)}$, a contradiction.

The second claim follows via base change to \bar{k} . □

In the algorithm, we first search for 1-dimensional k -vector subspaces T_i of K which correspond to group subvarieties B_i of \mathbb{A}_k^n whose preimages in $\text{Res}_k^K(E_a)$ with respect to $\text{Res}_k^K(x|_{E_a})$ are geometrically irreducible. Then we search for suitable k -vector subspaces U_i of K containing T_i . The U_i then correspond to group subvarieties A_i of \mathbb{A}_k^n which contain B_i , and it follows that their preimages V_i are geometrically irreducible.

Every 1-dimensional group subvariety of \mathbb{A}_k^n is the image of \mathbb{A}_k^1 under a homomorphism in the category of group varieties. As \mathbb{A}_k^n is the Weil restriction of \mathbb{A}_K^1 with respect to $K|k$, there is a canonical bijection between the set of K -morphisms from \mathbb{A}_K^1 to \mathbb{A}_K^1 and the set of k -morphisms from \mathbb{A}_k^1 to \mathbb{A}_k^n . This restricts to a bijection between the corresponding sets of homomorphisms in the category of group varieties. Similarly to diagram (5) we have a commutative diagram of isomorphisms of k -vector spaces

$$\begin{array}{ccc} \text{Hom}_{Gr}(\mathbb{A}_K^1, \mathbb{A}_K^1) & \xrightarrow{\alpha \rightarrow \alpha \otimes} & \text{Hom}_{Gr}(\mathbb{A}_k^1, \mathbb{A}_k^n) \\ \uparrow & & \uparrow \\ K & \longrightarrow & k^n, \end{array}$$

where the vertical isomorphisms are the canonical ones and the lower vertical

isomorphism is given by the basis b_1, \dots, b_n .

In this way, we obtain a bijection between K^*/k^* and the set of 1-dimensional group subvarieties of \mathbb{A}_k^n which is given by $\mu \mapsto (\alpha_a^{-1})_{\odot}(\mathbb{A}_k^1)$ with $\alpha_a := \mu x : \mathbb{A}_K^1 \rightarrow \mathbb{A}_K^1$.

Let some $\mu \in K^*$ be given, let α_a be the corresponding automorphism of \mathbb{A}_K^1 and α its extension to \mathbb{P}_K^1 . We set $\varphi := \alpha \circ x|_E$ and then $B_a := (\alpha^{-1})_{\odot}(\mathbb{A}_k^1)$. By the considerations at the beginning of this section, $W_a := x|_E^{-1}(B_a)$ is then the preimage of $\iota(\mathbb{A}_k^1)$ in $\text{Res}_k^K(E_a)$ with respect to the covering $\text{Res}_k^K(\varphi_a)$. This is very closely related to the situation studied in [Die11, Section 2.2] – the only difference is that here we use automorphisms of the group variety \mathbb{A}_K^1 instead of automorphisms of \mathbb{P}_K^1 and we restrict ourselves to the “affine parts”.

Lemma 2.6 *There are $> q^n - 4(n-1) \cdot q^{n/2}$ elements $\mu \in K^*$ such that with W_a as defined as above, W_a is geometrically irreducible.*

Proof. By assumption on k and E , the covering $x|_E : E \rightarrow \mathbb{P}^1$ has at least 2 branch points, thus there is at least one branch point not equal to $\infty \in \mathbb{P}_K^1$.

Let $\lambda_1, \dots, \lambda_s \in \mathbb{F}_{q^{6n}} - \{0\}$ with $s \in \{1, 2, 3, 4\}$ be the branch points of $x|_{E_a} : (E_a)_{\bar{k}} \rightarrow \mathbb{A}_k^1$. Let $\mu \in K^*$ and let $\alpha := \mu x$. Then the branch points of $\alpha \circ x|_{E_a} : E_a \rightarrow \mathbb{A}_K^1$ are $\mu\lambda_i$. Therefore Condition 2.7 from [Die11] is equivalent to the following condition.

Condition 2.7 There exists an $i = 1, \dots, s$ such that for $j = 1, \dots, n-1$, $(\mu\lambda_i)^{q^j} \notin \{\mu\lambda_1, \dots, \mu\lambda_s\}$.

As shown in [Die11, Proposition 4.9], if this condition is satisfied, W_a is geometrically irreducible.

We are interested in the probability that for $j = 1, \dots, n-1$, $(\mu\lambda_1)^{q^j} \notin \{\mu\lambda_1, \dots, \mu\lambda_s\}$.

The condition $(\mu\lambda_1)^{q^j} = \mu\lambda_k$ is equivalent to $\mu^{q^j-1} = \frac{\lambda_k}{\lambda_1^{q^j}}$. As the cardinality of the kernel of the map $K^* \rightarrow \bar{k}^*$, $a \mapsto a^{q^j-1}$ is $q^{\text{gcd}(j,n)} - 1$ (see next lemma), there are either no or exactly $q^{\text{gcd}(j,n)} - 1$ such elements μ .

The situation is now very similar to the situation in [Die11, Lemma 2.10]: In total there are at most $s \cdot \sum_{j=1}^{n-1} (q^{\text{gcd}(j,n)} - 1)$ elements μ for which the condition in the lemma is not satisfied.

Now a crude estimate is that $s \cdot \sum_{j=1}^{n-1} q^{\text{gcd}(j,n)-1} < s \cdot (n-1) \cdot q^{n/2}$. \square

Lemma 2.8 *Let q be a prime power and $m, n \in \mathbb{N}$. Then $q^m - 1 | q^n - 1$ if and only if $m | n$. Moreover $\text{gcd}(q^m - 1, q^n - 1) = q^{\text{gcd}(m,n)} - 1$.*

Proof. If $m|n$ then clearly $q^m - 1|q^n - 1$. So assume that $q^m - 1 \nmid q^n - 1$. For $a \in \mathbb{F}_{q^m}^*$ we have $a^{q^m - 1} = 1$ and by assumption also $a^{q^n - 1} = 1$. But this means that $a \in \mathbb{F}_{q^n}^*$. Thus \mathbb{F}_{q^m} is a subfield of \mathbb{F}_{q^n} and thus $m|n$.

For the second statement, consider the set $G := \{a \in \mathbb{F}_{q^n} \mid a^{q^m - 1} = 1\}$. On the one hand, as G is a subgroup of the cyclic group $\mathbb{F}_{q^m}^*$, it has $\gcd(q^m - 1, q^n - 1)$ elements. On the other hand, $G \cup \{0\}$ is a subfield of \mathbb{F}_{q^n} , and therefore there exists some $a|n$ with $\#G = q^a - 1$. The result now follows with the first statement. \square

2.5 The algorithm for the factor base

Let a field extension $K|k$ as above, an elliptic curve E/K , two points $A, B \in E(K)$ with $B \in \langle A \rangle$ as well as $m \in \mathbb{N}$ with $m \leq n$ be given, where $\#K \geq 16$. As always, let $d := \lceil \frac{n}{m} \rceil$ and $\delta := dm - n$.

We first choose – with a randomized algorithm – some point $P_0 \in E_a(K)$ which is not a ramification point of $x|_E$ and pass from E to its image under the automorphism of \mathbb{P}_K^2 given by $P = (X(P) : Y(P) : Z(P)) \mapsto (X(P) - x(P_0)Z(P) : Y(P) : Z(P))$. Let \tilde{E} be the resulting curve. This is again a curve in Weierstraß form, $x|_{\tilde{E}}$ is unramified above 0 and the preimage of 0 consists of two K -rational points. Clearly, this computation can be performed in an expected time which is polynomially bounded in $\log(q^n)$.

So let us now assume that there exists a K -rational point in $E(K)$ which is unramified under $x|_E$ and mapped to 0.

Given an instance as described, we wish to compute a decomposition $K = \bigoplus_{i=1}^m U_i$ with $\dim(U_i) = d - 1$ for $i = 1, \dots, \delta$ and $\dim(U_i) = d$ for $i = \delta + 1, \dots, m$ such that

- $\#\{P \in E_a(K) \mid x(P) \in U_i - \{0\}\} \geq \frac{1}{4}q^{\dim(U_i)}$;
- if $\text{char}(k)$ is odd: V_1, \dots, V_m are irreducible.

The factor base is then defined as described in Equations (8) and (9) above.

We now give an algorithm for the task just mentioned under the condition that $m \leq \frac{n}{2}$ and that $n \geq 12$ and $q \geq 16$. This is sufficient for the algorithm for Theorem 2.

Algorithm to compute a decomposition of K defining a suitable factor base

Input: A field extension $\mathbb{F}_{q^n}|\mathbb{F}_q$ with $n \geq 12$ and $q \geq 16$, an elliptic curve E/\mathbb{F}_{q^n} in Weierstraß form with respect to x and y such that there is a

K -rational point of E which is unramified under $x|_E$ and mapped to 0, two points $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$ and a natural number $m \leq \frac{n}{2}$.

Output: A decomposition $\mathbb{F}_{q^n} = \bigoplus_{i=1}^m U_i$ with $\dim(U_i) = d - 1$ for $i = 1, \dots, \delta$ and $\dim(U_i) = d$ for $i = \delta + 1, \dots, m$ such that the conditions mentioned above are satisfied.

1. If q is not a power of 2
 - For $i = 1, \dots, m$ do
 - Repeat
 - Choose $\mu_i \in \mathbb{F}_{q^n}^*$ uniformly at random.
 - Let $T_i \leftarrow \mu_i^{-1}(k) \subseteq \mathbb{F}_{q^n}$.
 - Until T_i is not contained in $\langle T_1, \dots, T_{i-1} \rangle$ and μ_i satisfies Condition 2.7.
 - If q is a power of 2, let $T_i \leftarrow \{0\}$ for $i = 1, \dots, m$.
2. Let $d \leftarrow \lceil \frac{n}{m} \rceil$ and $\delta \leftarrow dm - n$.
 - For $i = 1, \dots, m$ do
 - If $i \leq \delta$, let $e \leftarrow d - 1$, otherwise let $e \leftarrow d$.
 - Repeat
 - Compute an \mathbb{F}_q -vector subspace U_i of \mathbb{F}_{q^n} which is uniformly randomly chosen from the set of e -dimensional \mathbb{F}_q -vector subspaces of \mathbb{F}_{q^n} containing T_i with intersection $\{0\}$ with $U_1 + \dots + U_{i-1} + T_{i+1} + \dots + T_m$.
 - Until $\{E_a(\mathbb{F}_{q^n}) \mid x(P) \in U_i - \{0\}\}$ contains at least $\frac{1}{4} \cdot q^e$ elements.
3. Output U_1, \dots, U_m .

Remark 2.9 We represent \mathbb{F}_q -vector subspaces by bases over \mathbb{F}_q . Therefore the definition of T_i is computationally void; we inserted it only to be able to reason about T_i later.

