Symmetrized summation polynomials: using small order torsion points to speed up elliptic curve index calculus

Jean-Charles Faugère, Louise Huot, Antoine Joux, Guénaël Renault, Vanessa Vitse

Symmetrized Summation Polynomials: Using Small Order Torsion Points to Speed up Elliptic Curve Index Calculus

Jean-Charles Faugère[1,2,3], Louise Huot[2,1,3], Antoine Joux[4,5,2,3], Guénaël Renault[2,1,3], and Vanessa Vitse[6]

[1] INRIA, POLSYS, Centre Paris-Rocquencourt, F-78153, Le Chesnay, France
[2] Sorbonne Universités, UPMC Univ Paris 06, LIP6 UPMC, F-75005, Paris, France
[3] CNRS, UMR 7606, LIP6 UPMC, F-75005, Paris, France
[4] CryptoExperts, Paris, France
[5] Chaire de Cryptologie de la Fondation UPMC
[6] Institut Fourier, Université Joseph Fourier, Grenoble I, France
jean-charles.faugere@inria.fr, louise.huot@lip6.fr, antoine.joux@m4x.org, guenael.renault@lip6.fr, vanessa.vitse@ujf-grenoble.fr

Abstract. Decomposition-based index calculus methods are currently efficient only for elliptic curves E defined over non-prime finite fields of very small extension degree n. This corresponds to the fact that the Semaev summation polynomials, which encode the relation search (or "sieving"), grows over-exponentially with n. Actually, even their computation is a first stumbling block and the largest Semaev polynomial ever computed is the 6-th. Following ideas from Faugère, Gaudry, Huot and Renault, our goal is to use the existence of small order torsion points on E to define new summation polynomials whose symmetrized expressions are much more compact and easier to compute. This setting allows to consider smaller factor bases, and the high sparsity of the new summation polynomials provides a very efficient decomposition step. In this paper the focus is on 2-torsion points, as it is the most important case in practice. We obtain records of two kinds: we successfully compute up to the 8-th symmetrized summation polynomial and give new timings for the computation of relations with degree 5 extension fields.

Keywords: ECDLP, elliptic curves, decomposition method, index calculus, Semaev polynomials, multivariate polynomial systems, invariant theory

1 Introduction

In the past decade, the resolution of the discrete logarithm problem (DLP) on elliptic curves defined over extension fields has made important theoretical advances. Besides transfer attacks such as GHS [7], a promising approach is the

This work has been partially supported by the LabExPERSYVAL-Lab(ANR-11-LABX-0025) and the HPAC grant of the French National Research Agency (HPAC ANR-11-BS02-013)

decomposition-based index calculus method pioneered by Gaudry and Diem [6,2], following ideas from Semaev [13]. As in any index calculus, this method is composed of two main steps: the relation search during which relations between elements of a factor base are collected, and the linear algebra stage during which the discrete logarithms are extracted using sparse matrix techniques. Since this second step is not specific to curve-based DLP, this article mainly focuses on the relation search.

In the standard decomposition method, the relations are obtained by solving, for given points $R \in E(\mathbb{F}_{q^n})$ related to the challenge, the equation

$$R = P_1 + \cdots + P_n, \quad P_i \in \mathcal{F} \tag{1}$$

where $\mathcal{F} \subset E(\mathbb{F}_{q^n})$ is the factor base (this is the so-called *point decomposition problem*). The resolution of this problem relies critically on the Weil restriction structure of E relative to the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$. In almost all preceding works [6,11,4], the usual factor base is defined as $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : x(P) \in \mathbb{F}_q\}$, where $x(P)$ stands for the abscissa of P, possibly after a change of equation of E. Then (1) translates algebraically using the *Semaev polynomial* $\mathrm{Sem}_{n+1} \in \mathbb{F}_{q^n}[X_1, \ldots, X_{n+1}]$ as

$$\mathrm{Sem}_{n+1}(x_1, \ldots, x_n, x(R)) = 0 \tag{2}$$

where the unknowns are $x_i = x(P_i) \in \mathbb{F}_q$. It is worth noticing that the resolution of this equation is the keystone of the relation search step. Thus, computing Semaev polynomials for larger values of n or finding ways to increase the efficiency of this resolution will undoubtedly enhance the practical impact of decomposition attacks and is the main goal of this paper.

Equation (2) is equivalent through a restriction of scalars to a multivariate polynomial system of n equations and n variables over $\mathbb{F}_q$, see [6]. The resolution of many instances of the multivariate polynomial systems arising from (2) (using for example Gröbner bases) is by far the main bottleneck of this index calculus approach. Recently Faugère *et al.* [4] have proposed to speed up the relation search using a 2-torsion point T naturally present on elliptic curves in the Edwards or Jacobi models. Their approach is based on the observation that in these models, the translation by T corresponds to a simple symmetry of the curve. This implies that the corresponding multivariate polynomial systems also admit an additional symmetry, allowing an easier resolution.

In this work, this approach is taken a step further as we investigate how to take advantage of the existence of some small order torsion points. To achieve this, we generalize ideas from Diem [2] who replaces the map $x : E \to \mathbb{F}_{q^n}$ by morphisms $\varphi : E \to \mathbb{P}^1$ of degree two. More precisely, we highlight new morphisms φ which let us take into account the existence of a torsion point T of small order m. The main idea relies on the construction of morphisms φ of degree divisible by m that satisfy the *equivariance property* $\varphi \circ \tau_T = f_T \circ \varphi$ for some homography (i.e. an automorphism of $\mathbb{P}^1$) $f_T \in \mathrm{PGL}_2(\mathbb{F}_q)$, where τ_T stands for the translation-by-T map $P \mapsto P + T$. A first important practical consequence of this setting is that the corresponding summation polynomials admit an additional invariance property, besides the classical one under any permutation of

the variables: this comes from the fact that if $(P_1, \ldots, P_n) \in \mathcal{F}^n$ is a solution to the point decomposition problem (1), then $(P_1 + [k_1]T, \ldots, P_n + [k_n]T)$ is also a solution as soon as $\sum_i k_i = 0\ [m]$. Using invariant theory, it is possible to express the summation polynomials in term of fundamental invariants. This new representation of the summation polynomials makes them very sparse and much easier to compute, and in particular we succeeded in computing new summation polynomials. This sparsity also leads to a significant simplification of the multivariate systems arising from the analog of (2). A second consequence is that the associated factor base $\mathcal{F} = \{P \in E : \varphi(P) \in \mathbb{P}^1(\mathbb{F}_q)\}$ becomes invariant under translations by multiples of T: this allows a division of the size of the factor base by the order m of T, thus speeding up by a factor m^2 the linear algebra step.

We begin in the next section by defining the summation polynomials associated to arbitrary morphisms $\varphi : E \to \mathbb{P}^1$ and explaining their use for index calculus. In section 3, we investigate the equivariance property satisfied by φ and explain the expected benefit when the small order points are accounted for. Then we focus in Section 4 on the fundamental case of degree 2 morphisms and their equivariance property with respect to translations by order 2 points. We finally give explicit examples of symmetrized summation polynomials and applications to the point decomposition problem on elliptic curves defined over degree 5 extension fields.

2 Summation polynomials and index calculus

Let E be a given elliptic curve defined over an extension $\mathbb{F}_{q^n}$ of degree $n > 2$ of $\mathbb{F}_q$, and let $\varphi : E \to \mathbb{P}^1$ be a morphism defined over $\mathbb{F}_{q^n}$. We recall that in order to perform a decomposition-based index calculus, we consider the factor base $\mathcal{F} = \{P \in E : \varphi(P) \in \mathbb{P}^1(\mathbb{F}_q)\}$ which has approximately q elements, and try to find relations (decompositions) of the form $R = P_1 + \cdots + P_n$, $P_i \in \mathcal{F}$ where R is a given point related to the challenge. Alternatively, it is possible to consider other type of relations, for instance of the form $R = P_1 + \cdots + P_{n-1}$ (see [11]) or of the form $P_1 + \cdots + P_{n+2} = \mathcal{O}$ (see [10]). To do so, we introduce the summation polynomials related to φ (which can be seen as a generalization of the one described in [2]):

Definition 1 *Let $E_{|K}$ be an elliptic curve defined over a field K and $\varphi : E \to \mathbb{P}^1$ be a non constant morphism. A polynomial $S \in K[X_1, \ldots, X_n]$ is called an* n-th summation polynomial *associated to φ if it satisfies*

$$S(a_1, \ldots, a_n) = 0 \Leftrightarrow \exists P_i \in E(\bar{K}),\ \varphi(P_i) = a_i \text{ and } \sum_{i=1}^{n} P_i = \mathcal{O}\,. \tag{3}$$

Note that in the following, we will always explicitly identify $\mathbb{P}^1(K)$ with $K \cup \{\infty\}$, so that it makes sense to consider $\varphi(P)$ as an element of K (unless P is a pole of φ). Also note that this definition, and in fact a large part of what follows, is actually independent of the index calculus context. A first result is that summation polynomials always exist and are uniquely determined by the considered morphism.

