Quasi-subfield polynomials and the elliptic curve discrete logarithm problem

Huang, Ming-Deh; Kosters, Michiel ; Petit, Christophe; Yeo, Sze Ling ; Yun, Yang

DOI:
10.1515/jmc-2015-0049

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Huang, M-D, Kosters, M, Petit, C, Yeo, SL & Yun, Y 2020, 'Quasi-subfield polynomials and the elliptic curve discrete logarithm problem', *Journal of Mathematical Cryptology*, vol. 14, no. 1, pp. 25-38. https://doi.org/10.1515/jmc-2015-0049

Research Article

Ming-Deh Huang*, Michiel Kosters, Christophe Petit, Sze Ling Yeo, and Yang Yun

Quasi-subfield Polynomials and the Elliptic Curve Discrete Logarithm Problem

https://doi.org/10.1515/jmc-2015-0049
Received Feb 05, 2020; accepted Feb 06, 2020

Abstract: We initiate the study of a new class of polynomials which we call quasi-subfield polynomials. First, we show that this class of polynomials could lead to more efficient attacks for the elliptic curve discrete logarithm problem via the index calculus approach. Specifically, we use these polynomials to construct factor bases for the index calculus approach and we provide explicit complexity bounds. Next, we investigate the existence of quasi-subfield polynomials.

Keywords: Elliptic Curve Discrete Logarithm Problem, Cryptanalysis, Finite Fields

2010 Mathematics Subject Classification: 94A60, 11T06, 11T71

1 Introduction

The hardness of the discrete logarithm problem (DLP) in cyclic groups has been one of the key mathematical problems underlying many public key cryptosystems in use today. In its most general form, given a generator g of a cyclic group $G = \langle g \rangle$ of order N, and an arbitrary element $h \in G$, DLP seeks for the smallest integer k such that $h = g^k$ (or $h = kg$ in the additive notation). For the purposes of cryptographic applications, the most common cyclic groups used are multiplicative subgroups of finite fields as well as subgroups of rational points on elliptic curves over finite fields.

The discrete logarithm problem in multiplicative groups of finite fields was the basis for one of the earliest public-key protocols, namely the Diffie-Hellman key exchange protocol [5]. Since then, remarkable progress has been made to improve the complexity of solving this problem. First, in [1], index calculus methods were proposed to solve DLP over finite fields in sub-exponential time. More impressive results were obtained in recent years with heuristic quasi-polynomial time bounds in the case of finite field of small characteristics [2].

By contrast, the elliptic curve discrete logarithm problem (ECDLP) has so far been more resistant to efficient attacks and the best attacks for groups of N rational points are generic algorithms such as Pollard's rho and Baby-Step-Giant-Step algorithms with a number of group operations proportional to $\sqrt{N}$. In this paper, we refer to the complexity bounds from these generic algorithms as generic bounds. In 2004, Semaev proposed an index calculus approach to solve ECDLP [23]. This inspired several subsequent works leading to sub-exponential attacks for some families of elliptic curves [4].

***Corresponding Author: Ming-Deh Huang:** University of Southern California, United States of America; Email: mdhuang@usc.edu
Michiel Kosters: University of California, Irvine, United States of America; Email: kosters@gmail.com
Christophe Petit: University of Birmingham, United Kingdom of Great Britain and Northern Ireland; Email: christophe.f.petit@gmail.com
Sze Ling Yeo: Institute for Infocomm Research (I2R) and Nanyang Technical University, Singapore; Email: slyeo@i2r.a-star.edu.sg
Yang Yun: School of science, Jinling Institute of Technology, China; Email: YANG0379@e.ntu.edu.sg

Essentially, the index calculus method seeks for a good factor basis that gives rise to an efficient relation search. Semaev's work converts this relation search into a problem of solving polynomial equations over finite fields. Factor bases that have been proposed include sets of elliptic curve points with the x-coordinates from finite subfields [4, 14] or more generally, vector spaces [11, 21]. The corresponding polynomial systems are typically solved via Weil descent, that is, transformed into polynomial systems over the base field and then solved using one of the existing polynomial solving methods such as Rojas' algorithm [22], Gröbner basis algorithms [8, 9] or resultants. Thus far, this approach works well for finite fields $\mathbb{F}_{q^n}$ with q being large. For q small and n a prime, heuristic sub-exponential results were proposed in [21]. However, experimental results in [16] gave some evidence against the heuristic assumption used. In other words, the best proven attack for the important class of elliptic curves over $\mathbb{F}_{2^n}$ for n prime are the generic attacks.

One therefore wonders if there exist factor bases that directly give rise to a more efficient polynomial solving technique. In this paper, we propose factor bases constructed from roots of polynomials of the form $X^{q^{n'}} - \lambda(X)$ which split completely in $\mathbb{F}_{q^n}$. When $\deg(\lambda)$ is small enough, we call $X^{q^{n'}} - \lambda(X)$ a *quasi-subfield* polynomial, by extension of the subfield case which has $\lambda(X) = X$. Using these polynomials, we construct a polynomial system over the field $\mathbb{F}_{q^n}$ such that the zero set gives a relation for the index calculus method. By employing Rojas's algorithm to solve this polynomial system, we give precise complexity results for our index calculus algorithm.

The next interesting question is to ask for the existence of the quasi-subfield polynomials. Apart from the above mentioned links to efficient attacks on the elliptic curve discrete logarithm problem, this problem is an interesting mathematical problem in its own right. What we are able to prove so far is that there exists a class of quasi-subfield polynomials such that our algorithm yields a time complexity that beats exhaustive search (exhaustive search runs in $O(N)$ steps). In addition, we investigate this problem by considering additive and multiplicative subgroups of fields. Statistical arguments suggest that for arbitrary q and n in general these groups are unlikely to give rise to quasi-subfield polynomials to achieve a time complexity better than generic bounds for ECDLP over $\mathbb{F}_{q^n}$. An interesting question is whether special families of $\{q, n\}$ can be identified where these groups do give rise to quasi-subfield polynomials. The search of quasi-subfield polynomials in general remains an open problem.

In Section 2 we recall previous ECDLP algorithms for elliptic curves defined over extension fields. In Section 3 we describe our new algorithm and we analyze its complexity depending on its various parameters. In Section 4 we discuss the existence of suitable parameters for our approach. We finally conclude the paper in Section 5.

2 Index Calculus Algorithms for ECDLP over Extension Fields

For the remainder of this paper, let q be a prime, $K = \mathbb{F}_{q^n}$ be a finite field with q^n elements, and let E be an elliptic curve defined over K. Let P be a rational point on E, and let Q be randomly chosen in the subgroup generated by P. As this is standard in cryptographic contexts, we assume that P generates a subgroup of large prime order N. We are interested in algorithms to compute the discrete logarithm of Q with respect to P, namely an integer s such that $Q = [s]P$. We are particularly interested in the case where q is a very small prime.

