HAL
open science

A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms

Faruk Göloğlu, Antoine Joux

To cite this version:

Faruk Göloğlu, Antoine Joux. A simplified approach to rigorous degree 2 elimination in discrete logarithm algorithms. Mathematics of Computation, 2019, pp.1. hal-01960765

HAL Id: hal-01960765

https://hal.science/hal-01960765v1

Submitted on 12 Jul 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A SIMPLIFIED APPROACH TO RIGOROUS DEGREE 2 ELIMINATION IN DISCRETE LOGARITHM ALGORITHMS

FARUK GÖLOĞLU AND ANTOINE JOUX

Abstract. In this paper, we revisit the ZigZag strategy of Granger, Kleinjung and Zumbrägel. In particular, we provide a new algorithm and proof for the so-called degree 2 elimination step. This allows us to provide a stronger theorem concerning discrete logarithm computations in small characteristic fields $\mathbb{F}_{q^{k_0 k}}$ with k close to q and k_0 a small integer. As in the aforementioned paper, we rely on the existence of two polynomials h_0 and h_1 of degree 2 providing a convenient representation of the finite field $\mathbb{F}_{q^{k_0 k}}$.

1. Introduction

Discrete logarithm computations in finite fields of small characteristic have been recently shown to be much easier than previously believed. However, the algorithms that have been produced in most papers remain heuristic. A notable exception is [2], where it is shown that:

Theorem 1. *For every prime p, there exist infinitely many explicit extension fields $\mathbb{F}_{p^n}$ for which the discrete logarithm problem in $\mathbb{F}_{p^n}^*$ can be solved in expected quasi-polynomial time*

$$\exp((1/\log 2 + o(1))\,(\log n)^2).$$

In fact, this comes as an easy corollary of another theorem also given in [2]:

Theorem 2. *Given a prime power $q > 61$ that is not a power of 4, an integer $k_0 \geq 18$, coprime polynomials $h_0, h_1 \in \mathbb{F}_{q^{k_0}}[X]$ of degree at most two and an irreducible degree k factor I of $h_1 X^q - h_0$, the discrete logarithm problem in $\mathbb{F}_{q^{k_0 k}}^*$ where $\mathbb{F}_{q^{k_0 k}}^* \cong \mathbb{F}_{q^{k_0}}[X]/(I)$ can be solved in expected time*

$$q^{\log_2 k + O(k_0)}.$$

Note that we have renamed the variables and parameters to match the notations of the present paper.

In this paper, we revisit the method. More precisely, we provide a slightly modified strategy and a new algorithm and analysis for the so-called degree 2 elimination step. This yields a simpler analysis of its success and allows us to derive a stronger theorem than Theorem 2 about the computation of discrete logarithms in small characteristic.

2. Preliminaries

A common feature to the recent algorithms for computing discrete logarithms in small characteristic is the way they represent the finite fields they are using.

Let q be a prime power, Q_0 a (small) power of q, h_0 and h_1 two polynomials of degree at most 2 with coefficients in $\mathbb{F}_{Q_0}$. Assume that the polynomial $h_1(X)X^q - h_0(X)$ has an irreducible factor I_k of degree k. Then, this irreducible polynomial can be used to

2010 *Mathematics Subject Classification.* 11Y-16, 12Y-05.

represent $\mathbb{F}_{{Q_0}^k}$ as $\mathbb{F}_{Q_0}[X]/(I_k)$. Moreover, if θ denotes a root of I_k in the algebraic closure of $\mathbb{F}_q$ we see that:

$$\theta^q = \frac{h_0(\theta)}{h_1(\theta)}.$$

Since, θ^q is the image of θ by the Frobenius map, this justifies the name of Frobenius representation used in [3].

Throughout the article, we follow this convention and let θ be a fixed root of I_k.

Many of the early record computations performed with these small characteristic algorithms focused on the case where h_0 and h_1 have degree at most one. Indeed, in that case, several specific speed-ups apply and they permit to perform much larger computations. Unfortunately, this special case strongly restricts the extension degrees that can be addressed, limiting the options to Kummer, twisted Kummer and Artin-Schreier extensions. In particular, the achievable extension degree using degree 1 polynomials divides the order of $PGL(2, \mathbb{F}_q)$, i.e, $q^3 - q$.

In more recent computations, the focus shifted to more general choices for the extension degree. This implies that the maximum of the degrees of h_0 and h_1 should be greater than 1. Computational evidence suggests that degree 2 should be enough to construct all finite fields with k up to $q + 2$, however this remains heuristic.

The main goal of the present article is to improve Theorem 2 in the case where the maximum of the degrees of h_0 and h_1 is exactly 2. For this, we present a slightly modified ZigZag descent in Section 3 and provide a new, simpler and tighter analysis of a core subroutine of the discrete logarithm computation in Section 4.

Putting the two contributions together, we derive the theorem:

Theorem 3. *Assume that we are given either a prime power $q \geq 13$ and an integer $k_0 \geq 6$ or a prime power $q \geq 149$ and an integer $k_0 \geq 5$. Then, given two coprime polynomials $h_0, h_1 \in \mathbb{F}_{q^{k_0}}[X]$ of maximum degree two and an irreducible degree k factor I of $h_1X^q - h_0$, the discrete logarithm problem in $\mathbb{F}^*_{q^{k_0k}}$ where $\mathbb{F}^*_{q^{kk_0}} \cong \mathbb{F}_{q^{k_0}}[X]/(I)$ can be solved within*

$$O\left(q^{4+k_0}\,(q+3)^{\lceil \log_2 k \rceil} + q^{3k_0}\right)$$

expected arithmetic operations in $\mathbb{F}_{q^{kk_0}}$ and $\mathbb{Z}/(q^{kk_0} - 1)\mathbb{Z}$.