Proposition 2 *For a given non-constant morphism $\varphi : E \to \mathbb{P}^1$ defined over a field K, the set of polynomials satisfying* (3) *is of the form $\{cP^k_{\varphi,n} : c \in K^*, k \in \mathbb{N}^*\}$ where $P_{\varphi,n} \in K[X_1, \ldots, X_n]$. The polynomial $P_{\varphi,n}$ is irreducible, unique up to multiplication by a constant, symmetric when $n \geq 3$, and is called* the n-th summation polynomial *associated to φ.*

Proof. Let $\psi : E^{n-1} \to K^n$ be the rational map such that $\psi(P_1, \ldots, P_{n-1}) = (\varphi(P_1), \ldots, \varphi(P_{n-1}), \varphi(-P_1 - \cdots - P_{n-1}))$. Then clearly $\psi(E^{n-1})$ is irreducible since E^{n-1} is irreducible, and has dimension $n-1$ since φ is surjective. This classically implies the existence of an irreducible polynomial $P_{\varphi,n}$, unique up to a multiplicative constant, such that $\psi(E^{n-1}) = V(P_{\varphi,n})$, and it is easy to check that it satisfies (3).

To prove that $P_{\varphi,n}$ is symmetric, we consider the morphism c from the group of permutations of n elements $\mathfrak{S}_n$ to K^*, such that $c(\sigma)$ is the constant satisfying $P^\sigma_{\varphi,n}(X_1, \ldots, X_n) = c(\sigma)P_{\varphi,n}(X_1, \ldots, X_n)$. This morphism is well-defined since $P^\sigma_{\varphi,n}(X_1, \ldots, X_n) = P_{\varphi,n}(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ is clearly an irreducible solution of (3). It is well-known that the only morphisms from $\mathfrak{S}_n$ to a commutative group are the identity map or the signature map; this means that $P_{\varphi,n}$ is symmetric or alternating. But this last case is incompatible with (3) as soon as $n \geq 3$: indeed, let $a, a_3 \ldots, a_{n-1} \in K$ and $B = \{P_1 + \cdots + P_{n-1} : \varphi(P_1) = \varphi(P_2) = a, \varphi(P_i) = a_i \text{ for } i \geq 3\}$. This set is obviously finite, of cardinality bounded by $\deg(\varphi)^{n-1}$. However if $P_{\varphi,n}$ is alternating, then $P_{\varphi,n}(a, a, a_3, \ldots, a_{n-1}, a_n)$ is always zero, and (3) implies that for all $a_n \in \bar{K}$, there exist $P \in B$ and $P_n \in E(\bar{K})$ such that $\varphi(P_n) = a_n$ and $P + P_n = \mathcal{O}$; thus B is infinite, which is a contradiction.

It is always possible to compute summation polynomials inductively as it is done for the classical Semaev polynomials by using resultants. For $\varphi(P) = x(P)$ (in a Weierstrass model) we recover of course the polynomials introduced by Semaev [13]. Heuristically, it is possible to estimate the degree of $P_{\varphi,n}$ in each variable (which is clearly the same for all variables by symmetry). Let $(a_1, \ldots, a_{n-1}) \in \bar{K}^{n-1}$. The set of solutions of $P_{\varphi,n}(a_1, \ldots, a_{n-1}, X_n) = 0$ can be obtained as in the following diagram, by considering the preimage A of $\{(a_1, \ldots, a_{n-1})\}$ by φ^{n-1} and taking its image by $\varphi \circ (-\sum)$.

$$\begin{array}{ccc} \{(P_1, \ldots, P_{n-1}) \in E(\bar{K})^{n-1} : \varphi(P_i) = a_i\} & \xrightarrow{-\sum} & \{-(P_1 + \cdots + P_{n-1}) : \varphi(P_i) = a_i\} \\ \downarrow \varphi \times \cdots \times \varphi & & \downarrow \varphi \\ \{(a_1, \ldots, a_{n-1})\} & & \{a_n : P_{\varphi,n}(a_1, \ldots, a_{n-1}, a_n) = 0\} \end{array}$$

If φ is separable, then for most $(n-1)$-tuples $(a_1, \ldots, a_{n-1})$, the cardinality of $A = \{(P_1, \ldots, P_{n-1}) \in E(\bar{K})^{n-1} : \varphi(P_i) = a_i\}$ is $(\deg \varphi)^{n-1}$. The map $-\sum : E^{n-1} \to E$ is of course not injective, but heuristically, if φ is a morphism with no special property, the restriction of $-\sum$ to A should be injective in general and the same holds for φ restricted to $-\sum(A)$. For a random map φ, the expected degree of $P_{\varphi,n}$ in each variable should be $(\deg \varphi)^{n-1}$. This is in any case an upper bound on the degree of $P_{\varphi,n}$. In the applications we need to be

able to solve (4) easily, and so we want the degree of $P_{\varphi,n}$ to be rather small; therefore most of this article focuses on the case where $\deg \varphi = 2$.

We detail two important cases where the degree is actually smaller than the bound given above.

1. The first case is when $\varphi(P) = \varphi(-P)$ and occurs in particular for Semaev polynomials (i.e. when $\varphi(P) = x(P)$). Then it is clear that $(P_1, \ldots, P_{n-1}) \in A$ if and only if $(-P_1, \ldots, -P_{n-1}) \in A$, thus $-\sum(A)$ is stable under $[-1] \in \mathrm{End}(E)$ and $\varphi_{|-\sum(A)}$ is 2-to-1. An upper bound on the degree $P_{\varphi,n}$ is then $(\deg \varphi^{n-1})/2$.
2. The second case is when φ factors through an isogeny $\psi : E \to E'$, i.e. $\varphi = \varphi' \circ \psi$ where $\varphi' : E' \to \mathbb{P}^1$. Then it is easy to check that $P_{\varphi,n} = P_{\varphi',n}$, and an upper bound on the degree is given by $(\deg \varphi')^{n-1}$.

In this second case, it is actually equivalent to perform the decomposition attack on E using φ or on E' using φ'. For this reason, we will usually only consider morphisms that do not factor through an isogeny.

For index calculus purposes, in order to compute a decomposition $R = P_1 + \cdots + P_n$, $P_i \in \mathcal{F}$, we use the $(n+1)$-th summation polynomial $P_{\varphi,n+1}$ associated to φ and try to find a solution $(a_1, \ldots, a_n) \in (\mathbb{F}_q)^n$ of the equation

$$P_{\varphi,n+1}(a_1, \ldots, a_n, \varphi(-R)) = 0\,. \tag{4}$$

We then look for points $P_1, \ldots, P_n \in E(\mathbb{F}_{q^n})$ such that $\varphi(P_i) = a_i$ and $P_1 + \cdots + P_n = R$. To solve the equation (4), we take the scalar restriction with respect to a linear basis of the extension $\mathbb{F}_{q^n}/\mathbb{F}_q$, leading to a multivariate polynomial system defined over $\mathbb{F}_q$.

3 Action of torsion points

3.1 Equivariant morphisms

We investigate in this section how the existence of a rational m-torsion point on an elliptic curve E can speed up the decomposition attack. Let $T \in E[m]$; as mentioned in the introduction, our goal is to construct equivariant morphisms $\varphi : E \to \mathbb{P}^1$, i.e. such that there exists $f_T \in \mathrm{Aut}(\mathbb{P}^1)$ satisfying $\varphi(P + T) = f_T(\varphi(P))$ for all $P \in E$: $\varphi \circ \tau_T = f_T \circ \varphi$.

Let d be the order of f_T; clearly d divides m. If d is strictly smaller than m, then $\varphi \circ \tau_{[d]T} = f_T^{\circ d} \circ \varphi = \varphi$. This implies that φ can be factorized through the quotient isogeny $\pi : E \to E/\langle [d]T \rangle$ as $\varphi = \varphi' \circ \pi$. In particular, the relation search on E using φ and T is equivalent to the relation search on $E' = E/\langle [d]T \rangle$ using φ' and $\pi(T) \in E'[d]$, which does not fully exploit the property of T being a m-torsion point. This condition that the homography f_T has order m implies some restriction about the degree of φ.