2.1 Existing Algorithms

Here we focus on algorithms specific to elliptic curves, and particularly index calculus algorithms [4, 11, 14, 21, 23].

Given q, n, E, P, Q, we first choose parameters m, n' and a vector space V of dimension n' over $\mathbb{F}_q$. We then define a *factor basis*

$$\mathcal{F} := \{(x, y) \in E(K) \mid x \in V\}.$$

Following standard index calculus algorithms for the discrete logarithm problem over finite fields, we then collect sufficiently many *relations* of the form

$$a_i P + b_i Q = \sum_{j=1}^{m} P_{ij}$$

with a_i, b_i randomly chosen and $P_{ij} \in \mathcal{F}$.

Finally, we perform linear algebra operations modulo N on the relations to obtain a new relation of the form $aP + bQ = 0$ from which one (almost always) deduces the discrete logarithm value $s = -a/b \bmod N$.

In this algorithm, for every index i, we need to solve an instance of the following problem:

Problem 1 (Point Decomposition Problem). *Fix a positive integer m. Given a point $R \in E(K)$, find, if any, m points $P_1, \ldots, P_m \in \mathcal{F}$, such that $R = P_1 + \ldots + P_m$.*

This is typically done using Semaev's summation polynomials [23], a *Weil descent* strategy, and an algorithm to solve systems of multivariate polynomial equations.

For every index $r \geq 2$, the *summation polynomial* $S_r \in K[X_1, X_2, \ldots, X_r]$ is a polynomial depending on E such that $S_r(x_1, x_2, \ldots, x_r) = 0$ if and only if there exist $y_i \in \overline{K}$ and $(x_i, y_i) \in E(\overline{K})$ with $(x_1, y_1) + (x_2, y_2) + \ldots + (x_r, y_r) = 0$ on $E(\overline{K})$. This is a symmetric polynomial with degree 2^{r-2} in each variable.

In order to solve the point decomposition problem above, we can solve

$$S_{m+1}(x_1, x_2, \ldots, x_m, x_R) = 0, \quad x_i \in V, \tag{1}$$

where x_R is the X coordinate of R, and for each of these solutions $x_1, \ldots, x_m$, one checks whether all the y_i are in K.

This problem is further reduced to a polynomial system as follows. We fix a basis $\{\theta_1, \ldots, \theta_n\}$ of K over $\mathbb{F}_q$ and a basis $\{v_1, \ldots, v_{n'}\}$ of V over $\mathbb{F}_q$. We then introduce mn' variables x_{ij} over $\mathbb{F}_q$, with $1 \leq i \leq m$ and $1 \leq j \leq n'$ such that $x_i = \sum_{j=1}^{n'} x_{ij} v_j$. Substituting in Equation 1 and projecting the equation over each component of the basis $\{\theta_1, \ldots, \theta_n\}$ of K over $\mathbb{F}_q$, we obtain a system of n equations in the mn' variables x_{ij}.

When q is reasonably large compared to n, one can take $V := \mathbb{F}_q$. The system is then solved using resultants or a Groebner basis algorithm [4, 14]. On the other hand when q is small, one adds the so-called *field equations* $x_{ij}^q - x_{ij} = 0$ to the system, and solves it using a Groebner basis algorithm [11, 21].

2.2 Complexity Analysis

The analysis of these algorithms has so far required several heuristic assumptions.

Fix a positive integer m. Heuristically, one can expect that roughly half of the values in V are the x-coordinates of exactly two points on the curve, and hence we approximate $|\mathcal{F}| \approx q^{n'}$. Moreover, assuming that most (unordered) tuples of m points in $\mathcal{F}$ produce a distinct sum, the probability that the randomly chosen point $R_i := a_i P + b_i Q$ can be split as a sum of m points in $\mathcal{F}$ is heuristically estimated by

$$\frac{|\mathcal{F}|^m}{m! \cdot q^n} \approx \frac{q^{n'm-n}}{m!}.$$

These heuristic assumptions appear reasonable, and they are common in the literature. Furthermore, we need about $|\mathcal{F}|$ decompositions to solve the discrete logarithm problem.

If we let $C(q, n, m, n')$ be the expected cost of Solving Problem 1, the *relation search* phase of the algorithm then has an expected cost of

$$q^{n'} \frac{m!}{q^{n'm-n}} C(q, n, m, n') = m! \cdot q^{n-n'm+n'} C(q, n, m, n').$$

In practice m will be small compared to $q^{n'}$, so a sparse linear algebra algorithm will be used for the linear algebra phase of the algorithm [25]. The expected cost of this phase can therefore be approximated by $mq^{2n'}$.

We then have:

Theorem 2.1. *Under plausible heuristic assumptions, the total cost of solving a discrete logarithm problem for a curve defined over K can be approximated by*

$$m! \cdot q^{n-n'm+n'} C(q, n, m, n') + mq^{2n'}$$

where C is as above.

Evaluating the cost $C(q, n, m, n')$ of solving Problem 1 has proven to be very difficult. The polynomial systems obtained after the Weil descent procedure are solved with Groebner basis or multivariate resultant algorithms. These algorithms reduce polynomial system solving to linear algebra. The main issue in estimating the cost of Problem 1 is estimating the size of this linear algebra problem.

Existing upper bounds seem to provide a good approximation for the cost of solving generic systems of polynomial equations, but have often been of little value for systems with special structure, and in particular those coming from cryptography [10, 16, 19].

For some ranges of the parameters n and q, these bounds suffice to show that the algorithm above with $V = \mathbb{F}_q$ outperforms generic algorithms [4, 14] and in the best case the algorithm has subexponential complexity. In the important case $q = 2$ and n prime, the bounds lead to an overall cost above the cost of generic algorithms [11], but studies of the polynomial systems suggest that the actual complexity of solving them may be lower [12, 17, 21, 24]. In [21] it was shown that under the *first fall degree assumption*, a heuristic previously used in other cryptanalysis work [6, 7, 10, 15], the overall cost of ECDLP over characteristic 2 fields would be subexponential. Since then Huang et al. [16] have provided some evidence against the first fall degree assumption, and the actual cost of the algorithm remains unknown.

2.3 Current Challenges

There are two main challenges related to the family of index calculus algorithm sketched in this section:

- Complexity estimates: the complexity of these algorithms is hard to analyze.
- Practical efficiency: solving ECDLP for curves used in cryptography is still very hard in practice.

This is in contrast to the particular case $V = \mathbb{F}_q$ where for some range of parameters, improvements over generic algorithms have been demonstrated both in theory and in practice [4, 14].