The constant implied by the $O()$ notation in the running time is an absolute constant independent of q, k_0 and k.

3. A modified ZigZag strategy

Our goal is to compute discrete logarithms in the multiplicative group of the finite field $\mathbb{F}_{q^{k_0k}}$, with $k_0 \geq 5$ and q a prime power. We let Q_0 denote q^{k_0}. For this, we are given as input a multiplicative generator $\mathfrak{g}$ of the group $\mathbb{F}^*_{q^{k_0k}}$ and an element $\mathfrak{h}$ in the group. The goal is to find an integer x (unique modulo ${Q_0}^k - 1$) such that $\mathfrak{h} = \mathfrak{g}^x$.

As in the preliminaries, we are given two polynomials h_0 and h_1 with coefficients in $\mathbb{F}_{Q_0}$ and $\max(\deg h_0, \deg h_1) = 2$ (to avoid the special cases) and an irreducible factor I_k of degree k of $h_1X^q - h_0$ in $\mathbb{F}_{Q_0}[X]$. We represent $\mathbb{F}_{q^{k_0k}}$ as $\mathbb{F}_{Q_0}[X]/(I_k)$. Note that, even if $\mathfrak{g}$ and $\mathfrak{h}$ are initially given in a different representation of $\mathbb{F}_{q^{kk_0}}$, it is easy to rewrite them in the representation $\mathbb{F}_{Q_0}[\theta]$. Indeed, if the initial representation is given by another irreducible polynomial J_k, it suffices to find a root of J_k in our representation to re-express $\mathfrak{g}$ and $\mathfrak{h}$.

In this setting, we rephrase and modify the strategy of [2] to compute discrete logarithms with a rigorous probabilistic algorithm. The goal, following an essential algorithmic

ingredient from [1] to achieve a provable algorithm, rather than a heuristic one, is to write many equations of the form:

$$\mathfrak{g}^r\mathfrak{h}^s = \Lambda \cdot h_1(\theta)^{E_{H_1}} \cdot \prod_{c\in\mathcal{E}\cup\mathbb{F}_{Q_0}} (\theta - c)^{E_c}, \tag{1}$$

where r and s are randomly chosen integers modulo $Q_0^k - 1$ and Λ is in $\mathbb{F}_{Q_0}$. The product ranges over the union of $\mathbb{F}_{Q_0}$ and a set of exceptional values $\mathcal{E}$, which contains the roots in $\bar{\mathbb{F}}_q$ of the two polynomials $h_1(X)X^q - h_0(X)$ and

$$h_1(X)^2 \left(h_1^\pi(h_0(X)/h_1(X))X^{q^2} - h_0^\pi(h_0(X)/h_1(X))\right).$$

Here h_0^π (resp. h_1^π) denotes the polynomial whose coefficients are those of h_0 (resp. h_1) raised to the power q. In other words, $h_0^\pi(X)$ is obtained by formally computing $h_0(X^{1/q})^q$ and similarly for $h_1^\pi(X)$. The factor $h_1(X)^2$ is there to clear the denominator and the complete polynomial has degree at most q^2+4. Thus, the total cardinality of the product set, counting $\mathcal{E}$, Q_0 and h_1 is at most $Q_0 + q^2 + q + 7$.

The main computational task is to determine the vector of exponents E. In order to do that, [2] introduced the Zig-Zag method. The idea is to first write $\mathfrak{g}^r\mathfrak{h}^s$ as a product of elements of the form $\theta - C$ with C in the union of a larger field and $\mathcal{E}$. From this point, each $\theta - C$ is rewritten as products of the same form in progressively smaller fields. The basic building block called degree 2 elimination, takes an element $\theta - C$ with C in $\mathbb{F}_{Q^2}$ and rewrites it as a product of $\theta - \tilde{C}$ with all the $\tilde{C}$ in $\mathcal{E}\cup\mathbb{F}_Q$, possibly with some power of h_1 thrown in. Here, Q is of the form $Q_0^{2^i}$ for some not too large integer i.

Thus, in our formulation, the Zig-Zag method makes use of a tower of quadratic extensions above $\mathbb{F}_{Q_0}$, all the way up to $\mathbb{F}_{Q_0^{2^\ell}}$, where ℓ is the smallest integer such that $2^\ell > k$.

Initial decomposition over $\mathbb{F}_{{Q_0}^{2^\ell}}$. We first pick r and s uniformly at random in $[0\cdots {Q_0}^k - 1]$ and compute $R = \mathfrak{g}^r\mathfrak{h}^s$ which is distributed uniformly at random in $\mathbb{F}^*_{{Q_0}^k}$. We now write $R = \mathcal{R}(\theta)$, picking for $\mathcal{R}$ a polynomial of degree 2^ℓ. This can be done using linear algebra, by considering all the linear dependencies over $\mathbb{F}_q$ of the elements 1, θ, θ^2, …, θ^{2^ℓ} and R and picking a random one that involves both R and θ^{2^ℓ}. After this process, $\mathcal{R}$ is a uniformly random polynomial of degree 2^ℓ in $\mathbb{F}_{Q_0}[X]$. As a consequence, it is irreducible with probability close to $2^{-\ell}$. If it is not, we restart the process. If it is irreducible, we know $\mathcal{R}$ splits over $\mathbb{F}_{{Q_0}^{2^\ell}}$ and we can write $\mathcal{R}(X) = \Lambda\prod_{i=0}^{2^\ell-1}(X - \gamma^{{Q_0}^i})$ where γ is a root of $\mathcal{R}$ in $\mathbb{F}_{{Q_0}^{2^\ell}}$ and Λ is in $\mathbb{F}_{Q_0}$. As a consequence, we have written

$$\mathfrak{g}^r\mathfrak{h}^s = \Lambda \prod_{i=0}^{2^\ell-1} (\theta - \gamma^{{Q_0}^i}),$$

thus in the desired form.