Proposition 3 *Let $T \in E[m]$ be a m-torsion point and $f_T \in Aut(\mathbb{P}^1)$ a homography of order m. Suppose there exists $\varphi : E \to \mathbb{P}^1$ such that $\varphi \circ \tau_T = f_T \circ \varphi$. Then m divides the degree of φ.*

Proof. Let us denote $e_\psi(P)$ the ramification index of a curve morphism $\psi : \mathcal{C}_1 \to \mathcal{C}_2$ at a point $P \in \mathcal{C}_1$. Then for any point $P \in E$, we have $e_{\varphi\circ\tau_T}(P) = e_{\tau_T}(P) \cdot e_\varphi(\tau_T(P)) = e_\varphi(P+T)$ and $e_{\varphi\circ\tau_T}(P) = e_{f_T\circ\varphi}(P) = e_\varphi(P)\cdot e_{f_T}(\varphi(P)) = e_\varphi(P)$ since f_T and τ_T are isomorphisms. In particular φ has the same ramification index at P and its translates $P+T, \ldots, P+[m-1]T$. We consider now a fixed point $z \in \mathbb{P}^1$ of f_T (which always exists in an extension of K). Then $\varphi^{-1}(\{z\})$ is stable under translation by T, so that for each point P in $\varphi^{-1}(\{z\})$, its m translates $P, P+T, \ldots, P+[m-1]T$ also belong to $\varphi^{-1}(\{z\})$ and have the same ramification index. Since $\deg(\varphi) = \sum_{P\in\varphi^{-1}(z)} e_\varphi(P)$, the degree of φ is necessarily a multiple of m.

More generally, if $E(K)$ has a subgroup G of small order, we would like to find an equivariant morphism $\varphi : E \to \mathbb{P}^1$ such that for any $T \in G$, there exists $f_T \in \mathrm{Aut}(\mathbb{P}^1(K)) \simeq \mathrm{PGL}_2(K)$ such that $\varphi \circ \tau_T = f_T \circ \varphi$. Then the map $\chi : T \mapsto f_T$ is a group morphism from G to $\mathrm{PGL}_2(K)$ that we want to be injective by the above remark (since otherwise φ would factorize through $E/\ker(\chi)$). Unfortunately the set of possible subgroups relevant for our purpose is very restricted.

Proposition 4 *Let G be a finite subgroup of $E(K)$ and $\chi : G \to \mathrm{PGL}_2(K)$ an injective group morphism. Then G is of one of the following forms:*

1. $G = E[2]$,
2. $G = \langle T\rangle$ *where* $T \in E[m]$ *with m coprime to char*(K),
3. $G = E[$*char*$(K)]$.

Proof. Since χ is injective, the commutative group G is isomorphic to a subgroup of $\mathrm{PGL}_2(K)$. It follows from the list in [14] that the only finite commutative subgroups of $\mathrm{PGL}_2(K)$ of order prime to the characteristic are either cyclic or isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; furthermore, it is easy to see that $\mathrm{PGL}_2(K)$ has no element whose order is a strict multiple of the characteristic. Thus the only subgroups of $E(K)$ that are of interest for our construction are either $E[2]$ or cyclic, generated by a point of order $\mathrm{char}(K)$ or prime to $\mathrm{char}(K)$.

In what follows, we only deal with the case where the homography f_T has order exactly m. Besides small torsion points, we would also like to take into account the automorphisms of the curve E; for most curves this only means the involution $[-1] : P \mapsto -P$. The group of permutations of E generated by the translation by T and $[-1]$ is isomorphic to the dihedral group $D_m = \mathbb{Z}/m\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$, so an equivariant morphism φ (if it exists) would give rise to an action on $\mathbb{P}^1$, i.e. a group morphism from D_m to $\mathrm{PGL}_2(K)$. As noted above, this map should be injective when restricted to the subgroup $\mathbb{Z}/m\mathbb{Z}$ generated by τ_T, since otherwise φ can be factorized through an isogeny. For $m > 2$, it is an easy exercise to show that such a group morphism is necessarily injective; in contrast, for $m = 2$ it is possible to impose the additional property $\varphi(-P) = \varphi(P)$ for all $P \in E$. Note that in the finite field case, $\mathrm{PGL}_2(\mathbb{F}_q)$ has a subgroup isomorphic to D_m if and only if $m|(q-1)$ or $m|(q+1)$ or $m = \mathrm{char}(\mathbb{F}_q)$ when $m > 2$.

3.2 Reducing the factor base

We consider an elliptic curve E defined over $\mathbb{F}_{q^n}$ with an m-torsion point T and denote by $\sim$ the equivalence relation given by $P \sim P'$ if and only if $P - P' \in \langle T \rangle$. Assume that there exists an equivariant morphism $\varphi : E \to \mathbb{P}^1(\mathbb{F}_{q^n})$ such that the associated homography f_T is in $\mathrm{PGL}_2(\mathbb{F}_q)$. Then the associated choice of factor base $\mathcal{F} = \{P \in E(\mathbb{F}_{q^n}) : \varphi(P) \in \mathbb{P}^1(\mathbb{F}_q)\}$ is invariant with respect to the translation by T, i.e. if $P \sim P'$ and $P \in \mathcal{F}$ then $P' \in \mathcal{F}$. Therefore, it is possible to divide the size of the factor base by m, by considering a reduced factor base $\mathcal{F}'$ that includes only one element for each equivalence class of elements of $\mathcal{F}$.

This modifies slightly the relation search. Each decomposition $R = P_1 + \cdots + P_n$, $P_i \in \mathcal{F}$ can be rewritten as $R = (Q_1 + [k_1]T) + \cdots + (Q_n + [k_n]T)$ with $0 \leq k_i < m$ and where $Q_i \in \mathcal{F}'$ satisfies $Q_i \sim P_i$. We then just store the essentially equivalent relation $[m]R = [m]Q_1 + \cdots + [m]Q_n$. The important fact is that subsequently we only need about $\#\mathcal{F}/m$ relations to compute the discrete logarithms, and that the dimension of the relation matrix used in the resulting linear algebra step is also divided by m providing a speed-up by a factor m^2. On the other hand, this decreases the probability that a random point R decomposes by a factor m^{n-1} (there are more tuples in each preimage of the map $\mathcal{F}^n \to E$, $(P_1, \ldots, P_n) \mapsto \sum_i P_i$, so there are less points in the image), but this is more than compensated by the improved resolution of the associated polynomial systems as explained below.

Of course, if φ is also equivariant with respect to the automorphism $[-1]$ then it is possible to further reduce the factor base by 2. If $m = 2$ and E has full 2-torsion it is often possible to construct a morphism φ equivariant with respect to $[-1]$ and translations by any 2-torsion points, thus allowing a division by 8 of the size of the factor base.

3.3 Symmetries of summation polynomials

We have seen in Prop.2 that the summation polynomials are always symmetric for $n \geq 3$. In particular, they can be expressed in terms of elementary symmetric polynomials $e_1, \ldots, e_n$ in the variables $X_1, \ldots, X_n$. This allows a reduction of the size and the total degree of the summation polynomials, thus simplifying their computation (for instance, it is possible to compute resultants of already partially symmetrized polynomials as was done in [11]). More importantly, this reduction has an impact on the resolution of the multivariate polynomial systems: instead of solving (4), we rather consider the (partially) symmetrized equation $P_{\varphi,n+1}(e_1, \ldots, e_n, \varphi(-R)) = 0, e_1, \ldots, e_n \in \mathbb{F}_q$. Of course, this adds a simple desymmetrization step in order to recover the corresponding solutions of (4) whenever they exist.