3 A new ECDLP Algorithm

The particular vector space $V = \mathbb{F}_q$ can be equivalently described as the set of elements $x \in K$ such that $x^q = x$. Let $m := n$ in this case. From the problem

$$S_{n+1}(x_1, x_2, \ldots, x_n, x_R) = 0, \quad x_i \in V,$$

we easily derive n equations

$$S^{(i)}(X_1, X_2, \ldots, X_n) := S_{n+1}^{q^i}(X_1, X_2, \ldots, X_n, x_R) \mod X_1^q - X_1, \ldots, X_n^q - X_n.$$

Clearly, all the equations above can be chosen to have the same degree. We thus have a system of n equations (letting $i = 0, 1, \ldots, n-1$) in n variables. The system can be solved using resultants or Groebner basis algorithms, leading to the good complexity results mentioned above.

Motivated by these ideas, we consider factor bases whose elements are roots of some "nice" polynomials. Concretely, our main idea in this paper is to replace the vector space V by the set of points satisfying an equation of the form $x^{q^{n'}} = \lambda(x)$ where λ is a polynomial of small degree.

3.1 Our Algorithm

Let q, n, E, P, Q as above, and suppose we want to solve the corresponding discrete logarithm problem. Furthermore, fix $\lambda(x) \in K[X]$ and positive integers n' and m.

Let $\mathcal{M}$ be the set of monomials in $K[X_1, \ldots, X_m]$. For a positive integer i and $f = \sum_{M \in \mathcal{M}} a_M M \in K[X_1, \ldots, X_m]$, we define the polynomial $F^i(f)$ as the polynomial $F^i(f) = \sum_M a_M^{q^i} M$, that is, we raise the coefficients of f to the power q^i. Let

$$\begin{aligned} \varphi : K[X_1, \ldots, X_m] &\to K[X_1, \ldots, X_m] \\ f(X_1, \ldots, X_m) &\to F^{n'}(f)(\lambda(X_1), \ldots, \lambda(X_m)). \end{aligned}$$

Observe that we have

$$f^{q^{n'}} \equiv \varphi(f) \pmod{X_1^{q^{n'}} - \lambda(X_1), \ldots, X_m^{q^{n'}} - \lambda(X_m)}.$$

Our algorithm has three steps:

1. **Choice of a "factor basis":** Set

$$V := \left\{ x \in K \mid x^{q^{n'}} - \lambda(x) = 0 \right\}$$

and a "factor basis"

$$\mathcal{F} := \{(x, y) \in E(K) \mid x \in V\}.$$

2. **Relation search:** let Δ be a small integer. For $i = 1, 2, \ldots, |\mathcal{F}| + \Delta$, we generate random $a_i, b_i \in \{0, \ldots, N-1\}$ and we compute $R_i := a_i P + b_i Q$. We let $S^{(0)}(X_1, X_2, \ldots, X_m) := S_{m+1}(X_1, X_2, \ldots, X_m, x_{R_i})$ and for $k = 1, \ldots, m-1$, we let

$$S^{(k)}(X_1, X_2, \ldots, X_m) := \varphi\left(S^{(k-1)}(X_1, X_2, \ldots, X_m)\right).$$

We solve the polynomial system $\mathcal{S} = \{S^{(k)}\}_{k=0}^{m-1}$ using Rojas' sparse resultant algorithm [22] and a univariate polynomial root finding algorithm. Given a solution $(x_1, \ldots, x_m)$, we check whether all the x values correspond to points in the factor basis in two steps:

   - Check if for each $j = 1, 2, \ldots, m$, $x_j \in V$, that is, $x_j^{q^{n'}} = \lambda(x_j)$.
   - Check if for each $j = 1, 2, \ldots, m$ there exists $y_j \in K$ such that $(x_j, y_j) \in E(K)$.

We then find signs such that the relation $R_i = \sum_{j=1}^{m} \pm(x_j, y_j)$ holds.
Once a solution is found, we store the corresponding relation.

3. **Linear algebra:** as in previous algorithms, we perform linear algebra operations on the relations to derive a relation of the form $aP + bQ = 0$, from which we deduce the discrete logarithm value.

Our goal in the relation search step is to solve the equation $S_{m+1}(x_1, \ldots, x_m, x_R) = 0$ with $x_i \in V$, $i = 1, \ldots, m$. This is equivalent to finding the zeros of the system $\mathcal{T} = \{S_{m+1}(X_1, \ldots, X_m, x_R), X_1^{q^{n'}} - \lambda(X_1), \ldots, X_m^{q^{n'}} - \lambda(X_m)\}$. In this paper we consider the system $\mathcal{S}$, which might have more solutions than the system $\mathcal{T}$. We make the assumption that $\mathcal{S}$ is zero-dimensional. We refer to Appendix B for an argument in support of this assumption.

We observe that a randomly chosen polynomial λ with small degree will usually result in a very small factor basis $\mathcal{F}$ (and in an impractically large m), while a randomly chosen set of around $q^{n'}$ elements from K will lead to a polynomial λ of large degree. The existence and construction of suitable parameters will be further discussed in Section 4.

3.2 Complexity Analysis

The next lemma (proved in Appendix A.1) evaluates the cost of Rojas' algorithm:

Lemma 3.1. *Let $d = \deg(\lambda)$. Consider the set $\mathcal{S} = \{S^{(k)} : k = 0, 1, \ldots, m-1\}$. Suppose that $\mathcal{S}$ is zero-dimensional. By applying Rojas's method [22], one can construct univariate polynomials $h(X), h_1(X), \ldots, h_m(X) \in K[X]$ such that the zero set of $\mathcal{S}$ on $(\overline{K}^*)^m$ is given by $\{(h_1(\theta), h_2(\theta), \ldots, h_m(\theta)) \in (\overline{K}^*)^m \mid h(\theta) = 0\}$. Moreover, these polynomials can be found in $\tilde{O}(m^{5.188} \cdot (3d)^{4.876m^2})$ arithmetic steps over (a small degree extension of) K.*

As in previous algorithms, we heuristically approximate $|\mathcal{F}| \approx |V|$ and we assume $|V| \approx q^{n'}$.

Under the assumptions recalled above, we can therefore evaluate the cost of our algorithm as follows:

Theorem 3.2. *Let $d :=$ deg λ. Under the assumptions listed in this section, the complexity of our algorithm is*

$$m! \cdot q^{n-n'm+n'} \cdot \tilde{O}\left(m^{5.188} \cdot (3d)^{4.876m^2}\right) + mq^{2n'}$$

arithmetic operations.

