On the discrete logarithm problem in elliptic curves II

Claus Diem

September 23, 2013

Abstract

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

For sequences of prime powers $(q_i)_{i\in\mathbb{N}}$ and natural numbers $(n_i)_{i\in\mathbb{N}}$ with $n_i \longrightarrow \infty$ and $\frac{n_i}{\log(q_i)^2} \longrightarrow 0$ for $i \longrightarrow \infty$, 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 [Die11b] we have shown that there exist sequences of finite fields over which the elliptic curve discrete logarithm problem can be solved in subexponential expected time in the bit-length of the input.

In this work, we strengthen the results from [Die11b]. We show that for larger classes of ground fields the problem can still be solved in subexponential expected time.

Recall that the main result from [Die11b] is as follows.

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 with $n_i \longrightarrow \infty$ and $\frac{n_i}{\log(q_i)} \longrightarrow 0$ for $i \longrightarrow \infty$, 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 $(q_i^{n_i})^{o(1)}$.

The main result of this work is the following stronger theorem.

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*

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

Note here that

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

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 $q_i \longrightarrow \infty$ and $\frac{n_i}{\log(q_i)^2} \longrightarrow 0$ for $i \longrightarrow \infty$ be given. Then 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 $\beta \in [\frac{1}{2}, 1]$ 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

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

   can be solved in an expected time of

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

   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: 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 $b^{1-\gamma} \cdot (n \log(q))^\gamma \geq n \cdot \log(q)^{1/2}$.

Additionally, except if $q = 2$, we have $\log(q) \geq \log(q)^\beta \geq \frac{1}{b} \cdot n$ and thus $n \cdot \log(q)^{1/2} \geq \frac{1}{b} \cdot n^{3/2}$.

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: $n^{\frac{3}{2}} \leq b^{\frac{3}{2}-\gamma} \cdot (n \cdot \log(q))^\gamma$.

As an application of Theorem 2 we now consider the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields of a fixed characteristic p. We first remark that Theorem 2 does not give a non-trivial result if q is set to p and n is set to the absolute extension degree of the ground field. We therefore consider a factorization of the absolute extension degree in the form mn, that is, we write the cardinality of the ground field in the form p^{mn}. We can then regard both m and n as the extension degree. One sees that it is advantageous to regard n as the extension degree provided that $n \leq m$ and m as the extension degree otherwise. In this way one obtains:

Theorem 3 *Let p be a fixed prime number. Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{p^{mn}}$ can be solved in an expected time of*

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

Here we have

$$\max(m,\, n,\, \min(m\cdot n^{1/2},\, n\cdot m^{1/2})) = \begin{cases} m & \text{for } n \le m^{1/2} \\ n\cdot m^{1/2} & \text{for } m^{1/2} \le n \le m \\ m\cdot n^{1/2} & \text{for } n^{1/2} \le m \le n \\ n & \text{for } m \le n^{1/2}\ . \end{cases}$$

For any fixed prime number p, Theorem 3 gives the following results:

4. Let $(m_i)_{i\in\mathbb{N}}$ and $(n_i)_{i\in\mathbb{N}}$ with $m_i, n_i \longrightarrow \infty$ for $i \longrightarrow \infty$. Then the discrete logarithm problem in the groups of rational points of elliptic curves over the finite fields $\mathbb{F}_{p^{m_i n_i}}$ can be solved in an expected time of

$$(p^{m_i n_i})^{o(1)}\ .$$

5. Let $\alpha \ge 3$ and $a, b > 0$. Then the discrete logarithm problem in the groups of rational points of elliptic curves over finite fields $\mathbb{F}_{p^{mn}}$ with

$$m \le a\cdot n^{\alpha} \quad \text{and} \quad n \le b\cdot m^{\alpha}$$

can be solved in an expected time of

$$e^{\mathcal{O}((\log(p^{mn})^{1-\frac{1}{1+\alpha}})}\ .$$

Just as Statement 1 above, Statement 4 is again immediate.

So we consider the last statement. Let $\alpha \ge 3$. Note first that $1-\frac{1}{1+\alpha} = \frac{\alpha}{1+\alpha} = \frac{1}{1+\frac{1}{\alpha}}$. We have $m^{1+\frac{1}{\alpha}} \le a^{1/\alpha}\cdot mn$ and therefore $m \le a^{\frac{1}{1+\alpha}}\cdot(mn)^{\frac{\alpha}{1+\alpha}}$. Similarly, $n \le a^{\frac{1}{1+\alpha}}\cdot(mn)^{\frac{\alpha}{1+\alpha}}$. Moreover, $1-\frac{1}{1+\alpha} \ge \frac{3}{4}$. Thus if $n \le m$, then $n\cdot m^{1/2} \le (mn)^{3/4} \le (mn)^{\frac{\alpha}{1+\alpha}}$. Analogously, if $m \le n$, then $m\cdot n^{1/2} \le (mn)^{\frac{\alpha}{1+\alpha}}$.

Some more information on the results

We give here some more information on the precise meaning of the statements above and similar statements throughout this article.

First, we choose some concrete representation of the "abstract input instances" (elliptic curves E over finite fields K and elements $a, b \in E(K)$

with $a \in \langle b \rangle$) by bit-strings. Every "abstract instance" is then given by at least one and finitely many bit-strings. Concretely, we represent elliptic curves by Weierstraß equations, as usual. We also choose some (uniform) randomized model of computation with an appropriate complexity measure, for example a usual randomized RAM model with logarithmic cost function or a randomized Turing model.

For a function f from some infinite countable set S to $\mathbb{R}_{>0}$, we define the sets $\mathcal{O}(f)$, $\tilde{\mathcal{O}}$, $o(f)$ and $\mathcal{P}oly(f)$ as usual (for the latter see also [Die11b]). We note here that it makes no difference if S is a subset of $\mathbb{N}$ or not.

The assertion in Theorem 1 is then as follows: There exists a machine in the given model and a constant $C > 0$ such that, if the machine is applied to an instance of the elliptic curve discrete logarithm problem over a field $\mathbb{F}_{q^n}$, the expected running time is bounded by $e^{C \cdot \max(\log(q), n^2)}$. The assertions in Theorem 2 and Theorem 3 are analogous. We stress that the expected value concerns only the internal choices of the computation; there is no averaging over input classes.

Statement 1 means the following: Let $(q_i)_{i \in \mathbb{N}}$ and $(n_i)_{i \in \mathbb{N}}$ be given as indicated. Then there exists a randomized machine and a sequence $(\epsilon_i)_{i \in \mathbb{N}}$ with $\epsilon_i \longrightarrow 0$ for $i \longrightarrow \infty$ such that the expected running time of the machine if applied to an instance over $\mathbb{F}_{q_i^{n_i}}$ is bounded by $(q_i^{n_i})^{\epsilon_i}$. Statement 4 is again analogous.

As usual, throughout this article we use the word "algorithm" instead of "machine". Also as usual, we use the word "algorithm" in an informal way when we outline a computation.

Outline

Just as the algorithm in [Die11b], the algorithm for Theorem 2 is based on the usual index calculus or relation generation and linear method. Again 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. Otherwise the index calculus algorithm in [Die11b] is not changed.

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 $c > 0$. In even characteristic the situation is more fortunate and we can complete the analysis if $n^c \leq q$ for a suitable constant $c > 0$. This does however not lead to an improvement over the result in Theorem 3 applied to fields of even characteristic.

The index calculus algorithm we employ has the same overall structure as the one in [Die11b] (see subsection 2.3 of that work). The changes we perform concern the definition of the factor base (Steps 4 and 5 of that algorithm) and the relation generation (Step 6), where a new decomposition algorithm is employed. Because the overall structure of the algorithm stays the same, we will focus on the parts of the index algorithm which need to be changed.

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 fourth and 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. Additionally, in an appendix we correct two misprints in our previous work [Die11b].

Throughout the article we use the same notation as in our previous work, with the exception that we now denote an affine defining polynomial for the elliptic curve by $f(x, y)$.

The application of the scalar restriction functor, that is, the formation of Weil restrictions, is crucial in this work. Furthermore, many arguments in this work are based on the consideration of tangent spaces. Background information on these topics is given at the end of this section. The reader should also be familiar with the first two sections of [Die11b]. Additionally, we assume some familiarity with toric geometry and its application to solving polynomial systems as given in [Ful93], [CLO05] and in particular in [Roj99].

A preliminary algorithm

The algorithm follows the usual "index calculus" strategy: After some preliminary computations to determine the group structure, we fix a so-called factor base, generate relations and finally solve the discrete logarithm problem via linear algebra.

Just as in [Die11b], 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.

The definition of the factor base and the relation generation are as follows:

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

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

$$P_1 + \cdots + P_m = P$$

with $P_i \in \mathcal{F}'$ for $i = 1, \ldots, \delta$ and $P_i \in \mathcal{F}$ for $i = \delta+1, \ldots, m$. 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 via summation polynomials.

Recall that the $(m+1)^{\text{th}}$ summation polynomial with respect to the covering $x_{|E} : E \longrightarrow \mathbb{P}^1_{\mathbb{F}_{q^n}}$ is an irreducible multihomogeneous polynomial $S_{m+1} \in \mathbb{F}_{q^n}[X_1, Y_1, \ldots, X_{m+1}, Y_{m+1}]$ such that for $P_1, \ldots, P_{m+1} \in E(\overline{\mathbb{F}}_q)$, $P_1 + \cdots + P_{m+1} = 0$ if and only if $s_{m+1}(x_{|E}(P_1), \ldots, x_{|E}(P_{m+1})) = 0$; see Proposition 2.1 and Section 3 of [Die11b]. The $(m+1)^{\text{th}}$ affine summation polynomial with respect to $x_{|E}$ is the dehomogenization of this polynomial with respect to $Y_1, \ldots, Y_m$. This is a polynomial $s_{m+1}(x_1, \ldots, x_{m+1}) \in \mathbb{F}_{q^n}[x_1, \ldots, x_{m+1}]$.

We expand the variables (or coordinates) $x_1, \ldots, x_m$ over $\mathbb{F}_q$ with respect to the basis. Then for $i = 1, \ldots, \delta$ and $i = \delta+1, \ldots, m$ we restrict the resulting systems of coordinates to U' and U, respectively. In this way the polynomial $s_{m+1}(x_1, \ldots, x_m, x(P))$ gives rise to a system of n polynomials in n variables. The polynomial $s_{m+1}(x_1, \ldots, x_m, x(P))$ has degree 2^{m-1} in each variable and therefore total degree at most $m \cdot 2^{m-1}$. Therefore each polynomial in the system has degree at most $m \cdot 2^{m-1}$. It follows that "with multiplicities" the system has at most $(m \cdot 2^{m-1})^n = m^n \cdot 2^{(m-1)\cdot n}$ isolated solutions over $\mathbb{F}_q$. Here by an *isolated solution* we mean an isolated point of the scheme defined by the system. (This can be seen by intersection theory in $\mathbb{P}^n_{\mathbb{F}_q}$, similarly to statement a) in Proposition 2.5 of [Die11b].)

