Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms - Simplified Setting for Small Characteristic Finite Fields

Antoine Joux, Cécile Pierrot

Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms

Simplified Setting for Small Characteristic Finite Fields

Antoine Joux[1,2] and Cécile Pierrot[2,3]

[1] CryptoExperts, France and Chaire de Cryptologie de la Fondation de l'UPMC
[2] Laboratoire d'Informatique de Paris 6, UPMC Sorbonnes Universités, Paris
[3] CNRS and Direction Générale de l'Armement
antoine.joux@m4x.org, Cecile.Pierrot@lip6.fr

Abstract. In this paper[4], we revisit the recent small characteristic discrete logarithm algorithms. We show that a simplified description of the algorithm, together with some additional ideas, permits to obtain an improved complexity for the polynomial time precomputation that arises during the discrete logarithm computation. With our new improvements, this is reduced to $O(q^6)$, where q is the cardinality of the basefield we are considering. This should be compared to the best currently documented complexity for this part, namely $O(q^7)$. With our simplified setting, the complexity of the precomputation in the general case becomes similar to the complexity known for Kummer (or twisted Kummer) extensions.

1 Introduction

Recently, the computation of discrete logarithms in small characteristic finite fields has been greatly improved [Jou14,GGMZ13a,BGJT14], with the introduction of a new family of Index Calculus algorithms for this case. In the sequel, we call the algorithms from this family: **Frobenius Representation algorithms**. Frobenius Representation algorithms can be seen as descendants of the pinpointing algorithm introduced in [Jou13a]. The first two Frobenius Representation algorithms appeared essentially simultaneously, one of them proposed by Joux in [Jou14] was first used in a discrete logarithm record in $\mathbb{F}_{2^{1778}}$ announced on Feb 11^{th} 2013 on the NMBRTHRY mailing list, while the first draft of the article describing the $L(1/4)$ complexity analysis of the algorithm was posted as [Jou13b] on Feb 20^{th} 2013. Between these two events, another Frobenius Representation algorithm with complexity $L(1/3)$ was proposed in [GGMZ13b] with a record in $\mathbb{F}_{2^{1971}}$ announced on Feb 19^{th} 2013 on the same mailing list. From an asymptotic point of view, the best current Frobenius Representation algorithm is the quasi-polynomial time algorithm proposed in [BGJT14]. In practice, a lot of options are open depending on the exact finite field we want to

address. However, there are currently many open questions about these algorithms. From a theoretical point of view, it would be extremely nice to remove the heuristic hypotheses that are used in the algorithms. A first step in this direction is proposed in [GKZ14b], with a simplified individual logarithms algorithm that only relies on the ability to descent finite field elements expressed by polynomials of even degree $2D$ to polynomials of degree D. Another theoretical question would be to get the complexity down to polynomial time instead of quasi-polynomial. From a practical point of view, the limiting step for setting records in the general case, as opposed to special cases such as Kummer extension, is usually the computation of the logarithm of the initial factor base elements. When working over a base field $\mathbb{F}_q$, the best documented complexity is $O(q^7)$ (see for example [AMORH14]). However, some authors mention an higher complexity, typically, for the computation performed in [GKZ14a], with $q = 2^6$, the authors explain that the dimension of the linear algebra is reduced from q^4 to $q^4/24 = q^4/\log_2(q^4)$. Asymptotically, with this approach the complexity would be $O(q^9/\log(q)^2)$. For specific cases such as Kummer extension, the complexity is lower of the order of $O(q^6)$.

In this paper, we give a new variation which achieves complexity $O(q^6)$ for the general case. Part of this work was already presented by the first-named author in several presentations during the development of our algorithm. It is presented here in writing for the first time. In these earlier talks, the variation was described as a simplified version with degraded performance, the main reason being that using polynomials of degree up to D over $\mathbb{F}_q$ seems essentially equivalent to using linear polynomials over $\mathbb{F}_{q^d}$, with $d = D$. However, instead of allowing us to compute logarithms in the field $\mathbb{F}_{q^{dk}}$ with k of the same order of magnitude as q, it only leads to logarithms in $\mathbb{F}_{q^k}$ and we lose the extra factor of d in the field exponent, which came for free with the standard approach (with a value of d usually between 2 and 4). Also note that a similar correspondance between low degree polynomials over a large field and higher degree polynomials over a smaller field also appears in [GKZ14b].

In order to make the algorithm efficient, D needs to be minimized. At first glance, it seems that we need to take at least $D = 3$ to bootstrap the computation. Our main contribution is that with this simplified approach, it is in fact possible, under a reasonable heuristic assumption, to reduce the degree of the polynomials in the initial factor base over $\mathbb{F}_q$ to $D = 2$. Once the initial factor base is computed, with a cost $O(q^5)$, we use it as a lever to obtain the logarithms of polynomials of degree $D = 3$ and $D = 4$ with a total cost $O(q^6)$. Using either the heuristic quasi-polynomial descent of [BGJT14] or the alternative version from [GKZ14b], it is possible to bring down arbitrary elements to $\mathbb{F}_{q^k}$ to this extended factor base formed of irreducible polynomials up to degree 4.

Outline of the article. As any recent discrete logarithms algorithms for small characteristic finite fields, our simplified setting has several phases:

- The Preliminary phase, that finds a representation of the target finite field.
- The Relation Collection and Linear Algebra phases, that permit to recover the discrete logarithms of a small set of elements, the factor base.

- The Extension phase, specific to small characteristic finite fields, in which we obtain the discrete logarithms of a larger set containing the factor base. We call this new set the extended factor base.
- The Descent phase, that recovers the discrete logarithm of an arbitrary element of the finite field by rewriting it as products of elements of the extended factor base.

Following this common structure we introduce our simplified setting in Section 2. We present then in Section 3 the computation of the discrete logarithms of the factor base together with the Extension phase. Section 4 gives a short analysis of the total improved asymptotic complexity obtained. Finally, in Section 5, we illustrate the efficiency of the algorithm with a practical computation of discrete logarithms in the general case of a prime extension degree which does not divide[5] $q(q+1)(q-1)$. More precisely, we perform the computation of the logarithms in $\mathbb{F}_{q^k}$ with $q = 3^5$ and extension degree $k = 479$ (the largest prime smaller than $2q$).

2 Simplified Setting for Small Characteristic Finite Fields

When trying to compute discrete logarithms in a given finite field, let us say $\mathbb{F}_{q^k}$, the first step is to choose a convenient way to construct it. We first expose in Section 2.1 how Frobenius Representation algorithms represent the target field with the help of two polynomials h_0 and h_1. We present then an improved way to choose these two cornerstone polynomials in Section 2.2. Last but not least, we propose in Section 2.3 a simpler factor base. It is the combination of these two simplified choices that permits to obtain an improvement in the asymptotic complexity of the Relation Collection, Linear Algebra and Extension phases.

2.1 Frobenius Representation Algorithms

Like all Frobenius Representation algorithms, the algorithm we propose relies on two key elements. The first element is the well-known fact that over $\mathbb{F}_q[X]$, the following polynomial identity holds:

$$\prod_{\alpha \in \mathbb{F}_q} (X - \alpha) = X^q - X. \tag{1}$$

The second element is to define the target finite field $\mathbb{F}_{q^k}$, where we want to compute discrete logarithms, by determining two polynomials h_0 and h_1 of degree at most H and by requiring that there exists a monic irreducible polynomial $I(X)$ of degree k over $\mathbb{F}_q[X]$ such that:

$$I(X) \text{ divides } h_1(X)X^q - h_0(X). \tag{2}$$

[5] The known special cases which are very efficient for record being Kummer extensions of degree dividing $q-1$, twisted Kummer extensions with degree dividing $q+1$ and Artin-Schreier extensions.