An ideal polynomial λ in our attack will have a small degree d. The case $V = \mathbb{F}_q$ is used in Diem and Gaudry's algorithms [4, 14], and it corresponds to $d = n' = 1$. Concretely, we have $m = n$ and $|V| = q$. Theorem 3.2 gives the time complexity of $n! \cdot q \cdot \tilde{O}\left(n^{5.188} 3^{4.876n^2}\right) + nq^2$ arithmetic steps. By letting n and q vary in a particular way, one can get a sub-exponential complexity (see [4]).

Remark 3.1. *Recall that generic algorithms use $O(q^{n/2})$ group operations, whereas brute force approaches require $O(q^n)$ group operations.*

- *Assume $d > q^{0.102\frac{n}{m^2}}$. Then Theorem 3.2 has a term which is at least $O(q^{n/2})$, suggesting that our algorithm does not beat generic algoritms.*
- *Fix an integer m and real number α with $0 < \alpha < 1$. Assume that $m \approx \alpha n/n'$ and furthermore that $d \approx q^{n'^2/n}$. Then our complexity reduces to*

$$\tilde{O}\left(q^{n-n'm+n'} \cdot d^{4.876m^2} + q^{2n'}\right) = \tilde{O}\left(q^{n(1-\alpha+4.876\alpha^2)+\alpha n/m} + q^{2\alpha n/m}\right)$$

For m large enough this gives a complexity of approximately $\tilde{O}\left(q^{n(1-\alpha+4.876\alpha^2+\epsilon)}\right)$. The minimum value of $1 - \alpha + 4.876\alpha^2$ is approximately 0.95. Hence when α is chosen properly (for example $\alpha = 0.1$), the complexity is $\tilde{O}(q^{0.95n})$ which beats brute force algorithms. Note that one can get better complexity estimates if $d \approx q^{\beta n'^2/n}$ where $\beta < 1$.

Definition 3.1. *In view of Remark 3.1, we call polynomials $X^{q^{n'}} - \lambda(X) \in K[X]$ dividing $X^{q^n} - X$ with $\log_q(d) = \log_q(\deg(\lambda)) < n'^2/n$ quasi-subfield polynomials.*

4 Finding Suitable Parameters and constructions

We now discuss the existence and computation of suitable parameters for our attack. We first give a general existential result. Then we focus on the case of additive subgroups of the finite field. We give a probabilistic argument in that context, followed by an explicit construction. In Appendix C we further study additive subgroups for Mersenne prime extensions of characteristic 2 fields, and we investigate multiplicative subgroups of the finite field.

4.1 Lower Bounds on deg λ

Let q, n, n', m, d and λ be as above, and suppose that deg $\lambda > 1$. Assume that $L(X) = X^{q^{n'}} - \lambda(X)$ splits over K, so that $|V| = q^{n'}$. The following lemma (proved in Appendix A.2) shows that deg λ cannot be too small.

Lemma 4.1. *Suppose that* $L(X) = X^{q^{n'}} - \lambda(X) \in K[X]$ *divides* $X^{q^n} - X$ *and that* $\ell := \log_q d = \log_q \deg \lambda > 0$. *Then we have*

$$\left\lfloor \frac{n}{n'} \right\rfloor \ell + (n \bmod n') \geq n'.$$

One can prove a similar result when $L(X)$ splits almost completely over K (see Lemma C.2). Remark that the above lemma does not apply when λ is linear.

The above constraints on $\ell = \log_q \deg \lambda$ are more strict when $n \bmod n'$ is smaller. When $n \bmod n'$ is too small, we see that our algorithm is often worse than generic algorithms by Remark 3.1.

We remark that random polynomials dividing $X^{q^n} - X$ are unlikely to be such that ℓ is small. On the other hand, a random polynomial of the shape of L with ℓ small is unlikely to have many roots in K. We will therefore need ad hoc constructions to build these polynomials. Perhaps, the most natural constructions are to consider additive and multiplicative subgroups of K. In what follows, we argue that these constructions may not provide us with the sparse polynomials we seek.

4.2 Additive Subgroups

In the remaining of this section we focus on polynomials L such that the corresponding set $V := \left\{ x \in K \mid x^{q^{n'}} = \lambda(x) \right\}$ is a vector space over $\mathbb{F}_q$. The factor bases considered are therefore a subset of the factor bases considered in [11, 21] and follow-up works, though of course our algorithm computes relations in a different way.

We recall that for any vector space V over $\mathbb{F}_q$, the associated polynomial $L(X) = \prod_{\alpha \in V}(X - \alpha)$ is a monic linearized polynomial, namely its only non-zero coefficients are coefficients of power of q terms [3, Ch. 11]. Any two distinct vector spaces correspond to distinct linearized polynomials, but not every linearized polynomial corresponds to a vector space. In fact, as shown in Appendix A.3, we have:

Lemma 4.2. *Let* $N(q, n, n')$ *be the number of distinct vector spaces over* $\mathbb{F}_q$ *of dimension* n' *that are contained in* K. *Assume* $n \geq n' \geq 1$. *Then:*

$$q^{n'(n-n')} \cdot (1 - n' q^{-(n-n'+1)}) \leq N(q, n, n') \leq q^{n'(n-n'+1)}.$$

If n is large in comparison to n', the previous lemma essentially tells us that there are about $q^{n'(n-n')}$ subspaces of K of dimension n'. There are exactly $q^{nn'}$ monic linearized polynomials of degree $q^{n'}$ over K, and there are $q^{n\ell}$ such polynomials with $\deg \lambda \leq q^\ell$. Heuristically, we may expect that linearized polynomials associated to vector spaces are as likely to have small d than other polynomials. We would therefore expect that the number of vector spaces of dimension n' such that $\deg \lambda \leq q^\ell$ is about

$$q^{n'(n-n')} q^{n(\ell-n')} = q^{n\ell - n'^2}.$$

In particular, we would expect no such polynomial to exist whenever $\ell << \frac{n'^2}{n}$.

On the other hand, as in Remark 3.1 parameters with $\ell > \frac{n'^2}{n}$ will result in a time complexity worse than brute force. Hence this approach might only work well for exceptional families of parameters. Indeed an exceptional family where the heuristic analysis does fail is where $n' | n$ and $\lambda(x) = x$, thus $\ell = 0 < \frac{n'^2}{n}$, and the subspace is none other than the subfield of degree n' over $\mathbb{F}_q$. The work of Diem [4] shows that there is an infinite family of such n and q where the ECDLP can be solved in subexponential time in that case.

In the next section we provide an explicit infinite family of parameters giving quasi-subfield polynomials.

In Appendix C.1, we further study the case of parameters where n is a Mersenne prime.