From $\mathbb{F}_{Q_0^{2^{v+1}}}$ down to $\mathbb{F}_{Q_0^{2^v}}$. We proceed by descending induction on v. Assume that we have already rewritten $\mathfrak{g}^r\mathfrak{h}^s$ as a product:

$$\Lambda \cdot h_1(\theta)^{e_{h_1}} \prod_{i=0}^{N_{v+1}-1} (\theta - C_i^{(v+1)})^{e_i},$$

where all $C_i^{(v+1)}$ belong to $\mathcal{E}\cup\mathbb{F}_{Q_0^{2^{v+1}}}$. Assume moreover that we have some invariance by Frobenius, precisely that whenever $\theta - C_i^{(v+1)}$ appears in the product, then $\theta - \left(C_i^{(v+1)}\right)^{Q_0}$ also appears and that furthermore the multiplicities of the two are the same. This property

is clear for the initial decomposition and is preserved throughout the process that we now describe.

Consider one term $\theta - C_i^{(v+1)}$ in the decomposition. Due to the above property, we see that $\theta - \left(C_i^{(v+1)}\right)^{Q_0^{2^v}}$ also appears (with the same multiplicity). Since the notation $\left(C_i^{(v+1)}\right)^{Q_0^{2^v}}$ is extremely cumbersome, we replace in the rest of the present section all occurences of $C_i^{(v+1)}$ by C_i for the sake of readability.

If $C_i = {C_i}^{Q_0^{2^v}}$, the term $\theta - C_i$ is already in $\mathbb{F}_{Q_0^{2^v}}$ and nothing needs to be done. If C_i belongs to $\mathcal{E}$, then it is also the case for ${C_i}^{Q_0^{2^v}}$ and nothing needs to be done either.

Otherwise, we can compute:

$$(\theta - C_i) \cdot \left(\theta - {C_i}^{{Q_0}^{2^v}}\right) = \theta^2 + \lambda_1\,\theta + \lambda_0,$$

where λ_0 and λ_1 are coefficients in $\mathbb{F}_{{Q_0}^{2^v}}$. From this point, the process of degree 2 elimination, which is detailed in Section 4 rewrites this quadratic polynomial as a product of linear terms in θ over $\mathbb{F}_{{Q_0}^{2^v}}$ with positive or negative exponents and possibly an extra power of $h_1(\theta)$. Thus, we obtain the following rewriting:

$$(\theta - C_i) \cdot \left(\theta - {C_i}^{{Q_0}^{2^v}}\right) = \Lambda_i \cdot h_1(\theta)^{\tilde{e}_{h_1}} \prod_j (\theta - \tilde{C}_j)^{\tilde{e}_j}.$$

Additionally, this rewriting satisfies:

$$\left(\theta - {C_i}^{Q_0}\right) \cdot \left(\theta - {C_i}^{{Q_0}^{2^v+1}}\right) = \Lambda_i^{Q_0} h_1(\theta)^{Q_0 \tilde{e}_{h_1}} \prod_j (\theta - \tilde{C}_j^{Q_0})^{\tilde{e}_j}.$$

As a consequence, it suffices to perform degree 2 elimination on one pair of conjugates C_i and ${C_i}^{Q_0^{2^v}}$ and copy the relation for all other Frobenius conjugates. With this consistent choice for the relations we are using, the induction hypothesis is preserved throughout the process.

Finalizing the discrete logarithm computation. After repeating the procedure all the way down to $\mathbb{F}_{Q_0}$, the total number of distinct elements possibly appearing in the right-hand side is (at most) $Q_0 + q^2 + q + 7$. Assume that we have written down $Q_0 + q^2 + q + 8$ such equations. Following [1], we can find a non-zero element in the kernel of the (row-)matrix of exponents modulo $Q_0^k - 1$, which is non-trivial thanks to a dimension argument. Taking the product corresponding to this kernel elements yields a random relation $\mathfrak{g}^R \mathfrak{h}^S = 1$ and thus the discrete logarithm of $\mathfrak{h}$ with probability $\phi(n)/n$, where $n = (Q_0^k - 1)$.

In extreme cases, $\phi(n)/n$ might become very small, thus degrading the performance of the algorithm. To avoid this issue, it is best to follow standard practice and to separate the computation of the discrete logarithm in two parts. First, compute the logarithm modulo small primes dividing n using exhaustive search or a square-root time algorithm. Then, use the above random relation to account for the remainder and paste everything together using Pohlig-Hellman technique [4].

To optimize efficiency, we consider prime factors of n below $M = \log n$ as small and the others as large. With this choice, the small part computation takes polynomial time and can be neglected. For the relation part the probability of success becomes:

$$\prod_{\substack{p \mid Q_0^k - 1 \\ p > \log n}} \frac{p-1}{p} \geq 1 - \sum_{\substack{p \mid Q_0^k - 1 \\ p > \log n}} \frac{1}{p} \geq 1 - \frac{1}{\log\log n}.$$

Indeed, there are at most $\log n / \log\log n$ such prime divisors of n.

The computation of the relation part costs $O(Q_0^3)$ arithmetic operations modulo a product of primes smaller than $Q_0^k - 1$.