This approach can be extended when φ is equivariant with respect to translation by an m-torsion point T. Let $(a_1, \ldots, a_n)$ be a solution of $P_{\varphi,n}(a_1, \ldots, a_n) = 0$, so that there exist points $P_1, \ldots, P_n \in E(\bar{K})$ such that $\varphi(P_i) = a_i$ and $\sum P_i = \mathcal{O}$. Then for any $k_1, \ldots, k_n$ such that $m | \sum k_i$, we have $\sum (P_i + [k_i]T) = \mathcal{O}$. Thus $P_{\varphi,n}(f_T^{k_1}(a_1), \ldots, f_T^{k_n}(a_n)) = 0$. In particular $P_{\varphi,n}(f_T^{k_1}(X_1), \ldots, f_T^{k_n}(X_n))$ is also

a solution of (3), except that it is a rational function instead of a polynomial if f_T is not an affine homography. We will see that $P_{\varphi,n}$, or an associated rational fraction $Q_{\varphi,n}$, is actually often invariant under this transformation; more formally, and taking into account Prop.2, it is invariant under an action of the group $G = (\mathbb{Z}/m\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$. Then $P_{\varphi,n}$, resp. $Q_{\varphi,n}$, belongs to the invariant ring $K[X_1, \ldots, X_n]^G$ or the invariant field $K(X_1, \ldots, X_n)^G$. In particular, it can be expressed in terms of generators of the invariant ring or field allowing a further reduction of the size and the total degree of the systems; this will be detailed in the next section for $m = 2$. For index calculus purpose when $K = \mathbb{F}_{q^n}$, it is necessary that these invariant generators lie in $\mathbb{F}_q(X_1, \ldots, X_n)$. This means that the action of G restricts to an action on $\mathbb{F}_q(X_1, \ldots, X_n)$.

4 Summation polynomials associated to degree two morphisms

We consider the simplest case where φ has degree 2 (note that in this case φ is necessarily separable).

Proposition 5 *Let E be an elliptic curve defined over a field K with Weierstrass coordinate functions x, y such that $[K(E) : K(x)] = 2$, and let $\varphi : E \to \mathbb{P}^1$ be a morphism of degree 2. Then there exist an homography $h \in \mathrm{PGL}_2(\bar{K})$ and a point $Q \in E(\bar{K})$ such that $\varphi = h \circ x \circ \tau_{-Q}$, i.e. $\varphi(P) = h(x(P - Q))$.*

Proof. Let $\mathcal{R}$ be the set of ramification points of φ, that is the set of points $P \in E$ such that the ramification index $e_\varphi(P)$ is strictly greater than 1. We easily deduce from the Hurwitz formula that the set $\mathcal{R}$ is non empty. For a given ramification point $Q \in E$, we consider an homography $\psi \in \mathrm{Aut}(\mathbb{P}^1)$ sending the point $\varphi(Q)$ to the point at infinity $[1 : 0]$ of $\mathbb{P}^1$. Let $\tau_Q : E \to E$ denote the translation by Q, then the morphism $\varphi' = \psi \circ \varphi \circ \tau_Q$ is ramified at $\mathcal{O} = [0 : 1 : 0]$. In particular, since φ has degree 2, φ' has a unique pole at $\mathcal{O}$ of order 2, so that there exist $a, b \in K$ such that $\varphi' = ax + b$. This shows that there exists an homography $h \in \mathrm{Aut}(\mathbb{P}^1)$ such that $\varphi(P) = h(x(P - Q))$.

To compute the associated summation polynomial, it is easy to check that the numerator of the rational fraction $\mathrm{Sem}_{n+1}(h^{-1}(X_1), \ldots, h^{-1}(X_n), x([n]Q))$ where Sem_{n+1} stands for $(n+1)$-th Semaev polynomial, satisfies the property (3). In the case where $Q = \mathcal{O}$ or more generally $Q \in E[n]$, the above expression can be simplified by considering the numerator of $\mathrm{Sem}_n(h^{-1}(X_1), \ldots, h^{-1}(X_n))$. The degree of $P_{\varphi,n}$ in each variable is then equal to 2^{n-1} if $Q \notin E[n]$ and 2^{n-2} otherwise. For index calculus, it is clear that φ should be of the form $h \circ x$: not only is the degree of P_φ smaller, but we also have $\forall P \in E, \varphi(-P) = \varphi(P)$. As mentioned above, this allows to reduce by a further 2 the size of the factor base.

4.1 Speeding up the relation search using one 2-torsion point

It turns out that every degree 2 morphism satisfies an equivariance property with respect to 2-torsion points; this is specific to the degree 2 case.

Lemma 6 *Let E be an elliptic curve defined over K with a 2-torsion point T, and let $\varphi : E \to \mathbb{P}^1$ be a morphism of degree 2. Then there exists $f_T \in \mathrm{PGL}_2(K)$ such that $\varphi(P+T) = f_T(\varphi(P))$ for all $P \in E$.*

Proof. In the special case of $\varphi = x$ where x is a Weierstrass coordinate function such that $[K(E) : K(x)] = 2$, the existence is given directly by the addition formula on E. Let $g_T \in \mathrm{PGL}_2(K)$ be this homography such that $x(P+T) = g_T(x(P))$ for all $P \in E$. For a more general morphism $\varphi = h \circ x \circ \tau_{-Q}$, the homography $f_T = h \circ g_T \circ h^{-1}$ satisfies the property.

In the remainder of this section, we denote by T a rational 2-torsion point, $\varphi : E \to \mathbb{P}^1$ a degree 2 rational map such that $\varphi(P) = \varphi(-P)$, and f_T the involution of $\mathbb{P}^1$ such that $\varphi(P+T) = f_T(\varphi(P))$ for all $P \in E$.

Let $W = \{(P_1, \ldots, P_n) : \sum P_i = \mathcal{O}\} \subset E^n$. This sub-variety has many symmetries besides the action of the symmetric group. As mentioned above, we consider the group $G_2 = (\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$, (called *dihedral Coxeter group* in [4]). It is an abstract reflexion group, corresponding to the Coxeter diagram D_n, and its elements will be denoted by $((\epsilon_1, \ldots, \epsilon_n), \sigma) \in \{0;1\}^n \times \mathfrak{S}_n$ where $\epsilon_1 + \cdots + \epsilon_n = 0 \mod 2$ (i.e. we explicitly identify G_2 with a subgroup of the group $(\mathbb{Z}/2\mathbb{Z})^n \rtimes \mathfrak{S}_n$ of isometries of the hypercube). The group G_2 acts on E^n by $((\epsilon_1, \ldots, \epsilon_n), \sigma) \cdot (P_1, \ldots, P_n) = ([\epsilon_1]T + P_{\sigma(1)}, \ldots, [\epsilon_n]T + P_{\sigma(n)})$ and leaves W globally invariant.

The image of W by φ^n is $V = V(P_{\varphi,n}) \subset (\mathbb{P}^1)^n$, the set of zeroes of the summation polynomial associated to φ. This set is also left globally invariant by the rational action of G_2 on $(\mathbb{P}^1)^n$ given by $((\epsilon_1, \ldots, \epsilon_n), \sigma) \cdot (a_1, \ldots, a_n) = (f_T^{\epsilon_1}(a_{\sigma(1)}), \ldots, f_T^{\epsilon_n}(a_{\sigma(n)}))$. This means that for any $g \in G_2$, $P^g_{\varphi,n}(X_1, \ldots, X_n) = P_{\varphi,n}(f_T^{\epsilon_1}(X_{\sigma(1)}), \ldots, f_T^{\epsilon_n}(X_{\sigma(n)}))$ is still a solution of (3), except that it is a rational fraction and no longer a polynomial unless f_T is affine. In particular, the summation polynomials associated to φ have additional symmetries, that are simple to handle only when f_T is affine, i.e. when we stay within the framework of polynomials and invariant rings.

Proposition 7 *Assume the involution $f_T \in \mathrm{PGL}_2(K)$ affine. Then for $n \geq 3$ the n-th summation polynomial $P_{\varphi,n}$ is invariant under the action of G_2 i.e. for all $g = (\underline{\epsilon}, \sigma) \in G_2$, $P_{\varphi,n}(X_1, \ldots, X_n) = P_{\varphi,n}(f_T^{\epsilon_1}(X_{\sigma(1)}), \ldots, f_T^{\epsilon_n}(X_{\sigma(n)}))$.*

Proof. A special case of this proposition has already been proved in [4]; for the sake of completeness, we rephrase the demonstration in our more general setting. Since $P^g_{\varphi,n}$ is again an irreducible summation polynomial associated to φ, there exist $c(g) \in K^*$ such that $P^g_{\varphi,n} = c(g)P_{\varphi,n}$. This gives us a morphism $c : G_2 = (\mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n \to K^*$ and from Prop.2 $c(\mathfrak{S}_n) = 1$. Let $u = ((1,1,0,\ldots,0), e)$ where $e \in \mathfrak{S}_n$ is the neutral element, and $v = (\underline{0}, (1\ 2\ 3))$. It is clear that G_2 is generated by u together with $\mathfrak{S}_n$, so that the image of c is completely determined by the value of u. Since $u^2 = 1$, we have $c(u) = \pm 1$. Now an easy computation shows that $(uv)^3 = 1$, so $1 = c(uv)^3 = c(u)^3 c(v)^3 = c(u)^3 = c(u)$.