Note here that at the end of each iteration of the For-loop in Step 2, we have a direct sum $U_1 \oplus \dots \oplus U_i \oplus T_{i+1} \oplus \dots \oplus T_m$ inside K , and for $j = 1, \dots, i$, U_j contains T_j . With the notations from above, T_i corresponds to a 1-dimensional group subscheme of A_i whose preimage in $\text{Res}_k^K(E)$ is geometrically irreducible by the arguments in Lemma 2.6. By Lemma 2.5, V_i is then also geometrically irreducible. Therefore an output of the algorithm defines a decomposition $K = \bigoplus_{i=1}^m U_i$ which satisfies the conditions given above.

We remark here that the algorithm itself is much more elementary than the geometric arguments.

The main result of this section is the following proposition.

Proposition 2.10 For $n \geq 12, m \leq \frac{n}{2}$ and $q \geq 16$, following the above algorithm, one can compute a decomposition of K with the desired properties in an expected time of $\mathcal{P}oly(n \cdot q^d) = \mathcal{P}oly(n \cdot q^{\frac{n}{m}})$.

Proof. We only have to consider the expected running time. For this, we discuss the steps of the algorithm.

Step 1 Let q be odd. We consider, for a particular iteration of the For-loop, the expected value of iterations of the Repeat-loop.

As $i \leq m$, the space $\langle T_1, \dots, T_{i-1} \rangle$ contains at most $q^{m-1} \leq q^{n/2}$ elements. By Lemma 2.6, there are $\geq q^n - 4(n-1) \cdot q^{n/2} - q^{n/2} \geq q^n - 4n \cdot q^{n/2}$ elements $\mu \in K^*$ which do not lie in $\langle T_1, \dots, T_{i-1} \rangle$ and which satisfy Condition 2.7. The probability that this is satisfied is therefore $\geq 1 - 4n \cdot \frac{1}{q^{n/2}} \geq 1 - \frac{4n}{2^{n/2}}$. For $n \geq 12$, which is the case by assumption, this is $\geq \frac{1}{4}$. The expected value of iterations of the Repeat-loop is therefore ≤ 4 . We can obtain an expected running time which is polynomially bounded in $n \cdot \log(q)$.

Step 2 In the Repeat loop, the space U_i can be computed in an expected time which is polynomially bounded in $n \cdot \log(q)$ by the next lemma. The counting of the set $\{E_a(\mathbb{F}_{q^n}) \mid x(P) \in U_i - \{0\}\}$ can be performed in a time which is polynomially bounded in q^d . The expected number of repetitions of the loop is ≤ 14 by Lemma 2.12 below. The expected running time of Step 2 is then polynomially bounded in q^d . \square

Lemma 2.11 Let S and T be two \mathbb{F}_q -vector subspaces of \mathbb{F}_q^n with $S \cap T = \{0\}$ and $S + T \subsetneq \mathbb{F}_q^n$, and let $e \in \mathbb{N}$ with $\dim(T) \leq e \leq n - \dim(S)$ be given. Then in an expected time which is polynomially bounded in $n \cdot \log(q)$ one can compute a \mathbb{F}_q -vector subspace U of \mathbb{F}_q^n which is uniformly randomly chosen from the set of e -dimensional \mathbb{F}_q -vector subspaces U of \mathbb{F}_q^n with $T \subseteq U$ and $S \cap U = \{0\}$.

Proof. Consider the following algorithm:

Input: Two \mathbb{F}_q -vector subspaces S and T of \mathbb{F}_q^n with $S \cap T = \{0\}$, and $e \in \mathbb{N}$ with $\dim(T) \leq e \leq n - \dim(S)$.

Output: An \mathbb{F}_q -vector subspace U satisfying the conditions given in the lemma.

Let $v_1, \dots, v_{\dim(T)}$ be the basis of T given with the input.

For $i = \dim(T) + 1, \dots, e$ do

Repeat

Choose $v_i \in \mathbb{F}_q^n$ uniformly at random.

Until $v_i \notin \langle v_1, \dots, v_{i-1} \rangle + S$.

Output $\langle v_1, \dots, v_e \rangle$.

Obviously the space $\langle v_1, \dots, v_e \rangle$ is uniformly randomly distributed in the set of e -dimensional subspaces U of \mathbb{F}_q^n with $T \subseteq U$ and $S \cap U = \{0\}$.

The claimed expected running time follows easily from the fact that the probability that v_i is in the $i - 1 + \dim(S)$ -dimensional vector subspace is $q^{(i-1)+\dim(S)-n} \leq \frac{1}{q}$. \square

Lemma 2.12 *For $q \geq 16$ and $n \geq 2$, elliptic curves E/\mathbb{F}_{q^n} in Weierstraß form, proper \mathbb{F}_q -vector subspaces S and T of \mathbb{F}_{q^n} with $S \cap T = \{0\}$ and $S + T \subsetneq \mathbb{F}_{q^n}$ and natural numbers $\dim(T) \leq e \leq n - \dim(S)$, the following holds:*

Let U be a uniformly randomly distributed vector subspace of \mathbb{F}_{q^n} of dimension e with $T \subseteq U$ and $S \cap U = \{0\}$. Then with a probability $\geq \frac{1}{14}$, $\#\{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in U - \{0\}\} \geq \frac{1}{4} \cdot q^e$.

Proof. Let first U be a uniformly randomly distributed e -dimensional \mathbb{F}_q -vector subspace of \mathbb{F}_{q^n} . Then as each point of $\mathbb{F}_{q^n} - \{0\}$ has the same probability of appearing in U , each point of $\mathbb{F}_{q^n} - \{0\}$ has a probability of

$$\frac{q^e - 1}{q^n - 1}$$

to appear in U .

Likewise, if S, T and e are as in the lemma and U is a uniformly randomly distributed e -dimensional vector subspace of \mathbb{F}_{q^n} with $T \subseteq U$ and $U \cap S = \{0\}$, each point of $\mathbb{F}_{q^n} - (S \cap T)$ has a probability of

$$\frac{q^e - q^{\dim(T)}}{q^n - q^{\dim(S)}} \geq \frac{1}{2} \cdot q^{e-n}$$

to appear in U .

Let

$$\begin{aligned} \mathcal{S} &:= \{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in S\}, \\ \mathcal{T} &:= \{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in T - \{0\}\}, \\ N &:= \#\{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in U - \{0\}\}. \end{aligned}$$

Then

$$\begin{aligned} \mathbb{E}[N] &= \#(E_a(\mathbb{F}_{q^n}) - (\mathcal{S} \cup \mathcal{T})) \cdot \frac{q^e - q^{\dim(T)}}{q^n - q^{\dim(S)}} + \#\mathcal{T} \\ &\geq (\#E_a(\mathbb{F}_{q^n}) - \#\mathcal{S}) \cdot \frac{q^e - q^{\dim(T)}}{q^n - q^{\dim(S)}} \\ &\geq (q^n - 2 \cdot q^{n/2} - 2 \cdot q^{\dim(S)}) \cdot \frac{1}{2} \cdot q^{e-n}, \end{aligned}$$

the last inequality by the Hasse-Weil bound.

As $q \geq 16$ and $n \geq 2$, $2 \cdot q^{n/2} \leq \frac{1}{8} \cdot q^n$ and $2 \cdot q^{\dim(S)} \leq 2 \cdot q^{n-1} \leq \frac{1}{8} \cdot q^n$. We obtain:

$$\mathbb{E}[N] \geq \frac{3}{8} \cdot q^n$$

On the other hand, $N \leq 2 \cdot q^e$. Altogether, we have

$$\frac{3}{8} \cdot q^e \leq \mathbb{E}[N] \leq \mathbb{P}[N < \frac{1}{4} \cdot q^e] \cdot \frac{1}{4} \cdot q^e + \mathbb{P}[N \geq \frac{1}{4} \cdot q^e] \cdot 2 \cdot q^e.$$

It follows that

$$\frac{3}{8} \leq (1 - \mathbb{P}[N \geq \frac{1}{4} \cdot q^e]) \cdot \frac{1}{4} + \mathbb{P}[N \geq \frac{1}{4} \cdot q^e] \cdot 2 = \frac{1}{4} + \frac{7}{4} \cdot \mathbb{P}[N \geq \frac{1}{4} \cdot q^e].$$

In other words:

$$\mathbb{P}[N \geq \frac{1}{4} \cdot q^e] \geq \frac{1}{14}$$

□

After suitable k -vector subspaces U_i of K have been computed, the sets $\mathcal{F}_i := \{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in U_i - \{0\}\}$ are enumerated and sorted for the elements in \mathcal{F}_i (such that given an element of \mathcal{F}_i one can easily find its number). The factor base is then $\mathcal{F} := \bigcup_{i=1}^m \mathcal{F}_i$.

The total expected running time for all these computations is polynomially bounded in $n \cdot q^d$.

3 The new decomposition algorithm

Just as in the successor [Die11] to this work, the relation generation relies on an algorithm to compute “decompositions”, and this algorithm is again based on solving systems of multivariate polynomials over \mathbb{F}_q . The definition of a “decomposition” is however different in this work from the previous one. Moreover, we do not use summation polynomials anymore, and more generally, we do not use the projection to a product of projective lines. The reason for this is that by avoiding the projection to projective lines, we can significantly improve the lower bound on the success probability of the relation generation algorithm. This improvement is crucial for the derivation of Theorem 2.

We start with some definitions.

As in the previous section, let q be a prime power, n a natural number, and let us set $k := \mathbb{F}_q$ and $K := \mathbb{F}_{q^n}$. Let E be an elliptic curve in Weierstraß form in x and y over K (with zero point at infinity). Let us fix a direct sum decomposition $K = \bigoplus_{i=1}^m U_i$ with $m \geq 2$ into k -vector subspaces. (In this whole section, we do not impose any conditions on $x|_E$ or the direct sum decomposition decomposition of K , except that the decomposition be non-trivial.) Let \mathcal{F}_i be defined as above. Finally, let $P \in E(K)$.

Definition 3.1 A tuple $(P_1, \dots, P_m) \in \mathcal{F}_1 \times \dots \times \mathcal{F}_m$ with $P_1 + \dots + P_m = P$ is called a *decomposition* of P with respect to the direct sum decomposition of K .

Let now A_i and V_i be defined as in the previous section. Then under the isomorphism $E(K) \simeq \text{Res}_k^K(E)(k)$, the set of decompositions of P corresponds to the set of tuples $(P_1, \dots, P_m) \in V_1(k) \times \dots \times V_m(k)$ with $\sum_i P_i = P_\odot$ and $\text{Res}_k^K(x)(P_i) \neq 0$. This is nothing but the set of k -rational points (P_1, \dots, P_m) of the fiber at P_\odot of the morphism

$$V_1 \times \dots \times V_m \longrightarrow \text{Res}_k^K(E)$$

induced by the addition morphism on $\text{Res}_k^K(E)$ with $\text{Res}_k^K(x)(P_i) \neq 0$ for all i .