4. Degree 2 elimination revisited

To make the strategy presented in Section 3 complete, we need to describe the degree 2 elimination process, that finds a relation between a single irreducible polynomial of degree 2 over some extension of $\mathbb{F}_{Q_0}$ and many linear polynomials.

In order to do that it suffices, given an irreducible polynomial f of degree 2 over $\mathbb{F}_Q[X]$, to find two linear polynomials $a_0 + a_1X$ and $b_0 + b_1X$ such that f divides:

$$F = (a_0 + a_1X)\,(b_0^q\, h_1(X) + b_1^q\, h_0(X)) - (b_0 + b_1X)\,(a_0^q\, h_1(X) + a_1^q\, h_0(X))$$

and F is not the zero polynomial.

Indeed, if f divides F, depending on the degree of F, we can write either $F = \lambda f$ or $F = \lambda(X+c)f$ for some constant c in $\mathbb{F}_Q$. As a consequence, evaluating at θ, we find that:

$$\begin{aligned}\lambda f(\theta)[\theta + c] &= h_1(\theta)\,[(a_0 + a_1\theta)(b_0^q + b_1^q\theta^q) - (b_0 + b_1\theta)(a_0^q + a_1^q\theta^q)] \\ &= h_1(\theta)(b_0 + b_1\theta) \prod_{\alpha\in\mathbb{F}_q} ((a_0 + a_1\theta) - \alpha(b_0 + b_1\theta))\,,\end{aligned}$$

where $[\theta + c]$ is omitted if F has degree 2. Factoring out the leading coefficient of each factor, this replaces f by a product of the desired form containing at most $q + 3$ terms.

Since f is irreducible, we can define a quadratic extension $\mathbb{F}_{Q^2}$ of $\mathbb{F}_Q$ by adjoining a root γ of f. The condition that f divides F can then be rewritten as $F(\gamma) = 0$. As f comes from the descent process of the discrete logarithm computation we know that $f \neq h_0$ and $f \neq h_1$. As a consequence, $h_0(\gamma) \neq 0$ and $h_1(\gamma) \neq 0$. Divide by $h_1(\gamma)$ and let $\gamma' = h_0(\gamma)/h_1(\gamma)$. We now want to solve the equation:

$$(a_0 + a_1\gamma)(b_0^q + b_1^q\gamma') - (b_0 + b_1\gamma)(a_0^q + a_1^q\gamma') = 0, \tag{2}$$

under the condition $F \neq 0$. We now show that $\gamma^q \neq \gamma'$ and $\gamma^{qQ} \neq \gamma'$. Indeed, if $\gamma^q = h_0(\gamma)/h_1(\gamma)$, then γ is a root of $h_1(X)X^q - h_0(X)$. Furthermore, if $\gamma^{qQ} = h_0(\gamma)/h_1(\gamma)$, we also have $\gamma^q = h_0(\gamma^Q)/h_1(\gamma^Q)$. This implies that:

$$\gamma^{q^2} = \frac{h_0^\pi(h_0(\gamma)/h_1(\gamma))}{h_1^\pi(h_0(\gamma)/h_1(\gamma))}$$

and that γ is a root of

$$h_1(X)^2 \left(h_1^\pi(h_0(X)/h_1(X))X^{q^2} - h_0^\pi(h_0(X)/h_1(X))\right).$$

In both cases, γ is in $\mathcal{E}$ and we excluded these values during the descent process described in Section 3.

We describe in Section 5 a process to find a quadruple (a_0, a_1, b_0, b_1) in expected $O(q^4)$ arithmetic operations. Since each rewriting creates at most $q + 3$ new factors, the total number of calls to the process for a given $\mathfrak{g}^r\mathfrak{h}^s$ is at most $(q + 3)^{\lceil \log_2 k\rceil}$. Since we need $O(Q_0)$ relations, the total cost is $O((q + 3)^{\lceil \log_2 k\rceil} q^{4+k_0})$ arithmetic operations.

4.1. The condition $F \neq 0$.

When $(a_0, a_1) = (0, 0)$ or $(b_0, b_1) = (\epsilon a_0, \epsilon a_1)$ with $\epsilon \in \mathbb{F}_q$, we see that $F = 0$. The following lemma states that the converse is also true.

Lemma 4. *Let q be a prime power and $\mathbb{F}_Q$ an extension field of $\mathbb{F}_q$. Let h_0 and h_1 be two coprime polynomials in $\mathbb{F}_q[X]$ such that* $\max(\deg(h_0), \deg(h_1)) = 2$. *Then, for any quadruple (a_0, a_1, b_0, b_1) in $\mathbb{F}_Q^4$, the polynomial:*

$$F = (a_0 + a_1X)\,(b_0^q\, h_1(X) + b_1^q\, h_0(X)) - (b_0 + b_1X)\,(a_0^q\, h_1(X) + a_1^q\, h_0(X))$$

is equal to zero, if and only if:

- $(a_0, a_1) = (0, 0)$ *or*

- *there exists* $\epsilon \in \mathbb{F}_q$ *such that* $(b_0, b_1) = (\epsilon a_0, \epsilon a_1)$.

Proof. We just need to prove the forward direction. Since $F = 0$ is equivalent to:

$$(a_0 + a_1 X)\,(b_0^q\, h_1(X) + b_1^q\, h_0(X)) = (b_0 + b_1 X)\,(a_0^q\, h_1(X) + a_1^q\, h_0(X))\,,$$

it is interesting to study the factorization of polynomials on each side of the equality. When the degree of $a_0^q\, h_1(X) + a_1^q\, h_0(X)$ is 2, we see that $a_0^q\, h_1(X) + a_1^q\, h_0(X)$ and $b_0^q\, h_1(X) + b_1^q\, h_0(X)$ must share some non-trivial common factor $\ell(X)$. By symmetry, this also holds when the degree of $b_0^q\, h_1(X) + b_1^q\, h_0(X)$ is 2.