If θ denotes a root of $I(X)$ in $\overline{\mathbb{F}}_q$, setting $\mathbb{F}_{q^k} = \mathbb{F}_q[X]/(I(X)) = \mathbb{F}_q(\theta)$ gives a representation of the finite field that satisfies $\theta^q = h_0(\theta)/h_1(\theta)$. Since the map that raises an element of $\overline{\mathbb{F}}_q$ to the power q is called the Frobenius map, this choice of representation explains the name of **Frobenius Representation** we use for this family of algorithms.

The dual Frobenius Representation variant There is an alternative option proposed in [GKZ14a] for constructing the extension field where we require that:

$$I(X) \text{ divides } h_1(X^q)X - h_0(X^q).$$

The advantage of this option is to allow a wider range of possible extension degrees k for a given basefield $\mathbb{F}_q$. However, using this variation slightly complicates the description of the algorithm. With this variation, the finite field representation satisfies $\theta = h_0(\theta^q)/h_1(\theta^q)$. When referring to the variation by name, we will call it a **dual Frobenius Representation** or equivalently a **Verschiebung Representation**.

2.2 Improved choice of h_0 and h_1

A really simple construction. We recall that the usual choice is to take two quadratic polynomials to allows the possibility of representing, at least heuristically, a large range of finite fields. Since we know that using linear polynomials for h_0 and h_1 does not allow such a large range, we propose a slightly different choice. **We take for h_0 an affine polynomial and for h_1 a quadratic polynomial.** We assume furthermore that the constant term of h_1 is equal to 0. Note that, by factoring out a constant in the defining Equation (2), we can assume, without loss of generality, that h_1 is monic. For simplicity of the presentation, it is convenient to rewrite:

$$h_0(X) = rX + s \quad \text{and} \quad h_1(X) = X(X + t) \tag{3}$$

A useful variant. Another natural option is to take for h_0 a quadratic polynomial with a contant term equal to 0 and for h_1 an affine polynomial. In this case, it is convenient to rewrite:

$$h_0(X) = X(X + w) \quad \text{and} \quad h_1(X) = uX + v. \tag{4}$$

At first sight, nothing indicates that one of the two choices is better, and in fact, both are equivalent in term of complexity. However, as we show in Section 3, the first one leads in practice to a simpler description of the algorithm. As a mnemonic we can notice that $(\mathbf{r}, \mathbf{s}, t)$ are the coefficients of the **r**eally **s**imple construction whereas $(\mathbf{u}, \mathbf{v}, w)$ are the one of the **u**seful **v**ariant.

2.3 Seeking a Natural Factor Base

Once the representation of the target field is chosen, we need to fix the factor base. With the aim of simplifying the description of the algorithm, we propose to get rid of polynomials with coefficients in an extension field.

Irreducible polynomials with coefficients in the basefield. We choose a parameter D and consider a factor base that contains all irreducible polynomials of degree $\leq D$ over $\mathbb{F}_q[X]$. This has to be compared with previous Frobenius Representation algorithms that consider irreducible polynomials with coefficients in an extension of $\mathbb{F}_q$. To generate equations, we let A and B be two polynomials of degree $\leq D$ and using Equations (1) and (2) we write:

$$\begin{aligned} B(\theta)\prod_{\alpha\in\mathbb{F}_q}(A(\theta)-\alpha B(\theta)) &= B(\theta)A(\theta)^q - A(\theta)B(\theta)^q \\ &= B(\theta)A(\theta^q) - A(\theta)B(\theta^q) \\ &= B(\theta)A\left(\frac{h_0(\theta)}{h_1(\theta)}\right) - A(\theta)B\left(\frac{h_0(\theta)}{h_1(\theta)}\right). \end{aligned}$$

For compactness, we match $B(\theta)$ with the point α at infinity on the projective line $\mathbb{P}_1(\mathbb{F}_q)$. This permits to rewrite throughout the sequel the first product as $\prod_{\alpha\in\mathbb{P}_1(\mathbb{F}_q)}(A(\theta)-\alpha B(\theta))$. We also introduce the following notation:

Definition 1. *Let D be an integer, and h_0, h_1, A, B be four polynomials such that A and B are of degree at most D. Then $[A,B]_D$ is called the D-bracket of A and B. It is defined as:*

$$[A,B]_D(X) = h_1(X)^D\left(B(X)A\left(\frac{h_0(X)}{h_1(X)}\right) - A(X)B\left(\frac{h_0(X)}{h_1(X)}\right)\right).$$

Proposition 1. *If h_0 and h_1 are polynomials of degree at most H and if A and B are polynomials of degree at most D then:*

- *$[A,B]_D$ is a polynomial of degree at most $(H+1)\cdot D$.*
- *The map $[.,.]_D$ is bilinear and antisymmetric. In particular, $[A,A]_D = 0$.*

The proof of the two items of the proposition is straightforward. With these two notations, we rewrite the equality as:

$$\prod_{\alpha\in\mathbb{P}_1(\mathbb{F}_q)}(A(\theta)-\alpha B(\theta)) = \frac{[A,B]_D(\theta)}{h_1(\theta)^D}. \tag{5}$$

Since the numerator $[A,B]_D$ of the **right-hand** side of Equation (5) has a bounded degree, under a classical heuristic, the probability that it factors into irreducible polynomials of degree at most D can be lower bounded by a constant p_H. When using a dual Frobenius Representation, we similarly get:

$$\prod_{\alpha\in\mathbb{P}_1(\mathbb{F}_q)}(A(\theta)-\alpha B(\theta)) = \left(\frac{[A,B]_D(\theta)}{h_1(\theta)^D}\right)^q. \tag{6}$$

Degree of the factor base polynomials. In order to choose the parameter D, we have to balance three ideas: to lower the complexity of the linear algebra phase we require to have a small factor base, but, we also need to be able to generate

enough good equations[6] and to descent larger polynomials to polynomials of the factor base. The polynomial degree of the factor base must not be too small in both cases, otherwise one at least of this two steps will not be possible. Let us give more details about this degree.

The previous degree 3 barrier. When we consider the general case where h_0 and h_1 are polynomials of degree bounded by H, the analysis is as follows. The number of equations that can be generated is obtained by counting the number of pairs of polynomials (A, B) that remains once we take into account the fact that the pairs are invariant under the action of $\mathrm{PGL}_2(\mathbb{F}_q)$. In other words, ignoring the cases where the degree is somehow reduced (see Appendix A for details) in the **left-hand** side of Equation (5) we can assume that:

$$A(X) = X^D + a(X) \quad \text{and} \quad B(X) = X^{D-1} + b(X),$$

where $a(X)$ and $b(X)$ have degree at most $D-2$. As a consequence, since polynomials of degree $D-2$ have $D-1$ coefficients, the number of good equations that can be generated in this manner is of the order of $p_H \cdot q^{2D-2}$. Moreover, the number of elements in the factor base, *i.e.* the number of irreducible of degree at most D is close to q^D/D. To get more equations than unknowns in the linear algebra phase, i.e. to obtain $D \cdot p_H \cdot q^{D-2} \geqslant 1$, unless enlarging a lot the probability p_H, we need that $D \geqslant 3$, as underlined in [GKZ14b].

As a consequence, the best hope we get for the complexity of computing the logarithms of factor base elements is of the order of $(q^D)^2 \cdot q \geq q^7$. Note that looking at the various existing record, this lower bound of q^7 is not always attained, since some computations need to enlarge the factor base to $D = 4$, which raises the complexity to $O(q^9)$. Typically, such an enlargement is performed in [GKZ14a], even if, thanks to a judicious use of Galois invariance, they reduce the cost of this enlargement compared to $O(q^9)$ by regrouping the degree 4 objects[7] into groups of 24 conjugates.

The reason for this enlargement is that the known techniques for descending polynomials of degree larger than 4 to degree 4 do not work completely to descent degree 4 polynomials to degree 3, since in most cases, only a fraction of degree 4 irreducible polynomials can be obtained in this manner. This is similar to the situation reported in [AMORH14], where half of the quadratic polynomials over a cubic extension can be derived with the descent algorithm from linear polynomials.