This leads to the next definition.

Definition 3.2 A decomposition (P_1, \dots, P_m) of P is called *isolated* if it corresponds to an isolated (k -rational) point of the fiber $(V_1 \times \dots \times V_m)_{P_\odot}$ just considered.

The “new decomposition problem” is now the computational problem with the following specification: The input consists of a prime power q , a natural number n , an elliptic curve $E \subseteq \mathbb{P}_{\mathbb{F}_{q^n}}^2$ in Weierstraß form with respect to x and y and point at infinity as zero point, a direct sum decomposition $\mathbb{F}_{q^n} = \bigoplus_{i=1}^m U_i$ of \mathbb{F}_{q^n} into \mathbb{F}_q -vector subspaces with $m \geq 2$ and a point $P \in E(\mathbb{F}_{q^n})$. The output consists of a list of decompositions of P with respect to the direct sum decomposition of \mathbb{F}_{q^n} , containing all isolated decompositions.

A randomized algorithm for this problem is then called a “new decomposition algorithm”.

For the relation generation, the first crucial result is the following proposition. Furthermore, we need a non-trivial lower bound on the probability that a uniformly randomly chosen point in $E(\mathbb{F}_{q^n})$ has an isolated decomposition with respect to the chosen decomposition of K , given that certain conditions are satisfied. Such bounds are established in the next section.

Proposition 3.3

- a) *There exists an absolute constant $C > 0$ such that the number of isolated decompositions of some point $P \in E(\mathbb{F}_{q^n})$ is $\leq e^{C \cdot mn}$.*
- b) *There exists a new decomposition algorithm whose expected running time is polynomially bounded in $e^{mn} \cdot \log(q)$.*

The rest of this section is devoted to the proof of this proposition.

We now give some background information on the idea of the algorithm and address claim a). Computational aspects will be discussed later.

Let us fix an instance as specified in b), and as above, let $K|k$ be the extension of finite fields under consideration.

We first make the following assumption:

$$x(P) \notin \bigcup_{i=1}^m U_i$$

At the end of the section we will discuss an easy modification of the following arguments and the algorithm for the case that $x(P) \in \bigcup_{i=1}^m U_i$.

The main idea is to use the isomorphism $E(K) \simeq \text{Cl}^0(E)$. Let us use the following notation (cf. [Sil86]): For $P \in E(K)$, the prime divisor defined by P is denoted by (P) .

For points $P_1, \dots, P_m \in E(K)$, we have $\sum_i P_i = P$ if and only if there exists a function $g \in K(E)^*$ with $(g) = (P_1) + \dots + (P_m) + (-P) - (m+1) \cdot (O)$. Moreover, g is uniquely determined “up to a constant” by the points.

Let us assume that $P \neq O$. (For the case $P = O$, the following considerations can easily be modified.) Let $p_1 := 1, p_{2i} = x^i, p_{2i+1} := x^{i-1}y$ for $i \in \mathbb{N}$. Note that for $\ell \in \mathbb{N}$, $(p_1)_{|E}, \dots, (p_\ell)_{|E}$ is a basis of $L(\ell O)$. Let $L_\ell := \langle p_1, \dots, p_\ell \rangle \cap \{f \in k[x, y] \mid f(-P) = 0\}$, and let g_1, \dots, g_m be a basis of L_{m+1} such that g_1, \dots, g_{m-1} is a basis of L_m . Then $(g_1)_{|E}, \dots, (g_m)_{|E}$ is a basis of $L((m+1) \cdot (O) - (-P))$ and $(g_m)_{|E} \notin L(m \cdot O - (-P))$. Now (P_1, \dots, P_m) is a decomposition of P if and only if there exists a tuple $(\alpha_1, \dots, \alpha_{m-1}) \in K^{m-1}$ with

$$(g_m + \alpha_{m-1}g_{m-1} + \dots + \alpha_1g_1) = (P_1) + \dots + (P_m) + (-P) - (m+1) \cdot (O). \quad (15)$$

Furthermore, there exists at most one such tuple $(\alpha_1, \dots, \alpha_{m-1})$ in \bar{k}^{m-1} . The set of decompositions of P is thus in canonical bijection to the set of tuples $(\alpha_1, \dots, \alpha_{m-1}, P_1, \dots, P_m) \in K^{m-1} \times E_a^m(K)$ with $x(P_i) \in U_i - \{0\}$ such that (15) holds. Note that in any such tuple the points P_1, \dots, P_m, P are distinct. (Recall that $x(P) \notin \bigcup_{i=1}^m U_i$ by assumption).

Let

$$f_{(i)} := f(x_i, y_i) \in K[x_1, y_1, \dots, x_m, y_m]$$

for all $i = 1, \dots, m$; $V(f_{(1)}, \dots, f_{(m)})$ is then equal to E_a^m in $\text{Spec}(K[x_1, y_1, \dots, x_m, y_m])$.

Let

$$h := g_m + a_{m-1}g_{m-1} + \dots + a_1g_1 \in K[x, y, a_1, \dots, a_{m-1}]$$

and let

$$\begin{aligned} h_{(i)} &:= g_m(x_i, y_i) + a_{m-1}g_{m-1}(x_i, y_i) + \dots + a_1g_1(x_i, y_i) \\ &\in K[a_1, \dots, a_{m-1}, x_1, y_1, \dots, x_m, y_m] \end{aligned}$$

for all $i = 1, \dots, m$.

The set of decompositions of P is then in canonical bijection to the set of K -rational points $(\alpha_1, \dots, \alpha_{m-1}, P_1, \dots, P_m)$ of the scheme $V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)})$ in $\text{Spec}(K[a_1, \dots, a_{m-1}, x_1, y_1, \dots, x_m, y_m])$ with $x(P_i) \in U_i - \{0\}$ for all i . Note that we have the canonical projection

$$V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)}) \longrightarrow V(f_{(1)}, \dots, f_{(m)}) = E_a^m,$$

given on Z -valued points for any k -scheme Z by

$$(\alpha_1, \dots, \alpha_{m-1}, P_1, \dots, P_m) \mapsto (P_1, \dots, P_m).$$

It is natural to pass to the Weil restriction of $V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)})$ here. Let us first fix some notations: As in the previous section, let A_i be the subgroup scheme of \mathbb{A}_k^n corresponding to U_i . Let W be defined by the diagram

$$\begin{array}{ccc} W \hookrightarrow & \text{Res}_k^K(V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)})) & \\ \downarrow & \downarrow & \\ V_1 \times \dots \times V_m \hookrightarrow & (\text{Res}_k^K(E))^m & \\ \downarrow & \downarrow & \\ A_1 \times \dots \times A_m \hookrightarrow & (\text{Res}_k^K(\mathbb{A}_K^1))^m & \end{array}$$

being Cartesian. Now the k -rational points of W correspond exactly to the K -rational points $(\alpha_1, \dots, \alpha_{m-1}, P_1, \dots, P_m)$ of $V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)})$ with $P_i \in U_i$.

We now give an explicit description of W via a polynomial system. This description will serve as a basis for the algorithm.

As in the previous section, let b_1, \dots, b_n be a k -basis of K . Moreover, for $i = 1, \dots, m$, let $b_{i,1}, \dots, b_{i,\dim(U_i)}$ be a basis of U_i . The scheme $W \subseteq \text{Res}_k^K(V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)}))$ can be described explicitly as follows: Let the polynomials $h_{(i),j}$ and $f_{(i),j}$ for $i = 1, \dots, m$, $j = 1, \dots, n$ in $k[(a_{\ell,j'})_{\ell=1,\dots,m-1,j'=1,\dots,n}, ((x_{i',j'})_{j'=1,\dots,\dim(U_i)}, (y_{i',j'})_{j'=1,\dots,n})_{i'=1,\dots,m}]$ be defined by

$$h_{(i)}\left(\left(\sum_{j'=1}^n a_{\ell,j'} b_{j'}\right)_{\ell=1,\dots,m-1}, \sum_{j'=1}^{\dim(U_i)} x_{i,j'} b_{j'}, \sum_{j'=1}^n y_{i,j'} b_{j'}\right) = \sum_{j=1}^n h_{(i),j} b_j.$$

and

$$f_{(i)}\left(\sum_{j'=1}^{\dim(U_i)} x_{i,j'} b_{i,j'}, \sum_{j'=1}^n y_{i,j'} b_{j'}\right) = \sum_{j=1}^n f_{(i),j} b_j.$$

We have canonical isomorphisms

$$V_i \simeq V((f_{(i),j})_{j=1,\dots,n}) \subseteq \text{Spec}(k[x_{i,1}, \dots, x_{i,\dim(U_i)}, y_{i,1}, \dots, y_{i,n}])$$

and

$$W \simeq V((f_{(i),j})_{i=1,\dots,m,j=1,\dots,n}, (h_{(i),j})_{i=1,\dots,m,j=1,\dots,n}).$$

In particular, the k -rational points of $V((f_{(i),j})_{i=1,\dots,m,j=1,\dots,n}, (h_{(i),j})_{i=1,\dots,m,j=1,\dots,n})$ correspond in an obvious way to the K -rational points $(a_1, \dots, a_{m-1}, P_1, \dots, P_m)$ of $V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)})$ with $x(P_i) \in U_i$. Such points with $x(P_i) \in U_i - \{0\}$ then correspond to the decompositions of P .

We have a polynomial system in $2mn$ variables and $2mn$ equations.

We want to obtain a suitable polytope which contains the exponents in the support of the system.

Let us first consider the total degrees of $h_{(i),j}$ and $f_{(i),j}$ with respect to the three systems of variables $(a_{\ell,j'})_{\ell,j'}$, $(x_{i',j'})_{i',j'}$ and $(y_{i,j'})_{i,j'}$. Concerning the $h_{(i),j}$ we have: the total degree with respect to the $a_{\ell,j'}$ is ≤ 1 , the total degree with respect to the $x_{i',j'}$ is $\leq \lfloor \frac{m}{2} \rfloor$, the total degree with respect to the $y_{i',j'}$ is ≤ 1 . Concerning the $f_{(i),j}$ we have: The total degree with respect to the $x_{i',j'}$ is ≤ 3 , the total degree with respect to the $y_{i',j'}$ is ≤ 2 .

We now consider the $a_{\ell,j'}$ and the $y_{i',j'}$ as one system of variables and the $x_{i',j'}$ as another system of variables. So we have $2^{(m-1)\cdot n}$ variables in the first system and the total degrees of all polynomials under consideration with respect to this system are ≤ 2 . Furthermore, we have 2^n polynomials in the second system and the total degrees with respect to this system are $\leq \max(3, \lfloor \frac{m}{2} \rfloor)$.