4.3 A Particular Family

Let F be a field of characteristic p. We recall that to any polynomial $f = \sum_{i=0}^{\ell} f_i X^i \in F[X]$, one can associate a linearized polynomial $L_f(X) = \sum_{i=0}^{\ell} f_i X^{q^i} \in F[X]$. Moreover this association is such that given any two

polynomials $f_1, f_2 \in F[x]$, we have

$$L_{f_1 f_2}(X) = L_{f_1} \circ L_{f_2}(X)$$

where $\circ$ denotes the polynomial composition [3, Ch. 11]. The polynomial $f \in F[X]$ divides $X^n - 1$ if and only if $L_f(X)$ divides $X^{q^n} - X$.

Lemma 4.3. *Let q' be powers of p. For $l \geq 0$ let $p_i = \sum_{i=0}^{l} q'^i$. Then in $F[X]$, where F is any field of characteristic p, one has for $k \geq 0$:*

$$(1 + \sum_{i=0}^{k} X^{p_i}) | (X^{p_{k+1}} - 1) \text{ and hence } (X + \sum_{i=0}^{k} X^{q^{p_i}}) | (X^{q^{p_{k+1}}} - X).$$

Proof. One has $p_{k+1} = q' p_k + 1$. Let $f = 1 + \sum_{i=0}^{k} X^{p_i}$. Modulo f we find:

$$0 \equiv X f^{q'} = X + \sum_{i=0}^{k} X (X^{p_i})^{q'} = X^{p_0} + \sum_{i=0}^{k} X^{p_{i+1}} = X^{p_{k+1}} + f - 1 \equiv X^{p_{k+1}} - 1.$$

□

We apply the construction in the above lemma to the case $F = K = \mathbb{F}_{q^n}$ with $n = p_{k+1}$. Note that $\deg(X + \sum_{i=0}^{k} X^{q^{p_i}}) = q^{p_k}$ and that $n' = p_k$. Furthermore, note that $\ell = p_{k-1} = \log_q(\deg(\lambda))$ where $\lambda = -\sum_{i=0}^{k-1} X^{q^{p_i}}$. Note that

$$\ell = p_{k-1} = \frac{p_{k-1} p_{k+1}}{p_{k+1}} = \frac{p_{k-1}(q' p_k + 1)}{p_{k+1}} = \frac{(q' p_{k-1} + 1) p_k - (p_k - p_{k-1})}{p_{k+1}} = \frac{p_k^2}{p_{k+1}} - \frac{(p_k - p_{k-1})}{p_{k+1}} < \frac{n'^2}{n}.$$

Hence our construction gives rise to quasi-subfield polynomials. By picking the right parameters, Remark 3.1 implies that our algorithm will run faster than brute force search. Note that since $n \equiv 1 \pmod{n'}$, we are in the worst case scenario of Lemma 4.1. We hope that there are better constructions giving rise to better complexity estimates.

5 Conclusion and Open Problems

In this paper we introduced quasi-subfield polynomials, which are polynomials over a finite field $\mathbb{F}_{q^n}$ of the form $X^{q^{n'}} - \lambda(X)$ which are nearly split and where λ has small degree. We showed that such polynomials could lead to faster algorithms for the elliptic curve discrete logarithm problem (ECDLP) over composite fields when $\deg \lambda$ is small enough. Finally, we investigated the existence of these polynomials, and provided one particular family leading to an ECDLP algorithm more efficient than exhaustive search.

It remains an open problem to find (or rule out) the existence of quasi-subfield polynomials where $\deg \lambda$ is small enough to improve on the best (generic) algorithms for ECDLP. A question of particular interest is whether the bound on $\deg \lambda$ provided by Lemma 4.1 is tight: in fact removing the term $n \bmod n'$ in this bound would show that our approach cannot beat generic algorithms. Besides the construction of better families of quasi-subfield polynomials, one may hope to beat generic algorithms by generalizing our approach in various directions: such generalizations could include using a rational function for λ, using an isogeny map for L (as in [20]), or adapting various tricks also used in other index calculus algorithms such as double large prime, unsymmetrized and unbalanced variations [12, 13, 18]. We hope that our paper will motivate further work in these directions.

References

[1] Leonard M. Adleman, A Subexponential Algorithm for the Discrete Logarithm Prob- lem with Applications to Cryptography (Abstract), in: *FOCS*, pp. 55–60, IEEE, 1979.

[2] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux and Emmanuel Thomé, A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic, in: *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Tech- niques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, pp. 1–16, 2014.

[3] E. R. Berlekamp, *Algebraic coding theory*, Aegean Park Press, Laguna Hills, CA, USA, 1984.

[4] Claus Diem, On the discrete logarithm problem in elliptic curves, *Compositio Math- ematica* **147** (2011), 75–104.

[5] Whitfield Diffie and Martin E. Hellman, New Directions in Cryptography, **IT-22** (1976), 644–654.

[6] Jintai Ding and Timothy J. Hodges, Inverting HFE Systems Is Quasi-Polynomial for All Fields, in: *CRYPTO* (Phillip Rogaway, ed.), Lecture Notes in Computer Science 6841, pp. 724–742, Springer, 2011.

[7] Vivien Dubois and Nicolas Gama, The Degree of Regularity of HFE Systems, in: *ASIACRYPT* (Masayuki Abe, ed.), Lecture Notes in Computer Science 6477, pp. 557–576, Springer, 2010.

[8] Jean-Charles Faugère, A new efficient algorithm for computing Gröbner bases (F4)., *Journal of Pure and Applied Algebra* **139** (1999), 61–88.

[9] Jean-Charles Faugère, A new efficient algorithm for computing Gröbner bases with- out reduction to zero (F5), in: *Proceedings of the 2002 international symposium on Symbolic and algebraic computation*, ISSAC '02, pp. 75–83, ACM, New York, NY, USA, 2002.

[10] Jean-Charles Faugère and Antoine Joux, Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases, in: *CRYPTO* (Dan Boneh, ed.), Lecture Notes in Computer Science 2729, pp. 44–60, Springer, 2003.

[11] Jean-Charles Faugère, Ludovic Perret, Christophe Petit and Guénaël Renault, Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields, in: *EUROCRYPT* (David Pointcheval and Thomas Johansson, eds.), Lecture Notes in Computer Science 7237, pp. 27–44, Springer, 2012.

[12] Steven D. Galbraith and Shishay W. Gebregiyorgis, Summation Polynomial Algo- rithms for Elliptic Curves in Characteristic Two, in: Progress in Cryptology *-IN- DOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014*, Proceedings (Willi Meier and Debdeep Mukhopad- hyay, eds.), Lecture Notes in Computer Science 8885, pp. 409–427, Springer, 2014.

[13] P. Gaudry, E. Thomé, N. Thériault and C. Diem, A double large prime variation for small genus hyperelliptic index calculus, *Math. Comp.* **76** (2007), 475–492 (elec- tronic).

