Factor Base Discrete Logarithms in Kummer Extensions

Dianyan Xiao[1]*, Jincheng Zhuang[2,3] **, and Qi Cheng[4]***

[1] Institute for Advanced Study,
Tsinghua University, Beijing, China
[2] State Key Laboratory of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
[3] State Key Laboratory of Mathematical Engineering and Advanced Computing
Wuxi, China
[4] School of Computer Science,
University of Oklahoma, Norman, OK, USA

Abstract. The discrete logarithm over finite fields of small characteristic can be solved much more efficiently than previously thought. This algorithmic breakthrough is based on heuristic polynomial time algorithms to compute the factor base discrete logarithm. In this paper, we concentrate on the Kummer extension $\mathbb{F}_{q^{2(q-1)}}$. We design a new heuristic algorithm with an improved bit complexity $\tilde{O}(q^{1+\theta})$ (or algebraic complexity $\tilde{O}(q^{\theta})$) to compute the discrete logarithms of elements in a factor base of cardinality q^2, where $\theta < 2.373$ is the matrix multiplication exponent. We reduce the correctness of the algorithm to a conjecture concerning the determinant of a simple $(q+1)-$dimensional lattice, rather than to elusive smoothness assumptions. We verify the conjecture numerically for all q's such that $\log_2(q^{2(q-1)}) \le 5000$, and provide theoretical supporting evidences.

Keywords: Discrete logarithm, Finite fields, Kummer extension

1 Introduction

One of the basic assumptions in cryptography is the difficulty of solving discrete logarithm over a finite field. While the assumption still holds now for a general field, in particular a prime order field, it has been weakened dramatically if the

* This work is supported by 973 Program(Grant NO.2013CB834205) and the National Natural Science Foundation of China(Grant NO.61133013).

** This work is supported by 973 Program(Grant NO.2011CB302400) and the Strategic Priority Research Program of the Chinese Academy of Sciences(Grant NO.XDA06010701) and the Open Project Program of the State Key Laboratory of Mathematical Engineering and Advanced Computing.

*** *2000 Mathematics Subject Classification.* Primary 12Y05, 68W30; Secondary 11Y16, 12D05, 13P05.

characteristic of the field is small, due to recent ground-breaking work [8, 14, 15, 3]. The new algorithms follow the same two-step strategy as in the index calculus, function field sieve and number field sieve [1, 2]. In the first step the discrete logarithms of elements in a factor base are calculated. In the second step, the discrete logarithm of the target element is computed. The factor base is closely related to the concept of smoothness, which plays a critical role in many algorithms attacking public key cryptosystems. An integer is smooth if all its prime factors are small. A polynomial is smooth if it can be factored into a product of irreducible polynomials of small degrees. Small prime numbers, or small degree irreducible polynomials, form a factor base. If a multiplicative relation among elements in the factor base can be found, one obtains a linear equation by taking logarithm. While previous approaches use exhaustive search to find relations, the new algorithms [8, 14, 15, 9] rely on a guided way, dubbed as "pinpointing" in [14]. It works very well in practice, inspires the first heuristic quasi-polynomial time algorithm [3], and produces a sequence of record-breaking numerical results. However, the correctness of these algorithms is based on smoothness assumptions that are impossible to prove using current number theoretical techniques.