Let $\Delta_\ell := \{\underline{x} \in \mathbb{R}_{\geq 0}^\ell \mid \sum_i x_i \leq 1\}$. With a suitable numeration, the exponents are contained in the polytope

$$\mathbf{P} := 2 \cdot \Delta_{(2m-1)\cdot n} \times \max(3, \lfloor \frac{m}{2} \rfloor) \cdot \Delta_n.$$

The toric variety $\mathcal{T}(\mathbf{P})$ defined by this polytope is $\mathbb{P}_k^{(2m-1)\cdot n} \times \mathbb{P}_k^n$. The volume of the polytope is $2^{(2m-1)\cdot n} \cdot \max(3, \lfloor \frac{m}{2} \rfloor)^n \cdot \frac{1}{((2m-1)\cdot n)!} \cdot \frac{1}{n!}$. The system of equations defines a system of sections of line bundles on $\mathcal{T}(\mathbf{P})$, and the degree of the 0-cycle in the Chow ring of $\mathcal{T}(\mathbf{P})$ defined by this system is

$$\begin{aligned} & 2^{(2m-1)\cdot n} \cdot \max(3, \lfloor \frac{m}{2} \rfloor)^n \cdot \binom{2mn}{n} \\ & < 2^{(2m-1)\cdot n} \cdot \max(3, \lfloor \frac{m}{2} \rfloor)^n \cdot 2^{2mn} < 2^{4mn} \cdot \max(3, \frac{m}{2})^n. \end{aligned}$$

It follows that the scheme defined by the sections on $\mathcal{T}(\mathbf{P})$ associated to the equations has at most $2^{4mn} \cdot \max(3, \frac{m}{2})^n$ \bar{k} -rational isolated

points. We have a natural embedding of \mathbb{A}_k^{2mn} into $\mathcal{T}(\mathbf{P})$, and the sections restrict to the equations under this embedding. Consequently, the scheme $V((f_{(i,j)})_{i=1,\dots,m,j=1,\dots,n}, (h_{(i,j)})_{i=1,\dots,m,j=1,\dots,n})$ has at most $2^{4mn} \cdot \max(3, \frac{m}{2})^n \in e^{\mathcal{O}(mn)}$ isolated \bar{k} -rational points.

Let us now turn to algorithmic aspects: It is straightforward to compute a system $(f_{(i,j)})_{i=1,\dots,m,j=1,\dots,n}, (h_{(i,j)})_{i=1,\dots,m,j=1,\dots,n}$ as above. We then use Rojas' algorithm ([Roj99]) for sparse polynomial systems to determine all isolated k -rational solutions. We apply the algorithm with the system of equations and the polytope \mathbf{P} defined above. The expected running time of the algorithm is then polynomially bounded in $e^{m \cdot n} \cdot \log(q)$. Explicitly, the expected running time of the algorithm depends on mixed volumes of various systems of polytopes, but all these polytopes are contained in the polytope \mathbf{P} , and therefore the mixed volumes are bounded by $2^{4mn} \cdot \max(3, \frac{m}{2})^n$.

We obtain the following intermediate result:

Lemma 3.4

- a) *A system $(f_{(i,j)})_{i=1,\dots,m,j=1,\dots,n}, (h_{(i,j)})_{i=1,\dots,m,j=1,\dots,n}$ as above has $e^{\mathcal{O}(mn)}$ isolated k -rational solutions.*
- b) *Given an instance of the “new decomposition problem”, one can compute a system $(f_{(i,j)})_{i=1,\dots,m,j=1,\dots,n}, (h_{(i,j)})_{i=1,\dots,m,j=1,\dots,n}$ as above and a list of k -rational solutions, containing all isolated k -rational solutions, in an expected time which is polynomially bounded in $e^{mn} \cdot \log(q)$.*

This is however not yet the statement we want to prove. Indeed, we still have to show that in this way we can obtain a list of decompositions of P which contains all isolated decompositions.

Let $P \in E_a(K)$.

We first study the geometric fibers of the morphism

$$V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)}) \longrightarrow V(f_{(1)}, \dots, f_{(m)}) = E_a^m.$$

Let $(P_1, \dots, P_m) \in E_a^m(\bar{k})$ such that the points P_1, \dots, P_m, P_\odot are distinct. Then there is at most one tuple $(\alpha_1, \dots, \alpha_{m-1}) \in \bar{k}^m$ such that (15) holds, depending on whether $\sum_i P_i = P_\odot$ or not.

Let now D be the closed subscheme of E_a^m given on Z -valued points for any k -scheme Z by

$$D(Z) = \{(P_1, \dots, P_m) \in E_a^m(Z) \mid \exists i \neq i' : P_i = P_{i'} \text{ or } \exists i : P_i = P\}.$$

Let $T := E_a^m - D$ and let S be the preimage of T in $V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)})$. Now the morphism $S \longrightarrow T$ induces an injection on the sets of geometric

points and its image consists of those points $(P_1, \dots, P_m) \in E_a^m(\bar{k})$ with $\sum_i P_i = P_\odot$.

We consider the restriction of the m -fold addition morphism $E^m \rightarrow E$ to T . Following the usual notation, let T_P be the fiber of this morphism at P . This is an open subscheme of a scheme isomorphic to E^{m-1} .

The morphism $S \rightarrow T$ induces a bijection $S(\bar{k}) \rightarrow T_P(\bar{k})$. As T_P is reduced, we have an induced morphism $S \rightarrow T_P$.

We now pass to Weil restrictions. Note first that we again have the addition $\text{Res}_k^K(E)^m \rightarrow \text{Res}_k^K(E)$ and the fiber $(\text{Res}_k^K(E)^m)_{P_\odot}$.

We have a canonical open embedding

$$\text{Res}_k^K(T) \subseteq \text{Res}_k^K(E_a^m) \simeq (\text{Res}_k^K(E_a))^m .$$

Note that under the canonical isomorphism $\text{Res}_k^K(E_a)^m(k) \simeq E_a^m(K)$, the points of $\text{Res}_k^K(T)(k)$ correspond to the points $(P_1, \dots, P_m) \in E^m(K)$ which are contained $T(K)$, that is, to points $(P_1, \dots, P_m) \in E^m(K)$ such that the points P_1, \dots, P_m, P are distinct.

Let

$$V^* := (V_1 \times \dots \times V_m) \cap \text{Res}_k^K(T) \subseteq (\text{Res}_k^K(E_a))^m$$

and let $V_{P_\odot}^*$ be the fiber of P_\odot under the restriction of the addition morphism $\text{Res}_k^K(E)^m \rightarrow \text{Res}_k^K(E)$ to V^* . We have

$$V_{P_\odot}^* = V^* \cap (\text{Res}_k^K(E_a)^m)_{P_\odot} = V^* \cap \text{Res}(T)_{P_\odot} . \quad (16)$$

Let now $P \notin \bigcup_{i=1}^m U_i$. The set of k -rational points of V^* contains all k -rational points of $\text{Res}_k^K(E_a)^m$ corresponding to decompositions of P . (There might be more points in $V^*(k)$ because there might be k -rational points (P_1, \dots, P_m) of V^* with $x_i(P) = 0$ for some $i \in \{1, \dots, m\}$.) As $\text{Res}_k^K(T)$ is open in $\text{Res}_k^K(E_a)^m$, a k -rational point of $V_1^* \times \dots \times V_m^*$ is open in $V_1^* \times \dots \times V_m^*$ if and only if it is open in $V_1 \times \dots \times V_m$. Therefore, the set of isolated k -rational points of V^* contains all k -rational points of $\text{Res}_k^K(E_a)^m$ corresponding to isolated decompositions of P .

Let W^* be the preimage of V^* in $\text{Res}_k^K(V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)}))$. Our goal is to show that the preimages of the isolated k -rational points of V^* are isolated k -rational points of W^* .

We have the Cartesian diagram

$$\begin{array}{ccc} \text{Res}_k^K(S) & \hookrightarrow & \text{Res}_k^K(V(f_{(1)}, \dots, f_{(m)}, h_{(1)}, \dots, h_{(m)})) \\ \downarrow & & \downarrow \\ \text{Res}_k^K(T) & \hookrightarrow & \text{Res}_k^K(E_a^m) \simeq \text{Res}_k^K(E_a)^m . \end{array}$$

Moreover, as the morphism $S \rightarrow T$ factors through the fiber T_P , by functoriality, the morphism $\text{Res}_k^K(S) \rightarrow \text{Res}_k^k(T)$ factors through the fiber $\text{Res}_k^K(T)_{P_\odot}$. We claim that we have an induced bijection between $\text{Res}_k^K(S)(\bar{k})$ and $\text{Res}_k^K(T)_{P_\odot}(\bar{k})$. For this, we can (obviously) apply the base change to $\bar{k}|k$. But over \bar{k} , the Weil restrictions become products of Galois twists of S respectively T , and we have already shown the claim for the factors of the product. The claim thus follows. By considering the Galois operation, we obtain that every algebraic field extension $\lambda|k$ we have a bijection between $\text{Res}_k^K(S)(\lambda)$ and $(\text{Res}_k^k(T))_{P_\odot}(\lambda)$. We are going to use this for $\lambda = k$.

As V^* is contained in $\text{Res}_k^K(T)$, W^* is contained in $\text{Res}_k^K(S)$, and we have a Cartesian diagram

$$\begin{array}{ccc} W^* & \hookrightarrow & \text{Res}_k^K(S) \\ \downarrow & & \downarrow \\ V^* & \hookrightarrow & \text{Res}_k^K(T) . \end{array}$$

The composition $W^* \rightarrow \text{Res}_k^K(T)$ (obviously) factors through V^* and – as we have just seen – it factors through $(\text{Res}_k^K(T))_{P_\odot}$. By (16) it factors through $V_{P_\odot}^*$. The morphism

$$W^* \rightarrow V_{P_\odot}^*$$

again induces a bijection

$$W^*(k) \rightarrow V_{P_\odot}^*(k) .$$

Let now (P_1, \dots, P_m) be an isolated k -rational point of V^* . This is a k -rational point of V^* which is open in V^* . Then the fiber over (P_1, \dots, P_m) in W^* is open in W^* , and it is a k -rational point. Therefore it is an isolated k -rational point of W^* and also of W .

We note again that for any isolated decomposition of P the corresponding point in $(V_1 \times \dots \times V_m)(k)$ lies in $V^*(k)$ and is isolated. Therefore every isolated decomposition of P defines an isolated k -rational point of W .

This finishes the proof of Proposition 3.3.

Modification for $x(P) \in \bigcup_{i=1}^m U_i$

We now discuss the modification for the case that $x(P) \in \bigcup_{i=1}^m U_i$. Except for finitely many instances, there exists a point $R \in E_a(K)$ with $x(R) \notin \bigcup_{i=1}^m U_i$ and $x(P - R) \notin \bigcup_{i=1}^m U_i$.