[14] Pierrick Gaudry, Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem, *J. Symb. Comput.* **44** (2009), 1690–1702.

[15] Louis Granboulan, Antoine Joux and Jacques Stern, Inverting HFE Is Quasipolynomial, in: *CRYPTO* (Cynthia Dwork, ed.), Lecture Notes in Computer Science 4117, pp. 345–356, Springer, 2006.

[16] Ming-Deh A. Huang, Michiel Kosters and Sze Ling Yeo, Last Fall Degree, HFE, and Weil Descent Attacks on ECDLP, in: *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015*, Proceedings, Part I, pp. 581–600, 2015.

[17] Yun-Ju Huang, Christophe Petit, Naoyuki Shinohara and Tsuyoshi Takagi, Improvement of Faugère et al.'s Method to Solve ECDLP, in: *IWSEC* (Kazuo Sakiyama and Masayuki Terada, eds.), Lecture Notes in Computer Science 8231, pp. 115–132, Springer, 2013.

[18] Antoine Joux and Vanessa Vitse, *Elliptic Curve Discrete Logarithm Problem over Small Degree Extension Fields*. Application to the static Diffie-Hellman problem on $E(\mathbb{F}_{q^5})$, Cryptology ePrint Archive, Report 2010/157. To appear in Journal of Cryptology., 2010, http://eprint.iacr.org/.

[19] Christophe Petit, *Bounding HFE with SRA*, https://www.cs.bham.ac.uk/~petitcz/files/SRA_GB.pdf.

[20] Christophe Petit, Michiel Kosters and Ange Messeng, Algebraic Approaches for the Elliptic Curve Discrete Logarithm Problem over Prime Fields, in: *Public-Key Cryptography - PKC 2016 - 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part II* (Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano and Bo-Yin Yang, eds.), Lecture Notes in Computer Science 9615, pp. 3–18, Springer, 2016

[21] Christophe Petit and Jean-Jacques Quisquater, On Polynomial Systems Arising from a Weil Descent, in: *Asiacrypt* (Xiaoyun Wang and Kazue Sako, eds.), Lecture Notes in Computer Science 7658, pp. 451–466, Springer, 2012.

[22] Maurice Rojas, Solving Degenerate Sparse Polynomial Systems Faster, *Journal of Symbolic Computation* **28** (1999), 155–186.

[23] Igor Semaev, *Summation polynomials and the discrete logarithm problem on elliptic curves*, Cryptology ePrint Archive, Report 2004/031, 2004, http://eprint.iacr.org/.

[24] Michael Shantz and Edlyn Teske, Solving the Elliptic Curve Discrete Logarithm Problem Using Semaev Polynomials, Weil Descent and Grb̈ner Basis Methods - An Experimental Study, in: *Number Theory and Cryptography - Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday*, pp. 94–107, 2013.

[25] Douglas H. Wiedemann, Solving sparse linear equations over finite fields, *IEEE Trans. Information Theory* **32** (1986), 54–62.

A Omitted Proofs

A.1 Proof of Lemma 3.1

Proof. The polynomial system has m equations $S^{(k)} = 0$ in m variables. The summation polynomial S_{m+1} has degree 2^{m-1} in each variable, and each application of φ increases the degree by a factor d in each variable, so the polynomial $S^{(k)}$ has degree $d^{k-1}2^{m-1}$ in each variable.

We compute the quantities $\mathcal{M}(E)$, $\mathcal{R}(\bar{E})$ and $\mathcal{S}(\bar{E})$ in Theorem 2.1 of [22]. Following the notations of [22] paper, E_k is the fundamental hypercube of dimension m and length $d^{k-1}2^m$, and $E_{m+1} = \triangle$ is the pyramid whose edges are all fundamental vectors. For $k = 1, \ldots, m$, let $\lambda_k = d^{k-1}2^{m-1}$, and let $\lambda_{m+1} = (m!)^{-1}$. We have

$$\mathcal{M}(E) = \mathrm{Vol}(E_1, \ldots, E_m) = \prod_{k=1}^{m} \lambda_k = 2^{m(m-1)} d^{\frac{m(m-1)}{2}}.$$

We have

$$\mathcal{R}(\bar{E}) = \prod_{k=1}^{m+1} \lambda_k \sum_{k=1}^{m+1} \lambda_k^{-1} \leq \mathcal{M}(E) + \frac{m}{2^{m-1}m!}\mathcal{M}(E) \leq 2\mathcal{M}(E) = 2^{m^2-m+1} d^{\frac{m(m-1)}{2}}.$$

We finally have

$$\mathcal{M}_{\bar{E}}^{ave} = \left(\frac{1}{m+1}\sum_{k=1}^{m+1} \lambda_k\right)^m \leq \lambda_m^m = (2d)^{m(m-1)},$$

hence

$$\mathcal{S}(\bar{E}) = O\left(\sqrt{m} e^m (2d)^{m(m-1)}\right).$$

Applying [22, Theorem 2.1], we obtain that Rojas' algorithm requires

$$\tilde{O}\left(m^{5.188} 2^{7.376m^2 - 3.948m + 2} d^{4.876m^2 - 4.876m}\right) = \tilde{O}\left(m^{5.188}(3d)^{4.876m^2}\right)$$

arithmetic steps. □

The univariate polynomials produced by Rojas' algorithm are of degree bounded by $\mathcal{M}(E)$. Over finite fields, root-finding is quasi-linear in this degree, and its cost can be neglected in the overall complexity estimation.

A.2 Proof of Lemma 4.1

Proof. To simplify notations, let us assume that λ is defined over $\mathbb{F}_q$ (the general proof follows the same lines). One has

$$X^{q^{2n'}} \equiv (X^{q^{n'}})^{q^{n'}} \equiv \lambda(X)^{q^{n'}} \equiv \lambda(X^{q^{n'}}) = \lambda(\lambda(X)) \bmod L(X).$$

Recursively, we have

$$X^{q^{n'k}} \equiv \lambda \circ \lambda \circ \ldots \circ \lambda(X) \bmod L(X)$$

where λ is composed k times with itself in this formula. We then have

$$X^{q^n} \equiv (\lambda \circ \lambda \circ \ldots \circ \lambda(X))^{q^{n \bmod n'}} \bmod L(X)$$

where λ is composed $\lfloor \frac{n}{n'} \rfloor$ times with itself in this formula. Since $X^{q^n} \equiv X \bmod L(X)$, we deduce the result. □