In the method of [15], to solve the discrete logarithm problems in small characteristic fields such as $\mathbb{F}_{q^{2n}} = \mathbb{F}_{q^2}[X]$, the factor base consists of the polynomial in $\mathbb{F}_{q^2}[X]$ of degree 1. From every element in $PGL_2(\mathbb{F}_{q^2})$, one obtains an equation, where the left hand side is a product of linear polynomials in $\mathbb{F}_{q^2}[X]$, and the right hand side is of low degree. A relation is found if the right hand side can be factored completely into linear factors. It has been observed that for the Kummer extension $\mathbb{F}_{q^{2(q-1)}}$, in the equation obtained from an element in the *Borel subgroup* of $PGL_2(\mathbb{F}_{q^2})$, the right hand is automatically linear [13]. The relations from the subgroup give us a linear system of $q^2 - 1$ variables and $O(q^2)$ many equations, without using smoothness assumptions. A natural question is whether it is sufficient to solve the discrete logarithm of linear factors from this system. In this paper, we first give a negative answer to the question. We then propose to add a few simple relations that are not derived from an element in $PGL_2(\mathbb{F}_{q^2})$. Our computation examples show that after adding them, the discrete logarithm can be computed. To analyze the algorithm, we formulate a conjecture concerning the determinant of a $(q + 1)$-dimensional lattice. If the conjecture is true, it implies that discrete logarithms of the factor base (of cardinality q^2) in $\mathbb{F}_{q^{2(q-1)}}$ can be solved in $\tilde{O}(q^{1+\theta})$ bit operations (or algebraic complexity $\tilde{O}(q^{\theta})$), which is an improvement over (algebraic) complexity $O(q^6)$, claimed in [16]. We have verified the conjecture numerically for all q's such that $\log_2(q^{2(q-1)}) \leq 5000$, which covers all the fields that are cryptographically relevant. We also provide theoretical evidences that support the conjecture.

Our Motivation Even though in cryptography, the Kummer extensions are not used, and fields with small characteristic are generally avoided, we feel that it is worthwhile to study the discrete logarithm problem in Kummer extensions:

- The Kummer extensions are usually the testbeds for new ideas on solving discrete logarithms. The efficiency of the algorithm in the Kummer case attains the upper bound, thus many of the numerical records are achieved in Kummer extensions.

- All the new algorithms are heuristic, even in the case of Kummer extensions, except a recent result in [10], where it is randomized. Removing the heuristic and/or the randomness from the algorithm, or even just weakening the heuristic, is an interesting and important problem. The Kummer extensions are naturally the first candidates for investigations.

1.1 New Method of Finding Relations

Let $\mathbb{F}_q$ be a finite field with q elements. Let $h_0(x)$ and $h_1(x)$ be polynomials over $\mathbb{F}_{q^2}$ of small degrees. Let g be an element in $\mathbb{F}_{q^2}$ such that $\langle g \rangle = \mathbb{F}_{q^2}^*$. Following Joux's idea, we start with the identity in $\mathbb{F}_{q^2}[x]$:

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

Apply the Möbius transformation

$$x \mapsto \frac{ax+b}{cx+d}$$

where the matrix $m = \begin{pmatrix} a\ b \\ c\ d \end{pmatrix} \in \mathbb{F}_{q^2}^{2\times 2}$ is nonsingular. We have

$$\prod_{\alpha \in \mathbb{F}_q} (\frac{ax+b}{cx+d} - \alpha) = (\frac{ax+b}{cx+d})^q - \frac{ax+b}{cx+d}.$$

Clearing the denominator, we get

$$\begin{aligned} &(cx+d) \prod_{\alpha \in \mathbb{F}_q} ((ax+b) - \alpha(cx+d)) \\ &= (ax+b)^q(cx+d) - (ax+b)(cx+d)^q \\ &= (a^q x^q + b^q)(cx+d) - (ax+b)(c^q x^q + d^q). \end{aligned}$$

Multiplying both sides by $h_1(x)$ and replacing $x^q h_1(x)$ by $h_0(x)$, we obtain

$$\begin{aligned} &h_1(x)(cx+d) \prod_{\alpha \in \mathbb{F}_q} ((ax+b) - \alpha(cx+d)) \\ =&(a^q h_0(x) + b^q h_1(x))(cx+d) - (ax+b)(c^q h_0(x) + d^q h_1(x)) \\ &\pmod{x^q h_1(x) - h_0(x)}. \end{aligned} \tag{1}$$

The left hand is a product of linear polynomials if $h_1(x)$ has degree ≤ 1. Let $f(x)$ be irreducible factor of $x^q h_1(x) - h_0(x)$ of degree n. If the right hand, which already has small degree, can be factored into linear factors, then we have a relation among factor base elements in $\mathbb{F}_{q^2}[x]/(f(x)) \cong \mathbb{F}_{q^{2n}}$. One hopes to find enough relations so that the factor base discrete logarithm can be found.