Let us fix such a point R and let $S := P - R$. Let $\tilde{L}_\ell := \langle p_1, \dots, p_\ell \rangle \cap \{f \in k[x, y] \mid f(-R) = 0, f(-S) = 0\}$. Let $\tilde{g}_1, \dots, \tilde{g}_m$ be a basis of \tilde{L}_{m+2}

such that $\tilde{g}_1, \dots, \tilde{g}_{m-1}$ is a basis of L_{m+1} . Now a tuple $(P_1, \dots, P_m) \in \mathcal{F}_1 \times \dots \times \mathcal{F}_m$ is a decomposition of P if and only if there exists a tuple $(\alpha_1, \dots, \alpha_{m-1}) \in K^{m-1}$ with

$$(\tilde{g}_m + \alpha_{m-1}\tilde{g}_{m-1} + \dots + \alpha_1\tilde{g}_1) = (P_1) + \dots + (P_m) + (-R) + (-S) - (m+1) \cdot (O).$$

Moreover, if such a tuple exists, it is unique. With this modifications, we obtain again the desired bound on the number of isolated decompositions. Moreover, by choosing a point $R \in E_a(K)$ uniformly randomly, we also obtain the algorithmic result. Note here that if P is in the factor base, we immediately have a relation, so we do not need to apply the decomposition algorithm. The bound on the number of isolated decompositions will however be used later.

4 Analysis and the final result

Let $K|k$ and E/K be as above and $m \leq \frac{n}{2}$. We assume that Condition 2.1 is satisfied. Furthermore, let a decomposition $K = \bigoplus_{i=1}^m U_i$ be given which satisfies the conditions in subsection 2.5. Moreover, let \mathcal{F}_i , A_i and V_i be defined as above.

As in subsection 2.3, let $P_0 \in E(K)$ be one of the two points in $E(K)$ lying over 0.

We want to obtain a lower bound on the number of points $P \in E(K)$ which have isolated decompositions. For this goal, we first want to derive an upper bound on the number of tuples $(P_1, \dots, P_m) \in \mathcal{F}_1 \times \dots \times \mathcal{F}_m$ which define non-isolated decompositions.

Let $a_m : \text{Res}_k^K(A) \rightarrow \text{Res}_k^K(E)$ be the m -fold addition morphism and $a'_m : V_1 \times \dots \times V_m \rightarrow \text{Res}_k^K(E)$ the restriction of a_m to $V_1 \times \dots \times V_m$.

We now consider a point $(P_1, \dots, P_m) \in E^m(K)$ with $x(P_i) \in U_i$ and let $P := \sum_{i=1}^m P_i$.

The morphism $a'_m : V_1 \times \dots \times V_m \rightarrow \text{Res}_k^K(E)$ is unramified at $((P_1)_\circ, \dots, (P_m)_\circ)$ if and only if $((P_1)_\circ, \dots, (P_m)_\circ)$ is an isolated reduced point of the fiber at P_\circ . We ask ourselves for which tuples (P_1, \dots, P_m) as above the morphism is ramified at $((P_1)_\circ, \dots, (P_m)_\circ)$. As already pointed out in the proof of Proposition 2.2 the morphism $a'_m : V_1 \times \dots \times V_m \rightarrow \text{Res}_k^K(E)$ is unramified at $((P_1)_\circ, \dots, (P_m)_\circ)$ if and only if the induced map on tangent spaces

$$(a'_m)_* : T_{((P_1)_\circ, \dots, (P_m)_\circ)}(V_1 \times \dots \times V_m) \rightarrow T_{P_\circ}(V_1 \times \dots \times V_m)$$

is injective.

We now consider points $(P_1, \dots, P_m) \in E(K)^m$ with $x(P_i) \in U_i$ for all i which satisfy the following condition.

Condition 4.1 The flat covering $x|_E$ is unramified at P_1, \dots, P_m .

This condition is equivalent to the condition that for every i , the flat covering $\text{Res}_k^K(E_a) \rightarrow \text{Res}_k^K(\mathbb{A}_k^1)$ is unramified at $(P_i)_\circ$. By base change, this implies that for every i , $V_i \rightarrow A_i$ is unramified (and thus étale) at $(P_i)_\circ$. Therefore, V_i is smooth at $(P_i)_\circ$ and we have an isomorphism of tangent spaces $T_{(P_i)_\circ}(V_i) \rightarrow T_{(x(P_i))_\circ}(A_i)$.

Let such a point (P_1, \dots, P_m) be given and let again $P := \sum_{i=1}^m P_i$. By Lemma 2.4 we have a commutative diagram

$$\begin{array}{ccc}
T_{((P_1)_\circ, \dots, (P_m)_\circ)}(V_1 \times \dots \times V_m) \xrightarrow{(a'_m)^*} T_{P_\circ}(\text{Res}_k^K(E)) & & \\
\downarrow (\tau_{(P_0-P_1)_\circ, \dots, (P_0-P_m)_\circ})^* & & \downarrow (\tau_{m \cdot (P_0-P)_\circ})^* \\
T_{((P_0)_\circ, \dots, (P_0)_\circ)}(V_1 \times \dots \times V_m) \xrightarrow{(a'_m)^*} T_{m(P_0)_\circ}(\text{Res}_k^k(E)) & & \\
\downarrow & & \uparrow (\tau_{(m-1) \cdot (P_0)_\circ})^* \\
T_{(P_0)_\circ}(V_1) \times \dots \times T_{(P_0)_\circ}(V_m) \longrightarrow T_{(P_0)_\circ}(\text{Res}_k^k(E)) & &
\end{array}$$

where the lower map is the addition on tangent spaces. Moreover, by the proof of Proposition 2.2, the two lower vertical homomorphisms are isomorphisms. Under the isomorphism $T_{(P_1)_\circ}(V_1) \times \dots \times T_{(P_m)_\circ}(V_m) \simeq T_{((P_1)_\circ, \dots, (P_m)_\circ)}(V_1 \times \dots \times V_m)$, the horizontal map on the left hand side is

$$\begin{aligned}
(\tau_{(P_0-P_1)_\circ})^* \times \dots \times (\tau_{(P_0-P_m)_\circ})^* : T_{(P_1)_\circ}(V_1) \times \dots \times T_{(P_m)_\circ}(V_m) &\longrightarrow \\
T_{(P_0)_\circ}(V_1) \times \dots \times T_{(P_0)_\circ}(V_m) . &
\end{aligned}$$

So the morphism $(a'_m)^*$ is unramified at $((P_1)_\circ, \dots, (P_m)_\circ)$ if and only if we have a direct sum decomposition

$$T_{(P_0)_\circ}(\text{Res}_k^K(E)) = \bigoplus_{i=1}^m (\tau_{(P_0-P_i)_\circ})^*(T_{(P_i)_\circ}(V_i)) . \quad (17)$$

We want to derive a condition under which we do have such a decomposition. For this, we make a case distinction into three cases: First q odd, second q even and $j \neq 0$, and third q even and $j = 0$.

The case that q is odd

We need some facts on tangent vectors of the projective line and the elliptic curve E . Here and in the following we assume that E_a is defined by a polynomial of the form $y^2 - f(x)$ (with f monic of degree 3).

Following our usual notation, let $\mathbb{P}_K^1 := \text{Proj}(K[X, Y])$. We set $x_{\mathbb{P}^1} := \frac{X}{Y} \in K(\mathbb{P}^1)$ (such that $K(\mathbb{P}^1) = K(x_{\mathbb{P}^1})$).

On \mathbb{P}_K^1 , we have the meromorphic cotangent vector field $dx_{\mathbb{P}^1}$ with divisor -2∞ and the corresponding tangent vector field $t_{x_{\mathbb{P}^1}}$. As an element of $\Gamma(\mathbb{P}_k^1, \mathcal{T}_{\mathbb{P}_k^1})$, the latter has divisor 2∞ .

Let R be the ramification divisor of the covering $x|_E$. Then the meromorphic cotangent vector field $dx|_E$ has divisor $-4(O) + R$, and we have the holomorphic cotangent vector field $\frac{dx|_E}{y|_E}$. This field is invariant under translation, that is, for every translation τ of E we have $\tau^*\left(\frac{dx|_E}{y|_E}\right) = \frac{dx|_E}{y|_E}$.

Dually, we have the meromorphic tangent vector field $t_{x|_E}$ with divisor $4(O) - R$ and the holomorphic tangent vector field $y|_E t_{x|_E}$, which corresponds to $\frac{dx|_E}{y|_E}$ under duality. Moreover, the field $y|_E t_{x|_E}$ is also invariant under translation, that is, for every translation τ of E , $\tau_*(y|_E t_{x|_E}) = y|_E t_{x|_E}$.

Following the notation fixed in the introduction, for some point $P \in E(K)$, we denote the tangent vector in $T_P(E)$ induced by $t_{x|_E}$ by $t_{x|_E}(P)$.

Let two K -rational points P_0 and P_1 of E which are not ramification points under $x|_E$ be given and let us consider the homomorphism $(\tau_{P_0-P_1})_* : T_{P_1}(E) \rightarrow T_{P_0}(E)$. This homomorphism given by $y(P_1)t_{x|_E}(P) \mapsto y(P_0)t_{x|_E}(P)$, that is,

$$t_{x|_E}(P) \mapsto \frac{y(P_0)}{y(P_1)} t_{x|_E}(P). \quad (18)$$

Let us fix a basis $(x_j)_j$ of K over k and bases $(x_{i,j})_j$ of the U_i as in the previous section. We have corresponding bases of the spaces $\Gamma(\mathbb{A}_k^n, \mathcal{T})$ and $\Gamma(A_i, \mathcal{T})$. We denote these bases by $(t_{x_j})_{j=1, \dots, n}$ for \mathbb{A}_k^n and $(t_{x_{i,j}})_{j=1, \dots, \dim(U_i)}$ for A_i . These fields define meromorphic vector fields $t_{(x_j)|_{\text{Res}_k^K(E_a)}}$ and $t_{(x_{i,j})|_{\text{Res}_k^K(E_a)}}$ on $\text{Res}(E_a)$ which are holomorphic and non-vanishing outside the ramification locus of $\text{Res}(x|_{E_a})$.

Let now $(P_1, \dots, P_m) \in E^m(K)$ with $x(P_i) \in U_i$ for all i satisfy Condition 4.1. We have a direct sum decomposition of $T_{P_\otimes}(\text{Res}_k^K(E))$ as in (17) if and only if the elements $(t_{(P_0-P_i)_\otimes})_*(t_{x_{i,j}}((P_i)_\otimes))$ for $i = 1, \dots, m, j = 1, \dots, \dim(U_i)$ form a k -basis of $T_{P_\otimes}(\text{Res}_k^K(E))$.