Breaking the barrier. Following the above argument, for $D = 2$ we expect about $q^2/2$ irreducible polynomials and assuming that $H = 2$, one would expect a value of p_H well below $1/2$. Thus, without any improvement on the probability, the expected number of equations is too small compared to the number of unknowns and it is not possible to derive the discrete logarithms of the small elements in this manner... Yet, in our simplified setting **the factor base consists in all the irreducible polynomial of degree 2 with coefficients in**

[6] We call **good equations** equations of the restricted form (5) where both right and left-hand side can be written with polynomials of the factor base only.

[7] Those objects are in fact quadratic polynomials over a degree 2 extension.

the base field. We explain in Section 3.1 how to get around this problem and to recover all the discrete logarithms of the factor base.

3 Improving Computations of the (extended) Factor Base

In this section, we present two contributions which allow us to reduce the global cost of the polynomial part of discrete logarithm computations. The first contribution in Section 3.1 describes how we can adapt the use of Equation (5) to be able to perform an initial computation with a reduced initial factor base corresponding to $D = 2$ for a cost $O(q^5)$. We also show, in Section 3.2, that once this is done, the enlargement to $D = 3$ can be performed with a reduced cost $O(q^6)$, instead of the expected $O(q^7)$.

The second contribution presented in Section 3.3 is a new descent technique that only requires a small subset of degree 4 irreducible polynomials to be able to compute on the fly the logarithm of an overwhelming fraction of other degree 4 polynomials. If there is enough available memory, it is also possible using a adaptation of this technique to obtain the logarithms corresponding to an enlarged basis with $D = 4$. Both options can be performed with a time complexity $O(q^6)$.

3.1 A Reduced Degree 2 Factor Base

As previously said, if we choose a degree 2 factor base, it seems that we don't have enough good equations compared to the number of unknowns. We propose two approaches to get rid of this problem. First, we show that thanks to our smaller degree polynomials h_0 and h_1, we can improve p_H, the bound on the probability to obtain a good equation, by exhibiting systematic factors. In addition, we also use another source of equations to complete the system. A secondary advantage is that this second source leads to much sparser equations that the use of Equation (5).

Improving the probability p_H thanks to systematic factors. Once we have fixed $A(X) = X^D + a(X)$ and $B(X) = X^{D-1} + b(X)$, we see that both the left-hand side and the denominator of the right-hand side of Equation (5) or (6) can be written as products of elements of the factor base. So, we have to analysis the probability that the numerator of the right-hand side, namely the D-bracket of A and B, can be factorized in products of polynomials of degree at most 2.

The simple construction: h_0 affine and h_1 quadratic. Proposition 1 allows to upper-bound the degree of $[A, B]_D$ by $(H + 1) \cdot D$. As a consequence, for $H = 2$ and $D = 2$, this degree is lower than 6. The probability that a random polynomial of degree 6 factors into terms of degree less than 2 is well too small to permits to obtain enough equations. Though, as mentioned in [GKZ14b], we remark that a systematic term appears in the factorization of $[A, B]_D(X)$. To be more precise, we have the following result:

Lemma 1 (Systematic factor of a D-bracket). *Let A and B be two polynomials of degree at most D. Then $[A,B]_D(X)$ is divisible by $Xh_1(X)-h_0(X)$.*

Proof. By bilinearity, if $A(X)=\sum_{i=0}^{D} a_i X^i$ and $B(X)=\sum_{i=0}^{D} b_i X^i$, we can write: $[A,B]_D=\sum_{i=0}^{D}\sum_{j=0}^{D} a_i b_j \left[X^i,X^j\right]_D$. Moreover, since $[.,.]_D$ is bilinear and anti-symmetric it is clear that $\left[X^i,X^j\right]_D=-\left[X^j,X^i\right]_D$ and $\left[X^i,X^i\right]_D=0$. Thus, it suffices to consider the D-bracket of X^i and X^j where $i<j$. Lets us compute:

$$\begin{aligned}\left[X^i,X^j\right]_D &= h_1^{D-j}(X)\left(X^j h_0(X)^i h_1(X)^{j-i} - X^i h_0(X)^j\right)\\ &= h_1^{D-j}(X)X^i h_0(X)^i\left((Xh_1(X))^{j-i} - h_0(X)^{j-i}\right)\\ &= h_1^{D-j}(X)X^i h_0(X)^i (Xh_1(X)-h_0(X))\sum_{k=1}^{j-i} h_0(X)^{k-1}(Xh_1(X))^{j-i-k}.\end{aligned}$$

As a consequence $Xh_1(X)-h_0(X)$ divides $\left[X^i,X^j\right]_D$ and the lemma follows. □

Thus, after dividing $[A,B]_D$ by this degree 3 systematic factor, the question is whereas a polynomial of degree 3 factors into terms of degree at most 2. Assuming that it behaves as a random polynomial in this respect, we can lower bound (see Appendix B) the probability by 2/3. Since this is higher than 1/2, we have now enough equations to compute the logarithms of the factor base.

The useful variant: h_0 quadratic and h_1 affine. We can check again that the numerator in the right-hand side of Equation (5) or (6) becomes systematically divisible by $\theta h_1(\theta)-h_0(\theta)$. Yet, in this variant, this systematic factor has degree 2 only. This partially improves the value of p_H, however, this is not sufficient to get enough equations.

To go further in reducing this degree, we have to remark that the bound on the degree of $[A,B]_D$ given in Proposition 1, which is $(H+1)\cdot D$, can in fact be improved in the specific case where h_1 is affine. In truth, the degree is now upper-bounded by $(H+1)\cdot D-1$. For $H=2$ and $D=2$, this reduces for free the degree from 6 to 5. As a consequence, after dividing by the degree 2 systematic factor of Lemma 1, there remains as previously a polynomial of degree 3. Again the probability p_H is lower-bounded by $2/3>1/2$. In both cases, this probability would already suffice to produce enough equations.

Additional equations. Despite the fact that the equations obtained with our improved choice of h_0 and h_1 in both the simple construction and the useful variant would suffice to solve the linear system with parameter $D=2$, proposing a source of extra equations is also helpful. In this section, to produce additional equations, we simply consider a variation on the systematic equations that were introduced in [BMV85] and often used in the Function Field Sieve.

More precisely, let $f(X)=X^2+f_1X+f_0$ be an irreducible polynomial of degree 2 in $\mathbb{F}_q[X]$. We can write :

$$f(\theta)^q = f\left(\frac{h_0(\theta)}{h_1(\theta)}\right) = \frac{h_0(\theta)^2+f_1\,h_0(\theta)h_1(\theta)+f_0\,h_1(\theta)^2}{h_1(\theta)^2}.$$

The numerator of the right-hand side is a polynomial of degree 4, since one of the two polynomials h_0 or h_1 is quadratic and the other one is affine. We remark that about half of these numerators are irreducible and the other half factor into a product of two degree 2 irreducible polynomials. For the case of a dual Frobenius Representation, the systematic equations are slightly different:

$$f(\theta) = f\left(\frac{h_0(\theta)}{h_1(\theta)}\right)^q = \left(\frac{h_0(\theta)^2 + f_1\, h_0(\theta)h_1(\theta) + f_0\, h_1(\theta)^2}{h_1(\theta)^2}\right)^q$$

but the principle remains identical. These systematic equations can easily be generalized to irreducible polynomials of arbitrary degree, with again a close to half/half repartition:

Lemma 2. *Let h_0 and h_1 be two polynomials such that one is affine and the other quadratic. If f is a degree D monic irreducible polynomial in $\mathbb{F}_q[X]$, then $h_1(X)^{2D} f(h_0(X)/h_1(X))$ is a polynomial of degree $2D$ that has a probability equal to $1-p$ to be irreducible and a probability equal to p to factor into two degree D irreducible polynomials, with:*

$$\frac{1}{q^D}\left(\frac{q^D-1}{2} - \frac{q^{\lfloor D/2\rfloor+1}-q}{q-1}\right) \le p \le \frac{q^D+3}{2\,q^D}.$$

Proof. Let h_0 and h_1 be two polynomials such that one is affine and the other quadratic. We define the polynomial P as $P(X) = h_1(X)^{2D} f(h_0(X)/h_1(X))$. One can remark that α is a root of P in $\overline{\mathbb{F}}_q$ if and only if $h_0(\alpha)/h_1(\alpha)$ is a root of f in $\overline{\mathbb{F}}_q$.