For any (n, q) ($n < q$) of cryptography interests, the small degree polynomials $h_0(x)$ and $h_1(x)$ can be found easily so that $x^q h_1(x) - h_0(x)$ has an irreducible factor of degree n. However proving that they exist in general is a very hard mathematical problem. One can compare it with the much weaker Hansen-Mullen Conjecture [11, Conjecture B] concerning the distribution of irreducible polynomials with some prefixed coefficients, and subsequent work such as [19]. Because this work focuses on provability of the computational complexity, we feel that the Kummer extension $\mathbb{F}_{q^{2(q-1)}}$ should be dealt with firstly. It can be modeled by $\mathbb{F}_{q^2}[x]/(x^{q-1} - A)$, where $A \in \mathbb{F}_{q^2}$ and $x^{q-1} - A$ is irreducible over $\mathbb{F}_{q^2}$. In this case, existence of h_0 and h_1 can be easily established, and in fact,

$$h_1(x) = 1, h_0(x) = Ax.$$

Equation (1) becomes

$$\begin{aligned}&(cx + d) \prod_{\alpha \in \mathbb{F}_q} ((ax + b) - \alpha(cx + d)) \\ &= (a^q Ax + b^q)(cx + d) - (ax + b)(c^q Ax + d^q) \pmod{x^q - Ax}.\end{aligned}$$

1.2 Our Contributions

If $a^q c = ac^q$, then the right hand side has degree one, which gives us a relation. To satisfy $a^q c = ac^q$, we can set $a = 0$, in which case c can be made to 1; or we set $c = 0$, in which case a can be made to 1; or we can set $a = 1$ and $c = 1$. One can verify that these three cases give us the same set of relations, since they are in the same $PGL_2(\mathbb{F}_q)-$coset of the group $PGL_2(\mathbb{F}_{q^2})$, and the elements in the same $PGL_2(\mathbb{F}_q)-$coset generate the same linear equation. W.l.o.g., we will assume that $c = 0$ and $d = 1$. Denote $X = x \pmod{x^{q-1} - A}$, we have

$$\prod_{\alpha \in \mathbb{F}_q} ((aX + b) - \alpha) = (a^q AX + b^q) - (aX + b).$$

If $b \notin \mathbb{F}_q$, then we can simply assume that $b = g$, and obtain

$$\prod_{\alpha \in \mathbb{F}_q} ((aX + g) - \alpha) = (a^q AX + g^q) - (aX + g).$$

We have

$$a^q \prod_{\alpha \in \mathbb{F}_q} (X + \frac{g - \alpha}{a}) = (a^q A - a)(X + \frac{g^q - g}{a^q A - a}).$$

Let log be the discrete logarithm based on a prefixed multiplicative generator of $(\mathbb{F}_{q^{2(q-1)}})^* / \mathbb{F}_{q^2}^*$. For example, $\log a = 0$ for every $a \in \mathbb{F}_{q^2}^*$. We obtain a linear system

$$\forall a \in \mathbb{F}_{q^2}^*, \sum_{\alpha \in \mathbb{F}_q} \log(X + \frac{g - \alpha}{a}) = \log(X + \frac{g^q - g}{a^q A - a}) \qquad (2)$$

of q^2-1 equations in q^2-1 variables, which represent $\log(x+h)$ ($h \in \mathbb{F}_{q^2}^*$). Define a matrix $M = (m_{i,j})_{0\le i,j\le q^2-2}$ such that

$$m_{i,j} = \begin{cases} 1, \text{if } \exists\ \alpha \in \mathbb{F}_q, s.t.\ g^i = (g+\alpha)\frac{Ag^{jq}-g^j}{g^q-g}; \\ 0, \text{otherwise.} \end{cases}$$

One can verify that the coefficient matrix of the linear system is $M-I$.

Note that

$$\left\{ \begin{pmatrix} a\ b \\ 0\ 1 \end{pmatrix} \mid a \in \mathbb{F}_{q^2}^*, b \in \mathbb{F}_{q^2} \right\}$$

is the Borel subgroup of $PGL_2(\mathbb{F}_{q^2})$. We should only consider $PGL_2(\mathbb{F}_q)-$coset representatives, which can be partitioned into two subsets

$$\left\{ \begin{pmatrix} a\ g \\ 0\ 1 \end{pmatrix} \mid a \in \mathbb{F}_{q^2}^* \right\} \cup \left\{ \begin{pmatrix} a\ 0 \\ 0\ 1 \end{pmatrix} \mid a \in \mathbb{F}_{q^2}^*/\mathbb{F}_q^* \right\}.$$