Now, with an algorithm by M. Rojas ([Roj99]), one can compute a list of solutions of the system over $\mathbb{F}_q$ containing all isolated solutions over $\mathbb{F}_q$ in an expected time of $\mathcal{P}oly(m^n \cdot 2^{n\cdot(m-1)} \cdot \log(q)) = \mathcal{P}oly(e^{mn} \cdot \log(q))$.

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

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

for the relation generation part.

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

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

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

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.

Weil restrictions and the scalar restriction functor

Let us recall the definition of the scalar restriction functor with respect to a finite field extension.

Let $K|k$ be a finite field extension. Now let X be a quasi-projective K-scheme of finite type. Then a representing object of the contravariant functor $Z \mapsto \mathrm{Hom}_K(Z \times_k K, X)$ from the category of k-schemes to the category of sets is called the Weil restriction of X with respect to $K|k$. We denote the representing k-scheme by $\mathrm{Res}_k^K(X)$; as usual we also fix a corresponding natural transformation. A reformulation of the definition is: The Weil restriction of X with respect to $K|k$ is a k-scheme $\mathrm{Res}_k^K(X)$ together with a morphism $u : \mathrm{Res}_k^K(X)_K = \mathrm{Res}_k^K(X) \times_k K \longrightarrow X$ satisfying the following universal property: For any k-scheme and any K-morphism $\alpha : Z_K = Z \times_k K \longrightarrow X$ there exists a unique k-morphism $\beta : Z \longrightarrow \mathrm{Res}_k^K(X)$ with $\alpha = u \circ \beta_K$. We denote β by $\alpha_\circledcirc$. Now, the formation of the

Weil restriction defines a functor from the category of quasi-projective K-schemes to the category of quasi-projective k-schemes; this functor is called the *scalar restriction functor*. Furthermore, if X a group scheme, so is the Weil restriction in an obvious way.

In this work, we very often use Weil restrictions of the affine line $\mathbb{A}^1_K = \mathrm{Spec}(K[x])$. Note here that $\mathrm{Res}^K_k(\mathbb{A}^1_K)(k) \simeq \mathbb{A}^1(K) = K$. One sees easily the following: Let $b_1, \ldots, b_n$ be a k-basis of K. Then $\mathbb{A}^n_k = \mathrm{Spec}(k[x_1, \ldots, x_n])$ together with the universal morphism $\mathbb{A}^n_K \longrightarrow \mathbb{A}^1_K$, given on Z-valued points for any K-scheme Z by $P \mapsto x_1(P)b_1 + \cdots + x_n(P)b_n$, is a Weil restriction of $\mathbb{A}^1_k$ with respect to $K|k$ (as a group variety). The choice of a k-basis of K of course corresponds to choosing a k-homomorphism $K \approx k^n$.

We would like to have an explicit and canonical description of the Weil restriction of $\mathbb{A}^1_k$ which does not depend on the choice of a basis. For this, let us define for any finite dimensional k-vector space V the polynomial algebra $k[V]$ in the usual way:

$$k[V] := \bigoplus_{i=0}^{\infty} V^{\overset{\otimes}{sym}\, i}$$

For some finite dimensional k-vector space V, let

$$\mathbb{A}_k[V] := \mathrm{Spec}(k[V^\vee]) \ ,$$

where $V^\vee$ is the dual space of V. Now for any k-algebra A, we have $\mathbb{A}_k[V](A) \simeq \mathrm{Hom}_k(V^\vee, A) \simeq A \otimes_k V$ in a natural way. Now, $A \otimes_k V$ is a k-vector space and therefore in particular an abelian group. We obtain in this way a commutative group structure on $\mathbb{A}_k[V]$. Clearly, $\mathbb{A}_k[V](k)$ is isomorphic to $(V, +)$ itself. The association $V \mapsto \mathbb{A}_k[V]$ gives rise to a covariant functor from the category of finite dimensional vector spaces over k to the category of affine group varieties over k. Here, an injective homomorphism $U \longrightarrow V$ gives a closed embedding $\mathbb{A}_k[U] \longrightarrow \mathbb{A}_k[V]$, and in particular for a vector subspace U of V, $\mathbb{A}_k[U]$ is a group subvariety of $\mathbb{A}_k[V]$.

As a special case of the preceding we have natural isomorphisms $\mathbb{A}_k[K](A) \simeq A \otimes_k K$ for any k-algebra A. Therefore $\mathbb{A}_k[K]$ is in a natural way a Weil restriction of $\mathbb{A}^1_K$ with respect to $K|k$. We remark that the universal morphism $u : \mathbb{A}_k[K] \times_k K \longrightarrow \mathbb{A}^1_K$ is given as follows: $\mathbb{A}_k[K] \times_k K$ is the affine scheme defined by the K-algebra $k[K^\vee] \otimes_k K \simeq \bigoplus_{i=0}^{\infty} (K^\vee)^{\otimes_{sym} i} \otimes_k K$, and the universal morphism corresponds to a homogeneous element of degree 1 in the algebra, that is, to an element of $K^\vee \otimes_k K$. This vector space is naturally isomorphic to the vector space of endomorphisms of K as a vector space over k. The universal morphism is the element of $K^\vee \otimes_k K$ corresponding to the identity in this space.

We also use Weil restrictions with respect to flat coverings, that is, finite and flat morphisms. For this and also for other aspects of the scalar restriction functor we refer to subsection 4.1 of [Die11b].

Tangent spaces and ramification

We make frequent use of homomorphisms between tangent spaces to address whether 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. Denoting by $\kappa(P)$ the residue field at P, we have a canonical isomorphism $k \simeq \kappa(P)$. We use the latter notation if we regard k as an $\mathcal{O}_{X,P}$-algebra.

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 X is $T_P(X) := \mathrm{Hom}_k(\mathfrak{m}_P/\mathfrak{m}_P^2, k)$. 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. A special case which is of importance in this work is: For any finite dimensional k-vector space V we have a canonical isomorphism $T_0(\mathbb{A}_k[V]) \simeq V$; we identify these spaces.

Let now X be a smooth k-scheme. Then the *tangent sheaf* of X is $\mathcal{T}_X := \Omega_X^\vee = \mathcal{H}om_{\mathcal{O}_X}(\Omega_X, \mathcal{O}_X)$. The canonical homomorphism

$$\begin{aligned} \mathcal{T}_{X,P} &\simeq \mathrm{Hom}_{\mathcal{O}_{X,P}}(\Omega_{X,P}, \mathcal{O}_{X,P}) \longrightarrow \mathrm{Hom}_{\mathcal{O}_{X,P}}(\Omega_{X,P}, \kappa(P)) \\ &\simeq \mathrm{Hom}_k(\Omega_{X,P} \otimes_{\mathcal{O}_{X,P}} \kappa(P), k) \simeq T_P(X) \end{aligned}$$

induces a homomorphism of k-vector spaces

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

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 $f : X \longrightarrow Y$ be a morphism of k-schemes and let $P \in X$. Then the local ring of P in its fiber over $f(P)$ is $\mathcal{O}_{X,P}/f^\#(\mathfrak{m}_{Y,f(P)})\mathcal{O}_{X,P}$, 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's lemma, this is the case if and only if the induced homomorphism between cotangent spaces $f^* : \mathfrak{m}_{f(P)}/\mathfrak{m}_{f(P)}^2 \longrightarrow \mathfrak{m}_P/\mathfrak{m}_P^2$ is surjective. Therefore, f is unramified at P if and only if the induced homomorphism between tangent spaces $f_* : T_P(X) \longrightarrow T_{f(P)}(Y)$ is injective.

Acknowledgment

I thank the anonymous referee for carefully reading this work and for suggestions. I thank Tian Song for pointing out the misprints in [Die11b] I mention in the appendix.

2 The factor base

2.1 Some general thoughts

In [Die11b] 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 [Die11b].

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 [Die11b], the factor base is defined as follows:

We fix a covering $\varphi : E \longrightarrow \mathbb{P}^1_K$ of degree 2 with $\varphi \circ [-1] = \varphi$ satisfying a certain condition (Condition 2.7 in [Die11b]). Then the factor base $\mathcal{F}$ is the set

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

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

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

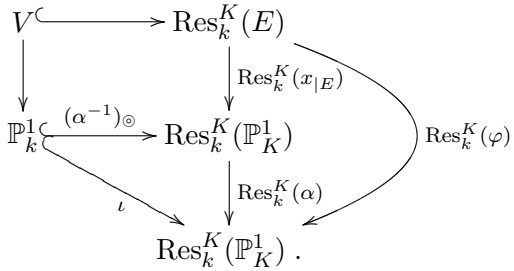
A geometric description of the definition of the factor base in (2) is as follows: Let $\iota = \mathrm{id}_{\circledcirc} : \mathbb{P}^1_k \longrightarrow \mathrm{Res}^K_k(\mathbb{P}^1_k)$ be the morphism corresponding to the identity on $\mathbb{P}^1_K$ under the universal property of the Weil restriction. This morphism is a closed immersion, it might be called the canonical immersion.

We define V by the diagram

$$\begin{array}{ccc} V & \hookrightarrow & \mathrm{Res}^K_k(E) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Res}^K_k(\varphi)} \\ \mathbb{P}^1_k & \overset{\iota}{\hookrightarrow} & \mathrm{Res}^K_k(\mathbb{P}^1_k) \end{array} \tag{4}$$

being Cartesian; cf. subsection 4.3 of [Die11b]. Then under the canonical isomorphism $E(K) \simeq \mathrm{Res}_k^K(E)(k)$, the factor base $\mathcal{F}$ corresponds to $V(k)$. Recall here that as the morphism $\varphi : E \longrightarrow \mathbb{P}^1_K$ is a flat covering of degree 2, the morphism $\mathrm{Res}_k^K(\varphi) : \mathrm{Res}_k^K(E) \longrightarrow \mathrm{Res}_k^K(\mathbb{P}^1_K)$ and the induced morphism $V \longrightarrow \mathbb{P}^1_k$ 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



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

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, $E_a := x_{|E}^{-1}(\mathbb{A}^1_K)$. Furthermore, as already mentioned above, let m be some natural number at most 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

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

We now give a geometric description. As mentioned in the introduction, the inclusion $U \hookrightarrow K$ gives rise to a closed immersion $\mathbb{A}_k[U] \longrightarrow \mathbb{A}_k[K]$, and thus $\mathbb{A}_k[U]$ is a group subvariety of $\mathbb{A}_k[K] = \mathrm{Res}_k^K(\mathbb{A}^1_K)$. Defining

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

$$\begin{array}{ccc} V_a & \hookrightarrow & \mathrm{Res}_k^K(E_a) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Res}_k^K(x_{|E_a})} \\ \mathbb{A}_k[U] & \hookrightarrow & \mathbb{A}_k[K] \ , \end{array} \tag{5}$$

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 $\mathcal{F}$. We define V_a' analogously to V_a with $\mathbb{A}_k[U]$ being substituted by $\mathbb{A}_k[U']$. Then $\mathcal{F}'$ corresponds to $V_a'(k)$. As the maps $V_a \longrightarrow A$ and $V_a' \longrightarrow A'$ are finite flat, every irreducible component of V_a has dimension m and every irreducible 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 $(\mathrm{Res}_k^K(E))^m \longrightarrow \mathrm{Res}_k^K(E)$ induces a dominant morphism from every irreducible component of $(V_a')^\delta \times V_a^{m-\delta}$ to $\mathrm{Res}_k^K(E)$.