Any common factor of $a_0^q\, h_1(X)+a_1^q\, h_0(X)$ and $b_0^q\, h_1(X)+b_1^q\, h_0(X)$ also divides arbitrary linear combinations of the two. As a consequence, if the matrix

$$\begin{pmatrix} a_0^q & a_1^q \\ b_0^q & b_1^q \end{pmatrix}$$

is invertible, we see that $\ell(X)$ divides both h_0 and h_1. This is impossible since h_0 and h_1 where chosen coprime. As a consequence, the matrix has a determinant equal to zero, which implies $a_0 b_1 = a_1 b_0$.

Similarly, if the degrees of both $a_0^q\, h_1(X) + a_1^q\, h_0(X)$ and $b_0^q\, h_1(X) + b_1^q\, h_0(X)$ are at most one, we have:

$$\begin{aligned} a_0^q\, h_1^{(2)} + a_1^q\, h_0^{(2)} &= 0 \quad \text{and} \\ b_0^q\, h_1^{(2)} + b_1^q\, h_0^{(2)} &= 0, \end{aligned}$$

where $h_0^{(2)}$ and $h_1^{(2)}$ are the coefficients of x^2 in h_0 and h_1. Since at least one of h_0 and h_1 is chosen to have degree 2, the pair $(h_0^{(2)}, h_1^{(2)})$ is non-zero. This means that two equations are linearly dependent, which again implies $a_0 b_1 = a_1 b_0$.

From the relation $a_0 b_1 = a_1 b_0$, we know that either $(a_0, a_1) = (0, 0)$ or there exists an element $\epsilon \in \mathbb{F}_Q$ such that $b_0 = \epsilon a_0$ and $b_1 = \epsilon a_1$. Substituting back in F, we find that:

$$(a_0 + a_1 X)\,(a_0^q\, h_1(X) + a_1^q\, h_0(X))\,(\epsilon^q - \epsilon) = 0.$$

Since $(a_0, a_1) \neq (0, 0)$, the polynomial on the left cannot be zero. Thus $\epsilon^q - \epsilon = 0$ and $\epsilon \in \mathbb{F}_q$. □

5. Existence of solutions to Equation (2)

In this section, we study a slightly larger class of equations and determine when they do have solutions. More precisely, we prove the following theorem:

Theorem 5. *Given an extension* $\mathbb{F}_Q$ *of* $\mathbb{F}_q$ *such that either* $Q \geq q^6$ *and* $q \geq 13$ *or* $Q \geq q^5$ *and* $q \geq 149$ *and two arbitrary elements* U *and* V *in* $\mathbb{F}_{Q^2} \setminus \mathbb{F}_Q$*, with* $U \neq V$ *and* $U \neq V^Q$*, there exists a non-trivial solution to the equation*

$$(x^q U^q + y^q)(zV + t) - (xV + y)(z^q U^q + t^q) = 0,$$

with $(x, y, z, t) \in \mathbb{F}_Q^4$*. In this context, non-trivial means that* $(x, y) \neq (0, 0)$ *and that* $(z, t) \neq (\epsilon x, \epsilon y)$ *for any* $\epsilon \in \mathbb{F}_q$*.*

Furthermore, such a solution of the above equation can be computed in $O(q^4)$ *arithmetic operations in* $\mathbb{F}_Q$*.*

To conclude, we apply this theorem with $V = \gamma$ and U the only solution of $U^q = \gamma'$. Since $\gamma^q \neq \gamma'$ and $\gamma^{qQ} \neq \gamma'$, the conditions $U \neq V$ and $U \neq V^Q$ are satisfied.

Proof. Since neither $xV + y$ nor $zV + t$ can be zero for a non-trivial solution, the equation can be rewritten as:

$$\frac{(xU + y)^q}{xV + y} = \frac{(zU + t)^q}{zV + t}.$$

In other words, we want to find a value $\lambda_1 \in \mathbb{F}_{Q^2}$ such that:

$$(xU+y)^q = \lambda_1(xV+y) \quad \text{and} \quad (zU+t)^q = \lambda_1(zV+t).$$

We remark that for any non zero solution (x_0, y_0) to the equation $(xU+y)^q = \lambda_1(xV+y)$ and for all $\epsilon \in \mathbb{F}_q$, the pair $(\epsilon x_0, \epsilon y_0)$ is also a solution of the same equation. The sum of two solutions is also a solution. In fact, we can see that for any λ_1 the set of solutions is a vector space over $\mathbb{F}_q$. As a consequence, the non-triviality condition means that we are searching for a $\lambda_1 \in \mathbb{F}_{Q^2}$ such that the equation:

$$(xU+y)^q = \lambda_1(xV+y) \tag{3}$$

has a set of solutions with dimension > 1 as an $\mathbb{F}_q$ vector space. In particular, the equation has more than q distincts solution pairs in $\mathbb{F}_Q^2$. Note that λ_1 cannot be 0 since U doesn't belong to $\mathbb{F}_Q$.