The linear system (2) is obtained by considering the first subset. The second subset gives us a system of $q+1$ equations:

$$\forall a \in \mathbb{F}_{q^2}^*/\mathbb{F}_q^*, \sum_{\alpha\in\mathbb{F}_q^*} \log(X + \frac{-\alpha}{a}) = 0. \tag{3}$$

None of the equations contains the variable corresponding to $\log X$, which is known as a trap [4]. But it is easy to calculate $\log(X)$ in the Kummer case since the order of X is small.

Note that the linear system (2), as well as (3), is homogeneous. If the solution space is one dimensional, then the discrete logarithms of linear factors can be determined up to a scalar that depends on the logarithm base. We will show that the linear system (2) is not sufficient for the purpose of solving discrete logarithm of the factor base. To achieve this, we prove that the eigenvalues of M, viewed as an integral matrix, include 1 with multiplicity at least $(q-1)/2$. We will also give a numerical example that shows adding (3) does not help.

We then propose to add a simple relation into the linear system. One observes that over $\mathbb{F}_{q^{2(q-1)}}^*/\mathbb{F}_{q^2}^*$, we have $(X+a)^{q^2} = X + \frac{a}{A^{q+1}}$, thus

$$\forall a \in \mathbb{F}_{q^2}^*, q^2 \log(X+a) = \log(X + \frac{a}{A^{q+1}}). \tag{4}$$

With this observation, given the value $\log(X+a)$ for any $a \in \mathbb{F}_{q^2}^*$, $\log(x+a\beta)$ for all $\beta \in \mathbb{F}_q^*$ can be computed, since $\frac{1}{A^{q+1}}$ is a generator of the multiplicative group $\mathbb{F}_q^*$. Therefore, after adding (4), we can reduce the number of variables in (2) from q^2-1 to $q+1$. This relation was studied in [14]. This improves the efficiency of solving the linear system to bit complexity $O(q^{3.4})$. Note that we can use

$$\forall a \in \mathbb{F}_{q^2}^*, q\log(X+a) = \log(X + \frac{a^q}{A}) \tag{5}$$

instead of (4) to have a slightly better algorithm. In this paper, since our goal is mainly about provability, we will use (4).

To analyze the new algorithm, we introduce a conjecture about the determinant of a simple $(q+1)-$dimensional lattice, derived from M. The conjecture implies that this more efficient algorithm can solve the factor base discrete logarithm for any $\mathbb{F}_{q^{2(q-1)}}$. We have done an extensive numerical study to confirm the conjecture. On the theoretical side, we prove that all the complex eigenvalues of M, other than $q, 1$ and -1, have complex norm $\sqrt{q}$, using the character sum technique. This allows us to bound the complex norm of eigenvalues of $M - I$ over the complex number $\mathbb{C}$, which provides a strong supporting evidence to our conjecture.

This paper is organized as follows. In Section 2, we decompose M into a block diagonal form, and show that adding (3) essentially removes one small block from M , thus will not have a big impact on the efficiency of the algorithm. In Section 3, we show that adding (4) allows us to select just one block from the block diagonal form of M, which greatly improves the efficiency. We formulate a conjecture that implies the correctness of our algorithm, and supply some numerical and theoretical evidences. We make some concluding remarks in the last section.

2 Block Diagonal Form of M over $\mathbb{C}$

In this section, we show that the linear system (2) is singular over $\mathbb{Q}$ with a kernel of dimension at least $(q-1)/2$. To this end, we first decompose M, viewed as a linear transformation of $\mathbb{C}[x]/(x^{q^2-1}-1)$,

$$M(x^k) = \sum_{i=0}^{q^2-2} m_{i,k} x^i = \sum_{\alpha\in\mathbb{F}_q} x^{\log_g\left((g+\alpha)\cdot\frac{Ag^{kq}-g^k}{g^q-g}\right)}, \text{ for all } 0 \le k \le q^2-2,$$

into a directed sum of linear operators. For the linear system (3), we have a corresponding transformation

$$C(x^k) = \sum_{\alpha\in\mathbb{F}_q} x^{\log_g\left(-\alpha\cdot\frac{Ag^{kq}-g^k}{g^q-g}\right)}, \text{ for all } 0 \le k \le q^2-2.$$