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 $(V_a')^\delta \times V_a^{m-\delta} \longrightarrow \mathrm{Res}_k^K(E)$ is generically 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 $(V_a')^\delta \times V_a^{m-\delta} \longrightarrow \mathrm{Res}_k^K(E)$ is surjective and therefore if V_a' and V_a are irreducible, the first item is satisfied; see [Die11b, 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 The point $0 \in \mathbb{P}^1_K$ is not a branch point of $x_{|E} : E \longrightarrow \mathbb{P}^1_K$ 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 for the definition of the factor base, 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. We then fix k-vector subspaces U_i of K of dimension $d-1$ for $i = 1, \ldots, \delta$ and of dimension d for $i = \delta + 1, \ldots, m$ such that we have a decomposition

$$K = \bigoplus_{i=1}^{m} U_i \tag{6}$$

and such that some further conditions are satisfied; cf. subsection 2.5 below. With

$$\mathcal{F}_i := \{P \in E_a(K) \mid x(P) \in U_i - \{0\}\} , \tag{7}$$

we define the factor base as

$$\mathcal{F} := \bigcup_{i=1}^{m} \mathcal{F}_i . \tag{8}$$

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

$$P_1 + \cdots + P_m = P$$

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

We now apply the geometric considerations of the previous subsection here. Decomposition (6) gives rise to a decomposition

$$\mathbb{A}_k[K] = \bigoplus_{i=1}^{m} \mathbb{A}_k[U_i] \tag{9}$$

in the category of commutative k-group varieties. Decomposition (6) is then obtained from (9) by taking k-valued points.

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

$$\begin{array}{ccc} V_i & \hookrightarrow & \mathrm{Res}_k^K(E_a) \\ \downarrow & & \downarrow \\ \mathbb{A}_k[U_i] & \hookrightarrow & \mathbb{A}_k[K] \end{array}$$

being Cartesian. Note that the morphism $\mathrm{Res}_k^K(E_a) \longrightarrow \mathbb{A}_k[K]$ is a flat covering of degree 2^n which is unramified at $0 \in \mathbb{A}_k[K]$. As flatness and unramifiedness are stable under base change, the morphism $V_i \longrightarrow \mathbb{A}_k[U_i]$ is a flat covering of degree 2^n which is unramified at $0 \in \mathbb{A}_k[U_i]$ too. In particular, V_i has the same dimension as the vector space U_i.

Let

$$a_m : \mathrm{Res}_k^K(E)^m \longrightarrow \mathrm{Res}_k^K(E) \tag{10}$$

be the m-fold addition morphism and

$$a'_m : V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}^K_k(E) \tag{11}$$

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 $\mathrm{Res}^K_k((P_0)_\circledcirc) = 0$. In particular, $(P_0)_\circledcirc$ is a k-rational point of all V_i.

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

Remark 2.3 As unramifiedness is an open property, we obtain: a'_m is unramified in an open neighborhood of $((P_0)_\circledcirc, \ldots, (P_0)_\circledcirc)$. Every irreducible 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 $\mathbb{A}_k[K]$). Thus the morphism a'_m is dominant. If furthermore $V_1, \ldots, V_m$ are irreducible, a'_m is generically unramified.

Proof of Proposition 2.2. We wish to show that

$$(a'_m)_* : T_{((P_0)_\circledcirc, \ldots, (P_0)_\circledcirc)}(V_1 \times \cdots \times V_m) \longrightarrow T_{m\cdot(P_0)_\circledcirc}(\mathrm{Res}^K_k(E))$$

is an isomorphism.

As the morphism $\mathrm{Res}^K_k(x_{|E})$ is unramified at $(P_0)_\circledcirc$, it induces an isomorphism of tangent spaces

$$T_{(P_0)_\circledcirc}(\mathrm{Res}^K_k(E_a)) \xrightarrow{\sim} T_0(\mathbb{A}_k[K]) \; . \tag{12}$$

Decomposition (9) induces a decomposition of tangent spaces $T_0(\mathbb{A}_k[K]) = \bigoplus_{i=1}^m T_0(\mathbb{A}_k[U_i])$ which is nothing but the original decomposition of vector spaces $K = \bigoplus_{i=1}^m U_i$. Under isomorphism (12), $T_{(P_0)_\circledcirc}(V_i)$ corresponds to $T_0(\mathbb{A}_k[U_i])$. Therefore, we have the decomposition

$$T_{(P_0)_\circledcirc}(\mathrm{Res}^K_k(E_a)) = \bigoplus_{i=1}^m T_{(P_0)_\circledcirc}(V_i) \; . \tag{13}$$

By the next lemma, we have the commutative diagram whose vertical maps are isomorphisms

$$\begin{array}{ccc} T_{((P_0)_\circledcirc, \ldots, (P_0)_\circledcirc)}(\mathrm{Res}^K_k(E)^{\,m}) & \xrightarrow{(a_m)_*} & T_{m(P_0)_\circledcirc}(\mathrm{Res}^K_k(E)) \\ \Big\downarrow{\scriptstyle ((p_1)_*, \ldots, (p_m)_*)} & & \Big\uparrow{\scriptstyle (\tau_{(m-1)\cdot(P_0)_\circledcirc})_*} \\ (T_{(P_0)_\circledcirc}(\mathrm{Res}^K_k(E)))^m & \xrightarrow{\sum} & T_{(P_0)_\circledcirc}(\mathrm{Res}^K_k(E)) \; . \end{array}$$

Here $p_i : \mathrm{Res}^K_k(E)^m \longrightarrow \mathrm{Res}^K_k(E)$ is the projection to the i^{th} coordinate and the map $\sum : T_{(P_0)_\circledcirc}(\mathrm{Res}^K_k(E)) \longrightarrow T_{(P_0)_\circledcirc}(\mathrm{Res}^K_k(E))$ is the addition of the k-vector space $T_{(P_0)_\circledcirc}(\mathrm{Res}^K_k(E))$.

By restriction of the horizontal maps we obtain the commutative diagram

$$\begin{array}{ccc} T_{((P_0)_\circledcirc,\ldots,(P_0)_\circledcirc)}(V_1 \times \cdots \times V_m) & \xrightarrow{(a_m)_*} & T_{m(P_0)_\circledcirc}(\mathrm{Res}_k^K(E)) \\ \downarrow & & \uparrow{\scriptstyle (\tau_{(m-1)\cdot(P_0)_\circledcirc})_*} \\ T_{(P_0)_\circledcirc}(V_1) \times \cdots \times T_{(P_0)_\circledcirc}(V_m) & \xrightarrow{\sum} & T_{(P_0)_\circledcirc}(\mathrm{Res}_k^K(E)) \ . \end{array}$$

Now because of decomposition (13), under the addition, $T_{(P_0)_\circledcirc}(V_1) \times \cdots \times T_{(P_0)_\circledcirc}(V_m)$ is mapped bijectively to $T_{(P_0)_\circledcirc}(\mathrm{Res}_k^K(E))$. This gives the desired statement. □

In the following lemma, we use this notation: Let U, V, W be k-vector spaces. If then $\varphi : U \longrightarrow W$ and $\psi : V \longrightarrow W$ are k-linear maps, we denote the induced map $U \times V \longrightarrow W$ by $\begin{pmatrix} \varphi & \psi \end{pmatrix}$. If $\varphi : W \longrightarrow U$ and $\psi : W \longrightarrow V$ are k-linear maps, we denote the induced map $W \longrightarrow U \times V$ by $\begin{pmatrix} \varphi \\ \psi \end{pmatrix}$.

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 $\iota_i : X_i \longrightarrow X_1 \times X_2$. Let $p_i : X_1 \times X_2 \longrightarrow X_i$ be the canonical projections. Then the maps $\begin{pmatrix} (\iota_1)_* & (\iota_2)_* \end{pmatrix} : T_{P_1}(X_1) \times T_{P_2}(X_2) \longrightarrow T_{(P_1,P_2)}(X_1 \times X_2)$ and $\begin{pmatrix} (p_1)_* \\ (p_2)_* \end{pmatrix} : T_{(P_1,P_2)}(X_1 \times X_2) \longrightarrow T_{P_1}(X_1) \times T_{P_2}(X_2)$ 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 $a : A \times A \longrightarrow A$ and neutral element O. Let $\iota_i : A \longrightarrow A \times A$ be the two canonical immersions. Then the map $a_* \circ \begin{pmatrix} (\iota_1)_* & (\iota_2)_* \end{pmatrix} : T_O(A) \times T_O(A) \longrightarrow T_O(A)$ 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

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

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

Proof. a) The k-linear map

$$T_{P_1}(X_1) \times T_{P_2}(X_2) \xrightarrow{\begin{pmatrix} (\iota_1)_* & (\iota_2)_* \end{pmatrix}} T_{(P_1,P_2)}(X_1 \times X_2) \xrightarrow{\begin{pmatrix} (p_1)_* \\ (p_2)_* \end{pmatrix}} T_{P_1}(X_1) \times T_{P_2}(X_2)$$

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 $a_* \circ \begin{pmatrix} (\iota_1)_* & (\iota_2)_* \end{pmatrix} : T_O(A) \times T_O(A) \longrightarrow T_O(A)$ agrees with the addition (which is also k-linear) on the first and second factor. But restricted to factor i, $a_* \circ \begin{pmatrix} (\iota_1)_* & (\iota_2)_* \end{pmatrix}$ 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). □

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 U be a vector subspace of K, and let V_a be defined as in (5). If $\mathbb{A}_k[U]$ contains an irreducible scheme containing 0 whose preimage in V_a is irreducible, then V_a is irreducible. Likewise, if $\mathbb{A}_k[U]$ 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 irreducible components of V_a. Let $\mathcal{A} \subseteq \mathbb{A}_k[U]$ be the étale locus of the flat covering $V_a \longrightarrow \mathbb{A}_k[U]$ and $\mathcal{V}_a$ its preimage on V_a. By Condition 2.1 the covering $E_a \longrightarrow \mathbb{A}^1_K$ is unramified at 0. Thus so is the covering $\mathrm{Res}^K_k(E_a) \longrightarrow \mathbb{A}_k[K]$ and the induced covering $V_a \longrightarrow \mathbb{A}_k[U]$. Thus 0 is contained in $\mathcal{A}$. In particular, $\mathcal{A}$ is non-empty and thus a non-empty open part of $\mathbb{A}_k[U]$.