Let α be a root of P in $\overline{\mathbb{F}}_q$ and $\sigma, \sigma^q, \cdots, \sigma^{q(D-1)}$ be the conjuguate roots of f in $\mathbb{F}_{q^D}$. Without loss of generality, we can assume that $h_0(\alpha)/h_1(\alpha) = \sigma$. With this notation, we deduce that α is a root of $h_0 - \sigma h_1 \in \mathbb{F}_{q^D}[X]$. The polynomial $h_0 - \sigma h_1$ is quadratic, thus is either irreducible in $\mathbb{F}_{q^D}[X]$ or splits into a product of two linear polynomials. In the first case, α does not belong to $\mathbb{F}_{q^D}$ and P is irreducible over $\mathbb{F}_q[X]$. In the second case, it has two, possibly equal roots, α and α' in $\mathbb{F}_{q^D}$ and P factors into two degree D irreducible polynomials.

To study the probability of both cases, we reformulate the problem and notice that P factors into degree D irreducibles when σ is the abcissa of a point defined over $\mathbb{F}_{q^D}$ on the curve :

$$C: \quad h_0(Y) - X\, h_1(Y).$$

C is a genus 0 curve, thus including (at most 2) points at infinity, it has q^D+1 points defined over $\mathbb{F}_{q^D}$. If (σ, α) is a point on C, then there is a another distinct point (σ, α'), with the same abscissa, unless $h_0(Y) - \sigma\, h_1(Y)$ is a square. We remark that there are at most 2 such exceptional values of σ. As a consequence, the number of possible abcissae of $\mathbb{F}_{q^D}$-points on C belongs to the interval $[(q^D-1)/2; (q^D+3)/2]$.

We now need to account for the extra restriction that σ is the root of an irreducible polynomial of degree D and thus does not belong to any strict subfield of $\mathbb{F}_{q^D}$. In order to do this, we bound the number of elements belonging to a

subfield and their contribution to the possible abscissae on C. Note that if $\mathbb{F}q^i$ is a strict subfield of $\mathbb{F}_{q^D}$ then $i \leq D/2$. Since there is at most one subfield of each degree, the total number of elements of subfields is upper bounded by:

$$\sum_{i=1}^{\lfloor D/2 \rfloor} q^i = \frac{q^{\lfloor D/2 \rfloor + 1} - q}{q-1}.$$

We conclude that the number of possible abcissae σ (of $\mathbb{F}_{q^D}$-points on C) not belonging to a strict subfield is in the interval:

$$[\frac{q^D - 1}{2} - \frac{q^{\lfloor D/2 \rfloor + 1} - q}{q-1}; \frac{q^D + 3}{2}].$$

□

In particular, note that for irreducible polynomials of degree 1, which are part of the initial factor base for $D = 2$, we always obtain a systematic equation relating the given polynomial either to two other affine polynomials or to one quadratic polynomial. Note that we could also use the systematic equations for higher degree polynomials in Section 3.3 to ease the computation of the logarithm of degree 4 polynomials.

3.2 Enlarging the Factor Base to Degree 3

In order to be able to enlarge the factor base to degree 3 without performing linear algebra on a matrix of dimension q^3, we follow an approach quite similar to the one presented in [Jou14]. Namely, we divide first the set of irreducible polynomials of degree 3 into groups and search then for a way to generate enough equations involving only the polynomials within a group and polynomials of degree 1 or 2 whose logarithms are already known.

Groups of degree 3 polynomials for the simple construction. To define a group of degree 3 polynomials we start from an element g in the base field $\mathbb{F}_q$ and we consider $\mathcal{P}_g$ the corresponding group of degree 3 polynomials such that:

$$\mathcal{P}_g = \{(X^3 + g) + \alpha X^2 + \beta X | (\alpha, \beta) \in {\mathbb{F}_q}^2\}.$$

Clearly, if we generate a relation using Equation (5), or (6), with $A(X) = (X^3 + g) + \alpha X^2$ and $B(X) = (X^3 + g) + \beta X$, with a and b in $\mathbb{F}_q$, then all degree 3 polynomials that appear in the left-hand side belong to $\mathcal{P}_g$. The elements of $\mathcal{P}_g$ can be divided into two groups:

- the reducible polynomials whose logarithms can be computed by taking the sum of the logarithms of their factors,
- and the irreducible polynomials which appear as unknowns. Note that the number of irreducible polynomials in a group $\mathcal{P}_g$ is approximately $q^2/3$.

For one fixed element g, by considering all possibilities for α and β, we find q^2 candidate relations. Yet, we keep only those whose right-hand side factors into terms of degree at most 2. The question is now whether we obtain enough equations to be able to solve the corresponding linear system.

For this, lets look into more details at the right-hand side. With our choice of h_0 and h_1 it is a polynomial of degree 9, as described in Proposition 1. Moreover, it follows from Lemma 1 that it is divisible by the degree 3 polynomial $\theta h_1(\theta) - h_0(\theta)$. As a consequence, we are left with a polynomial of degree 6 to factor in terms of degree at most 2. The probability to obtain a good relation is not yet higher than 1/3. To improve on this probability, we first remark that with our specific choice of A and B the polynomial degree of the numerator of the right-hand side is in fact 8. Thus we are left with a polynomial of degree 5 to factor in terms of degree at most 2. Besides, we reveal a very simple systematic factor.

Lemma 3 (Systematic factor of particular 3-brackets in the simple construction). *Let h_0, h_1, A and B be four polynomials such that h_0 is affine, $h_1(X) = X(X+t)$, $A(X) = (X^3+g) + \alpha X^2$ and $B(X) = (X^3+g) + \beta X$, with t, g, α and β in $\mathbb{F}_q$. Then $[A,B]_3$ is a polynomial of degree at most 8 divisible by X.*

Proof. By bilinearity and antisymmetry we have $[A,B]_3 = \alpha\left[X^2, X^3+g\right]_3 + \beta\left[X^3+g, X\right]_3 + \alpha\beta\left[X^2, X\right]_3$. Let us compute the following 3-brackets:

$$\begin{aligned}
\left[X, X^2\right]_3 &= X^2 h_0 h_1^2 - X h_0^2 h_1 \\
\left[X^3+g, X\right]_3 &= X(h_0^3 + g h_1^3) - (X^3+g)\, h_0 h_1^2 \\
&= X[h_0^3 + g h_1^3 - (X^3+g)\, h_0\, X(X+t)^2] \\
\left[X^3+g, X^2\right]_3 &= X^2(h_0^3 + g h_1^3) - (X^3+g)\, h_0^2 h_1 \\
&= X[X(h_0^3 + g h_1^3) - (X^3+g)\, h_0^2\, (X+t)]
\end{aligned}$$

The result of the lemma comes from the fact that all the 3-brackets involved in the computation of $[A,B]_3$ are divisible by X. Moreover, considering the polynomials degrees of these elements we remark that $\left[X, X^2\right]_3$ has degree 6 whereas $\left[X^3+g, X\right]_3$ has degree 7 and $\left[X^3+g, X^2\right]_3$ has degree 8. □

As a direct consequence, the remaining factor in the right-hand side when considering these groups is of degree 4. According to Appendix B the heuristic probability that it factors into terms of degree at most 2 is close to 41%. Since these is greater than 1/3, we expect to find enough equations to compute all the discrete logarithms of the irreducible polynomials belonging to $\mathcal{P}_g$. Moreover, it is clear that any monic and irreducible polynomial of degree 3 belongs to one $\mathcal{P}_g$.