We now convert this equation from a bivariate equation with solutions in $\mathbb{F}_Q$ to a univariate equation in $\mathbb{F}_{Q^2}$. This transformation, which preserves the fact that the set of solutions is an $\mathbb{F}_q$–vector space and leaves its dimension unchanged, is done by setting

$$X = xU + y.$$

This implies,

$$X^Q = xU^Q + y \quad \text{and} \quad X - X^Q = x(U - U^Q)$$

or equivalently

$$x = \frac{X - X^Q}{U - U^Q}.$$

Note that $U - U^Q \neq 0$, otherwise we would have $U \in \mathbb{F}_Q$ which does not correspond to our choice of U. Similarly,

$$y = X - xU = X - \frac{X - X^Q}{U - U^Q}U$$

and Equation (3) becomes:

$$\frac{X^q}{\lambda_1} = W(X - X^Q) + X, \tag{4}$$

with $W = \frac{V-U}{U-U^Q}$.

Note: The condition $U \neq V$ in the Theorem is equivalent to $W \neq 0$ and the condition $U \neq V^Q$ to $W \neq -1$.

Given two X and Y non-zero solutions of Equation (4) with X/Y not in $\mathbb{F}_q$, we have:

$$(W(X - X^Q) + X)Y^q = (W(Y - Y^Q) + Y)X^q,$$

indeed both sides are equal to $(XY)^q/\lambda_1$. Equivalently (since $W \neq 0$):

$$\frac{1}{W} = \frac{(Y - Y^Q)X^q - (X - X^Q)Y^q}{XY^q - YX^q}. \tag{5}$$

Conversely, if X and Y are non-zero elements with X/Y not in $\mathbb{F}_q$ such that (X, Y) is a solution of Equation (5), we can go backward and find a λ_1 such that Equation (3) has more than q solutions.

Writing $Y = ZX$ for Z in $\mathbb{F}_{Q^2} \setminus \mathbb{F}_q$, this becomes:

$$\begin{aligned} \frac{1}{W} &= \frac{(Z - Z^q)X^{q+1} - (Z^Q - Z^q)X^{Q+q}}{X^{q+1}(Z^q - Z)} \\ &= -1 + X^{Q-1}\frac{Z^Q - Z^q}{Z - Z^q}. \end{aligned}$$

Letting:

$$\Lambda_X = \frac{W+1}{W \cdot X^{Q-1}},$$

we want to find X such that the equation:

$$Z^Q + (\Lambda_X - 1)Z^q - \Lambda_X Z = 0$$

has more than q solutions in $\mathbb{F}_{Q^2}$. We remark that it always has the elements of $\mathbb{F}_q$ as solutions.

For Z in $\mathbb{F}_{Q^2} \setminus \mathbb{F}_q$, this is equivalent to:

$$\frac{Z^Q - Z^q}{Z - Z^q} = \Lambda_X, \tag{6}$$

which implies:

$$\left(\frac{Z^Q - Z^q}{Z - Z^q}\right)^{Q+1} = \left(\frac{W+1}{W}\right)^{Q+1}. \tag{7}$$

This equation is independent of X. Its right-hand side is the norm of $(W+1)/W$ down to $\mathbb{F}_Q$ and it cannot be 0 because $W \neq -1$. Conversely, for any root Z of this equation, we can find X such that (6) is satisfied.

Since $((W+1)/W)^{Q+1}$ belongs to $\mathbb{F}_Q^*$, we can use the following lemma to conclude that Equation (7) has roots in $\mathbb{F}_{Q^2} \setminus \mathbb{F}_q$. □

Lemma 6. *Assume that :*

- *either q is a prime power ≥ 13 and that $Q = q^d$ with $d \geq 6$;*
- *or q is a prime power ≥ 149 and that $Q = q^d$ with $d \geq 5$.*

Then, for any $a \in \mathbb{F}_Q^*$, the equation

$$\left(\frac{X^q - X^Q}{X^q - X}\right)^{Q+1} = a$$

has a solution $X \in \mathbb{F}_{Q^2} \setminus \mathbb{F}_q$.

Furthermore, it can be computed in $O(q^4)$ arithmetic operations in $\mathbb{F}_Q$.

Proof. The case $a = 1$ is easy. Indeed, for any X is in $\mathbb{F}_Q \setminus \mathbb{F}_q$, we have $(X^q - X^Q)/(X^q - X) = 1$. Moreover such an X cannot be a solution of the equation for any $a \neq 1$.

To deal with the other cases, we want to show for any $a \in \mathbb{F}_Q \setminus \{0, 1\}$, the equation

$$\left(\frac{X^q - X^Q}{X^q - X}\right)^{Q+1} = a \tag{8}$$

has a solution $X \in \mathbb{F}_{Q^2} \setminus \mathbb{F}_Q$ (for $X \in \mathbb{F}_Q \setminus \mathbb{F}_q$ it is equal to 1).

Since we look for solutions in $\mathbb{F}_{Q^2} \setminus \mathbb{F}_Q$, we have $X^{Q^2} = X$. As a consequence, Equation (8) implies:

$$(X^q - X^Q)(X^{qQ} - X) - a(X^q - X)(X^{qQ} - X^Q) = 0. \tag{9}$$

Conversely, any solution in $\mathbb{F}_{Q^2} \setminus \mathbb{F}_Q$ of this new equality is also a solution of the original one. Note that all elements of $\mathbb{F}_q$ are parasitical solutions of Equation (9) for all values of a.

We now let $X_1 = X$ and $X_2 = X^Q$, and rewrite the equation as:

$$(X_1^q - X_2)(X_2^q - X_1) - a(X_1^q - X_1)(X_2^q - X_2) = 0.$$

This equation describes a curve over $\mathbb{F}_Q$, let's call it $\mathcal{C}_1$.