For $i = 1, 2$, the map $V_a^{(i)} \longrightarrow \mathbb{A}_k[U]$ is surjective. (As the map $V_a^{(i)} \longrightarrow \mathbb{A}_k[U]$ is flat and finite, by [Har77, Chapter III, Corollary 9.6], $V_a^{(i)}$ has the same dimension as $\mathbb{A}_k[U]$. The dimension of $V_a^{(i)}$ is equal to the dimension of its image. Thus the dimension of the image is equal to $\mathbb{A}_k[U]$. Therefore

the map is dominant. As the map is finite, it is in particular closed, and therefore the image is equal to $\mathbb{A}_k[U]$.) 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 $\mathbb{A}_k[U]$ is smooth so is $\mathcal{A}$, and as furthermore $\mathcal{V} \longrightarrow \mathcal{A}$ 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 $\mathbb{A}_k[U]$ as in the first claim of the lemma. As $V_a \longrightarrow \mathbb{A}_k[U]$ 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 $\overline{k}$. □

In the algorithm, we first search for 1-dimensional k-vector subspaces T_i of K such that the preimages of $\mathbb{A}_k[T_i]$ in $\mathrm{Res}_k^K(E_a)$ with respect to $\mathrm{Res}_k^K(x_{|E_a})$ are geometrically irreducible. Then we search for suitable k-vector subspaces U_i of K containing T_i. The preimages V_i of the corresponding group subvarieties $\mathbb{A}_k[U_i]$ of $\mathbb{A}_k[K]$ then contain $\mathbb{A}_k[T_i]$ and are therefore geometrically irreducible.

To choose the spaces T_i we employ ideas from the first subsection of this section and of our previous work.

Let $\mu \in K^*$, and let us consider the vector subspace $\mu^{-1} \cdot k$ of K and the associated group subvariety $\mathbb{A}[\mu^{-1} \cdot k]$ of $\mathbb{A}_k[K]$. Furthermore, let W_a be the preimage of $\mathbb{A}[\mu^{-1} \cdot k]$ in $\mathrm{Res}_k^K(E_a)$.

Clearly, the group subvariety $\mathbb{A}[\mu^{-1} \cdot k]$ is the image under the closed immersion $\mathbb{A}_k^1 \longrightarrow \mathbb{A}_k[K]$ induced by the injective homomorphism of vector spaces $k \longrightarrow K$, $a \mapsto \mu^{-1}a$. This morphism can also be given as follows: Let $\alpha_a := \mu x : \mathbb{A}_k^1 \longrightarrow \mathbb{A}_k^1$. Then the morphism $\mathbb{A}_k^1 \longrightarrow \mathbb{A}_k[K]$ is equal to $(\alpha_a^{-1})_\circledcirc$.

We now essentially apply the considerations of subsection 2.1 here, restricting ourselves to the "affine parts". We set $\varphi_a := \alpha_a \circ x_{|E_a}$. Now W_a is the preimage of $\iota(\mathbb{A}_k^1)$ in $\mathrm{Res}_k^K(E_a)$ with respect to the covering $\mathrm{Res}_k^K(\varphi_a)$. This is very closely related to the situation studied in [Die11b, 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 more than $q^n - 3(n-1) \cdot q^{n/2}$ 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 $x_{|E} : E_{\overline{k}} \longrightarrow \mathbb{P}^1_{\overline{k}}$ has two or

four branch points, one of which is at infinity. Thus there are exactly one or three branch points not equal to infinity.

Let $\lambda_1, \ldots, \lambda_s \in \mathbb{F}_{q^{6n}} - \{0\}$ with $s \in \{1, 3\}$ be the branch points of $x_{|E_a} : (E_a)_{\overline{k}} \longrightarrow \mathbb{A}^1_{\overline{k}}$. Let $\mu \in K^*$ and let $\alpha := \mu x$. Then the branch points of $\alpha \circ x_{|E_a} : (E_a)_{\overline{k}} \longrightarrow \mathbb{A}^1_{\overline{k}}$ are $\mu\lambda_1, \ldots, \mu\lambda_s$. Therefore Condition 2.7 from [Die11b] is equivalent to the following condition.

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

As shown in [Die11b, Proposition 4.9], if this condition is satisfied, W_a is geometrically irreducible.

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

For $j = 1, \ldots, n-1$ and $\ell = 1, \ldots, s$, the condition $(\mu\lambda_1)^{q^j} = \mu\lambda_\ell$ is equivalent to $\mu^{q^j-1} = \frac{\lambda_\ell}{\lambda_1^{q^j}}$. As the cardinality of the kernel of the map $K^* \longrightarrow \overline{k}^*$, $a \mapsto a^{q^j-1}$ is $q^{\gcd(j,n)} - 1$ (see next lemma), there are either no or exactly $q^{\gcd(j,n)} - 1$ such elements μ.

The situation is now very similar to the situation in [Die11b, Lemma 2.10]: In total there are at most $s \cdot \sum_{j=1}^{n-1}(q^{\gcd(j,n)} - 1)$ elements μ for which the condition in the lemma is not satisfied.

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

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

Proof. If $m \mid n$ then clearly $q^m - 1 \mid q^n - 1$. So assume that $q^m - 1 \mid q^n - 1$. 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. □

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 $2 \leq m \leq n$ 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 un-

der the automorphism of $\mathbb{P}^2_K$ 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 of E 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 $i = 1, \ldots, \delta$ and $\dim(U_i) = d$ for $i = \delta + 1, \ldots, m$ such that

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

The factor base is then defined as described in Equations (7) and (8) above.

We now give an algorithm for the task just mentioned under the condition that $m \leq \frac{n}{2}$ and $q \geq 4$. This is sufficient for the algorithm for Theorem 2.

Algorithm to compute a suitable decomposition of K

Input: A field extension $\mathbb{F}_{q^n}|\mathbb{F}_q$ with $q \geq 4$, 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 with $2 \leq m \leq \frac{n}{2}$.

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

1. If q is not a power of 2
   For $i = 1, \ldots, m$ do
   Repeat
   Choose $\mu_i \in \mathbb{F}_{q^n}^*$ uniformly at random.
   Until μ_i is not contained in $\langle T_1, \ldots, T_{i-1} \rangle$ and μ_i satisfies Condition 2.7.
   Let $T_i \longleftarrow \mu_i^{-1} \cdot \mathbb{F}_q < \mathbb{F}_{q^n}$.

   If q is a power of 2, let $T_i \longleftarrow \{0\}$ for $i = 1, \ldots, m$.

2. Let $d \longleftarrow \lceil \frac{n}{m} \rceil$ and $\delta \longleftarrow dm - n$.

   For $i = 1, \ldots, m$ do
   If $i \leq \delta$, let $e \longleftarrow d - 1$, otherwise let $e \longleftarrow d$.
   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 $U_1 + \cdots + U_{i-1} + T_{i+1} + \cdots + T_m$.
   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 $U_1, \ldots, U_m$.

Remark 2.9 We represent $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^n}$ 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 $U_1 \oplus \cdots \oplus U_i \oplus T_{i+1} \oplus \cdots \oplus T_m$ inside K, where for $j = 1, \ldots, i$, U_j contains T_j, $\dim(U_j) = d - 1$ if $j \leq \delta$ and $\dim(U_j) = d$ if $j > \delta$. The vector space T_i corresponds to a 1-dimensional group subscheme of $\mathbb{A}_k[K]$ whose preimage in $\mathrm{Res}_k^K(E)$ 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 $2 \leq m \leq \frac{n}{2}$ and $q \geq 4$, 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 $\langle T_1, \ldots, T_{i-1} \rangle$ contains at most $q^{m-1} \leq q^{n/2}$ elements. By Lemma 2.6, there are at least $q^n - 3(n-1) \cdot q^{n/2} - q^{n/2} \geq q^n - 3n \cdot q^{n/2}$ elements $\mu \in K^*$ which do not lie in $\langle T_1, \ldots, T_{i-1} \rangle$ and which satisfy Condition 2.7. The probability that this is satisfied is therefore at least $1 - 3n \cdot \frac{1}{q^{n/2}}$. For $n \geq 4$ and $q \geq 4$, which is the case by assumption, this is at least $1 - \frac{3n}{2^n} \geq 1 - \frac{12}{16} = \frac{1}{4}$. The expected value of iterations of

the Repeat-loop is therefore at most 4. We can obtain an expected running time which is polynomially bounded in $n \cdot \log(q)$.

Step 2 We always have $e \geq 2$. 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 at most 14 by Lemma 2.12 below. The expected running time of Step 2 is then polynomially bounded in q^d. □

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 an $\mathbb{F}_q$-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 $\mathbb{F}_q$ 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 $v_1, \ldots, v_{\dim(T)}$ be the basis of T given with the input.

For $i = \dim(T) + 1, \ldots, e$ do
    Repeat
        Choose $v_i \in \mathbb{F}_q^n$ uniformly at random.
    Until $v_i \notin \langle v_1, \ldots, v_{i-1} \rangle + S$.
Output $\langle v_1, \ldots, v_e \rangle$.

Obviously the space $\langle v_1, \ldots, v_e \rangle$ 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 $q^{(i-1)+\dim(S)-n} \leq \frac{1}{q}$. □

Lemma 2.12 *For $q \geq 4$ and $n \geq 4$, 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 $\dim(S) \leq n - 2$, $S \cap T = \{0\}$ and $S + T \subsetneq \mathbb{F}_q^n$ and a natural number e with $\dim(T) < e \leq n - \dim(S)$, 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 of at least $\frac{1}{14}$, $\#\{P \in E_a(\mathbb{F}_{q^n}) \mid x(P) \in U - \{0\}\} \geq \frac{1}{4} \cdot q^e$.

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

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

The expected value of N, $\mathbb{E}[N]$, can be expressed as follows:

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

the last inequality by the Hasse-Weil bound.

As $q \geq 4$ and $n \geq 4$, $2 \cdot q^{n/2} \leq \frac{1}{8} \cdot q^n$. As $q \geq 4$ and $\dim(S) \leq n - 2$, $2 \cdot q^{\dim(S)} \leq 2 \cdot q^{n-2} \leq \frac{1}{8} \cdot q^n$. We obtain:

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

On the other hand, $N \leq 2 \cdot q^e$. The claimed bound on the probability that $N \geq \frac{1}{4} \cdot q^e$ now follows by the following elementary probability theoretic argument. We have

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

and thus

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

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 predecessor [Die11b] 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 at least 2, 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), and let $f(x, y) \in K[x, y]$ be the defining polynomial of the affine part E_a. (The notation for the defining polynomial is different from the one in [Die11b].) 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 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 $(P_1, \ldots, P_m) \in \mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ with $P_1 + \cdots + P_m = P$ is called a *decomposition* of P with respect to the direct sum decomposition of K.

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

$$V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}_k^K(E)$$

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

This leads to the next definition.

Definition 3.2 A decomposition $(P_1, \ldots, P_m)$ of P is called *isolated* if it corresponds to an isolated (k-rational) point of the fiber $(V_1 \times \cdots \times V_m)_{P_\odot}$ 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 $E \subseteq \mathbb{P}^2_{\mathbb{F}_{q^n}}$ 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.