A.3 Proof of Lemma 4.2

Proof. We have $N(q,n,n') = \frac{N_1(q,n,n')}{N_2(q,n,n')}$, where N_1 is the number of choices of n' elements over $\mathbb{F}_q^n$ that are linearly independent over $\mathbb{F}_q$, and N_2 is the number of such choices defining the same vector space. One has

$$N_1 = \left(q^n - 1\right)\left(q^n - q\right)\left(q^n - q^2\right)\ldots\left(q^n - q^{n'-1}\right) \leq q^{nn'}.$$

Also, one finds, using that for $0 \leq \epsilon \leq 1$ one has $(1-\epsilon)^n \geq 1 - n\epsilon$:

$$N_1 \geq q^{nn'}(1 - q^{n'-1-n})^{n'} \geq q^{nn'} \cdot (1 - n'q^{(n'-1)/n}).$$

Furthermore, one finds

$$q^{(n'-1)n'} \leq N_2 = \left(q^{n'} - 1\right)\left(q^{n'} - q\right)\left(q^{n'} - q^2\right)\ldots\left(q^{n'} - q^{n'-1}\right) < q^{n'^2}.$$

Since $N = N_1/N_2$, the result follows. □

B On the dimension of our polynomial systems

Throughout this section we let $K = \mathbb{F}_{q^n}$, $\overline{K}$ the algebraic closure of K, and $A = K[X_1, \ldots, X_m]$. If S is a set of polynomials in A, then $Z(S)$ denotes the zero set $\{P \in \overline{K}^m | F(P) = 0 \text{ for all } F \in S\}$. If I is an ideal of A, then $V(I) \subset \mathrm{Spec}A$ denotes the set of all prime ideals which contain I. Note that $Z(S)$ is finite if $\dim \wp = 0$ for all prime ideal $\wp \in V(I)$ where I is the ideal generated by S.

In our algorithm, finding a relation is reduced to solving a polynomial system $S = \{S^{(i)}, i = 0, \ldots, m-1\}$. Here $S^{(0)}(X_1, X_2, \ldots, X_m) = S_{m+1}(X_1, X_2, \ldots, X_m, \xi_R)$ where ξ_R is the x-coordinate of a point R which is a random linear combination of the points P and Q, and inductively $S^{(i+1)} = \varphi(S^{(i)})$ for $i \geq 0$, where $\varphi : A \to A : f(X_1, X_2, \ldots, X_m) \to F^{n'}(f)(\lambda(X_1), \lambda(X_2), \ldots, \lambda(X_m))$, which is a ring morphism. Here F raises the coefficients of a polynomial to the power q, and λ is a polynomial. In the main text we make the heuristic assumption that for random R, $Z(S)$ is likely finite. The goal of this section is to provide theoretical analysis in support of this heuristic assumption.

If I be an ideal of A, then I_φ denotes the ideal generated by $\varphi(I)$. Let $I^{(0)} = I$ and inductively $I^{(i+1)} = (I^{(i)})_\varphi$ for $i \geq 0$. Let J_i be the ideal generated by $I^{(0)} \cup \ldots \cup I^{(i)}$ for $i \geq 0$. Our goal is to characterize when $\dim Z(J_{m-1})$ is 0. The situation considered in our algorithm is a special case where I is the ideal generated by $S_{m+1}(X_1, X_2, \ldots, X_m, \xi_R)$.

For $u, v \in \mathrm{Spec}A$, we write $u \xrightarrow{\varphi} v$ if $\dim u = \dim v$ and $v_\varphi \subset u$. We will show that for every $u \in \mathrm{Spec}A$, there is a unique v such that $u \xrightarrow{\varphi} v$. In fact $v = \varphi^{-1}(u)$.

We say that a sequence of prime ideals u_0, ..., u_i in Spec$A$ is a *φ-chain* of length i led by u_0 if $u_0 \xrightarrow{\varphi} u_1 \xrightarrow{\varphi} \ldots \xrightarrow{\varphi} u_i$. We will show that for $i \geq 0$, $V(J_i)$ is the set $\wp \in V(I)$ such that $\wp$ leads a φ-chain of length i in $V(I)$.

There are only finitely many minimal primes in $V(I)$. In general it is likely the case that there are no minimal primes u and v in $V(I)$ such that $u \xrightarrow{\varphi} v$, in which case $\dim J_1 < \dim I$. Inductively there are finitely many minimal prime ideals in $V(J_i)$, each leading a φ-chain of length i. It is likely that there are no minimal primes u and v in $V(J_i)$ such that $u \xrightarrow{\varphi} v$, in which case no minimal prime in $V(J_i)$ leads a φ-chain of length $i+1$, hence $\dim J_{i+1} < \dim J_i$. Consequently J_{m-1} is likely of dimension 0.

In our situation I is the ideal generated by $S_{m+1}(X_1, X_2, \ldots, X_m, \xi_R)$, and the heuristic assumption is that for R being a random combination of P and Q the ideal I is likely in the good case hence J_{m-1} is likely of dimension 0.

The rest of this section is devoted to proving the above-mentioned property of φ-chains and characterization of J_i in terms of φ-chains in $V(I)$.

It is easy to see that $\varphi : A \to A$ is an integral ring morphism, that is A is integral over $\varphi(A)$. Therefore if $u \in \mathrm{Spec}A$, $\varphi^{-1}(u) \in \mathrm{Spec}A$ and $\dim u = \dim \varphi^{-1}(u)$. Let $v = \varphi^{-1}(u)$. Then $\varphi(v) \subset u$, so $v_\varphi \subset u$, so $u \xrightarrow{\varphi} v$.

Let $w \in \mathrm{Spec}A$. If $\dim w = \dim u$ and $w_\varphi \subset u$. Then $\varphi(w) \subset u$. So $w \subset \varphi^{-1}u = v$. Since $\dim w = \dim u = \dim v$, we must have $w = v$. We have proved the following:

Lemma B.1. *Let $u \in SpecA$. Then there is a unique $v \in SpecA$ such that $u \xrightarrow{\varphi} v$. In fact $v = \varphi^{-1}(u)$.*

Theorem B.2. *Suppose I is an ideal of A. Let J be the ideal generated by I and I_φ. Then $V(J) = \{\wp | \wp \xrightarrow{\varphi} u$ and $\wp, u \in V(I)\}$.*

To prove the theorem, observe that for $\wp \in \mathrm{Spec}A$, $\wp \in V(J)$ if and only $\wp \in V(I)$ and $\wp \in V(I_\varphi)$.

It is straightforward to verify that for $\wp \in \mathrm{Spec}A$,

$$I_\varphi \subset \wp \Leftrightarrow \varphi(I) \subset \wp \Leftrightarrow I \subset \varphi^{-1}(\wp).$$

From Lemma B.1 it follows that

$$V(J) = \{\wp | \wp \xrightarrow{\varphi} u \text{ and } \wp, u \in V(I)\}.$$

The theorem is proved.