This means that $P_{\varphi,n} \in K[X_1, \ldots, X_n]^{G_2}$, the ring of invariants of G_2. Since the action of G_2 is generated by pseudo-reflections, the Chevalley-Shephard-Todd theorem states that $K[X_1, \ldots, X_n]^{G_2}$ is itself a polynomial ring when the

characteristic of K is greater than n; we will show later that it is in fact true in any characteristic. But first, we give a condition on E and T to assure the existence of a degree 2 morphism φ such that the corresponding homography f_T is affine. Moreover when this condition is satisfied, we can take without loss of generality f_T equal to $x \mapsto -x$ in odd characteristic or $x \mapsto x+1$ in characteristic 2.

Proposition 8 *Let E be an elliptic curve defined over a field K.*
(i) If $char(K) \neq 2$, then there exist $T \in E(K)[2]$ and $\varphi : E \to \mathbb{P}^1$ a degree 2 morphism such that $\varphi(P+T) = -\varphi(P)$ and $\varphi(-P) = \varphi(P)$ if and only if there exist $T' \in E[4]$ such that $x(T') \in K$. In this case $T = [2]T'$ and the curve E has an equation of the form $y^2 = x^3 + ax^2 + bx$ where $T = (0,0)$ and b is a square in K; moreover, φ is of the form

$$\lambda \frac{x(P) + \sqrt{b}}{x(P) - \sqrt{b}},$$

for a choice of the square root of b and $\lambda \in K$.
(ii) If $char(K) = 2$ and $j(E) \neq 0$, then E admits an equation of the form $y^2 + xy = x^3 + ax^2 + b$ with a unique non-trivial 2-torsion point $T = (0, \sqrt{b})$. Then the morphisms φ such that $\varphi(-P) = \varphi(P)$ and $\varphi(P+T) = \varphi(P) + 1$ are of the form

$$\frac{b^{1/4}}{x(P) + b^{1/4}} + \lambda, \text{ where } \lambda \in K.$$

If $char(K) = 2$ and $j(E) = 0$, there is no non-trivial 2-torsion point.

Proof. (i) Suppose there exists a 2-torsion point $T \in E(K)[2]$, then up to a translation we can assume that $T = (0,0)$ and that E has an equation of the form $y^2 = x^3 + ax^2 + bx$. From the addition formula, we get $x(P+T) = g_T(x(P)) = b/x(P)$. Let φ be a degree 2 morphism such that $\varphi(-P) = \varphi(P)$. From Prop.5, there exists $h \in \mathrm{PGL}_2(K)$ such that $\varphi = h \circ x$, and $\varphi(P+T) = f_T(\varphi(P))$ where $f_T = h \circ g_T \circ h^{-1}$. Thus we are looking for an homography $h \in \mathrm{PGL}_2(K)$ conjugating g_T to $z \mapsto -z$. By considering the associated matrices or the set of fixed points, it is easy to see that there exists such an $h \in \mathrm{PGL}_2(K)$ if and only if b is a square, and that all such h are of the form $h(x) = \lambda \left(\frac{x-\sqrt{b}}{x+\sqrt{b}}\right)^{-1}$.

Now, if b is a square in K, then any of the points $T' \in E(\bar{K})$ of abscissa $\pm\sqrt{b}$ satisfies $[2]T' = T$, and are thus in $E(K)$. Reciprocally, if there exists $T' \in E[4]$ such that $x(T') \in K$, then $[2]T'$ is in $E(K)[2]$, and up to a translation E has an equation as above with b square in K.
(ii) It is already well-known that in characteristic 2 an elliptic curve has a non-trivial 2-torsion point if and only if $j(E) \neq 0$. If E has an equation of the form $y^2 + xy = x^3 + ax^2 + b$ and $T = (0, \sqrt{b})$, the addition formula gives $x(P+T) = g_T(x(P)) = \sqrt{b}/x(P)$. Now in characteristic 2, there always exists $h \in \mathrm{PGL}_2(K)$ that conjugates the homography $g_T(x) = \frac{\sqrt{b}}{x}$ to $x \mapsto x+1$, and it is easy to see that all such h are of the form $x \mapsto \frac{b^{1/4}}{x+b^{1/4}} + \lambda$, $\lambda \in K$.

The first part of Prop.8 generalizes the results given in [4], where the morphism φ is obtained as a projection onto a coordinate for curves in twisted Edwards form. The fact that the morphism φ depends of a parameter $\lambda \in K$ is important for index calculus applications, since it allows to define different factor bases depending on the choice of λ.

Remark 9 *Lemma 6 shows that every degree* 2 *morphism satisfies an equivariance property* $\varphi(P+T) = f_T(\varphi(P))$*; the above proposition only describes the cases for which* f_T *is as simple as possible. In odd characteristic, about half of the curves with a* 2*-torsion point have a coefficient* b *that is a square, and thus satisfies directly the hypotheses of the proposition. However if the curve has full* 2*-torsion (i.e.* a^2-4b *is a square) then it is* 2*-isogenous to a curve with a rational* 4*-torsion point, again satisfying the hypotheses. Overall, this proposition applies in odd characteristic to about* $3/4$ *of curves with a* 2*-torsion point.*

4.2 Action of the full 2-torsion.

In this subsection, K is a field of characteristic different from 2. Let E be an elliptic curve having a complete rational 2-torsion (in the finite field case, this is equivalent up to a 2-isogeny to the cardinality of E being divisible by 4). Let T_0, T_1 and $T_2 = T_0 + T_1$ be the three non-trivial 2-torsion points of E. According to Lem.6, for any degree 2 morphism φ, there exist homographic involutions f_0, f_1 and $f_2 = f_0 \circ f_1$ such that $\forall P \in E, \forall i \in \{0;1;2\}, \varphi(P+T_i) = f_i(\varphi(P))$. In the same way as before, we can consider the action on $(\mathbb{P}^1)^n$ of the reflexion group $G_4 = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^{n-1} \rtimes \mathfrak{S}_n$ seen as a subgroup of $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^n \rtimes \mathfrak{S}_n$ which is given by

$$((\epsilon_1, \ldots, \epsilon_n), (\epsilon'_1, \ldots, \epsilon'_n), \sigma) \cdot (a_1, \ldots, a_n) = (f_0^{\epsilon_1} \circ f_1^{\epsilon'_1}(a_{\sigma(1)}), \ldots, f_0^{\epsilon_n} \circ f_1^{\epsilon'_n}(a_{\sigma(n)}))\,.$$

This means that for any $g \in G_4$, the rational fraction

$$P^g_{\varphi,n}(X_1, \ldots, X_n) = P_{\varphi,n}(f_0^{\epsilon_1} \circ f_1^{\epsilon'_1}(X_{\sigma(1)}), \ldots, f_0^{\epsilon_n} \circ f_1^{\epsilon'_n}(X_{\sigma(n)}))$$

satisfies again (3). But it is no longer possible that $P^g_{\varphi,n}$ is a polynomial for all $g \in G_4$. Indeed, f_0, f_1 and f_2 must commute because of the commutativity of the group law on E, but it is easy to check that two distinct affine involutions cannot commute. Thus the best we can hope is that one of the three involutions is affine, without loss of generality equal to $z \mapsto -z$; then the two remaining involutions are necessarily of the form $z \mapsto c/z$ and $z \mapsto -c/z$ since they all commute. We give below a condition for the best case where $c = 1$.