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 distributed 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 at most $e^{C \cdot mn}$.

b) The "new decomposition problem" can be solved in an expected running time which 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 $E(K) \simeq \mathrm{Cl}^0(E)$. 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 $P_1, \ldots, P_m \in E(K)$, we have $\sum_i P_i = P$ if and only if there exists a function $g \in K(E)^*$ with $(g) = (P_1)+\cdots+(P_m)+(-P)-(m+1)\cdot(O)$. 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 $\ell \in \mathbb{N}$, $(p_1)_{|E}, \ldots, (p_\ell)_{|E}$ is a basis of $L(\ell O)$. Let $L_\ell := \langle p_1, \ldots, p_\ell \rangle \cap \{f \in k[x,y] \mid f(-P) = 0\}$, and let $g_1, \ldots, g_m$ be a basis of L_{m+1} such that $g_1, \ldots g_{m-1}$ is a basis of L_m. Then $(g_1)_{|E}, \ldots, (g_m)_{|E}$ is a basis of $L((m+1)\cdot(O) - (-P))$ and $(g_m)_{|E} \notin L(m \cdot O - (-P))$. Now $(P_1, \ldots, P_m)$ is a decomposition of P if and only if there exists a tuple $(\alpha_1, \ldots, \alpha_{m-1}) \in K^{m-1}$ with

$$(g_m+\alpha_{m-1}g_{m-1}+\cdots+\alpha_1 g_1) = (P_1)+\cdots+(P_m)+(-P)-(m+1)\cdot(O)\ . \quad (14)$$

Furthermore, there exists at most one such tuple $(\alpha_1, \ldots, \alpha_{m-1})$ in $\overline{k}^{m-1}$. The set of decompositions of P is thus in canonical bijection to the set of tuples $(\alpha_1, \ldots, \alpha_{m-1}, P_1, \ldots, P_m) \in K^{m-1} \times E_a^m(K)$ with $x(P_i) \in U_i - \{0\}$ such that (14) holds. Note that in any such tuple the points $P_1, \ldots, P_m, P$ are distinct. (Recall that $x(P) \notin \bigcup_{i=1}^{m} U_i$ by assumption).

Let us recall that the defining polynomial of E_a is denoted by f. Let now

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

for all $i = 1, \ldots, m$; the scheme $V(f_{(1)}, \ldots, f_{(m)})$ is therefore equal to E_a^m in $\mathrm{Spec}(K[x_1, y_1, \ldots, x_m, y_m])$.

Let

$$h := g_m + a_{m-1}g_{m-1} + \cdots a_1 g_1 \in K[x, y, a_1, \ldots, a_{m-1}]$$

and let

$$\begin{aligned} h_{(i)} := g_m(x_i, y_i) + a_{m-1}g_{m-1}(x_i, y_i) + \cdots + a_1 g_1(x_i, y_i) \\ \in K[a_1, \ldots, a_{m-1}, x_1, y_1 \ldots, x_m, y_m] \end{aligned}$$

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

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

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

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

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

It is natural to pass to the Weil restriction of $V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})$ here. Let us first fix some notations: Let W be defined by the diagram

$$\begin{array}{ccc} W & \hookrightarrow & \mathrm{Res}_k^K(V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})) \\ \downarrow & & \downarrow \\ V_1 \times \cdots \times V_m & \hookrightarrow & (\mathrm{Res}_k^K(E_a))^m \\ \downarrow & & \downarrow \\ \mathbb{A}_k[U_1] \times \cdots \times \mathbb{A}_k[U_m] & \hookrightarrow & \mathbb{A}_k[K] \end{array}$$

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

Let $b_1, \ldots, b_n$ be a k-basis of K. (In the algorithm, such a basis is given with the input.) With this basis, we now identify K with k^n and also $\mathbb{A}_k[K]$ with $\mathbb{A}_k^n$. Moreover, for $i = 1, \ldots, m$, let $b_{i,1}, \ldots, b_{i,\dim(U_i)}$ be a basis of U_i. The scheme $W \subseteq \mathrm{Res}_k^K(V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)}))$ can be described explicitly as follows: Let the polynomials $h_{(i),j}$ and $f_{(i),j}$ for $i = 1, \ldots, m$, $j = 1, \ldots, n$ in $k[(a_{\ell,j'})_{\ell=1,\ldots,m-1,j'=1,\ldots,n}, ((x_{i',j'})_{j'=1,\ldots,\dim(U_i)}, (y_{i',j'})_{j'=1,\ldots,n})_{i'=1,\ldots,m}]$ be defined by

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

and

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

We have isomorphisms

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

and

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

(which are canonical for the chosen basis).

The k-rational points of $V((f_{(i),j})_{i=1,\ldots,m,j=1,\ldots,n}, (h_{(i),j})_{i=1,\ldots,m,j=1,\ldots,n})$ correspond in an obvious way to the K-rational points $(a_1, \ldots, a_{m-1}, P_1, \ldots, P_m)$

of $V(f_{(1)},\ldots,f_{(m)},h_{(1)},\ldots,h_{(m)})$ 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 at most 1, the total degree with respect to the $x_{i',j'}$ is at most $\lfloor\frac{m}{2}\rfloor$, the total degree with respect to the $y_{i',j'}$ is at most 1. Concerning the $f_{(i),j}$ we have: The total degree with respect to the $x_{i',j'}$ is at most 3, the total degree with respect to the $y_{i',j'}$ is at most 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 $2\cdot(m-1)\cdot n$ variables in the first system and the total degrees of all polynomials under consideration with respect to this system are at most 2. Furthermore, we have n variables in the second system and the total degrees with respect to this system are at most $\max(3,\lfloor\frac{m}{2}\rfloor)$.

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

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

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

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

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

Let us now turn to algorithmic aspects: It is straightforward to compute a system $(f_{(i),j})_{i=1,\ldots,m,j=1,\ldots,n},(h_{(i),j})_{i=1,\ldots,m,j=1,\ldots,n}$ as above. We then use Rojas' algorithm ([Roj99]) for sparse polynomial systems to determine all isolated k-rational solutions. The input and output structure as well as the

running time of the algorithm are given in [Roj99, Main Theorem 2.1]; all the following statements on the algorithm refer to this theorem.

We apply the algorithm with the system of equations and the polytope $\boldsymbol{P}$ defined above. The output of the algorithm is a system of univariate polynomials $h, h_1, \ldots, h_{2mn}$ the degrees of which are all bounded by the degree of the 0-cycle defined by the given system of sections in the Chow ring of $\mathcal{T}(\boldsymbol{P})$ and thus by $2^{4mn} \cdot \max(3, \frac{m}{2})^n$. By factoring h and applying the system $h_1, \ldots, h_{2mn}$ to the rational roots, we obtain a list of points in k^{2mn}. This list consists of solutions to the system and contains all isolated k-rational solutions of the system on $\mathbb{A}_k^{2mn}$.

The running time of Rojas' algorithm is polynomially bounded in $e^{m \cdot n} \cdot \log(q)$, and in an expected time which is also polynomially bounded in $e^{m \cdot n} \cdot \log(q)$ we can factor the univariate polynomial h. Explicitly, the running time of Rojas' algorithm depends on mixed volumes of various systems of polytopes all of which are contained in the polytope $\boldsymbol{P}$. Therefore these mixed volumes are also bounded by $2^{4mn} \cdot \max(3, \frac{m}{2})^n$.

We obtain the following intermediate result:

Lemma 3.4

a) A system $(f_{(i),j})_{i=1,\ldots,m,j=1,\ldots,n}, (h_{(i),j})_{i=1,\ldots,m,j=1,\ldots,n}$ 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 $(f_{(i),j})_{i=1,\ldots,m,j=1,\ldots,n}, (h_{(i),j})_{i=1,\ldots,m,j=1,\ldots,n}$ 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

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

Let $(P_1, \ldots, P_m) \in E_a^m(\overline{k})$ such that the points $P_1, \ldots, P_m, P_\circledcirc$ are distinct. Then there is at most one tuple $(\alpha_1, \ldots, \alpha_{m-1}) \in \overline{k}^m$ such that (14) holds, depending on whether $\sum_i P_i = P_\circledcirc$ or not.

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

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

Let $T := E_a^m - D$ and let S be the preimage of T in $V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)})$. Now the morphism $S \longrightarrow T$ induces an injection on the sets of geometric points and its image consists of those points $(P_1, \ldots, P_m) \in E_a^m(\overline{k})$ with $\sum_i P_i = P_\circledcirc$.

We consider the restriction of the m-fold addition morphism $E^m \longrightarrow E$ 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 $S \longrightarrow T$ induces a bijection $S(\overline{k}) \longrightarrow T_P(\overline{k})$. As T_P is reduced, we have an induced morphism $S \longrightarrow T_P$.

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

We have a canonical open embedding

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

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

Let

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

and let $V^*_{P_\circledcirc}$ be the fiber of $P_\circledcirc$ under the restriction of the addition morphism $\mathrm{Res}_k^K(E)^m \longrightarrow \mathrm{Res}_k^K(E)$ to V^*. We have

$$V^*_{P_\circledcirc} = V^* \cap (\mathrm{Res}_k^K(E_a)^m)_{P_\circledcirc} = V^* \cap \mathrm{Res}(T)_{P_\circledcirc} \ . \tag{15}$$

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

Let W^* be the preimage of V^* in $\mathrm{Res}_k^K(V(f_{(1)}, \ldots, f_{(m)}, h_{(1)}, \ldots, h_{(m)}))$. 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

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

Moreover, as the morphism $S \longrightarrow T$ factors through the fiber T_P, by functoriality, the morphism $\mathrm{Res}_k^K(S) \longrightarrow \mathrm{Res}_k^k(T)$ factors through the fiber $\mathrm{Res}_k^K(T)_{P_\otimes}$. We claim that we have an induced bijection between $\mathrm{Res}_k^K(S)(\overline{k})$ and $\mathrm{Res}_k^K(T)_{P_\otimes}(\overline{k})$. For this, we can (obviously) apply the base change to $\overline{k}|k$. But over $\overline{k}$, the two Weil restrictions become products of Galois twists of S and 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 for every algebraic field extension $\lambda|k$ we have a bijection between $\mathrm{Res}_k^K(S)(\lambda)$ and $(\mathrm{Res}_k^k(T))_{P_\otimes}(\lambda)$. We are going to use this for $\lambda = k$.

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

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

The composition $W^* \longrightarrow \mathrm{Res}_k^K(T)$ (obviously) factors through V^* and – as we have just seen – it factors through $(\mathrm{Res}_k^K(T))_{P_\otimes}$. By (15) it factors through $V^*_{P_\otimes}$. The morphism

$$W^* \longrightarrow V^*_{P_\otimes}$$

again induces a bijection

$$W^*(k) \longrightarrow V^*_{P_\otimes}(k) \ .$$

Let now $(P_1, \ldots, P_m)$ 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 $(P_1, \ldots, P_m)$ 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 $(V_1 \times \cdots \times V_m)(k)$ 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 under the assumption that $x(P) \notin \bigcup_{i=1}^m U_i$.