The main result of this section is the next theorem.

Theorem B.3. *The set $V(J_i)$ consists of primes $\wp \in V(I)$ that leads a φ-chain of length i in $V(I)$. In particular,* $\dim J_{m-1} = 0$ *if and only if every φ-chain of length $m-1$ in $V(I)$ is of dimension 0.*

Proof of Theorem B.3 The case $i = 1$ follows directly from Theorem B.2. For $i > 1$, since $V(J_i) = V(J_{i-1} \cup (J_{i-1})_\varphi)$, Theorem B.2 implies that $V(J_i)$ consists of primes $\wp \in V(J_{i-1})$ such that $\wp \xrightarrow{\varphi} u_1$ with $u_1 \in V(J_{i-1})$. By induction since $u_1 \in V(J_{i-1})$, u_1 leads a φ-chain of length $i-1$ in $V(I)$. That is, $u_1 \xrightarrow{\varphi} u_2 \ldots \xrightarrow{\varphi} u_i$ with $u_2, \ldots, u_i \in V(I)$. So $\wp \xrightarrow{\varphi} u_1 \xrightarrow{\varphi} u_2 \ldots \xrightarrow{\varphi} u_i$. That is $\wp$ leads a φ-chain of length i in $V(I)$.

For the converse suppose $\wp$ leads a φ-chain of length i in $V(I)$. Thus $\wp \xrightarrow{\varphi} u_1 \xrightarrow{\varphi} u_2 \ldots \xrightarrow{\varphi} u_i$ with $\wp, u_1, \ldots, u_i \in V(I)$. Applying induction to $\wp$, u_1, ..., u_{i-1} we conclude that $\wp \in V(J_{i-1})$. Similarly applying induction to u_1, ..., u_i we conclude that $u_1 \in V(J_{i-1})$. Since $\wp \xrightarrow{\varphi} u_1$, Theorem B.2 implies that $\wp \in V(J_i)$. This completes the proof of the theorem.

C Further comments on the existence of quasi-subfield polynomials

In this section we further develop our analysis of additive subgroups of $\mathbb{F}_{q^n}$, specializing to the case of Mersenne prime degree extensions when $q = 2$.

We also investigate the case of multiplicative subgroups of $\mathbb{F}_{q^n}^\star$.

C.1 Mersenne Prime Degree Extensions over $\mathbb{F}_2$

We first expand on the construction of Section 4.2.

A plausible attempt for finding good parameters is to seek for parameters such that the polynomial $X^n - 1$ has many small degree factors over $\mathbb{F}_q$. This polynomial is then a priori more likely to have a large number of (non necessarily irreducible) factors of degree n', maximizing the chance that one of these factors is sparse enough. We would then take L as the linearized polynomial corresponding to that factor.

Mersenne prime degree extensions of $\mathbb{F}_2$ look particularly promising in that respect. Indeed when $n = 2^k - 1$ is prime, the polynomial $(X^n - 1)/(X - 1)$ has $(n-1)/k$ irreducible factors of degree k over $\mathbb{F}_2$.

In the following, let $N(k, n')$ be the number of distinct polynomials of degree n' that divide $X^n - 1 \in \mathbb{F}_2[X]$. We have:

Lemma C.1. *Let k such that $n = 2^k - 1$ is prime. Then $N(k, n') = \binom{\lfloor n/k \rfloor}{\lfloor n'/k \rfloor}$ if $n' \bmod k \in \{0, 1\}$, and $N(k, n') = 0$ otherwise.*

Note that we have

$$\log \binom{n/k}{n'/k} \approx (n'/k)\log(n/k) - (n'/k)\log(n'/k) \approx (n'/k)\log(n/n') \approx (n'/k)\log m.$$

The number of monic polynomials of degree n' over $\mathbb{F}_2$ is $2^{n'}$, and there are 2^ℓ such polynomials of the form $X^{n'} + s(X)$ with $s(X)$ of degree at most ℓ. Heuristically assuming that the density of "sparse enough" polynomials is identical for factors of $X^n - 1$ and for random polynomials, we expect that the number of polynomials of degree n' that divide $X^n - 1$ and are sparse enough can be approximated by

$$N(k, n')2^{\ell - n'}.$$

In particular, the existence of such polynomials a priori depends on whether ℓ is bigger or smaller than $n' - (n'/k)\log m$.

To improve on generic algorithms, we want $\ell < 0.102\frac{n}{m^2}$ as in Remark 3.1. Together with the above constraint on ℓ, this leads to a constraint

$$0.102n/m^2 > n' - (n'/k)\log m.$$

Using $mn' \approx n$ and $k = \log n$, this inequality implies

$$\frac{\log n'}{n'} < 0.102\frac{\log n}{n}$$

but on the other hand we have $\log n/n < \log n'/n'$ since $n' < n$. We conclude that this approach cannot lead to interesting parameters for our attack, unless the above probabilistic argument fails significantly.

C.2 Multiplicative Subgroups

We now attempt to construct V as a multiplicative subgroup of $K^\star$. Such a subgroup can be characterized by an equation of the form

$$X^r - 1 = 0$$

where r is a divisor of $q^n - 1$. Let $n' \geq \log_q r$. The above equation implies

$$L(X) := X^{q^{n'}} - X^a = 0$$

where $a := q^{n'} \bmod r$. Note that the set V corresponding to this polynomial L contains the element 0 in addition to the subgroup of order r.

In this context, we note the following generalization of Lemma 4.1:

Lemma C.2. *Suppose that* $\ell := \log_q d = \log_q \deg \lambda > 0$. *Then we have*

$$\left\lfloor \frac{n}{n'} \right\rfloor \ell + (n \bmod n') \geq \log_q |V|.$$

Proof. There exists a polynomial $a(X)$ of degree $2^{n'} - |V|$ such that $L(X) = X^{q^{n'}} + \lambda(X)$ divides $(X^{q^n} - X)a(X)$. Following the same reasoning as for Lemma 4.1, we obtain an inequality

$$d^{\frac{n}{n'}} q^{(n \bmod n')} + \deg a \geq q^{n'}$$

from which we deduce the result. □

It is a priori a good idea to choose q and n such that $q^n - 1$ has many distinct small prime factors, as this will give more options for r. The number of choices for r is maximal when $q^n - 1$ has $n\log q/\log(n\log q)$ distinct prime factors bounded by $\log(n\log q)$. In that case there are approximately

$$\binom{n\log q/\log(n\log q)}{n'\log q/\log(n\log q)}$$

options for r. In general, we expect far less options for r.

We observe the similarity of this formula with the value of $N(k, n')$ given by Lemma C.1 for the Mersenne case. We similarly do not expect to improve on generic algorithms this way, except maybe for exceptional parameters.