As we show below, the polynomial defining $\mathcal{C}_1$ is absolutely irreducible, i.e., the curve $\mathcal{C}_1$ is irreducible.

Additionally, since the equation of $\mathcal{C}_1$ is symmetric, it can be completely expressed using the elementary symmetric polynomials[1] $T = X_1 + X_2$ and $N = X_1 \cdot X_2$. Moreover, writing

[1]The names T and N are chosen to remind that when X is a solution of the original equation in $\mathbb{F}_{Q^2} \setminus \mathbb{F}_Q$ the two respectively become the trace and norm of X down to $\mathbb{F}_Q$.

the symmetrized expression $S(T,N)$ shows that it has total degree $d = q+1$. We call $\mathcal{C}_2$ the curve defined over $\mathbb{F}_Q$ by $S(T,N) = 0$. It is irreducible, otherwise substituting T and N by their expression in terms of X_1 and X_2 in a factor of $S(T,N)$ would imply that $\mathcal{C}_1$ isn't irreducible either.

Let's consider a point (t,n) of $\mathcal{C}_2$ and denote by (x_1,x_2) the two roots of $X^2 - t\,X + n$ in $\mathbb{F}_{Q^2}$. We have two distincts possibilities, either x_1 and x_2 are both in $\mathbb{F}_Q$ or they are both in $\mathbb{F}_{Q^2} \setminus \mathbb{F}_Q$. In the latter case, they are conjuguate roots, thus $x_2 = x_1^Q$ and x_1 is a solution of Equation (8). In the former case, (x_1,x_2) and (x_2,x_1) are (possibly equal) points of $\mathcal{C}_1$.

Thus, to conclude about roots of Equation (8), it suffices to prove that there exist points (t,n) of $\mathcal{C}_2$ belonging to the latter case and that they are easy to compute. We first show that there exist many such points by the following counting argument:

- Let N_1 denote the number of points of $\mathcal{C}_1$, including its two points at infinity $(1:0:0)$ and $(0:1:0)$. Note that there are exactly q points (x_1,x_2) of $\mathcal{C}_1$ with $x_1 = x_2$. Precisely, the points (x_1,x_1) with x_1 in $\mathbb{F}_q$. For any other point (x_1,x_2), we see that (x_2,x_1) is a distinct point of $\mathcal{C}_1$.
- Let N_2 denote the number of points of $\mathcal{C}_2$, including its point at infinity $(1:0:0)$.
- Consider the image of $\mathcal{C}_1$ in $\mathcal{C}_2$ by the map that sends (x_1,x_2) to $(x_1+x_2, x_1\,x_2)$ and any point at infinity to the point at infinity. Since (x_1,x_2) and (x_2,x_1) are mapped to the same value, the image has size $(N_1+q)/2$ due to the q points of the form (x_1,x_1).
- As a consequence, the number of points (t,n) of $\mathcal{C}_2$ with $X^2 - t\,X + n$ irreducible in $\mathbb{F}_{Q^2}$:
$$N_{\text{good}} = (2\,N_2 - N_1 - q)/2.$$

In order to give a lower bound on this number, it suffices to provide a lower bound on N_2 and an upper bound on N_1. Thanks to the Hasse-Weil bound, we know that:

$$\begin{aligned} N_1 &\leq Q + 1 + 2g_1\sqrt{Q} \quad \text{and} \\ N_2 &\geq Q + 1 - 2g_2\sqrt{Q}, \end{aligned}$$

where g_1 (resp. g_2) is the genus of $\mathcal{C}_1$ (resp. $\mathcal{C}_2$). Since the equation of $\mathcal{C}_1$ has degree $2q$ and the equation of $\mathcal{C}_2$ has degree $q+1$, the genus–degree formula states that:

$$\begin{aligned} g_1 &\leq (2q-1)(2q-2)/2 \leq 2q^2 \quad \text{and} \\ g_2 &\leq q(q-1)/2 \leq q^2/2. \end{aligned}$$

As a consequence:

$$N_{\text{good}} \geq (Q+1-q)/2 - (5/2)\,q^2\sqrt{Q}.$$

We would like to have $N_{\text{good}} \geq Q/4$. To achieve that it is sufficient to have:

$$Q/4 \geq 3q^2\sqrt{Q} \quad \text{i.e.} \quad Q \geq (12)^2\,q^4.$$

Under the assumption $Q \geq q^6$, it thus suffices to have $q \geq 13$. Alternatively, under the assumption $Q \geq q^5$, it suffices to have $q \geq 149$. Note that $13 = 12+1$ is a prime and that 149 is the smallest prime above $(12)^2$.

Computing a good point on $\mathcal{C}_2$. Since there are more than $Q/4$ points and since the partial degree in N of the equation $S(T,N)$ is q, there are at least $Q/4q$ distinct values of T in $\mathbb{F}_Q$ that correspond to a good point. This gives us the following procedure:

- Pick a random t in $\mathbb{F}_Q$, then a random root n of $S(t,N) = 0$ (if any, otherwise restart). This gives a good point with probability at least $1/4q^2$.
- Check that $X^2 - tX + n$ is irreducible in $\mathbb{F}_Q$. If it is, any root in $\mathbb{F}_{Q^2}$ yields a solution of Equation (8). Otherwise, restart the random picking.

Thus, the computation costs $O(q^2)$ factorization of degree q polynomials of $\mathbb{F}_Q[X]$, which is less that $O(q^4)$ arithmetic operations in $\mathbb{F}_Q$.