Let for $j = 0, \dots, n-1$ $f_j \in k[x_1, \dots, x_n, y_1, \dots, y_n]$ be defined by $f = \sum_{j=1}^n b_j \cdot f_j$. Let $u : (\text{Res}_k^K(E_a))_K \rightarrow E_a$ be the universal morphism. We have the isomorphism

$$(u, \sigma(u), \dots, \sigma^{n-1}(u)) : (\text{Res}_k^K(E_a))_K \xrightarrow{\sim} \prod_{s=0}^{n-1} \sigma_{K|k}^s(E_a)$$

corresponding to the isomorphism of K -algebras

$$\bigotimes_{s=0}^{n-1} K[x^{(s)}, y^{(s)}] / (\sigma_{K|k}^s(f)(x^{(s)}, y^{(s)})) \xrightarrow{\sim} K[x_1, \dots, x_n, y_1, \dots, y_n] / (f_1, \dots, f_n),$$

$$x^{(s)} \mapsto \sum_{j=1}^n \sigma_{K|k}^s(b_j) \cdot x_j, \quad y^{(s)} \mapsto \sum_{j=1}^n \sigma_{K|k}^s(b_j) \cdot y_j.$$

We have an induced isomorphism $\Gamma(\text{Res}_k^K(E_a)_K, \Omega) \simeq \bigoplus_{s=0}^{n-1} \Gamma(\sigma^s(E_a), \Omega)$ and, dually, an isomorphism $\Gamma(\text{Res}_k^K(E_a)_K, \mathcal{T}) \simeq \prod_{s=0}^{n-1} \Gamma(\sigma^s(E_a), \mathcal{T})$. Under these isomorphisms, $d(x^{(s)})|_{\sigma^s(E_a)}$ corresponds to $\sum_{j=1}^n \sigma_{K|k}^s(b_j) \cdot d(x_j)|_{\text{Res}_k^K(E_a)}$. Dually, $(t_{x_j})|_{\text{Res}_k^K(E_a)}$ corresponds to $(\sigma_{K|k}^s(b_j) \cdot (t_{(x^{(s)})|_{\sigma^s(E_a)}}))_{s=0, \dots, n-1}$.

On each of the factors of the product $\prod_{s=0}^{n-1} \sigma_{K|k}^s(E_a)$, we can apply the considerations above. We obtain that $(\tau_{(P_0-P_i)_\odot})_*((t_{x_j})|_{\text{Res}_k^K(E_a)}((P_i)_\odot))$ corresponds to

$$\begin{aligned} & (\sigma_{K|k}^s(b_j) \cdot \frac{y^{(s)}(P_0)}{y^{(s)}(P_i)} \cdot (t_{(x^{(s)})|_{\sigma^s(E_a)}}(\sigma^s(P_0))))_{s=0, \dots, n-1} \\ = & (\sigma_{K|k}^s(b_j) \cdot \frac{\sum_{\ell=1}^n \sigma_{K|k}^s(b_\ell) \cdot y_\ell((P_0)_\odot)}{\sum_{\ell=1}^n \sigma_{K|k}^s(b_\ell) \cdot y_\ell((P_i)_\odot)} \cdot (t_{(x^{(s)})|_{\sigma^s(E_a)}}(\sigma^s(P_0))))_{s=0, \dots, n-1}. \end{aligned}$$

This vector is of course Galois invariant. Let C be the inverse of the matrix $((\sigma^s(b_j))_{s=0, \dots, n-1, j=1, \dots, n})$; this is a matrix of the form $((\sigma^s(c_u))_{u=1, \dots, n, s=0, \dots, n-1})$. Going back, we have

$$\begin{aligned} & (\tau_{(P_0-P_i)_\odot})_*((t_{x_j}|_{\text{Res}_k^K(E_a)}((P_i)_\odot)) \\ = & \sum_{s=0}^{n-1} \sigma_{K|k}^s(b_j) \cdot \frac{\sum_{\ell=1}^n \sigma_{K|k}^s(b_\ell) \cdot y_\ell((P_0)_\odot)}{\sum_{\ell=1}^n \sigma_{K|k}^s(b_\ell) \cdot y_\ell((P_i)_\odot)} \cdot (\sum_{u=1}^n \sigma^s(c_u) (t_{(x_u)}|_{\text{Res}_k^K(E_a)}((P_0)_\odot))) \\ = & \sum_{u=1}^n \sum_{s=0}^{n-1} \sigma_{K|k}^s(b_j \cdot \frac{\sum_{\ell=1}^n b_\ell \cdot y_\ell((P_0)_\odot)}{\sum_{\ell=1}^n b_\ell \cdot y_\ell((P_i)_\odot)} \cdot c_u) \cdot (t_{(x_u)}|_{\text{Res}_k^K(E_a)}(P_0)_\odot). \end{aligned}$$

Let $c_{j,u} := b_j c_u \cdot (\sum_{\ell=1}^n b_\ell \cdot y_\ell(P_0)_\odot) \in K$. (Note here that these constants are independent of P_1, \dots, P_m .) Then

$$\begin{aligned} & (\tau_{(P_0-P_i)_\odot})_*((t_{x_j}|_{\text{Res}_k^K(E_a)}((P_i)_\odot)) \\ & = \sum_{u=1}^n \sum_{s=0}^{n-1} \sigma_{K|k}^s \left(\frac{c_{j,u}}{\sum_{\ell=1}^n b_\ell \cdot y_\ell((P_i)_\odot)} \right) \cdot t_{(x_u)}|_{\text{Res}_k^K(E_a)}((P_0)_\odot). \end{aligned}$$

Let $\iota_i : V_i \hookrightarrow \text{Res}_k^K(E)$ be the immersions. It follows that there are

constants $c_{i,j,u} \in K$ (again independent of P_1, \dots, P_m) with

$$\begin{aligned} & ((\tau_{(P_0-P_i)_\odot})_* \circ (l_i)_*)(t_{(x_{i,j})|V_i}((P_i)_\odot)) \\ &= \sum_{u=1}^n \sum_{s=0}^{n-1} \sigma_{K|k}^s \left(\frac{c_{i,j,u}}{\sum_{\ell=1}^n b_\ell \cdot y_{i,\ell}((P_i)_\odot)} \right) \cdot t_{(x_u)|\text{Res}_k^K(E_a)}((P_0)_\odot). \end{aligned}$$

Let

$$M_0 := \left(\left(\sum_{s=0}^{n-1} \sigma_{K|k}^s \left(\frac{c_{i,j,u}}{\sum_{\ell=1}^n b_\ell \cdot y_{i,\ell}} \right) \right) \right)_{u=1, \dots, n, (i=1, \dots, m, j=1, \dots, \dim(U_i))}$$

$$\in k((y_{i',j'})_{i'=1, \dots, m, j'=1, \dots, n})^{\{1, \dots, n\} \times (\cup_{i=1}^m \cup_{j=1}^{\dim(U_i)} \{(i,j)\})} \simeq k((y_{i',j'})_{i'=1, \dots, m, j'=1, \dots, n})^{n \times n}.$$

We have a direct sum decomposition of $T_0(\text{Res}_k^K(E))$ as in (17) if and only if the matrix $M_0((P_1)_\odot, \dots, (P_n)_\odot)$ is non-singular.

By Proposition 2.2 we know that this matrix is non-singular for $(P_1, \dots, P_n) = (P_0, \dots, P_0)$. In particular, the matrix M_0 itself is non-singular.

Let

$$M := \left(\prod_{i=1}^m \prod_{s=0}^{n-1} \sigma^s \left(\sum_{\ell=1}^n b_\ell \cdot y_{i,\ell} \right) \right) \cdot M_0.$$

Note that $\prod_{i=1}^m \prod_{s=0}^{n-1} \sigma^s \left(\sum_{\ell=1}^n b_\ell \cdot y_{i,\ell} \right)$ lies in $k[(y_{i',j'})_{i',j'}]$, and thus M is a matrix over $k[(y_{i',j'})_{i',j'}]$. Note further that for no $(P_1, \dots, P_m) \in E^m(K)$ with $x(P_i) \in U_i$ for all i satisfying Condition 4.1 and for no i, j , $\sum_{\ell=1}^n b_\ell \cdot y_{i,\ell}$ vanishes at $((P_1)_\odot, \dots, (P_n)_\odot)$.

Let $\mathbf{d} := \det(M) \in k[(y_{i',j'})_{i',j'}]$. Again for (P_1, \dots, P_m) as above, \mathbf{d} vanishes at $((P_1)_\odot, \dots, (P_m)_\odot)$ if and only if the homomorphism a'_m is unramified at $((P_1)_\odot, \dots, (P_m)_\odot)$.

We want to study the vanishing locus of \mathbf{d} on $V_1 \times \dots \times V_m$ and derive an upper bound on the number of k -rational points in the locus.

As said above, M is a matrix over $k[(y_{i',j'})_{i',j'}]$. The total degree of each entry of M is $mn - 1$. Therefore the total degree of $\mathbf{d} \in k[(y_{i',j'})_{i',j'}]$ is $mn^2 - n$. We know that \mathbf{d} does not vanish identically on $V_1 \times \dots \times V_m$ because it does not vanish at $((P_0)_\odot, \dots, (P_0)_\odot)$.

We want to prove:

Proposition 4.2 *The number of k -rational points in the locus of \mathbf{d} on $V_1 \times \dots \times V_m$ is $\leq n^5 \cdot 4^n \cdot q^{n-1}$.*

Let us first mention the following general fact.

Lemma 4.3 *Let F be a non-trivial polynomial in $\mathbb{F}_q[x_1, \dots, x_n]$ of total degree d . Then $V(F)$ contains at most $d \cdot q^{n-1}$ \mathbb{F}_q -rational points.*

Proof. As $\mathbb{F}_q[x_1, \dots, x_n]$ is factorial, we are immediately reduced to the case that F is irreducible. Let us wlog. furthermore assume that F is a non-trivial polynomial with respect to x_n . The content of F as a polynomial in $\mathbb{F}_q[x_1, \dots, x_{n-1}][x_n]$ is 1, or with other words, for every specialization of x_n , the resulting polynomial in $\mathbb{F}_q[x_1, \dots, x_{n-1}]$ is non-trivial. The result now follows by induction on n . \square

We will use resultants to eliminate the “ y -variables”. Let us consider the polynomials f , f_j and $f_{(i),j}$ as polynomials in the “ y -variables”. Now let

$$\begin{aligned} F &:= Z^2 \cdot f\left(x, \frac{Y}{Z}\right) \in K[x][Y, Z], \\ F_j &:= Z^2 \cdot f_j\left(x_1, \dots, x_n, \frac{Y_1}{Z}, \dots, \frac{Y_n}{Z}\right) \in k[x_1, \dots, x_n][Y_1, \dots, Y_n, Z], \\ F_{(i),j} &:= Z^2 \cdot f_{(i),j}\left(x_{i,1}, \dots, x_{i,\dim(U_i)}, \frac{Y_{i,1}}{Z}, \dots, \frac{Y_{i,n}}{Z}\right) \\ &\in k[x_{i,1}, \dots, x_{i,\dim(U_i)}][Y_{i,1}, \dots, Y_{i,n}, Z] \end{aligned}$$

be the homogeneous polynomials of degree 2 obtained by “homogenizing with respect to the y -variables to a homogeneous degree 2 polynomial”.