Groups of degree 3 polynomials for the useful variant. In this setting, computing discrete logarithms of degree 3 polynomials is a bit more tricky. To

define a group in this case, we start from a triple (g_1, g_2, g_3) of elements in $\mathbb{F}_q$. The corresponding group of degree 3 polynomials is defined as:

$$\mathcal{P}_{g_1,g_2,g_3} = \{X^2(X-g_1) + \alpha X(X-g_2) + \beta(X-g_3) | (\alpha,\beta) \in {\mathbb{F}_q}^2\}.$$

Let us fix $(g_1, g_2, g_3) \in {\mathbb{F}_q}^3$. If we generate a relation using Equation (5) with $A(X) = X^2(X-g_1)+\alpha(X-g_3)$ and $B(X) = X(X-g_2)+\beta(X-g_3)$, with α and β in $\mathbb{F}_q$, then all degree 3 polynomials that appear in the left-hand side belong to the corresponding group $\mathcal{P}_{g_1,g_2,g_3}$. After keeping only the q^2 candidate relations whose right-hand side factors into terms of degree at most 2, the question is, again, whether we obtain enough equations to solve the linear system where the unknown are the $q^2/3$ irreducible polynomials of $\mathcal{P}_{g_1,g_2,g_3}$.

When h_0 is quadratic and h_1 affine, the right-hand side is still a polynomial of degree 8 divisible by $\theta h_1(\theta) - h_0(\theta)$. We are left with a polynomial of degree 6 to factor in terms of degree at most 2. Yet, without any further improvement, the probability of this remaining polynomial to factor into terms of degree at most 2 is still too small to obtain enough equations.

To overcome this obstacle, we no longer consider the general groups of this form. Our goal is to point out some groups in which we now that the right-hand sides have some extra systematic factors. Another argument for considering few special groups only comes when we remark that the number of degree 3 polynomials produced with all those general groups is way too large. Taking all q^3 groups of the form $\mathcal{P}_{g_1,g_2,g_3}$ is a clear overkill since they each contain q^2 elements whereas there are only q^3 monic polynomials of degree 3. In fact we expect that these polynomials could be mostly covered by q groups only. To put it in a nutshell, we restrict ourselves to the specific choice of g_1, g_2 and g_3 where we first choose a value $g_1 \in \mathbb{F}_q$ and compute then:

$$g_2 = G(g_1) \quad \text{and} \quad g_3 = G(g_2)$$

where $G : \mathbb{F}_q \mapsto \mathbb{F}_q$ is a particular map. We propose to consider:

$$G : g \mapsto \frac{v(v+w)}{(1+u)(v+w-g)}. \tag{7}$$

We recall that u, v, w denote the coefficients of the polynomials h_0 and h_1, as given in (4). Assuming that both g_1 and g_2 are not equal to $v+w$ then all three values (g_1, g_2, g_3) are well-defined. With this specific choice, the right-hand side that now appear in Equation (5) or (6) gains a new systematic degree 2 factor $\theta h_1 + h_0 + (v+w)h_1 = (1+u)\theta^2 + (1+u)(v+w)\theta + vw + v^2$ as given in Lemma 4. Again, the remaining factor in the right-hand side when considering these groups is of degree 4. Since the probability of a degree 4 polynomial to factor in terms of degree at most 2 is higher than 1/3, we can recover all the discrete logarithms of the irreducible polynomials of $\mathcal{P}_{g_1,G(g_1),G(G(g_1))}$.

Lemma 4 (Systematic factor of particular 3-brackets in the useful variant). *Let G denote the map of (7) and let h_0, h_1, A and B be four polynomials such that $h_0(X) = X(X+w)$, $h_1(X) = uX + v$, $A(X) = X^2(X-g) +$*

$a(X - G(G(g)))$ and $B(X) = X(X - G(g)) + b(X - G(G(g)))$, with u, v, w, a, b and g in $\mathbb{F}_q$. Then $[A, B]_3$ is divisible by $(1+u)X^2 + (1+u)(v+w)X + vw + v^2$.

Proof. By bilinearity and antisymmetry: $[A, B]_3 = \left[X^2(X-g), X(X - G(G(g)))\right]_3 + b\left[X^2(X-g), X - G(G(g))\right]_3 + a[X - G(G(g)), X(X - G(G(g)))]_3$. The result of the lemma comes from the computation of the 3 bracket of the three pairs of different elements made with $X^2(X-g)$, $X(X - G(g))$ and $X - G(G(g))$. □

Fraction of degree 3 polynomials covered by our groups. Since we can recover all the discrete logarithms of the irreducible polynomials that appear in a group, the question that remains is whether every polynomial belongs to one of these groups at least.

Valid groups. In the sequel we restrict ourselves to the case where $v + w \neq 0$. Yet, if $v + w = 0$ then G is the zero mapping. This case is studied in the extended version of our article. To study the properties of our group, it is convenient to remark that since G is an homography, we can transform it into a permutation of the projective line $\mathbb{P}_1(\mathbb{F}_q)$. As classically done, we add the two following values of G:

$$G(\infty) = 0 \quad \text{and} \quad G(v + w) = \infty.$$

With this additional definition, we see that the groups we consider are indexed by triple $(g, G(g), G(G(g)))$ which do not contain the value ∞. Since $v + w \neq 0$ then ∞ belongs to a cycle of length at least 3. Thus, there are $q - 2$ valid groups corresponding to the values of g in $\mathbb{F}_q - \{G^{-1}(\infty), G^{-1}(G^{-1}(\infty))\}$. With this description we reach at best $q^3 - 2q^2$ polynomials of degree 3.

Groups at infinity. To reach more polynomials we define three additional groups $\mathcal{P}_{g,G(g),G(G(g))}$ when $g, G(g)$ or $G(G(g))$ is equal to ∞. These groups are given by the following descriptions:

$$\mathcal{P}_{\infty,0,G(0)} = \left\{ X\left(X^2 + \frac{vw + v^2}{1+u}\right) + \alpha X^2 + \beta (X - G(0)) | (\alpha, \beta) \in \mathbb{F}_q^2 \right\}.$$

$$\mathcal{P}_{\infty^{-1},\infty,0} = \left\{ X^2(X - \infty^{-1}) + \alpha X + \beta \left(X^2 + \frac{vw + v^2}{1+u}\right) | (\alpha, \beta) \in \mathbb{F}_q^2 \right\}.$$

$$\text{and} \quad \mathcal{P}_{\infty^{-2},\infty^{-1},\infty} = \{X^2(X - \infty^{-2}) + \alpha X(X - \infty^{-1}) + \beta | (\alpha, \beta) \in \mathbb{F}_q^2\}.$$

where ∞^{-1} stands for $G^{-1}(\infty)$ and ∞^{-2} for $G^{-1}(G^{-1}(\infty))$. We remark that these three extra groups at infinity satisfy the same systematic divisibility properties as the usual groups. Moreover, we enlarge the number of available polynomials to $q^3 + q^2$, which is now enough to possibly cover all the monic degree 3 polynomials.