Proposition 10 *Let* E *be an elliptic curve in twisted Legendre form* $y^2 = cx(x-1)(x-\lambda)$*. Let* $\Delta_0 = \lambda$*,* $\Delta_1 = (1-\lambda)$ *and* $\Delta_2 = -\lambda(1-\lambda)$*. Then there exists a degree* 2 *morphism* φ *such that* $\varphi(-P) = \varphi(P)$ *and the associated involutions are* $\{f_0; f_1; f_2\} = \{z \mapsto -z; z \mapsto \frac{1}{z}; z \mapsto -\frac{1}{z}\}$ *if and only if there are at least two squares among* $\{\Delta_0; \Delta_1; \Delta_2\}$*.*

Proof. Let $T_0 = (0,0)$, $T_1 = (1,0)$ and $T_2 = (\lambda, 0)$ be the non-trivial 2-torsion points of E. Then the abscissa of $P + T_i$ is equal to $g_i(x_P)$, where

$$g_0(x) = \frac{\lambda}{x}, \quad g_1(x) = \frac{x-\lambda}{x-1}, \quad g_2 = g_0 \circ g_1 = g_1 \circ g_0 \,.$$

To determine if these involutions can be conjugated to $z \mapsto -z$, $z \mapsto \frac{1}{z}$ and $z \mapsto -\frac{1}{z}$, we look at their fixed points. Let Fix_i be the set of fixed points of g_i for $i = 0, 1, 2$; then Fix_i is non empty if and only Δ_i is a square. As $\{0; \infty\}$ and $\{\pm 1\}$ are the set of fixed points of $z \mapsto -z$ and $z \mapsto \frac{1}{z}$ respectively, we deduce easily that there must be at least two squares among $\{\Delta_0; \Delta_1; \Delta_2\}$. Reciprocally, if there are two squares among $\{\Delta_0; \Delta_1; \Delta_2\}$, then it is possible to find an homography $h \in \mathrm{PGL}_2(K)$ sending the fixed points of the corresponding involutions to $\{0; \infty\}$ and $\{\pm 1\}$, and we can take $\varphi(P) = h(x(P))$.

Remark 11 *The condition that Δ_i is a square in K is equivalent to the existence of a 4-torsion point T_i' with a rational x-coordinate such that $[2]T_i' = T_i$. If $p \equiv 1$ [4] then $\Delta_0\Delta_1\Delta_2$ is a square so there are exactly one or three squares among $\{\Delta_0; \Delta_1; \Delta_2\}$, and heuristically the latter should occur for about one curve out of four. Similarly if $p \equiv 3$ [4] then there are exactly zero or two squares among the Δ_i, the latter occurring heuristically for $3/4$ of the curves. Overall about half of the curves in twisted Legendre form will satisfy the hypotheses of the above proposition. For the remaining curves one has to work with degree 2 morphisms whose equivariance property has a less simple expression.*

Proposition 12 *Suppose that the hypotheses of Prop.10 are satisfied. Then the rational fraction*

$$Q_{\varphi,n}(X_1, \ldots, X_n) = \frac{P_{\varphi,n}(X_1, \ldots, X_n)}{(X_1 \cdots X_n)^{2^{n-3}}}$$

is invariant under the action of G_4 for $n \geq 3$, i.e. for all $g = ((\underline{\epsilon}, \underline{\epsilon}'), \sigma) \in G_4$,

$$\begin{aligned} Q_{\varphi,n}(X_1, \ldots, X_n) &= Q_{\varphi,n}(f_0^{\epsilon_1} \circ f_1^{\epsilon_1'}(X_{\sigma(1)}), \ldots, f_0^{\epsilon_n} \circ f_1^{\epsilon_n'}(X_{\sigma(n)})) \\ &= Q_{\varphi,n}((-1)^{\epsilon_1} X_{\sigma(1)}^{(-1)^{\epsilon_1'}}, \ldots, (-1)^{\epsilon_n} X_{\sigma(n)}^{(-1)^{\epsilon_n'}}) \,. \end{aligned}$$

Proof. From Prop.7 the polynomial $P_{\varphi,n}$ is invariant under the action of G_2 (identified with the subgroup of G_4 whose elements are of the form $(\underline{\epsilon}, \underline{0}, \sigma)$), and it is also obviously true for the denominator $(X_1 \cdots X_n)^{2^{n-3}}$. Since G_4 is generated by G_2 and $u' = (\underline{0}, (1,1,0,\ldots,0), e)$ (where $e \in \mathfrak{S}_n$ is the neutral element), it is sufficient to check that $Q_{\varphi,n}^{u'} = Q_{\varphi,n}$. The degree of $P_{\varphi,n}$ is 2^{n-2} in each variable, so $P'(X_1, \ldots, X_n) = (X_1X_2)^{2^{n-2}} P_{\varphi,n}(1/X_1, 1/X_2, X_3, \ldots, X_n)$ is an irreducible polynomial of $K[X_1, \ldots, X_n]$ satisfying (3); in particular, there exists $c \in K$ such that $P' = c \cdot P_{\varphi,n}$ and consequently

$$Q_{\varphi,n}^{u'}(X_1, \ldots, X_n) = Q_{\varphi,n}(1/X_1, 1/X_2, X_3, \ldots, X_n) = c \cdot Q_{\varphi,n}(X_1, \ldots, X_n) \,.$$

Now the same reasoning as in the proof of Prop.7 shows that $c = 1$.

4.3 Invariant fields and invariant rings

We have seen that when the action of the 2-torsion points is taken into account in the choice of the morphism φ, the associated summation polynomial $P_{\varphi,n}$ and rational fraction $Q_{\varphi,n}$ belong respectively to the invariant ring $K[X_1,\dots,X_n]^{G_2}$ and the invariant field $K(X_1,\dots,X_n)^{G_4}$. Hilbert's finiteness theorem implies that the invariant ring $K[X_1,\dots,X_n]^{G_2}$ is finitely generated, and Galois theory states that $K(X_1,\dots,X_n)^{G_4}$ is a subfield of $K(X_1,\dots,X_n)$ with corresponding extension degree $|G_4| = 4^{n-1}n!$. The goal of this section is to determine generators for these two structures.

We recall that the action of G_2 on $K[X_1,\dots,X_n]$ and $K(X_1,\dots,X_n)$ is given by permutations of variables and any even change of signs, while the action of G_4 on $K(X_1,\dots,X_n)$ also includes taking the inverse of an even number of variables. As already mentioned, the group G_2 is a normal subgroup of $G_2' = (\mathbb{Z}/2\mathbb{Z})^n \rtimes \mathfrak{S}_n$, as is $(\mathbb{Z}/2\mathbb{Z})^n$, and the action of G_2 trivially extends to an action on G_2' by allowing any number of sign changes. This means that we have the following diagram of Galois extensions:

$$\begin{array}{ccccc} & & K(X_1,\dots,X_n) & & \\ & \overset{2^n}{\nearrow} & & \overset{2^{n-1}n!}{\searrow} & \\ K(X_1,\dots,X_n)^{(\mathbb{Z}/2\mathbb{Z})^n} & & & & K(X_1,\dots,X_n)^{G_2} \\ & \underset{n!}{\searrow} & & \underset{2}{\nearrow} & \\ & & K(X_1,\dots,X_n)^{G_2'} & & \end{array}$$

It is easy to verify that $K(X_1,\dots,X_n)^{(\mathbb{Z}/2\mathbb{Z})^n}$ is equal to $K(X_1^2,\dots,X_n^2)$ in odd or zero characteristic and equal to $K(X_1^2+X_1,\dots,X_n^2+X_n)$ in characteristic 2, since the latter is clearly invariant and has the correct extension degree. Let $Y_i = X_i^2 + X_i$ if $\mathrm{char}(K) = 2$ or $Y_i = X_i^2$ otherwise. Then $K(X_1,\dots,X_n)^{G_2'} = K(Y_1,\dots,Y_n)^{\mathfrak{S}_n}$ since $G_2'/(\mathbb{Z}/2\mathbb{Z})^n \simeq \mathfrak{S}_n$, so this invariant field consists of symmetric rational fractions in the Y_i, which is known to be generated by the elementary symmetric polynomials $s_1 = Y_1 + \cdots + Y_n, \dots, s_n = Y_1 \cdots Y_n$. Now let $e_1 = X_1 + \cdots + X_n$ in characteristic 2 and $e_n = X_1 \cdots X_n$ otherwise; we have $e_1^2 + e_1 = s_1$, resp. $e_n^2 = s_n$. Then $K(e_1, s_2, \dots, s_n)$, resp. $K(s_1,\dots,s_{n-1},e_n)$, is invariant under G_2 and a degree 2 extension of $K(s_1,\dots,s_n) = K(X_1,\dots,X_n)^{G_2'}$, hence is equal to the invariant field $K(X_1,\dots,X_n)^{G_2}$. Finally, since $s_1,\dots,s_n$ and e_1 (resp. e_n) belong to $K[X_1,\dots,X_n]$, we have the following proposition

Proposition 13 $K[X_1,\dots,X_n]^{G_2} = \begin{cases} K[e_1,s_2,\dots,s_n] & \textit{in characteristic 2,} \\ K[s_1,\dots,s_{n-1},e_n] & \textit{otherwise.} \end{cases}$