Let us consider $k[x][Y, Z]$, $k[x_1, \dots, x_n][Y_1, \dots, Y_n, Z]$ and $k[x_{i,1}, \dots, x_{i,\dim(U_i)}][Y_{i,1}, \dots, Y_{i,n}, Z]$ as graded rings in the second set of variables. Let \bar{V}_i be the scheme defined by $(F_{(i),j})_{j=1, \dots, n}$ in $\text{Proj}(k[x_{i,1}, \dots, x_{i,\dim(U_i)}][Y_{i,1}, \dots, Y_{i,n}, Z]) \simeq \mathbb{A}_k^{\dim(U_i)} \times \mathbb{P}_k^n$. We have a commutative diagram of canonical embeddings

$$\begin{array}{ccc} V_i^{\subset} & \xrightarrow{\quad} & \bar{V}_i \\ \downarrow & & \downarrow \\ \text{Res}_k^K(E) = V(f_1, \dots, f_n)^{\subset} & \xrightarrow{\quad} & V(F_1, \dots, F_n). \end{array}$$

Lemma 4.4 *For each i , the embedding $V_i \hookrightarrow \bar{V}_i$ is an isomorphism.*

Proof. We have to show that \bar{V}_i has no points “at infinity”, that is, the intersection $V(Z) \cap \bar{V}_i$ is trivial. We show in fact the stronger statement that $V(Z) \cap V(F_1, \dots, F_n)$ is trivial.

Let $f^{(s)} := \sigma_{K|k}^s(f)(x^{(s)}, y^{(s)})$ and let $F^{(s)} := F(x^{(s)}, Y^{(s)}, Z)$ for $s = 0, \dots, n-1$.

Let us consider the isomorphism of graded K -algebras

$$K[x_1, \dots, x_n][Y_1, \dots, Y_n, Z] \longrightarrow K[x^{(1)}, \dots, x^{(n)}][Y^{(1)}, \dots, Y^{(n)}, Z]$$

$$x^{(s)} \mapsto \sum_{j=1}^n \sigma_{K|k}^s(b_j) \cdot x_j, \quad Y^{(s)} \mapsto \sum_{j=1}^n \sigma_{K|k}^s(b_j) \cdot Y_j, \quad Z \mapsto Z.$$

We have the following commutative diagram over K :

$$\begin{array}{ccc}
\text{Spec}(K[x_1, \dots, x_n]) & \xrightarrow{\quad} & \text{Spec}(K[x^{(1)}, \dots, x^{(n)}]) \\
\times & & \times \\
\text{Spec}(K[y_1, \dots, y_n]) & & \text{Spec}(K[y^{(1)}, \dots, y^{(n)}]) \\
\uparrow & & \uparrow \\
\text{Res}_k^K(E) = V(f_1, \dots, f_n)_K & \longrightarrow & V(f^{(1)}, \dots, f^{(n)}) = \prod_{s=0}^{n-1} \sigma_{K|k}^s(E_a) \\
\downarrow & & \downarrow \\
V(F_1, \dots, F_n)_K & \longrightarrow & V(F^{(1)}, \dots, F^{(n)}) \\
\downarrow & & \downarrow \\
\text{Spec}(K[x_1, \dots, x_n]) & & \text{Spec}(K[x^{(1)}, \dots, x^{(n)}]) \\
\times & & \times \\
\text{Proj}(K[Y_1, \dots, Y_n, Z]) & \longrightarrow & \text{Proj}(K[Y^{(1)}, \dots, Y^{(n)}, Z])
\end{array}$$

Here the horizontal maps are induced by the isomorphism mentioned above. They are clearly isomorphisms. One can easily see that the middle morphism on the right is an isomorphism: We have $F(x^{(s)}, Y^{(s)}, 0) = (Y^{(s)})^2$, and the scheme $V((Y^{(1)})^2, \dots, (Y^{(n)})^2, Z)$ is trivial. Therefore the middle morphism on the left is an isomorphism too. \square

Let us fix the following notation: For $b \in \mathbb{N}_0$, $(P_0)_\odot^b$ is the point $((P_0)_\odot, \dots, (P_0)_\odot)$ with b entries. Let now for $\ell = 0, \dots, m$ the k -scheme \mathcal{V}_ℓ be the following subscheme of $V_1 \times \dots \times V_m$:

$$\mathcal{V}_\ell := V_1 \times \dots \times V_\ell \times (P_0)_\odot^{m-\ell}.$$

Furthermore, let $\mathbf{d}_\ell \in k[(y_{i',j'})_{i',=1, \dots, \ell, j'=1, \dots, n}]$ be the polynomial obtained from \mathbf{d} by evaluating $y_{i',j'}$ for $i' = \ell + 1, \dots, m$ and $j' = 1, \dots, n$ at $(P_0)_\odot$. Note that \mathbf{d}_ℓ does not vanish identically on \mathcal{V}_ℓ because it does not vanish at $(P_0)_\odot^\ell$.

We want to show by induction on ℓ :

$$\#(\mathcal{V}_\ell \cap V(\mathbf{d}))(k) \leq \ell \cdot n^4 \cdot 2^n \cdot (2q)^{(\sum_{i=1}^\ell \dim(V_i)) - 1}$$

The induction base is $\ell = 0$. As \mathbf{d} does not vanish at $(P_0)_{\odot}^{\ell}$, the set $\mathcal{V}_0 \cap V(\mathbf{d})$ is empty. Therefore the claim holds.

So let $\ell \leq m$ be given and let us assume that the claim holds for $\ell - 1$.

The set $(\mathcal{V}_{\ell} \cap V(\mathbf{d}))(k)$ can be divided into two disjoint parts: The first part consists of the points (P_1, \dots, P_{ℓ}) with $\mathbf{d}_{\ell-1}(P_1, \dots, P_{\ell-1}) = 0$. The second part consists of the points (P_1, \dots, P_{ℓ}) with $\mathbf{d}_{\ell-1}(P_1, \dots, P_{\ell-1}) \neq 0$.

We first consider points in the first part. As over each point of $\mathbb{A}^1(K)$ there lie at most 2 points of $E_a(K)$, over each point $\mathbb{A}^n(k)$ lie at most two points of $\text{Res}_k^K(E_a)$. In particular, over each point of $A_{\ell}(k)$ lie at most 2 points of $V_{\ell}(k)$. Because of this and because of the induction hypothesis, there are

$$\begin{aligned} &\leq (2q)^{\dim(V_{\ell})} \cdot (\ell - 1) \cdot n^4 \cdot 2^n \cdot (2q)^{(\sum_{i=1}^{\ell-1} \dim(V_i)) - 1} \\ &= (\ell - 1) \cdot n^4 \cdot 2^n \cdot (2q)^{(\sum_{i=1}^{\ell} \dim(V_i)) - 1} \end{aligned}$$

points in the first part.

We now consider points in the second part.

Let $(P_1, \dots, P_{\ell-1}) \in V_1(k) \times \dots \times V_{\ell-1}(k)$ with $\mathbf{d}_{\ell-1}(P_1, \dots, P_{\ell-1}) \neq 0$, that is, $\mathbf{d}_{\ell}(P_1, \dots, P_{\ell-1}, (P_0)_{\odot}) \neq 0$.

The polynomial $\mathbf{d}_{\ell}(P_1, \dots, P_{\ell-1})$ (a polynomial in $x_{\ell,1}, \dots, x_{\ell, \dim(U_{\ell})}, y_{\ell,1}, \dots, y_{\ell,n}$) is now non-trivial on V_{ℓ} . As – by the conditions we have imposed – V_{ℓ} is irreducible, $V_{\ell} \cap V(\mathbf{d}_{\ell}(P_1, \dots, P_{\ell-1}))$ has dimension $n - 1$ by Krull's Hauptidealsatz. Let $\bar{\mathbf{d}} \in k[Y_{\ell,1}, \dots, Y_{\ell,n}, Z] \subseteq k[x_{\ell,1}, \dots, x_{\ell, \dim(U_{\ell})}][Y_{\ell,1}, \dots, Y_{\ell,n}, Z]$ be the polynomial obtained by homogenizing $\mathbf{d}_{\ell}(P_1, \dots, P_{\ell-1})$ with respect to $y_{\ell,1}, \dots, y_{\ell,n}$. This is a homogeneous polynomial of degree $n^2 - \dim(U_{\ell})$ with respect to $Y_{\ell,1}, \dots, Y_{\ell,n}, Z$. As $V_{\ell} = \bar{V}_{\ell}$ (Lemma 4.4), we have

$$\begin{aligned} V_{\ell} \cap V(\mathbf{d}_{\ell}(P_1, \dots, P_{\ell-1})) &= \bar{V}_{\ell} \cap V(\bar{\mathbf{d}}) = \\ V(F_{(\ell),1}, \dots, F_{(\ell),n}, \bar{\mathbf{d}}) &\subseteq \mathbb{A}_k^n \times \text{Proj}(k[Y_{\ell,1}, \dots, Y_{\ell, \dim(U_{\ell})}]). \end{aligned}$$

Let $\text{Res} = \text{Res}(G_1, \dots, G_{n+1})$ be the dense multivariate resultant for $n+1$ homogeneous variables and polynomials of (homogeneous) degrees $2, \dots, 2, n^2 - \dim(U_i)$. Here, the G_1, \dots, G_{n+1} are independent generic polynomials, that is, polynomials with algebraically independent coefficients.

By taking the resultant of the system $F_{(\ell),1}, \dots, F_{(\ell),n}, \bar{\mathbf{d}}$ with respect to $Y_{\ell,1}, \dots, Y_{\ell,n}, Z$, we obtain $\text{Res}(F_{(\ell),1}, \dots, F_{(\ell),n}, \bar{\mathbf{d}})$, which is a non-trivial polynomial in $k[x_{\ell,1}, \dots, x_{\ell, \dim(V_{\ell})}]$. For some point $Q \in \mathbb{A}^n(\bar{k})$, the resultant $\text{Res}(F_{(\ell),1}, \dots, F_{(\ell),n}, \bar{\mathbf{d}})$ vanishes at Q if and only if there is a \bar{k} -rational point in $\bar{V}_{\ell} \cap V(\bar{\mathbf{d}}) = V_{\ell} \cap V(\mathbf{d}_{\ell}(P_1, \dots, P_{\ell-1}))$ over Q .