Covering every degree 3 *polynomials.* Let $P(X) = X^3+a_2X^2+a_1X+a_0$ be an arbitrary monic polynomial of degree 3. If P belongs to a valid group $\mathcal{P}_{g,G(g),G(G(g))}$, there exist α and β such that:

$$\begin{aligned} \alpha - g &= a_2, \\ \beta - \alpha\, G(g) &= a_1, \\ \text{and } -\beta\, G(G(g)) &= a_0. \end{aligned}$$

Substituting the equations into each other, we find that this implies:

$$a_0 = -\left(a_1 + (a_2 + g)\, G(g)\right) \cdot G(G(g)). \tag{8}$$

After simplification this becomes $H_{a_1,a_2}(g) = a_0$, where H_{a_1,a_2} is an homography whose coefficients depend on a_1 and a_2. If there is no degenerescence inside the coefficients of H_{a_1,a_2}, there is exactly one possible value for g. Let us write the homography $H_{a_1,a_2}(g) = \frac{\lambda+\mu g}{\lambda'+\mu' g}$ where $\lambda = -v(w+v)((1+u)a_1 + va_2)$, $\mu = v((1+u)a_1 - v(v+w))$, $\lambda' = (1+u)(u(v+w)+w)$ and $\mu' = -(1+u)^2$. Thus, several cases appear:

- If $a_0 \neq \mu/\mu'$, then the homography is invertible.
  - As a consequence, as long as $g \neq \infty^{-1}$ and $g \neq \infty^{-2}$, the polynomial P belongs to the valid group generated by $g = H^{-1}_{a_1,a_2}(a_0), G(g)$ and $G(G(g))$, and only to this one. There are $q^3 - 3q^2$ such polynomials.
  - If $g = \infty^{-1}$ then $H_{a_1,a_2}(\infty^{-1}) = a_0$ becomes $a_0(\lambda'+\mu'(v+w)) = \lambda+\mu(v+w)$ and finally $a_0 = \infty^{-1}v(a_2+\infty^{-1})/(1+u)$. Besides, P belongs to the group at infinity $\mathcal{P}_{\infty^{-1},\infty,0}$ if there exists α and β such that $\beta - \infty^{-1} = a_2$, $\alpha = a_1$, and $\beta v(v+w)/(1+u) = a_0$. Substituting the previous equations in β into each other, we find that this implies $a_0 = \infty^{-1}v(a_2+\infty^{-1})/(1+u)$. Thus, the polynomial P belongs to $\mathcal{P}_{\infty^{-1},\infty,0}$. There are q^2-q such polynomials.
  - Similarly, if $g = \infty^{-2}$ then P belongs to the group at infinity $\mathcal{P}_{\infty^{-2},\infty^{-1},\infty}$ and, again, there are $q^2 - q$ such polynomials.
- If $a_0 = \mu/\mu'$ then Equation (8) is equivalent to $0 = g(a_0\mu' - \mu) = \lambda - \lambda'$. Moreover requiring $\lambda = \lambda'$ leads to $a_2 = \kappa(\kappa' a_1 + \kappa'')$ where $\kappa = (1+u)/(v^2(v+w))$, $\kappa' = v(v+w)$ and $\kappa'' = -u(v+w) - w$.
  - If $a_2 = \kappa(\kappa' a_1 + \kappa'')$ then P belongs to all the valid groups. There are q such polynomials.
  - If $a_2 \neq \kappa(\kappa' a_1 + \kappa'')$ the question is whether the $q^2 - q$ remaining polynomials belong to a group at infinity. Hopefully, if α denotes a_2 and β denotes $a_1 - v(v+w)/(1+u)$ then we have the following equality between polynomials: $X(X^2 + v(w+v)/(1+u)) + \alpha X^2 + \beta(X - G(0)) = X^3 + a_2X^2 + a_1X + v(v(v+w) - a_1(1+u))/(1+u)^2 = P(X)$. As a consequence, P belongs to the group at infinity $\mathcal{P}_{\infty,0,G(0)}$.

Remark 1. The previous proof does not interact with the restriction on a_2. Thus, the q polynomials satisfying $a_0 = \mu/\mu'$ and $a_2 = \kappa(\kappa' a_1 + \kappa'')$ belong also to the group at infinity $\mathcal{P}_{\infty,0,G(0)}$. Moreover, we notice that each intersection between two groups at infinity consists in q polynomials.

3.3 Discrete Logarithms of Degree 4 Polynomials

Previous deadlocks. The natural approach for computing the logarithm of $I_4(\theta)$ where I_4 is an irreducible polynomial of degree 4 is to start from the two polynomials $A(X) = X^3 + a_1X + a_0$ and $B(X) = X^2 + b_1X + b_0$, construct a relation from Equation (5) and require that I_4 divides $[A, B]_3$. Rewriting this last condition as $[A, B]_3 = 0 \pmod{I_4}$, we obtain 4 bilinear equations in the 4 unknowns (a_0, a_1, b_0, b_1). Experimentally, as explained in [Jou14], this system is easy to solve using standard Gröbner basis algorithms. However, on average, the system has solutions only for half of the degree 4 polynomials. As a consequence, the other half polynomials are not accessible using this technique.

Another idea, already present in [AMORH14], is to use the additional relations from Section 3.1 to improve the probability of success. For an irreducible of degree 4 that failed to by expressed in terms of degree 3 polynomials, there is a 1/2 chance that its image by Frobenius, whose degree is 8, factors into 2 quartic polynomials. Each of them has a 1/2 chance to be expressed in terms of degree 3 polynomials. Thus, for a polynomial that failed, we have a 1/8 chance to compute its logarithms through this process. This increases the global probability of success for a degree 4 irreducible to 9/16. Repeating the process, we can further improve the success probability. Heuristically, we expect to have a probability of $p_0 = (4 - \sqrt{8})/2 \approx 0.586$. Unfortunately, this does not suffice to obtain all degree 4 polynomials. In order to bypass this problem, several techniques have been considered but none of them are sufficient in the general case. We propose here an approach that fits to the simple construction whereas the useful (but tricky) variant is detailed in the extended version of the article.

Improved approach for degree 4 polynomials for the simple construction. The general approach we propose consists in dividing the degree 4 polynomials in groups of size q^3 and following an approach close to the case of the degree 3 polynomials presented in Section 3.2. We first compute all the discrete logarithms of a group $\mathcal{Q}_g$ of degree 4 polynomials of the form:

$$\mathcal{Q}_g = \{(X^4 + g) + \alpha X^3 + \beta X^2 + \gamma X | (\alpha, \beta, \gamma) \in \mathbb{F}_q^3\}. \tag{9}$$

To do so, we use a partition of this group $\mathcal{Q}_g = \cup_{g' \in \mathbb{F}_q} \mathcal{Q}_{g,g'}$ where:

$$\mathcal{Q}_{g,g'} = \{(X^4 + g) + \alpha X^3 + \beta X^2 + g'X | (\alpha, \beta) \in \mathbb{F}_q^2\}. \tag{10}$$

To build relations involving the polynomials from $\mathcal{Q}_{g,g'}$ we apply Equation (5) with polynomials of the form $A(X) = (X^4+g)+aX^2+g'X$ and $B(X) = X^3+bX^2$. With the simple construction, Lemma 5 shows that $[A, B]_4$ is of degree 11 and has a systematic factor of degree one. Together with the general degree 3 systematic factor coming from Lemma 1, we are left with a polynomial of degree 7. According to Appendix B the probability that it factors in terms of degree at most 3 is about 24%.

Besides, the number of irreducible polynomials in $\mathcal{Q}_{g,g'}$ is close to $q^2/4$. Combining with previous techniques, after removing the irreducibles whose logarithms can be obtained, we are left with approximately $(1-0.586)\cdot q^2/4 \approx 0.10\, q^2$

unknowns. Thus we obtain enough equations to solve the linear system. Finally, we recover the discrete logarithms of $\mathcal{Q}_g$ by computing the ones of its q subgroups.