Definition 1. *Define two linear transformations G and T over the $\mathbb{C}$-linear space $\mathbb{C}[x]/(x^{q^2-1}-1)$ as:*

$$G(x^k) = x^k \sum_{\alpha\in\mathbb{F}_q} x^{\log_g(g+\alpha)}, \quad T(x^k) = x^k x^{\log_g \frac{Ag^{k(q-1)}-1}{g^q-g}}.$$

Note that M, C, G and T are well-defined, since $\log_g$ is a map from $\mathbb{F}_{q^2}^*$ to $\mathbb{Z}/(q^2-1)\mathbb{Z}$ if g is a multiplicative generator of $\mathbb{F}_{q^2}$.

Theorem 1. *We have $M = GT$.*

Proof. For any $0 \leq k \leq q^2 - 2$,

$$\begin{aligned} M(x^k) &= \sum_{\alpha \in \mathbb{F}_q} x^{\log_g \left((g+\alpha) \cdot \frac{Ag^{kq} - g^k}{g^q - g}\right)} \\ &= \left(\sum_{\alpha \in \mathbb{F}_q} x^{\log_g (g+\alpha)} \right) \cdot x^{\log_g \frac{Ag^{kq} - g^k}{g^q - g}}, \end{aligned}$$

which proves the theorem. □

According to Chinese Remainder Theorem, we have a ring isomorphism:

$$\mathbb{C}[x]/(x^{q^2-1} - 1) \rightarrow \bigoplus_{i=0}^{q-2} \mathbb{C}[x]/(x^{q+1} - \zeta_{q-1}^i),$$

where $\zeta_{q-1} = e^{\frac{2\pi \mathbf{i}}{q-1}}$. It decomposes the linear space $\mathbb{C}[x]/(x^{q^2-1} - 1)$ into $q - 1$ subspaces, each has dimension $q + 1$. The following theorem shows that each of the components is an invariant subspace for T and G, thus M can be represented by a block-diagonal matrix.

Theorem 2. *The linear transformation M over $\mathbb{C}[x]/(x^{q^2-1} - 1)$ defined above is similar to a block-diagonal matrix:*

$$M = U^{-1} \begin{pmatrix} M_0 & & & \\ & M_1 & & \\ & & \ddots & \\ & & & M_{q-2} \end{pmatrix} U, \tag{6}$$

where for $i = 0, 1, \cdots, q - 2$, $M_i = M \mid_{\mathbb{C}[x]/(x^{q+1} - \zeta_{q-1}^i)}$, denoting the transformation of M acting on the invariant subspace $\mathbb{C}[x]/(x^{q+1} - \zeta_{q-1}^i)$, and U is an invertible matrix.

Proof. Let $V_{i,j}$ be the polynomial

$$x^j \prod_{k \neq i} (x^{q+1} - \zeta_{q-1}^k)$$

in $\mathbb{C}[x]/(x^{q^2-1} - 1)$. It is easy to see that for any $0 \leq j \leq q, 0 \leq i \leq q - 2$, if $k \neq i$, we have

$$V_{i,j} = 0 \pmod{x^{q+1} - \zeta_{q-1}^k}.$$

And $V_{i,0}, V_{i,1}, \cdots, V_{i,q}$ is a basis of subspace $C[x]/(x^{q+1} - \zeta_{q-1}^i)$. One can verify that

$$\begin{aligned} T(x^{m(q+1)} x^n) &= x^{m(q+1)} x^n x^{\log_g \frac{Ag^{(n+m(q+1))(q-1)} - 1}{g^q - g}} \\ &= x^{m(q+1)} x^n x^{\log_g \frac{Ag^{n(q-1)} - 1}{g^q - g}} \\ &= x^{m(q+1)} T(x^n) \end{aligned}$$

for any integer m and n. We have $T(V_{i,j}) = yV_{i,j'}$ for some integer j' and $y \in \mathbb{C}$. Thus, the space spanned by $V_{i,0}, V_{i,1}, \cdots, V_{i,q}$ is invariant under T. It is also invariant under G, the block diagonal structure of M is derived. □

2.1 The Linear Transformation *T*

It turns out that T is a very simple transformation.