Absolute irreducibility. Changing the sign of the equation of $\mathcal{C}_1$ and expanding as a polynomial in X_1 with coefficients in $\mathbb{F}_Q[X_2]$, we obtain:

$$f(X_1, X_2) = X_1^{q+1} + ((a-1)X_2^q - aX_2)\, X_1^q + ((a-1)X_2 - aX_2^q)\, X_1 + X_2^{q+1}.$$

By contradiction, assume that, in the algebraic closure of $\mathbb{F}_q$, we have $f = F_1\, F_2$ where F_1 and F_2 have respective degrees d_1 and d_2 in X_1, with $d_1+d_2 = q+1$. Possibly permuting the roles of F_1 and F_2, we may also assume that $d_1 \leq d_2$. Evaluating at $X_2 = 0$, we find that: $X_1^{q+1} = F_1(X_1, 0) \cdot F_2(X_1, 0)$. As a consequence, there exists an element λ of $\bar{\mathbb{F}_q}^*$, such that $F_1(X_1, 0) = \lambda\, X_1^{d_1}$ and $F_2(X_1, 0) = \lambda^{-1}\, X_1^{d_2}$. Multiplying F_1 by λ^{-1}, F_2 by λ and renaming the polynomials, we have:

$$\begin{aligned} F_1 &= X_1^{d_1} + X_2\, G_1(X_1, X_2) \quad \text{and} \\ F_2 &= X_1^{d_2} + X_2\, G_2(X_1, X_2). \end{aligned}$$

Considering the identity $f = F_1\, F_2$ modulo X_2^2 we find that:

$$X_1^{q+1} - aX_2X_1^q + (a-1)X_2X_1 = X_1^{q+1} + X_2X_1^{d_1}G_2(X_1, 0) + X_2X_1^{d_2}G_1(X_1, 0).$$

When $a \neq 1$, in order to recover the monomial X_1X_2, it is necessary that $d_1 = 1$, since by assumption it is the smaller of the two degrees. Moreover, $G_2(X_1, 0) = (a-1)$.

Since $d_1 = 1$, we can rewrite $F_1 = X_1 - H(X_2)$, with $H \neq 0$ since X_1 doesn't divide f. Recall that the fact that F_1 divides f when F_1 has this special form is equivalent to $f(H(X_2), X_2) = 0$. Now, let λX_2^n with $\lambda \neq 0$ be the lowest degree monomial of H and consider $f(H(X_2), X_2) \pmod{X_2^{n+2}}$. We see that:

$$\begin{aligned} f(H(X_2), X_2) &\equiv \lambda^{q+1}X_2^{(q+1)n} + ((a-1)X_2^q - aX_2)\, \lambda^q X_2^{qn} + \\ &\quad ((a-1)X_2 - aX_2^q)\, \lambda X_2^n + X_2^{q+1} \pmod{X_2^{n+2}} \\ &\equiv \lambda(a-1)X_2^{n+1} + X_2^{q+1} \pmod{X_2^{n+2}} \end{aligned}$$

Since $a \neq 1$ and $\lambda \neq 0$ this can only vanish when $n = q$. In that case, due to the fact that the total degree of f is $2q$, we necessarily have $F_1 = X_1 - \lambda X_2^q$. To conclude, returning to the initial form of f, before expanding in X_1, we compute:

$$f(\lambda X_2^q, X_2) = -(\lambda^q X_2^{q^2} - X_2)(1-\lambda)X_2^q + a(\lambda^q X_2^{q^2} - \lambda X_2^q)(X_2^q - X_2).$$

This is non-zero unless $a = 0$ (and $\lambda = 1$).

As consequence, when a is neither 0 nor 1, the curve $\mathcal{C}_1$ is irreducible.

Shape of S. The polynomial S is of the form:

$$S(T, N) = (1-a)(N^q + N) - \sum_{i=0}^{\lfloor (q+1)/2 \rfloor} \gamma_i T^{q+1-2i} N^i.$$

Indeed, by inspection, the equation of $\mathcal{C}_1$ can be rewritten as:

$$(1-a)\,((X_1X_2)^q + X_1X_2) - (X_1^{q+1} + X_2^{q+1}) - a(X_1X_2)(X_1^{q-1} + X_2^{q-1}).$$

It suffices to replace X_1X_2 by N and the two sums of powers by their symmetrized expressions to conclude. □

Acknowledgments

This work has been supported in part by the European Union's H2020 Programme under grant agreement number ERC-669891. It has also been supported by GAČR Grant 18-19087S-301-13/201843.

We would like to thank an anonymous reviewer for pointing out an improvement of the constants in Lemma 6.

References

[1] Leonard M. Adleman and Jonathan DeMarrais. A subexponential algorithm for discrete logarithms over all finite fields. *Mathematics of Computation*, 61(203):1–15, 1993.

[2] Robert Granger, Thorsten Kleinjung, and Jens Zumbrägel. On the discrete logarithm problem in finite fields of fixed characteristic. Cryptology ePrint Archive, Report 2015/685, 2015.

[3] Antoine Joux and Cécile Pierrot. Improving the polynomial time precomputation of Frobenius representation discrete logarithm algorithms. In *Advances in Cryptology: ASIACRYPT'2014*, pages 378–397, 2014.

[4] Stephen C. Pohlig and Martin E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (corresp.). *IEEE Transactions on Information Theory*, 24(1):106–110, 1978.

Email address: farukgologlu@gmail.com

Charles University in Prague

Email address: Antoine.Joux@m4x.org

Chaire de Cryptologie de la Fondation SU, Sorbonne Université, Institut de Mathématiques de Jussieu–Paris Rive Gauche, CNRS, INRIA, Univ Paris Diderot. Campus Pierre et Marie Curie, F-75005 Paris, France