Lemma 5 (Systematic factor of particular 4-brackets in the simple construction[8]). *Let h_0, h_1, A and B be four polynomials in $\mathbb{F}_q[X]$ such that h_0 is affine, $h_1(X) = X(X+t)$, $A(X) = (X^4+g) + \alpha X^2 + \alpha' X$ and $B(X) = X^3 + \beta X^2 + \beta' X$. Then $[A,B]_4$ is a polynomial of degree at most 11 divisible by X.*

Computing the remaining discrete logarithms. Let $I_4 \notin \mathcal{Q}_g$ be a degree 4 polynomial. We start again from $A(X) = (X^4+g) + aX^2 + a'X$ and $B(X) = X^3 + bX^2 + b'X$, and apply Equation (5) to construct a relation such that I_4 divides $[A,B]_4$. As in [Jou14], the heuristic probability to find a solution from the bilinear system is 1/2. Extracting the degree one factor of Lemma 5 and the general degree 3 systematic factor of Lemma 1, and dividing then the degree 11 polynomial $[A,B]_4$ by our degree 4 polynomial I_4, we are left with a polynomial of degree 3, which logarithm is already known. Thus, with only one group of the form described in (9) we recover the discrete logarithms of approximately half[9] the irreducible missing polynomials of degree 4.

To obtain the remaining polynomials, we recursively apply this method to other groups of the form (9). We show in Section 4.3 that $O(\log(q))$ such groups suffice and that the cost of their computations is asymptotically dominated by the cost of the first one, which is $O(q^6)$, as announced.

4 Asymptotic Complexities

4.1 Recovering Discrete Logs of Degree 2 Irreducible Polynomials

We require to collect about q^2 equations in the Relation Collection phase. Since the probability to obtain a good relation is lower-bounded by 2/3, this phase costs $O(q^2)$ operations. We perform then a sparse linear algebra phase on a matrix of size $O(q^2)$. We recall that due to the form of the relations that are created, the number of entries in each row is $O(q)$. The total cost to recover the discrete logarithms of degree 2 polynomials is so $O((q^2)^2 \cdot q) = O(q^5)$.

4.2 Recovering Discrete Logs of Degree 3 Irreducible Polynomials

With the really simple construction. Since each group $\mathcal{P}_g$ contains $O(q^2)$ unknowns and since the linear algebra is done with a matrix containing $O(q)$ entries per line, the cost of computing a single group is $O(q^5)$. There are q such groups and the global cost is, thus, $O(q^6)$.

[8] The proof of this lemma works as the one of Lemma 3.

[9] The probability to recover the logarithm of a missing polynomial is in fact higher than 1/2, since we can use additional equations as presented in Section 3.1. Even there are very useful in practice, the 1/2 probability already suffices for the analysis.

With the useful variant. We consider 3 groups at infinity and $q-2$ valid groups with $O(q^2)$ unknowns each. Thus the global cost of this phase is $O(q^6)$.

4.3 Recovering Discrete Logs of Degree 4 Irreducible Polynomials

With the simple construction. We compute first the discrete logarithms of one group of the form (10). Since we have a system of dimension $O(q^2)$ with $O(q)$ entries per line, it can be solved for a cost of $O(q^5)$. To recover the logarithms of one group of the form (9), we need thus $O(q^6)$ operations.

Besides, the probability to recover the logarithm of an irreducible degree 4 polynomial from the first group of the form (9) is heuristically 1/2. Considering that the probabilities are independent, with k such groups, the proportion of discrete logarithms that are left unknown is $1/2^k$. Clearly, as the number of available groups grows, this proportion quickly tends to 0. With $O(\log(q))$ such groups we expect to obtain all degree 4 polynomials. As a consequence, performing the computation of $O(\log(q))$ groups in this direct way, we would obtain a global complexity of $O(q^6 \log q)$. However, this overlooks the fact that for each new group that we wish to compute, the size of the corresponding linear system decreases and the rate of decrease follows a geometric progression[10]. As a consequence, the cost of computing the required $O(\log(q))$ groups is dominated by the computation of the first one.

Hence, the total complexity[11] of the precomputation phases becomes $O(q^6)$. This has to be compared with the previous $O(q^7)$ complexity for the same phases. However, we recall that the part of the algorithm that dominates the asymptotic complexity of each Frobenius Representation algorithm is the Descent phase, which is not under consideration in this article.

5 A Computational Example in Characteristic 3

To illustrate our algorithm, we have implemented our new ideas for a real-sized example in characteristic 3. Namely, we let $q = 3^5$ and define $\mathbb{F}_q = \mathbb{F}_3[\alpha]$, where α satisfies $\alpha^5 - \alpha + 1 = 0$. Choosing $h_0 = X^2 + \alpha^{111} X$ and $h_1 = \alpha X + 1$ we see that $X\, h_1(X^q) - h_0(X^q)$ has an irreducible factor of prime degree 479. We let U denote a root of this irreducible polynomial and construct $\mathbb{F}_{3^{5\cdot 479}}$ as $\mathbb{F}_q[U]$.

[10] Another option is to continue the computation for all groups. Due to the geometric progression, the complexity of this part is the same. Yet, it yields a total runtime lower than the option of recomputing on the fly the missing degree 4 polynomials logarithms when required but as a side effect it raises the required amount of storage.

[11] We consider here algorithms of Wiedmann or Lanczos families, that has a complexity of $O(n^2)$ for a square matrix with n columns. Yet, using dense linear algebra with fast matrix multiplication instead of sparse linear algebra would lower the asymptotic complexity from $O(q^6)$ to $O(q^{5.746})$. We do not choose to consider these algorithms here since there are not at all competitive in practice.

The cardinality of the finite field we consider is a 3796-bit integer. A good point of comparison is the computation over $\mathbb{F}_{2^{12\cdot 367}}$ performed in [GKZ14a]. Indeed, even if the bitsize of this computation was slightly larger than ours, being on 4404 bits, this total size included a factor of two in the exponent which comes for free when using the older Frobenius Representation algorithms. More precisely, the main drawback of our approach is that instead of computing logarithms in the field $\mathbb{F}_{q^{dk}}$ it only computes in $\mathbb{F}_{q^k}$. Many cryptographers have commented on this free factor, claiming that it is not really relevant in practice and that one should rather consider extension field of prime degree that can be embedded in the target field. For us, this is $\mathbb{F}_{3^{479}}$ a 760-bit field. This can also be compared to the largest computation of this form currently performed in the finite field $\mathbb{F}_{2^{809}}$ (see [BBD+13]). However, the most relevant comparison is the previous general record in characteristic 3, performed in the 1551-bit finite field $\mathbb{F}_{3^{6*163}}$ and presented in [AMORH14].

With this example, computing all the discrete logarithms of the factor base with $D = 2$, containing 29 646 irreducible polynomials, required 16 sequential hours on a single core of an Intel Core i7 at 2.7 GHz. The equations themselves took 35 seconds to produce, the 16 hours being the cost of the linear algebra modulo:

$$M = \frac{3^{5\cdot 479} - 1}{488246858}.$$

Enlarging the factor base to degree 3 polynomials was performed with 244 independent computations, each involving 19 602 unknowns in the corresponding linear system. On the same machine, the sequential cost of one such computation is 6.5 hours. Since these computations are independent, they are straightforward to parallelize.

For degree 4 polynomials, the first subset of 243 independent computations we considered contained on average 7 385 unknowns in each linear system. The largest system contained 7 571 unknowns and the smallest 7 212. Note that this used a suboptimal variation of the technique obtained in Section 3.3 and induced slightly larger system. Using the correct variation, we would expect a smaller number of unknowns per linear system (around 6100).

The second subset has on average 3 674 unknowns, the third 1 829, the fourth 909, the fifth 452. We see that as predicted, the rate of decrease is very steep, essentially a geometric series of ratio 1/2. As a consequence, the runtimes for these subsets rapidly becomes negligible compared to the main part of the computation consisting in tackling the degree 3 polynomials. Here again, our implementation is suboptimal, but this was not a critical part of the computation. In fact, for all subsets beyond the fifth, we only tried to the logarithms of the elements in terms of the first four subsets. Indeed, the resulting systems were so small (around 450 unknowns) and sparse that they could be solve with a straightforward Gaussian elimination. Thus for these subsets, the running time was dominated by the generation of the equations (around 2h for each subset) and it did not make sense to insist on reducing the size of the linear systems. In total, we computed 30 subsets and they were enough to express the logarithms of all the degree 4 elements encountered further during the computation.