Theorem 3. *Let $0 \le i \le q-2$ be an integer. Note that since $\frac{1-A^{q+1}}{(g^q-g)^2} \in \mathbb{F}_q^*$, there must exist a unique complex number τ that is congruent to*

$$x^{\log_g \frac{1-A^{q+1}}{(g^q-g)^2}} \pmod{x^{q+1} - \zeta_{q-1}^i}.$$

The linear transformation $T_i = T \mid_{\mathbb{C}[x]/(x^{q+1}-\zeta_{q-1}^i)}$ can be represented by

$$\begin{pmatrix} D & & & & & & & \\ & 0 & y_1 & & & & & \\ & \tau/y_1 & 0 & & & & & \\ & & & 0 & y_2 & & & \\ & & & \tau/y_2 & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & 0 & y_d \\ & & & & & & \tau/y_d & 0 \end{pmatrix}$$

where $D = diagonal(\gamma_1, \cdots, \gamma_t)$ satisfying $\gamma_j^2 = \tau$ for all $1 \le j \le t$. In addition, we have: $t = 1$, if q is even; t is 0 or 2, if q is odd.

Proof. In the polynomial ring $\mathbb{C}[x]/(x^{q+1} - \zeta_{q-1}^i)$, we have

$$T^2(x^k) = x^{\log_g \frac{1-A^{q+1}}{(g^q-g)^2}} \cdot x^k = \tau x^k.$$

since

$$\frac{A\left(\frac{Ag^{kq}-g^k}{g^q-g}\right)^q - \frac{Ag^{kq}-g^k}{g^q-g}}{g^q-g} = g^k \cdot \frac{1-A^{q+1}}{(g^q-g)^2}.$$

For any integer $0 \le k_1 \le q$, there must exist an integer k_2 and $y \in \mathbb{C}$, such that $T(x^{k_1}) = yx^{k_2}$, and $T(x^{k_2}) = \frac{\tau}{y}x^{k_1}$. When $k_1 = k_2$, we have $T(x^{k_1}) = \gamma x^{k_1}$ with $\gamma^2 = \tau$. We claim that the number of these k_1 is at most 2.

Observe that $T(x^k) = \gamma x^k$ for some $\gamma \in \mathbb{C}$ if and only if $\frac{Ag^{k(q-1)}-1}{(g^q-g)} \in \mathbb{F}_q$. Then we must have

$$(\frac{Ag^{k(q-1)}-1}{g^q-g})^q = \frac{Ag^{k(q-1)}-1}{g^q-g},$$

Namely $Ag^{2k(q-1)} - 2g^{k(q-1)} + A^q = 0$, which is a quadratic equation in $g^{k(q-1)}$. In addition, g^{q-1} has order $q+1$, thus there are at most two $0 \le k \le q$ satisfying the formula.

With proper order of the basis $\{1, x, x^2, \cdots, x^q\}$, we obtain our conclusion. □

Corollary 1. *The characteristic polynomial of the linear transformation* $T_0 = T\mid_{\mathbb{C}[x]/(x^{q+1}-1)}$ *is*

- $(x^2-1)^{q/2}(x-1)$ *if* q *is even;*
- $(x^2-1)^{(q+1)/2}$ *if* q *is odd and* $t=0$*;*
- $(x^2-1)^{(q-1)/2}(x-1)^2$ *if* q *is odd and* $t=2$.

Let us consider the action of M on subspace $\mathbb{C}[x]/(x^{q+1}-1)$. By Chinese Remainder Theorem,

$$\mathbb{C}[x]/(x^{q+1}-1) \cong \mathbb{C}[x]/(x-1) \oplus \mathbb{C}[x]/(x^q + x^{q-1} + \cdots + 1).$$