We can use the same argument for the action of G_4 on $K(X_1,\dots,X_n)$, which extends to an action of $G_4' = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^n \rtimes \mathfrak{S}_n$, by considering the normal subgroups G_4 and $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^n$.

$$\begin{array}{ccccc} & & K(X_1,\dots,X_n) & & \\ & \overset{4^n}{\nearrow} & & \overset{4^{n-1}n!}{\searrow} & \\ K(X_1,\dots,X_n)^{(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})^n} & & & & K(X_1,\dots,X_n)^{G_4} \\ & \underset{n!}{\searrow} & & \underset{4}{\nearrow} & \\ & & K(X_1,\dots,X_n)^{G_4'} & & \end{array}$$

The leftmost field $K(X_1,\dots,X_n)^{(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})^n}$ is easily seen to be equal to $K(Z_1,\dots,Z_n)$ where $Z_i = X_i^2 + X_i^{-2}$, and the bottom field $K(X_1,\dots,X_n)^{G_4'}$ is then generated by the elementary symmetric polynomials $\sigma_1 = Z_1 + \cdots + Z_n, \dots, \sigma_n = Z_1 \cdots Z_n$. Finding generators for the invariant field of G_4 is less obvious. Let s_i be the i-th elementary symmetric polynomial in $X_1^2,\dots,X_n^2$ (with the convention that $s_0 = 1$), $w_0 = \sum_{i=0}^{\lfloor n/2\rfloor} s_{2n}/(X_1\cdots X_n)$ and $w_1 = \sum_{i=1}^{\lfloor (n-1)/2\rfloor} s_{2n+1}/(X_1\cdots X_n)$. Then it is only a matter of computation to check that w_0 and w_1 are indeed invariant under the action of G_4; actually, replacing an odd number of variables by their inverse exchanges w_0 and w_1. Moreover, direct computations show that w_0 and w_1 are roots of the polynomial

$$Z^4 - \left(\sum_{i=0}^{\lfloor n/2\rfloor} 2^{2i}\sigma_{n-2i}\right) Z^2 + \left(\sum_{i=0}^{\lfloor (n-1)/2\rfloor} 2^{2i}\sigma_{n-(2i+1)}\right)^2 \in K(X_1,\dots,X_n)^{G_4'}[Z]$$

so they are algebraic of degree 4 over $K(X_1,\dots,X_n)^{G_4'}$. This shows the following proposition

Proposition 14 $K(X_1,\dots,X_n)^{G_4} = K(\sigma_1,\dots,\sigma_n,w_0) = K(\sigma_1,\dots,\sigma_n,w_1) = K(\sigma_1,\dots,\sigma_n,w_0,w_1)$.

These families of generators are of course not algebraically independent. We can in fact choose n generators among them: either removing from the first two families any generator of the form σ_{n-2i}, or removing in the last family any two generators of the σ_i's. From an algorithmic point of view, it is not clear which set of generators is the most efficient for computations of summation polynomials.

5 Examples and applications

5.1 Computation of summation polynomials

Characteristic 2 Let $E : y^2 + xy = x^3 + ax^2 + b$ be an elliptic curve defined over a characteristic 2 field and $\varphi : P \mapsto \frac{\gamma}{x(P)+\gamma} + \lambda$ where $\gamma^4 = b$, as in Prop.8. Then the first summations polynomials associated to φ, expressed in term of the generators $e_1, s_2, \dots, s_n$ of the invariant ring $K[X_1,\dots,X_n]^{G_2}$, are equal to

$$P_{\varphi,3} = s_3 + Ls_2 + L^2(e_1^2 + e_1) + L^3 + \gamma(e_1+\lambda)^2\,,$$

$$P_{\varphi,4} = e_1^2(s_4 + Ls_3 + L^2 s_2 + L^3(e_1^2+e_1) + L^4) + (s_3 + (e_1^2+e_1)L^2 + e_1^2\gamma)^2\,,$$

where $L = \lambda^2+\lambda$. The next polynomials become too large to be reproduced with λ and γ as formal parameters, so we give them for $\lambda = 0$. Note that it is possible to recover the general expression for a different value of λ by replacing X_i by $X_i+\lambda$, which corresponds to replacing e_1 by $e_1+n\lambda$ and s_k by $\sum_{j=0}^{k}\binom{n-j}{k-j}L^{k-j}s_j$. For $n = 5$, we obtain

$$P_{\varphi,5} = e_1^8\gamma^8 + e_1^6 s_5\gamma^5 + e_1^4 s_4^2\gamma^4 + e_1^2 s_3^2 s_5\gamma^3 + s_3^4\gamma^4 + e_1^2 s_5^3\gamma + s_2^2 s_5^2\gamma^2 + s_5^4 + s_5^3\gamma\,.$$

Again, the next polynomials become too large to be reproduced in their entirety; for example, we obtain

$$P_{\varphi,6} = s_5^8 + e_1^2 s_5^6 s_6 + s_5^6 s_6 + \cdots + e_1^{12} s_5^2 \gamma^{10} + e_1^{14} s_6 \gamma^{12} + e_1^{16} \gamma^{16} \,,$$

which has 50 terms in $\mathbb{F}_2(\gamma)[e_1, s_2, \ldots, s_6]$. We observe that when $\lambda = 0$ or 1, the polynomials $P_{\varphi,3}, P_{\varphi,4}$ and $P_{\varphi,5}$ only involve even exponents of the $n-1$ first variables. This fact is true in general: for $L = 0$, $P_{\varphi,n}(e_1, s_1, \ldots, s_n) = \tilde{P}_{\varphi,n}(e_1^2, s_2^2, \ldots, s_{n-1}^2, s_n)$, which simplifies the inductive computation of these polynomials in characteristic 2.

We sum up in Table 1 the number of monomials of Semaev polynomials and our symmetrized summation polynomials (for $\lambda = 0$), as well as the timings of their computation. For $n \leq 7$, we used resultants of partially symmetrized polynomials followed by a symmetrization at each step. The computation was intractable in this way for $n = 8$. Thus, we implemented a dedicated interpolation algorithm to compute this new record. Here we briefly describe this computation. The 8-th symmetrized polynomial is the result of the symmetrized version of the relation

$$P_{\varphi,8}(X_1, \ldots, X_8) = \mathrm{Res}_X(P_{\varphi,6}(X_1, \ldots, X_5, X), P_{\varphi,4}(X_6, \ldots, X_8, X) \,,$$

but with $P_{\varphi,4}$ and especially $P_{\varphi,6}$ already in partially symmetrized form. We thus begin by evaluating $P_{\varphi,8}(e_1, s_2, \ldots, s_8)$ on a very large sample of points, which can be done by computing the above resultant with all variables (except X) instantiated. However, in order to apply fast sparse evaluation-interpolation techniques [15], we have to precisely control the instantiations of $e_1, s_2, \ldots, s_8$; thus we cannot simply evaluate the X_i to deduce a sample point, but have to do the converse instead. Moreover, because of the huge size of the sample, each of these evaluations has to be done as efficiently as possible. Actually, since we work with symmetrized polynomials, each instantiation corresponds to the computation of the values of the generators of the invariant ring in $X_1, \ldots, X_5$ and $X_6, \ldots, X_8$ respectively, from an instantiation of $e_1, s_2, \ldots, s_8$. Such a computation is not at all straightforward; it can be done by solving a polynomial system but, even by using the most efficient existing implementations, the timings are too slow to obtain $P_{\varphi,8}$ in a reasonable time. Thus, we investigated new methods to solve this problem and finally reduced it, by using the underlying symmetries, to the almost instantaneous resolution of a univariate polynomial. This efficient resolution is mainly based on a careful study of the factorization of this polynomial and a clever choice of the sample points, which let us avoid half of the most time-consuming steps of the algorithm. The sparse-interpolation step is less tricky but we need also a careful implementation in order to obtain the required efficiency. The complete computation of the 8-th symmetrized summation polynomial was achieved in about 40.5 CPU.hours using Magma [1], whereas previous attempts using the direct approach were all stopped after at least one month of computations.