For the descent phase, we followed the state of the art and were able to express the seeked discrete logarithm using a total of under 41 millions polynomials of degree 4 (and of course also polynomials of lower degree). For lack of space, we leave out the details, they will be reported in the extended version of this article. The total running time of the computation was under 8600 CPU-hours.

6 Conclusion

In this paper, we proposed an improved Frobenius Representation algorithm for the computation of discrete logarithms in small characteristic. Together with the aim of simplifying the description of previous algorithms, we reduce the complexity of the precomputation phase to $O(q^6)$ for general extension degree. Computations with such a cost were previously available only for special degrees such as Kummer extension.

References

[AMORH14] Gora Adj, Alfred Menezes, Thomaz Oliveira, and Francisco Rodríguez-Henríquez. Computing discrete logarithms in $\mathbb{F}_{3^{6\cdot 137}}$ and $\mathbb{F}_{3^{6\cdot 163}}$ using Magma. Cryptology ePrint Archive, Report 2014/057, 2014.

[BBD+13] Razvan Barbulescu, Cyril Bouvier, Jérémie Detrey, Pierrick Gaudry, Hamza Jeljeli, Emmanuel Thomé, Marion Videau, and Paul Zimmermann. Discrete logarithm in $\mathbb{F}_{2^{809}}$ with ffs. Cryptology ePrint Archive, Report 2013/197, 2013.

[BGJT14] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *EUROCRYPT*, pages 1–16, 2014.

[BMV85] I.F. Blake, R.C. Mullin, and S.A. Vanstone. Computing logarithms in $\mathbb{F}_{2^n}$. In *Advances in Cryptology, Proceedings of CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 73–82. 1985.

[GGMZ13a] Faruk Göloglu, Robert Granger, Gary McGuire, and Jens Zumbrägel. On the function field sieve and the impact of higher splitting probabilities - application to discrete logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{3^{3164}}$. In *CRYPTO (2)*, pages 109–128, 2013.

[GGMZ13b] Faruk Göloglu, Robert Granger, Gary McGuire, and Jens Zumbrägel. On the function field sieve and the impact of higher splitting probabilities: Application to discrete logarithms in $\mathbb{F}_{2^{1971}}$. Cryptology ePrint Archive, Report 2013/074, 2013.

[GKZ14a] Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. Breaking '128-bit secure' supersingular binary curves (or how to solve discrete logarithms in $\mathbb{F}_{2^{4\cdot 1223}}$ and $\mathbb{F}_{2^{12\cdot 367}}$). Cryptology ePrint Archive, Report 2014/119, 2014.

[GKZ14b] Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. On the powers of 2. Cryptology ePrint Archive, Report 2014/300, 2014.

[Jou13a] Antoine Joux. Faster index calculus for the medium prime case application to 1175-bit and 1425-bit finite fields. In *EUROCRYPT*, pages 177–193, 2013.

[Jou13b] Antoine Joux. A new index calculus algorithm with complexity L(1/4 + $o(1)$) in very small characteristic. Cryptology ePrint Archive, Report 2013/095, 2013.

[Jou14] Antoine Joux. A new index calculus algorithm with complexity L(1/4 + $o(1)$) in very small characteristic. In *Selected Areas in Cryptography-SAC 2013*, volume 8282 of *Lecture Notes in Computer Science*, pages 355–382. Springer, 2014.

A Action of $\mathbf{PGL_2}(\mathbb{F}_q)$ on Polynomials

We detail here the reason why we can restrict ourselves to the case $A(X) = X^D + a(X)$ and $B(X) = X^{D-1} + b(X)$, with a and b polynomials of degree $D-2$.

Assume that we are initially given an equation for two degree D polynomials A_0 and B_0. We may assume that these two polynomials are monic by multiplying Equation (5) by the inverse of the product of their leading coefficients. Moreover, thanks to Proposition 1 we have $[A_0, B_0]_D = [A_0, B_0 - A_0]_D$. Thus, we can replace B_0 by $B_1 = B_0 - A_0$. If there is no unexpected fall of degree (i.e. in the general case), B_1 has degree $D-1$. We can again assume that it is monic. If the coefficient of X^{D-1} in A_0 is a_{D-1}, remarking that:

$$[A_0, B_1]_D = [A_0 - a_{D-1}B_1, B_1]_D,$$

we can replace A_0 by a polynomial A_1 whose coefficient of X^{D-1} is 0. Thus, the pair (A_1, B_1) generates the same equation as (A_0, B_0) and has the announced restricted form.

B Estimating Probabilities of Factoring Polynomials

Throughout the paper, we need to estimate the probabilities that a polynomial of degree D factors into terms of degree at most d. This is often done by using the heuristic rule that the polynomial behaves in this respect like a random polynomial.

In this appendix, we analyze these probabilities for random polynomials. Let us start we a simple example and consider the probability that a random monic polynomial of degree D splits into linear factors. Over the finite field $\mathbb{F}_q$ there are q^D distinct monic polynomials of degree D. Among those it is easy to count the number of squarefree polynomials that split into linear terms, there are in correspondance with their D distinct roots in $\mathbb{F}_q$, thus there are precisely $\binom{q}{D} = \frac{q\cdot(q-1)\cdots(q-(D-1))}{D!}$ such polynomials. Hence, the fraction of polynomials that split is lower bounded by $\binom{q}{D} \cdot q^{-D}$, which tends to $1/D!$ as q tends to infinity.

To obtain an upper bound, we also need to count the polynomials that split and have multiple roots. The formula is more complex since we need to compute a sum over partitions of D into multiplicities. However, the number of terms in this sum is independent of q and each term is a multinomial that chooses the correct number of roots with each multiplicity. Since each term contains at most

$D-1$ roots, we can upper bound the contribution by $C(D)\,q^{D-1}$ where $C(D)$ does not depend on q. Thus, as q tends to infinity, the upper bound on the total fraction of polynomials that split tends to $1/D!$ too.

For more complex decomposition, this kind of analysis remains doable but messy for arbitrary fixed values of D and d. Thankfully, in the present paper, we are only considering values such that:

$$d+1 > D/2.$$

Under this constraint the analysis becomes quite easy. Indeed, if a polynomial P of degree D does not factor into terms of degree at most d, it must have at least one factor F_k of large degree $k \geq d+1$. Since $k > D/2$, this factor is unique. Now, the probability that P can be written as $F_k \cdot Q$, with F_k an irreducible of degree k and Q an arbitrary polynomial of degree $D-k$ is precisely $(N_k \cdot q^{D-k})/q^D = N_k/q^k$, where N_k denotes the number of irreducible polynomials of degree k over $\mathbb{F}_q$. Thus, the probability is precisely the fraction of irreducibles among degree k polynomials and it is well-known that this tends to $1/k$ as q tends to infinity. As a consequence, as q tends to infinity the probability that a degree D polynomial factors into terms of degree at most d, when $d+1 > D/2$ tends to:

$$1 - \sum_{k=d+1}^{D} \frac{1}{k}.$$

Using this we can easily estimate the probabilities required in the paper:

- For $D=3$ and $d=2$ the probability is $1-\frac{1}{3}=\frac{2}{3}$.
- For $D=4$ and $d=2$ the probability is $1-\frac{1}{3}-\frac{1}{4}=\frac{5}{12}\approx 0.4167$.
- For $D=7$ and $d=3$ the probability is $1-\frac{1}{4}-\frac{1}{5}-\frac{1}{6}-\frac{1}{7}=\frac{101}{420}\approx 0.2405$.