We want to determine the multidegree of this polynomial. First we consider the degrees of Res as a polynomial on the coefficients of the G_j .

By [GKZ94, subsection 3.3 A] we have: For $j = 1, \dots, n$, Res is a homogeneous polynomial of degree $(n^2 - \dim(U_j)) \cdot 2^{n-1} \leq n^2 \cdot 2^{n-1}$ in the coefficients of G_j . Furthermore, Res is a homogeneous polynomial of degree 2^n in the coefficients of G_{n+1} . Moreover, $F_{(\ell),j}$ has degree ≤ 3 in the $x_{\ell,j'}$ ($j' = 1, \dots, \dim(U_j)$) and $\bar{\mathbf{d}}$ obviously has degree 0 in the $x_{\ell,j'}$.

Therefore, $\text{Res}(F_{\ell,1}, \dots, F_{\ell,n}, \bar{\mathbf{d}})$ has degree $\leq n \cdot 3 \cdot n^2 \cdot 2^{n-1}$ in each of the variables $x_{\ell,j'}$. Its total degree is thus $\leq 3n^4 \cdot 2^{n-1}$. By Lemma 4.3, the locus the resultant contains at most $3n^4 \cdot 2^{n-1} \cdot q^{\dim(V_\ell)-1}$ k -rational points. As over each of these points lie at most two k -rational points of $V_\ell \cap V(\mathbf{d}(P_1, \dots, P_{\ell-1}))$, there are at most $6n^4 \cdot 2^{n-1} \cdot q^{\dim(V_\ell)-1} \cdot (2q)^{\sum_{i=1}^{\ell-1} \dim(U_i)} = 6n^4 \cdot 2^{n-1} \cdot 2^{\sum_{i=1}^{\ell-1} \dim(V_i)} \cdot q^{\sum_{i=1}^{\ell-1} \dim(V_i)-1} < n^4 \cdot 2^n \cdot (2q)^{(\sum_{i=1}^{\ell-1} \dim(V_i))-1}$ points in the second part of the set $(\mathcal{V}_a \cap V(\mathbf{d}))(k)$. (We use that $\dim(V_\ell) = \dim(U_\ell) \geq 2$ as $m \leq \frac{n}{2}$.)

Altogether, there are $\leq \ell \cdot n^4 \cdot 2^n \cdot (2q)^{(\sum_{i=1}^{\ell-1} \dim(V_i))-1}$ points in $(\mathcal{V}_\ell \cap V(\mathbf{d}))(k)$.

This concludes the proof of Proposition 4.2. \square

There are at most 3 K -rational ramification points in E_a under $x|_{E_a}$. Therefore, there are at most $3 \cdot 2^{m-1} \cdot q^{n-1} < 2^n \cdot q^{n-1}$ points in $\mathcal{F}_1 \times \dots \times \mathcal{F}_m$ which do not satisfy Condition 4.1. Proposition 4.2 gives therefore:

Proposition 4.5 *The number of points in $\mathcal{F}_1 \times \dots \times \mathcal{F}_m$ which do not define isolated decompositions is $\leq (n^5 \cdot 4^n + 2^n) \cdot q^{n-1}$. For $5^n \leq q$ and n large enough, this is $\leq \frac{1}{4} \cdot q^n$.*

The case that q is even and $j \neq 0$

Let $a \in K$ be the ramification point of E_a over \mathbb{A}_K^1 . Then $\frac{dx|_E}{x|_{E-a}}$ is a holomorphic differential on E .

Proceeding just as above, we obtain a non-trivial polynomial $\mathbf{d} \in k[(x_{i,j})_{i=1, \dots, m, j=1, \dots, \dim(U_i)}]$ of total degree $n^3 - n$ such that for points $(P_1, \dots, P_m) \in E(K)^m$ with $x(P_i) \in U_i$ satisfying Condition 4.1, $((P_1)_\circ, \dots, (P_m)_\circ)$ is an isolated reduced point in its fiber if and only if $\mathbf{d}((P_1)_\circ, \dots, (P_m)_\circ) = 0$.

There are $\leq (n^3 - n) \cdot q^{n-1}$ points in the locus of \mathbf{d} on \mathbb{A}_k^n . Moreover, over each point of $\mathbb{A}^1(K)$ are at most two points of $E(K)$. The number of points $(P_1, \dots, P_m) \in V_1(k) \times \dots \times V_m(k)$ satisfying Condition 4.1 which are not isolated reduced points in their fiber is therefore $\leq 2^m \cdot (n^3 - n) \cdot q^{n-1}$. Therefore:

Proposition 4.6 *The number of points in $\mathcal{F}_1 \times \dots \times \mathcal{F}_m$ which do not define isolated decompositions is $\leq 2^m \cdot n^3 \cdot q^{n-1}$. For $m \leq \lceil \sqrt{\log_2(q)} \rceil$, $n^4 \leq q$ and n large enough this is $\leq \frac{1}{4} \cdot q^n$.*

The case that q is even and $j = 0$

In this case, $dx|_E$ itself is a holomorphic differential on E . It follows that $((\tau_{(P_0-P_i)_\otimes})_* \circ (\iota_i)_*)(t_{(x_{i,j})|_{V_i}}) = (\iota_i)_*(t_{(x_{i,j})|_{V_i}})$. Therefore, the morphism $a'_m : V_1 \times \cdots \times V_m \rightarrow \text{Res}_k^K(E)$ is unramified everywhere and we obtain:

Proposition 4.7 *Every decomposition is isolated.*

The final result of the analysis

All in all, we have:

Proposition 4.8 *For*

- $5^n \leq q$
or
- $q = 2$ and $n^4 \leq q$ and $m \leq \lceil \sqrt{\log(q)} \rceil$

the following holds: The probability that a uniformly randomly chosen point of $E(K)$ has an isolated decomposition is in $\frac{1}{e^{\Omega(mn)}}$.

Proof. It follows from Propositions 4.5, 4.6 and 4.7 that, under the conditions on n, q and m and for n large enough, the probability that a uniformly randomly chosen element in $\mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ defines an isolated decomposition is $\geq \frac{1}{2}$. The result then follows with Proposition 3.3 a). \square

Derivation of Theorem 2

Finally, we show how Theorem 2 follows.

As already mentioned in the outline in the introduction, the basic structure of the index calculus algorithm is the same as that in the previous work. So we only discuss the constructions surrounding the definition of the factor base and briefly the relation generation and the linear algebra part, using the results proved above. For an overview over the complete algorithm, we refer to subsection 2.3 of our previous work.

The input to the index calculus algorithm consists of a field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, an elliptic curve E/\mathbb{F}_{q^n} and points $A, B \in E(\mathbb{F}_{q^n})$ and $B \in \langle A \rangle$ such that $5^n \leq q$ or $q = 2$ and $n^5 \leq q$. The following considerations hold for q and n large enough. An algorithm for all instances under consideration running in the claimed expected time can be obtained by running the index calculus algorithm “in parallel” with a brute force computation.

Similarly to the “preliminary algorithm”, we set $m := \min\{\lceil \sqrt{\log_2(q)} \rceil, \lfloor \frac{n}{2} \rfloor\}$. (We need $m \leq \frac{n}{2}$ in order to be able to apply the algorithm for the construction of a decomposition of K in subsection 2.5.) So $d = \lceil \frac{n}{m} \rceil \leq \max(\frac{n}{\sqrt{\log_2(q)}} + 1, 3)$ and thus $\mathcal{Poly}(q^d) \subseteq e^{\mathcal{O}(\max(\log(q), n \cdot \sqrt{\log(q)}))}$.

The expected running time of the construction of the decomposition of K and the definition of the factor base is in $\mathcal{Poly}(n \cdot q^d)$ which is also in $e^{\mathcal{O}(\max(\log(q), n \cdot \sqrt{\log(q)}))}$ (see Proposition 2.10). We have a new decomposition algorithm with an expected running time of $\mathcal{Poly}(e^{mn} \cdot \log(q)) \subseteq e^{\mathcal{O}(n \cdot \sqrt{\log(q)})}$ and a success probability of $e^{\frac{1}{\Omega(mn)}}$ (see Propositions 3.3 and 4.8). Therefore the expected running time of the relation generation part is in $\mathcal{Poly}(e^{n \cdot \sqrt{\log(q)}} \cdot m \cdot q^d) \subseteq e^{\mathcal{O}(\max(\log(q), n \cdot \sqrt{\log(q)}))}$. The linear algebra part has an expected running time of $\mathcal{Poly}(m \cdot q^d) \subseteq e^{\mathcal{O}(\max(\log(q), n \cdot \sqrt{\log(q)}))}$.

In total, we obtain an expected running time of

$$e^{\mathcal{O}(\max(\log(q), n \cdot \sqrt{\log(q)}))}.$$

We recall again that we only considered instances with $5^n \leq q$ or $q = 2$ and $n^5 \leq q$ so far. The derivation of Theorem 2 is now analogous to the derivation of Theorem 1 from [Die11, Proposition 2.11].

For the first result, we make the following case distinction: If $8^n \leq q$, we apply the index calculus algorithm directly. If $8^n > q$, we set $a := \lceil \frac{3n}{\log_2(q)} \rceil$ and apply the index calculus algorithm to the curve $E_{\mathbb{F}_{q^{an}}}$, the field extension $\mathbb{F}_{q^{an}}|\mathbb{F}_{q^a}$ and A, B . Now $5^n \leq 8^n \leq q^a$, thus we can conclude that the index calculus algorithm runs in an expected running time of $e^{\mathcal{O}(\max(\log(q^a), n \cdot \sqrt{\log(q^a)}))} = e^{\mathcal{O}(n^{3/2})}$.

The derivation of the second result is analogous. We only consider instances with q even now. For $n^5 \leq q$ we apply the index calculus algorithm directly. For $n^5 \geq q$, we set $a := \lceil \frac{5 \log_2(n)}{\log_2(q)} \rceil$ and proceed as above. We obtain an expected running time of $e^{\mathcal{O}(n \cdot \sqrt{\log(n)})}$.

A final remark is that, as pointed out in [Die11], the field extension $\mathbb{F}_{q^n}|\mathbb{F}_q$ need not be given with the input data. Rather one can apply the above algorithm with all possible field extensions “in parallel”.

References

- [Die11] C. Diem. On the discrete logarithm problem in elliptic curves. *Compos. Math.*, 147, 2011.
- [GKZ94] I. Gelfand, M. Kapranov, and A. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Birkäuser, 1994.
- [Har77] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, 1977.
- [Roj99] J.M. Rojas. Solving degenerate sparse polynomial systems faster. *J. Symbolic Computation*, 28:155–186, 1999.
- [Sil86] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.