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 $\tilde{L}_\ell := \langle p_1, \ldots, p_\ell \rangle \cap \{f \in k[x,y] \mid f(-R) = 0\,,\ f(-S) = 0\}$. Let $\tilde{g}_1, \ldots, \tilde{g}_m$ be a basis of $\tilde{L}_{m+2}$ such that $\tilde{g}_1, \ldots, \tilde{g}_{m-1}$ is a basis of L_{m+1}. Now a tuple $(P_1, \ldots, P_m) \in \mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ is a decomposition of P if and only if there exists a tuple $(\alpha_1, \ldots, \alpha_{m-1}) \in K^{m-1}$ with

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

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 $m \in \mathbb{N}$ with $2 \leq m \leq \frac{n}{2}$. 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 $\mathcal{F}_i$ and V_i be 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 $(P_1, \ldots, P_m) \in \mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ which define non-isolated decompositions.

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

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

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

$$(a'_m)_* : T_{((P_1)_\circledcirc, \ldots, (P_m)_\circledcirc)}(V_1 \times \cdots \times V_m) \longrightarrow T_{P_\circledcirc}(V_1 \times \cdots \times V_m)$$

is injective.

We now consider points $(P_1, \ldots, P_m) \in E(K)^m$ 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 $P_1, \ldots, P_m$.

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

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

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

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 $T_{(P_1)_\circledcirc}(V_1) \times \cdots \times T_{(P_m)_\circledcirc}(V_m) \simeq T_{((P_1)_\circledcirc,\ldots,(P_m)_\circledcirc)}(V_1 \times \cdots \times V_m)$, the horizontal map on the left hand side is

$$(\tau_{(P_0-P_1)_\circledcirc})_* \times \cdots \times (\tau_{(P_0-P_m)_\circledcirc})_* : T_{(P_1)_\circledcirc}(V_1) \times \cdots \times T_{(P_m)_\circledcirc}(V_m) \longrightarrow T_{(P_0)_\circledcirc}(V_1) \times \cdots \times T_{(P_0)_\circledcirc}(V_m) \; .$$

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

$$T_{(P_0)_\circledcirc}(\mathrm{Res}_k^K(E)) = \bigoplus_{i=1}^m (\tau_{(P_0-P_i)_\circledcirc})_*(T_{(P_i)_\circledcirc}(V_i)) \; . \tag{16}$$

We want to derive a condition under which we do have such a decomposition. For this, we distinguish between three cases: q odd; q even and $j \neq 0$; and 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 the defining polynomial f of E_a is of the form $y^2 - v(x)$ (with v monic of degree 3).

Following our usual notation, let $\mathbb{P}^1_K := \mathrm{Proj}(K[X,Y])$. 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 $\mathbb{P}^1_K$, we have the meromorphic cotangent vector field $dx_{\mathbb{P}^1}$ with divisor -2∞. Under duality, this corresponds to a tangent vector field which we denote by $t_{\mathbb{P}^1} \in \Gamma(\mathbb{P}^1_k, \mathcal{T}_{\mathbb{P}^1_k})$ and which 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 $\tau^*(\frac{dx_{|E}}{y_{|E}}) = \frac{dx_{|E}}{y_{|E}}$.

Again under duality, $dx_{|E}$ corresponds to a meromorphic tangent vector field; we denote this by t_E. It has divisor $4(O) - R$. So we have the holomorphic tangent vector field $y_E\, t_E$, which corresponds to $\frac{dx_{|E}}{y_{|E}}$ under duality. Moreover, the field $y_E\, t_E$ is also invariant under translation, that is, for every translation τ of E, $\tau_*(y_{|E}\, t_E) = y_{|E}\, t_E$.

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_E by $t_E(P)$.

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 $(\tau_{P_0-P_1})_* : T_{P_1}(E) \longrightarrow T_{P_0}(E)$. This homomorphism is given by $y(P_1)\, t_E(P_1) \mapsto y(P_0)\, t_E(P_0)$, that is,

$$t_E(P_1) \mapsto \frac{y(P_0)}{y(P_1)}\, t_E(P_0)\ . \tag{17}$$

As in the previous section, Let us fix a basis $(b_j)_j$ of K over k and bases $(b_{i,j})_j$ of the U_i. Let us denote the corresponding dual bases by $(x_j)_j$ and $(x_{i,j})_j$. The bases $(b_j)_j$ and $(b_{i,j})_j$ define bases of the spaces $\Gamma(\mathbb{A}_k[K], \mathcal{T})$ and $\Gamma(\mathbb{A}_k[U_i], \mathcal{T})$. We denote these bases by $(t_j)_{j=1,\ldots,n}$ for $\mathbb{A}_k[K]$ and $(t_{i,j})_{j=1,\ldots,\dim(U_i)}$ for $\mathbb{A}_k[U_i]$.

Let $P \in E(K)$ such that $x_{|E}$ is unramified at P. Then $\mathrm{Res}^K_k(x_{|E_a})$ defines an isomorphism of tangent spaces $(\mathrm{Res}^K_k(x_{|E_a}))_* : T_{P_\circledcirc}(\mathrm{Res}^K_k(x_{|E_a})) \longrightarrow T_{x(P)_\circledcirc}(\mathbb{A}[K])$. Now for $t \in \Gamma(\mathbb{A}[K], \mathcal{T})$, we define $t(P_\circledcirc) := ((\mathrm{Res}^K_k(x_{|E_a}))_*)^{-1}(t(x(P)_\circledcirc))$. The isomorphism of tangent vector spaces restricts to an isomorphism of tangent vector spaces $T_{P_\circledcirc}(V_i) \longrightarrow T_{x(P)_\circledcirc}(\mathbb{A}[U_i])$. Thus $t(P_\circledcirc)$ is in $T_{P_\circledcirc}(V_i)$ if and only if $t(x(P)_\circledcirc)$ is in $T_{x(P)_\circledcirc}(\mathbb{A}[U_i])$.

Just as the bases $(t_j(x(P)_\circledcirc))_j$ and $(d(x_j)(x(P)_\circledcirc))_j$ are dual to each other, so are the bases $(t_j(P_\circledcirc))_j$ and $(d(x_j)_{|\,\mathrm{Res}^K_k(E_a)}(P_\circledcirc))_j$.

Let A_i be the coordinate matrix of $(b_{i,j})_j$ with respect to $(b_j)_j$. Then this is also the coordinate matrix of $(t_{i,j})_j$ with respect to $(t_j)_j$, and for any $P \in E(K)$ as above, it is also the coordinate matrix of $(t_{i,j}(P_\circledcirc))_j$ with respect to $(t_j(P_\circledcirc))_j$. For the following, it is important that the matrix does not depend on P.

Let now $(P_1, \ldots, P_m) \in E^m(K)$ with $x(P_i) \in U_i$ for all i satisfy Condition 4.1. Then for each $i = 1, \ldots, m$, the system $(t_{i,j}((P_i)_\circledcirc))_j$ is a basis of the k-vector space $T_{(P_i)_\circledcirc}(V_i)$. We have a direct sum decomposition of $T_{(P_0)_\circledcirc}(\mathrm{Res}_k^K(E))$ as in (16) if and only if the elements $(t_{(P_0-P_i)_\circledcirc})_*(t_{i,j}((P_i)_\circledcirc))$ for $i = 1, \ldots, m, j = 1, \ldots, \dim(U_i)$ form a k-basis of $T_{P_\circledcirc}(\mathrm{Res}_k^K(E))$.

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

$$(u, \sigma(u), \ldots, \sigma^{n-1}(u)) : (\mathrm{Res}_k^K(E_a))_K \tilde{\longrightarrow} \prod_{s=0}^{n-1} \sigma^s_{K|k}(E_a) \tag{18}$$

corresponding to the isomorphism of K-algebras

$$\bigotimes_{s=0}^{n-1} K[x^{(s)}, y^{(s)}]/(\sigma^s_{K|k}(f)(x^{(s)}, y^{(s)})) \tilde{\longrightarrow} K[x_1, \ldots, x_n, y_1, \ldots, y_n]/(f_1, \ldots, f_n) \ ,$$

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

Note that for $P \in E(K)$, under isomorphism (18) the point $P_\circledcirc \in \mathrm{Res}_k^k(E)(k) \subseteq \mathrm{Res}_k^K(E)(K)$ corresponds to the point $(\sigma^s(P))_{s=0,\ldots,n-1} \in \prod_{s=0}^{n-1} \sigma^s_{K|k}(E_a)(K)$.

We have an induced isomorphism $\Gamma(\mathrm{Res}_k^K(E_a)_K, \Omega) \simeq \bigoplus_{s=0}^{n-1} \Gamma(\sigma^s(E_a), \Omega)$ under which $d(x^{(s)})_{|\sigma^s(E_a)}$ corresponds to $\sum_{j=1}^n \sigma^s_{K|k}(b_j) \cdot d(x_j)_{|\,\mathrm{Res}_k^K(E_a)}$. This isomorphism induces an isomorphism between the cotangent spaces at $P_\circledcirc$ and $(\sigma^s(P))_{s=0,\ldots,n-1}$. Let again $x_{|E}$ be unramified at P. If we then apply the duality between cotangent and tangent spaces, we obtain that $t_j(P_\circledcirc)$ corresponds to $\big(\sigma^s_{K|k}(b_j) \cdot t_{\sigma^s(E_a)}(\sigma^s(P))\big)_{s=0,\ldots,n-1}$ under the induced isomorphism of tangent spaces at $P_\circledcirc$ and $(\sigma^s(P))_{s=0,\ldots,n-1}$.

On each of the factors of the product $\prod_{s=0}^{n-1} \sigma^s_{K|k}(E_a)$, we can apply the considerations above. We obtain that $(\tau_{(P_0-P_i)_\circledcirc})_*(t_j((P_i)_\circledcirc))$ corresponds to

$$\begin{aligned}
& \big((\tau_{(\sigma(P_0)-\sigma(P_i))})_*(\sigma^s_{K|k}(b_j) \cdot t_{\sigma^s(E_a)}(\sigma^s(P_0)))\big)_{s=0,\ldots,n-1} \\
= \ & \big(\sigma^s_{K|k}(b_j) \cdot \frac{y^{(s)}(\sigma(P_0))}{y^{(s)}(\sigma(P_i))} \cdot t_{\sigma^s(E_a)}(\sigma^s(P_0))\big)_{s=0,\ldots,n-1} \\
= \ & \big(\sigma^s_{K|k}(b_j) \cdot \frac{\sum_{\ell=1}^n \sigma^s_{K|k}(b_\ell) \cdot y_\ell((P_0)_\circledcirc)}{\sum_{\ell=1}^n \sigma^s_{K|k}(b_\ell) \cdot y_\ell((P_i)_\circledcirc)} \cdot t_{\sigma^s(E_a)}(\sigma^s(P_0))\big)_{s=0,\ldots,n-1} \ .
\end{aligned}$$

This vector is of course invariant under the Galois operation of $K|k$. Let C be the inverse of the matrix $((\sigma^s(b_j)))_{s=0,\ldots,n-1,j=1,\ldots,n}$; this is a matrix of the form