In the component $\mathbb{C}[x]/(x-1) \cong \mathbb{C}$, $x^q + x^{q-1} + \cdots + 1 \in \mathbb{C}[x]/(x^{q+1}-1)$ is the base. Acting on the base, $G_0 = G\mid_{\mathbb{C}[x]/(x^{q+1}-1)}$ is just a multiplication by q, and T fixes the base. In the other component $\mathbb{C}[x]/(x^q + x^{q-1} + \cdots + 1)$, one base is $\{x^i(x-1) | 0 \le i \le q-1\}$. The action G_0 is a multiplication by

$$\sum_{\alpha\in\mathbb{F}_q} x^{\log_g(g+\alpha)} = \sum_{1\le i\le q} x^i = -1,$$

since for any $\alpha \in \mathbb{F}_q, \beta \in \mathbb{F}_q$, $(g+\alpha)/(g+\beta) \notin \mathbb{F}_q$ if $\alpha \neq \beta$. The eigenvalue of M_0 is thus equal to the negation of eigenvalue of T_0. Hence

Theorem 4. *Let* $f_0(x)$ *be the characteristic polynomial of* M_0*, we have*

$$f_0(x) = \begin{cases} (x-q)(x^2-1)^{\frac{q}{2}}, & q \textit{ is even;} \\ (x-q)(x^2-1)^{\frac{q-1}{2}}(x\pm 1), & q \textit{ is odd.} \end{cases}$$

From Theorem 4 , we conclude that M has eigenvalue 1 with multiplicity at least $(q-1)/2$. Hence $M - I$ has a kernel space of dimension $(q-1)/2$ over $\mathbb{Q}$. It means that the $q^2 - 1$ relations in the linear system (2) are not enough to compute the discrete logarithms of linear factors.

2.2 The Linear Transformation *C*

Theorem 5. *We have*

$$C = U^{-1} \begin{pmatrix} (q-1)T_0 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} U$$

where T_0 *is a permutation matrix, and* U *is the same base change matrix in (6).*

Proof. It is easy to verify that $C = HT$, where H is a linear transformation over $\mathbb{C}$-linear space $\mathbb{C}[x]/(x^{q^2-1}-1)$ defined as:

$$H(x^k) = x^k \sum_{\alpha\in\mathbb{F}_q^*} x^{\log_g(-\alpha)},$$

and T is defined in Definition 1.

In the ring $\mathbb{C}[x]/(x^{1+q}-1)$, we have

$$\sum_{\alpha\in\mathbb{F}_q^*} x^{\log_g(-\alpha)} = \sum_{1\leq j\leq q-1} (x^{q+1})^j = q-1.$$

That is, for any polynomial $P \in \mathbb{C}[x]/(x^{q^2-1}-1)$,

$$\begin{aligned} C(P(x)) &= HT(P(x)) \\ &= T(P(x)) \cdot \sum_{\alpha\in\mathbb{F}_q^*} x^{\log_g(-\alpha)} \\ &= (q-1)T(P(x)) \neq 0. \end{aligned}$$

On the other hand, in the ring $\mathbb{C}[x]/(x^{1+q}-\zeta_{q-1}^i)$, $1 \leq i \leq q-2$, we have

$$\sum_{\alpha\in\mathbb{F}_q^*} x^{\log_g(-\alpha)} = \sum_{1\leq j\leq q-1} (x^{q+1})^j = \sum_{0\leq j\leq q-1} (\zeta_{q-1}^i)^j = 0.$$

Then for any $P(x)$, one may obtain:

$$C(P(x)) = T(P(x)) \cdot \sum_{\alpha\in\mathbb{F}_q^*} x^{\log_g(-\alpha)} = 0.$$

We conclude that the solution space of (3) belongs to the solution space of M_i, $1 \leq i \leq q-2$, but not M_0. □

Corollary 2. *Adding the equations of (3) to the equations of (2), we obtain a linear system $M' - I$ where*

$$M' = M_1 \oplus M_2 \oplus \cdots M_{q-2}.$$

The corollary basically shows that after adding (3), the dimension of the linear system that we need to solve drops from q^2-1 to q^2-q-2, which is only a negligible improvement.