Odd characteristic Let $E : y^2 = cx(x-1)(x-\lambda)$ be an elliptic curve in twisted Legendre form over an odd characteristic field K. As in Prop.10, we assume that

Table 1. Comparison of the number of terms of symmetrized Semaev polynomials and summation polynomials using a 2-torsion point in characteristic 2 ($\lambda = 0$). The crosses correspond to computations that stopped unsuccessfully after several weeks.

n		3	4	5	6	7	8
Semaev polynomials	nb of monomials	3	6	39	638	–	–
	timings	0 s	0 s	26 s	725 s	×	×
$P_{\varphi,n}$	nb of monomials	2	3	9	50	2 247	470 369
	timings	0 s	0 s	0 s	1 s	383 s	40.5 h

Table 2. Comparison of the number of terms of symmetrized classical Semaev polynomials and summation polynomials in odd characteristic using either a single 2-torsion point or the complete 2-torsion

n	3	4	5	6
Semaev polynomial	5	36	940	–
$P_{\varphi,n}(s_1, \ldots, s_{n-1}, e_n)$	5	13	182	4125
$Q_{\varphi,n}(\sigma_1, \ldots, \sigma_{n-2}, w_0, w_1)$	3	6	32	396

λ and $1-\lambda$ are squares, so that there exists $t \in K$ such that $\sqrt{\lambda} = (1-t^2)/(1+t^2)$ and $\sqrt{1-\lambda} = 2t/(1+t^2)$. Let $T_0 = (0,0)$ and $T_1 = (1,0)$; then a map $\varphi : E \to \mathbb{P}^1$ satisfying $\varphi(-P) = \varphi(P)$, $\varphi(P+T_0) = -\varphi(P)$ and $\varphi(P+T_1) = 1/\varphi(P)$ is given by

$$\varphi(P) = \frac{\sqrt{\lambda}+1}{\sqrt{1-\lambda}} \frac{x(P)-\sqrt{\lambda}}{x(P)+\sqrt{\lambda}}\,.$$

We can compare the summation polynomials $P_{\varphi,n}$ symmetrized with respect to G_2 (corresponding to the action of a single 2-torsion point T_0), the associated rational fractions $Q_{\varphi,n}$ symmetrized with respect to G_4 (corresponding to the action of the complete 2-torsion), and the classical Semaev polynomials, expressed with the elementary symmetric polynomials $e_1, \ldots, e_n$ in the variables $X_1, \ldots, X_n$. For $n = 3$ and 4, we have

$$\begin{aligned}
\mathrm{Sem}_3 &= e_2^2 - 4e_1e_3 + 2e_2\lambda - 4e_3(\lambda+1) + \lambda^2\,,\\
P_{\varphi,3} &= t^3e_3^2 + 2(1-t^4)e_3 + t^3s_1 - ts_2 - t\,,\\
Q_{\varphi,3} &= t^3w_1 - tw_0 - 2t^4 + 2\,.\\
P_{\varphi,4} &= t^2(s_1^2 - 2s_1s_3 - 4s_2e_4^2 + 8s_2e_4 - 4s_2 + s_3^2 + 8e_4^3 - 16e_4^2 + 8e_4) +\\
&\quad 4(t^4+1)(s_1e_4^2 - s_1e_4 - s_3e_4 + s_3)\,,\\
Q_{\varphi,4} &= 4(t^4+1)\sigma_1 - 4t^2\sigma_2 + t^2w_1^2 - 4(t^4+1)w_1 + 8t^2w_0 - 32t^2\,.
\end{aligned}$$

Table 2 sums up the number of terms of the computable polynomials for comparison.

5.2 Index calculus on $E(\mathbb{F}_{q^5})$

IPSEC Oakley key determination 'Well Know Group' 3 curve An interesting target for the decomposition attack is the IPSEC Oakley key determina-

tion 'Well Know Group' 3 curve [9] defined over the binary field $\mathbb{F}_{2^{155}} = \mathbb{F}_{(2^{31})^5}$. Since this is a degree 5 extension field, the decomposition-based index calculus uses a 6-th summation polynomial. The cardinality of the curve is 12 times a prime number; according to Prop.4, we can only consider the action of the 2-torsion or the 3-torsion points. With the 2-torsion point and the morphism φ of Prop.8 for $\lambda = 0$, the reduced factor base has 536 864 344 elements, which as expected is very close to $2^{31}/4$. Using the corresponding 6-th symmetrized summation polynomial computed above, a decomposition test takes 10.28 sec (3.44 sec for the Gröbner basis computation for a well-chosen order and 6.84 sec for the change of order with FGLM [5]) using FGb [3] on a Intel Core i7-4650U CPU at 1.70 GHz. Alternatively, the same computation with Magma V2.18-3 (on an AMD Opteron 6176 SE at 2.3 GHz) takes 995 sec for the Gröbner basis and about 6 hours for the order change[1].

To put this in perspective, we can compare to the only other existing method computing decompositions on this curve, namely the "$n-1$" approach of [11]: the computation of only one relation was estimated in [8] to take about 37 years on a single core, whereas with our results the expected time to get one relation is $2^4 \times 5! \times 10.28\,\text{sec} \approx 5.5\,\text{hr}$. Even if it is still too slow to seriously threaten the DLP on this IPSEC standard, these experiments show that other non-standard problems like the oracle-assisted static Diffie-Hellman problem [12] are no longer secure on this curve.

Random curve in odd characteristic with full 2-torsion To test the speed-up provided by the presence of the full 2-torsion subgroup, we considered a random curve in Legendre form over the optimal extension field $\mathbb{F}_{(2^{31}+413)^5}$, with a near-prime cardinality and satisfying the condition of Prop.10. Using the 6-th symmetrized summation polynomial as computed above, a decomposition test takes only 6.66 sec (2.82 sec for the Gröbner basis and 3.84 sec for FGLM) using FGb on a 3.47 GHz Intel Xeon X5677 CPU, or about 5 hours (55 min for the GB and 4h25 for FGLM) using Magma. By comparison, in [4] only one 2-torsion was accounted for (in a twisted Edwards model) and the authors reported a timing of 2 732 sec for one decomposition test. Once again, this shows the total weakness of some non-standard problems on such curves.

6 Conclusion

The introduction of summation polynomials associated to any morphism φ from an elliptic E to $\mathbb{P}^1$ opens new perspectives for the decomposition based index calculus. In particular, we have been able to use equivariant morphisms to take advantage of 2-torsion points in any characteristic. As demonstrated by our examples and timings, the speed-up over the classical approach is far from negligible and allows to seriously threaten more curves. The framework we have

[1] The performance gap between Magma and FGb can be partially explained by the non-optimized arithmetic operations of Magma when the field size exceeds 25 bits. Experiments on smaller fields showed a significantly smaller gap.

developed also applies to higher order torsion points, which will be more detailed in an extended version of this article.

References

1. W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
2. C. Diem. On the discrete logarithm problem in elliptic curves. *Compos. Math.*, 147(1):75–104, 2011.
3. J.-C. Faugère. FGb: A Library for Computing Gröbner Bases. In *Mathematical Software - ICMS 2010*, pages 84–87, 2010. Springer Berlin Heidelberg.
4. J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault. Using symmetries in the index calculus for elliptic curves discrete logarithm. *J. Cryptology*, pages 1–41, 2013. DOI: 10.1007/s00145-013-9158-5.
5. J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, 16(4):329–344, 1993.
6. P. Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *J. Symbolic Comput.*, 44(12):1690–1702, 2008.
7. P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15(1):19–46, 2002.
8. R. Granger, A. Joux, and V. Vitse. New timings for oracle-assisted SDHP on the IPSEC Oakley 'Well Known Group' 3 curve. Announcement on the NBRTHRY mailing list, July 2010. `http://listserv.nodak.edu/archives/nmbrthry.html`.
9. IETF. The Oakley key determination protocol, IETF RFC 2412, 1998.
10. A. Joux and V. Vitse. Cover and Decomposition Index Calculus on Elliptic Curves made practical. Application to a seemingly secure curve over $\mathbb{F}_{p^6}$. In *Advances in cryptology—EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Comput. Sci.*, pages 9–26, Berlin, 2012. Springer.
11. A. Joux and V. Vitse. Elliptic curve discrete logarithm problem over small degree extension fields. *J. Cryptology*, 26(1):119–143, 2013.
12. N. Koblitz and A. Menezes. Another look at non-standard discrete log and Diffie-Hellman problems. *J. Math. Cryptol.*, 2(4):311–326, 2008.
13. I. A. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. Cryptology ePrint Archive, Report 2004/031, 2004.
14. J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
15. R. Zippel. Interpolating polynomials from their values. *Journal of Symbolic Computation*, 9(3):375 – 403, 1990.