$((\sigma^s(c_u)))_{u=1,\dots,n,s=0,\dots,n-1}$. Going back, we have

$$\begin{aligned}
&(\tau_{(P_0-P_i)_\circledcirc})_*(t_j((P_i)_\circledcirc))\\
=\ &\sum_{s=0}^{n-1}\sigma^s_{K|k}(b_j)\cdot\frac{\sum_{\ell=1}^n\sigma^s_{K|k}(b_\ell)\cdot y_\ell((P_0)_\circledcirc)}{\sum_{\ell=1}^s\sigma^s_{K|k}(b_\ell)\cdot y_\ell((P_i)_\circledcirc)}\cdot(\sum_{u=1}^n\sigma^s(c_u)(t_u((P_0)_\circledcirc)))\\
=\ &\sum_{u=1}^n\sum_{s=0}^{n-1}\sigma^s_{K|k}\big(b_j\cdot\frac{\sum_{\ell=1}^n b_\ell\cdot y_\ell((P_0)_\circledcirc)}{\sum_{\ell=1}^s b_\ell\cdot y_\ell((P_i)_\circledcirc)}\cdot c_u\big)\cdot(t_u(P_0)_\circledcirc)\ .
\end{aligned}$$

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

$$\begin{aligned}
&(\tau_{(P_0-P_i)_\circledcirc})_*(t_j((P_i)_\circledcirc))\\
&\qquad=\sum_{u=1}^n\sum_{s=0}^{n-1}\sigma^s_{K|k}\big(\frac{c_{j,u}}{\sum_{\ell=1}^n b_\ell\cdot y_\ell((P_i)_\circledcirc)}\big)\cdot t_u((P_0)_\circledcirc)\ .
\end{aligned}$$

Let $\iota_i:V_i\hookrightarrow\mathrm{Res}^K_k(E)$ be the immersions. It follows that there are constants $c_{i,j,u}\in K$ (again independent of $P_1,\dots,P_m$) with

$$\begin{aligned}
&\big((\tau_{(P_0-P_i)_\circledcirc})_*\circ(\iota_i)_*\big)t_{i,j}((P_i)_\circledcirc)\\
&\qquad=\sum_{u=1}^n\sum_{s=0}^{n-1}\sigma^s_{K|k}\big(\frac{c_{i,j,u}}{\sum_{\ell=1}^n b_\ell\cdot y_{i,\ell}((P_i)_\circledcirc)}\big)\cdot t_u((P_0)_\circledcirc)\\
&\qquad=\sum_{u=1}^n\sum_{s=0}^{n-1}\big(\frac{\sigma^s_{K|k}(c_{i,j,u})}{\sum_{\ell=1}^n\sigma^s_{K|k}(b_\ell)\cdot y_{i,\ell}((P_i)_\circledcirc)}\big)\cdot t_u((P_0)_\circledcirc)\ .
\end{aligned}$$

Let

$$\begin{aligned}
M_0:=&\big(\big(\sum_{s=0}^{n-1}\frac{\sigma^s_{K|k}(c_{i,j,u})}{\sum_{\ell=1}^n\sigma^s_{K|k}(b_\ell)\cdot y_{i,\ell}}\big)\big)_{u=1,\dots,n\,,\,(i=1,\dots,m,j=1,\dots,\dim(U_i))}\\
&\in k((y_{i',j'})_{i'=1,\dots,m,j'=1,\dots,n})^{\{1,\dots,n\}\times(\bigcup_{i=1}^m\bigcup_{j=1}^{\dim(U_i)}\{(i,j)\})}\ .
\end{aligned}$$

Note here that as indicated M_0 is a matrix over $k((y_{i',j'})_{i'=1,\dots,m,j'=1,\dots,n}$ because the entries are invariant under the Galois operation. The matrix has the size $n\times n$. It is however more convenient to use the indicated indices for the columns. 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,s, $\sum_{\ell=1}^n\sigma^s(b_\ell)\cdot y_{i,\ell}$ vanishes at $((P_1)_\circledcirc,\dots,(P_n)_\circledcirc)$.

We have a direct sum decomposition of $T_0(\mathrm{Res}^K_k(E))$ as in (16) if and only if the matrix $M_0((P_1)_\circledcirc,\dots,(P_n)_\circledcirc)$ is non-singular.

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

We now multiply the columns of M by polynomials such that the entries of the resulting matrix are polynomials. Concretely, we multiply all columns with column index (i, j) with the polynomial $\prod_{t=0}^{n-1}(\sum_{\ell=1}^{n} \sigma_{K|k}^{t}(b_\ell) \cdot y_{i,\ell})$. The resulting matrix is

$$M = \Big(\big(\sum_{s=0}^{n-1} \sigma_{K|k}^{s}(c_{i,j,u}) \cdot \prod_{\substack{t=0 \\ t \neq s}}^{n-1} \big(\sum_{\ell=1}^{n} \sigma_{K|k}^{t}(b_\ell) \cdot y_{i,\ell} \big) \big) \Big)_{u=1,\ldots,n\,,\,(i=1,\ldots,m, j=1,\ldots,\dim(U_i))}$$

$$\in k[(y_{i',j'})_{i'=1,\ldots,m, j'=1,\ldots,n}] \,.$$

Let $\boldsymbol{d} := \det(M) \in k[(y_{i',j'})_{i',j'}]$. Again for $(P_1, \ldots, P_m)$ as above, $\boldsymbol{d}$ vanishes at $((P_1)_\circledcirc, \ldots, (P_m)_\circledcirc)$ if and only if the homomorphism a'_m is unramified at $((P_1)_\circledcirc, \ldots, (P_m)_\circledcirc)$. Furthermore $\boldsymbol{d}$ does not vanish identically on $V_1, \times \cdots \times V_m$ because it does not vanish at $((P_0)_\circledcirc, \ldots, (P_0)_\circledcirc)$.

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

An entry of M with column index (i, j) is a homogeneous polynomial in the variables $y_{i,1}, \ldots, y_{i,n}$ of degree $n-1$. Therefore $\boldsymbol{d}$ is multihomogeneous with respect to the sets of variables $(y_{i,1}, \ldots, y_{i,n})_{i=1,\ldots,m}$ of multidegree $(\dim(U_1) \cdot (n-1), \ldots, \dim(U_m) \cdot (n-1))$. The total degree is therefore $n^2 - n$. We want to prove:

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

Proof. Let us first mention the following general fact.

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

Proof. As $\mathbb{F}_q[x_1, \ldots, x_n]$ is factorial, we are immediately reduced to the case that f is irreducible. If now $f = x_n - a$ for some $a \in \mathbb{F}_q$, we are done. Let us assume that this is not the case and let $a \in \mathbb{F}_q$. Now f is not divisible by $x_n - a$. This means that not every coefficient of f as a polynomial in $\mathbb{F}_q[x_n][x_1, \ldots, x_{n-1}]$ is divisible by $x_n - a$, in other words, the polynomial $f(x_1, \ldots, x_{n-1}, a)$ is non-trivial. The result now follows by induction on n. □

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

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

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

$$\begin{array}{ccc}
V_i & \hookrightarrow & \overline{V}_i \\
\downarrow & & \downarrow \\
\mathrm{Res}_k^K(E) = V(f_1, \ldots, f_n) & \hookrightarrow & V(F_1, \ldots, F_n) \ .
\end{array}$$

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

Proof. We have to show that $\overline{V}_i$ has no points "at infinity", that is, the intersection $V(Z) \cap \overline{V}_i$ is trivial. We show in fact the stronger statement that $V(Z) \cap V(F_1, \ldots, F_n)$ 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 $s = 0, \ldots, n-1$.

Let us consider the isomorphism of graded K-algebras

$$\begin{aligned}
K[x_1, \ldots, x_n][Y_1, \ldots, Y_n, Z] &\longrightarrow K[x^{(1)}, \ldots, x^{(n)}][Y^{(1)}, \ldots, Y^{(n)}, Z] \\
x^{(s)} \mapsto \sum_{j=1}^n \sigma_{K|k}^s(b_j) \cdot x_j \ , \ Y^{(s)} &\mapsto \sum_{j=1}^n \sigma_{K|k}^s(b_j) \cdot Y_j \ , \ Z \mapsto Z \ .
\end{aligned}$$

We have the following commutative diagram over K:

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

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. □

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

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

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

We want to show by induction on ℓ:

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

Recall here that $\dim(U_i) = \dim(V_i)$.

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

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

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

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 $\mathrm{Res}_k^K(E_a)(k)$. In particular, over each point of $\mathbb{A}_k[U_\ell](k)$ lie at most 2 points of $V_\ell(k)$. Because of this and because of the induction hypothesis, there are

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

points in the first part.

We now consider points in the second part.

Let $(P_1, \ldots, P_{\ell-1}) \in V_1(k) \times \cdots \times V_{\ell-1}(k)$ with $\boldsymbol{d}_{\ell-1}(P_1, \ldots, P_{\ell-1}) \neq 0$, that is, $\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1}, (P_0)_\circledcirc) \neq 0$.

The polynomial

$$\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1}) \in k[y_{\ell,1}, \ldots, y_{\ell,n}] \subseteq k[x_{\ell,1}, \ldots, x_{\ell,\dim(U_\ell)}, y_{\ell,1}, \ldots, y_{\ell,n}]$$

is now non-trivial on V_ℓ. As – by the conditions we have imposed – V_ℓ is irreducible, $V_\ell \cap V(\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1}))$ is of codimension 1 in V_ℓ by Krull's Hauptidealsatz, with other words, it is of dimension $\dim(U_\ell) - 1$.

The polynomial $\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1})$ is already homogeneous with respect to $y_{\ell,1}, \ldots, y_{\ell,n}$; let $\overline{\boldsymbol{d}} \in k[Y_{\ell,1}, \ldots, Y_{\ell,n}, Z] \subseteq k[x_{\ell,1}, \ldots, x_{\ell,\dim(U_\ell)}][Y_{\ell,1}, \ldots, Y_{\ell,n}, Z]$ be the polynomial obtained by substituting $Y_{\ell,n}$ for $y_{\ell,n}$. This is a homogeneous polynomial of degree $\dim(U_\ell) \cdot (n-1)$ with respect to $Y_{\ell,1}, \ldots, Y_{\ell,n}, Z$. As $V_\ell = \overline{V}_\ell$ (Lemma 4.4), we have

$$V_\ell \cap V(\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1})) = \overline{V}_\ell \cap V(\overline{\boldsymbol{d}}) =$$

$$V(F_{(\ell),1}, \ldots, F_{(\ell),n}, \overline{\boldsymbol{d}}) \subseteq \mathrm{Spec}(k[x_{\ell,1}, \ldots, x_{\ell,\dim(U_\ell)}]) \times \mathrm{Proj}(k[Y_{\ell,1}, \ldots, Y_{\ell,n}, Z]) \; .$$

Let $\mathrm{Res} = \mathrm{Res}(G_1, \ldots, G_{n+1})$ be the dense multivariate resultant for $n+1$ homogeneous variables and polynomials of (homogeneous) degrees $2, \ldots, 2$, $\dim(U_i) \cdot (n-1)$. Here, the $G_1, \ldots, G_{n+1}$ are independent generic polynomials, that is, polynomials with algebraically independent coefficients. (As in [Die11b], the similarity between the notation for the Weil restriction and the resultant is accidental.)

By taking the resultant of the system $F_{(\ell),1}, \ldots, F_{(\ell),n}, \overline{\boldsymbol{d}}$ with respect to $Y_{\ell,1}, \ldots, Y_{\ell,n}, Z$, we obtain $\mathrm{Res}(F_{(\ell),1}, \ldots, F_{(\ell),n}, \overline{\boldsymbol{d}})$, which is a non-trivial polynomial in $k[x_{\ell,1}, \ldots, x_{\ell,\dim(U_\ell)}]$. For some point $Q \in \mathbb{A}^n(\overline{k})$, the resultant $\mathrm{Res}(F_{(\ell),1}, \ldots, F_{(\ell),n}, \overline{\boldsymbol{d}})$ vanishes at Q if and only if there is a $\overline{k}$-rational point in $\overline{V}_\ell \cap V(\overline{\boldsymbol{d}}) = V_\ell \cap V(\boldsymbol{d}_\ell(P_1, \ldots, P_{\ell-1}))$ 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 $j = 1, \ldots, n$, Res is a homogeneous polynomial of degree $\dim(U_j) \cdot (n-1) \cdot 2^{n-1} < n^2 \cdot 2^{n-2}$ in the coefficients of the G_j. The inequality is obtained as follows: As $m \geq 2$, $\dim(U_j) \leq \lceil \frac{n}{2} \rceil \leq \frac{n+1}{2}$. Furthermore, Res is a homogeneous polynomial of degree 2^n in the coefficients of G_{n+1}. Moreover, $F_{(\ell),j}$ has degree at most 3 in the $x_{\ell,j'}$ $(j' = 1, \ldots, \dim(U_i))$ and $\overline{\boldsymbol{d}}$ obviously has degree 0 in the $x_{\ell,j'}$.

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

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

This concludes the proof of Proposition 4.2. □

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

Proposition 4.5 *The number of tuples in $\mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ which do not define isolated decompositions is at most $(n^5 \cdot 4^n + 2^n) \cdot q^{n-1}$.*

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

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

Proceeding just as above, we obtain a non-trivial polynomial $\boldsymbol{d} \in k[(x_{i,j})_{i=1,\ldots,m,j=1,\ldots,\dim(U_i)}]$ of total degree $n^2 - n$ such that for points $(P_1, \ldots, P_m) \in E(K)^m$ with $x(P_i) \in U_i$ satisfying Condition 4.1, $((P_1)_\circledcirc, \ldots, (P_m)_\circledcirc)$ is an isolated reduced point in its fiber if and only if $\boldsymbol{d}((P_1)_\circledcirc, \ldots, (P_m)_\circledcirc) = 0$.

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

Proposition 4.6 *The number of tuples in $\mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ which do not define isolated decompositions is at most $2^m \cdot n^2 \cdot q^{n-1}$.*

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

In this case, $dx_{|E}$ itself is a holomorphic differential on E. It follows that $(\tau_{(P_0-P_i)_\circledcirc})_*(t_{i,j}((P_i)_\circledcirc)) = (t_{i,j}((P_0)_\circledcirc))$ for any $P \in E_a(K)$. Therefore, the morphism $a'_m : V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}_k^K(E)$ 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*

- $2^{5n} \leq q$

  or

- *q even, $n^3 \leq q$ and $m \leq \lceil \sqrt{\log_2(q)} \rceil$*

the following holds: The probability that a uniformly randomly distributed point of $E(K)$ has an isolated decomposition is in

$$\frac{1}{e^{\mathcal{O}(mn)}} = \left(\frac{1}{e^{mn}}\right)^{\Omega(1)}.$$

We remark here that the condition $m \leq \lceil \sqrt{\log_2(q)} \rceil$ is satisfied for m in the preliminary algorithm presented in the introduction.

Proof. Let first q be odd and the first condition satisfied. By the conditions in subsection 2.5, we have $\#\mathcal{F}_i \geq \frac{1}{4} \cdot q^{\dim(U_i)}$ for all i and therefore $\#(\mathcal{F}_1 \times \cdots \times \mathcal{F}_m) \geq \frac{1}{4^m} \cdot q^n \geq \frac{1}{4^n} \cdot q^n$. By Proposition 4.5, at most $(n^5 \cdot 4^n + 2^n) \cdot q^{n-1}$ of these tuples do not define isolated decompositions. So if $n^5 \cdot 4^n + 2^n \leq \frac{1}{2} \cdot \frac{1}{4^n} \cdot q$, we have at least $\frac{1}{2} \cdot \frac{1}{4^n} \cdot q^n$ tuples which do define isolated decompositions. This is for example the case if $2^{5n} \leq q$ and n is large enough, and for every fixed n it holds if q is large enough. By Proposition 3.3 a) the image of the set of tuples in $\mathcal{F}_1 \times \cdots \times \mathcal{F}_m$ which define isolated decompositions has a size of $\frac{1}{e^{\mathcal{O}(mn)}} \cdot q^n$. The probability that a uniformly randomly distributed point in $E(\mathbb{F}_{q^n})$ has an isolated decomposition is therefore in $\frac{1}{e^{\mathcal{O}(mn)}}$.

We now consider the case that q is even. The proof is similar to the previous one, only that we now apply propositions 4.6 and 4.7. We now want that the condition $2^m \cdot n^2 \leq \frac{1}{2} \cdot \frac{1}{4^m} \cdot q$ is satisfied, that is, $2 \cdot 2^{3m} \cdot n^2 \leq q$. This is always satisfied under the first condition, that is, $2^{5n} \leq q$. Furthermore, under the condition that $m \leq \lceil \sqrt{\log_2(q)} \rceil$ the desired condition is in particular satisfied if $2n^2 \leq 2^{\log_2(q) - 3\lceil \sqrt{\log_2(q)} \rceil}$. This condition is for example

satisfied if $n^3 \leq q$ and n is large enough, and it holds for every fixed n if q is large enough. $\square$

Derivation of Theorem 2

Finally, we show how Theorem 2 follows. In addition we show that in characteristic 2 one can obtain a result which on first sight seems to be an improvement over Theorem 2 but is in fact further improved upon by Theorem 3 which relies solely on Theorem 2.

As already mentioned in the outline in the introduction, the basic structure of the index calculus algorithm is the same as that in [Die11b]. 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 $2^{5n} \leq q$ or q is even and $n^3 \leq q$. 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 $\mathcal{P}oly(q^d) \subseteq e^{\mathcal{O}(\max(\log(q), n\cdot\sqrt{\log(q)}))}$.

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

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 $2^{5n} \leq q$ or q even and $n^3 \leq q$ so far. The derivation of Theorem 2 is now analogous to the derivation of Theorem 1 from [Die11b, Proposition 2.11].

We make the following case distinction: If $2^{5n} \leq q$, we apply the index calculus algorithm directly. If $2^{5n} > q$, we set $a := \lceil \frac{5n}{\log_2(q)} \rceil$ 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 $2^{5n} \leq q^a$, thus we can conclude that the index calculus algorithm runs in an expected running time of $e^{\mathcal{O}(\max(\log(q^a), n \cdot \sqrt{\log(q^a)}))} = e^{\mathcal{O}(n^{3/2})}$.

This gives Theorem 2 except that in the theorem the field extension $\mathbb{F}_{q^n}|\mathbb{F}_q$ is not given with the input data. As already pointed out in [Die11b], one can apply the above algorithm with all possible field extensions "in parallel" to obtain the desired result.

In addition to the derivation of Theorem 2 we now consider only instances in characteristic 2. Under this condition, we can proceed as follows: For $n^3 \leq q$ we apply the index calculus algorithm directly. For $n^3 > q$, we set $a := \lceil \frac{3\log_2(n)}{\log_2(q)} \rceil$ and proceed as above. We obtain an expected running time of $e^{\mathcal{O}(n \cdot \sqrt{\log(n)})}$. In total, we obtain an expected running time of

$$e^{\mathcal{O}(\max(\log(q), n \cdot \log(q)^{1/2}, n \cdot \log(n)^{1/2}))} ; \tag{19}$$

with $q = 2^m$ this is

$$e^{\mathcal{O}(\max(m, n \cdot m^{1/2}, n \cdot \log(n)^{1/2}))} . \tag{20}$$

We note however that for the derivation of Theorem 3 we only apply Theorem 2 under the condition that $n \leq m$. Under this condition, we do not have an improvement upon the expected time given in Theorem 2, and in fact Theorem 3 improves upon the expected time given by (20) if $m \in o(n)$.

References

[CLO05] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer, 2005.

[Die11a] C. Diem. On the discrete logarithm problem in class groups of curves. *Math. Comp.*, 80:443 – 475, 2011.

[Die11b] C. Diem. On the discrete logarithm problem in elliptic curves. *Compos. Math.*, 147, 2011.

[Ful93] W. Fulton. *Introduction to Toric Varieties.* Princeton University Press, 1993.

[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.

Appendix: Misprints in the previous work

I would like to take the opportunity to correct two misprints in [Die11b].

- In subsection 4.2 the following situation is considered: Let k be a field, let $n_1 > n_2$, and let $p : (\mathbb{P}^1_k)^{n_1} = \prod_{i=1}^{n_1} \mathrm{Proj}(k[X_i, Y_i]) \longrightarrow (\mathbb{P}^1_k)^{n_2} = \prod_{i=1}^{n_2} \mathrm{Proj}(k[X_i, Y_i])$ be the projection to the first n_2 factors. Let h_i be the class of $V(X_i)$ in any of the two Chow rings. Lemma 4.6 is on the push-forward map $p_* : \mathrm{CH}((\mathbb{P}^1_k)^{n_1}) \longrightarrow \mathrm{CH}((\mathbb{P}^1_k)^{n_2})$, which is a group homomorphism. There is a misprint in the lemma. The correct statement is:

  Let $\underline{e} \in \{0,1\}^{n_1}$. Then $p_*(h_1^{e_1} \cdots h_{n_1}^{e_1}) = h_1^{e_1} \cdots h_{n_2}^{e_2}$ (rather than being 1) if $e_{n_2+1} = \cdots = e_{n_1} = 1$ and $p_*(h_1^{e_1} \cdots h_{n_1}^{e_1}) = 0$ otherwise.

  Computations with the push-forward map are used only once in the analysis of the algorithm, namely in equalities (6) in subsection 4.5. Here, the correct statement is applied.

- In Proposition 4.28 a subset M of $\{(P_1, \ldots, P_n) \in E(K)^n \mid \forall i = 1, \ldots, n : \varphi(P_i) \in \mathbb{P}^1(k)\}$ is fixed and a lower bound on the number of elements $P \in E(K)$ such that there exists a φ-isolated decomposition $(P_1, \ldots, P_n)$ of P or $-P$ with $P_1, \ldots, P_n \in M$ is given. This lower bound is a difference, and in the subtrahend a factor of $n!$ is missing. The correct lower bound is:

$$\frac{\#M - n^3 \cdot n! \cdot 2^{2n^2-n} \cdot (q+1)^{n-1}}{n! \cdot 2^{n^2}}$$

  In a similar way, the next lower bound is also incorrect. All following bounds are correct again and no further changes have to be performed for the proof of Proposition 4.29. Proposition 4.28 is also cited for Proposition 5.9 in [Die11a], which is concerned with an application for fixed n. This proposition is not at all affected by the cited misprint.