3 The Main Theorem and the Conjecture

Assume that $q^{2(q-1)}-1$ has factorization

$$q^{2(q-1)}-1 = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}N,$$

where $p_1, \cdots, p_s$ are primes less than q^2, and N is free of prime factors less than q^2. Denote $S = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$. To solve the discrete logarithm problem in $\mathbb{F}_{q^{2(q-1)}}$, we observe the group isomorphism

$$\mathbb{F}_{q^{2(q-1)}}^* \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/S\mathbb{Z}.$$

The discrete logarithm in the subgroup of order S can be solved in $O(q^2)$ by Pohlig-Hellman algorithm [17], since the group order is smooth. So we should focus on the subgroup of order N. To compute the discrete logarithm in this subgroup, we will have to solve the equation system (2) combining with (3) over $\mathbb{Z}/NZ$. Ideally it is preferable to solve linear systems in a finite field $\mathbb{F}_l$, where $l|N$, as there are no zero divisors in a field. However it is hard to factor N in general. For this reason, we should solve the linear system by computing the Hermite Normal Form, instead of using the Gauss Elimination.

As we have shown in the previous sections, the system (2) alone is not enough, since it has a kernel over $\mathbb{Q}$ of dimension much bigger than 1. Can we avoid the problem by adding the linear equations (3)? We found that when $q = 31$, M' has eigenvalue 1 with multiplicity 2 over $\mathbb{F}_l$ for the prime factor $l = 2521$ of N, thus the $M' - I$ have a kernel of dimension 2 over $\mathbb{F}_l$. Here we include the details:

> For the case $q = 31$, we build the extension field $\mathbb{F}_{q^2} = \mathbb{F}_q[x]/(x^2-2x+3)$. Let $g = x \pmod{x^2 - 2x + 3}$. One can verify that g is a multiplicative generator of $\mathbb{F}^*_{q^2}$. The element A is selected to be g, We compute $h(x)$, the characteristic polynomial of $M^{'}$, and find that when $l = 2521$, the power of the factor $x - 1$ in $h(x) \pmod{l}$ is 2.

This shows that the discrete logarithm over the subgroup of size l can not be uniquely determined by the linear system (2) plus (3). Furthermore, even in the case that (2) plus (3) is sufficient, it is not efficient, since we need to solve a linear system with $O(q^2)$ many variables.

Nevertheless if we add (4), numerical data confirm that discrete logarithm can always be found. The new linear system have only $q + 1$ variables, and the coefficient matrix can be described by the action of G and T, as defined in Definiton 1, on the $\mathbb{Z}/NZ$-module $(\mathbb{Z}/NZ)[x]/(x^{q+1} - \tilde{\mu}(g^{1+q}))$, where $\tilde{\mu}$ is homomorphism from $\mathbb{F}^*_q$ to $\langle q^2 \rangle \in (\mathbb{Z}/NZ)^*$ satisfying

$$\tilde{\mu}(1/A^{1+q}) = q^2.$$

We will denote the coefficient matrix of GT in base $\{x^i | 0 \leq i \leq q\}$ by $\tilde{M_1}$, which can be regarded as an integer matrix. We use L to denote the map from an integer matrix to the lattice generated by the row vectors of the matrix. Construct a lattice

$$\mathcal{L}_1 = L(\tilde{M_1} - I) + N\mathbb{Z}^{q+1}.$$

Theorem 6. *We have* $N|\det(\mathcal{L}_1)|N^{q+1}$.

Proof. Note that $\mathcal{L}_1$ is a sublattice of $N\mathbb{Z}^{q+1}$, we conclude that $\det(\mathcal{L}_1)|N^{q+1}$.

The linear factors $X + a$ ($a \in \mathbb{F}_{q^2}$) generate the cyclic multiplicative group $\mathbb{F}^*_{q^{2(q-1)}}$ [5]. From (4), we conclude that $\langle X + g^i | 0 \leq i \leq q \rangle$ contains the cyclic multiplicative group $\mathbb{F}^*_{q^{2(q-1)}}/\langle X \rangle$, which includes the subgroup of cardinality N. There is an injection from this subgroup into of $\mathbb{Z}^{q+1}/\mathcal{L}_1$, thus $N|\det(\mathcal{L}_1)$. Note that if we need use a different base for the $\mathbb{Z}/NZ$-module $(\mathbb{Z}/NZ)[x]/(x^{q+1} - \tilde{\mu}(g^{1+q}))$, the determinant of lattice remains the same. □

We make the following conjecture

Conjecture 1. $\det(\mathcal{L}_1) = N$.

It implies that we can use Smith Normal Form of $\mathcal{L}_1$ to find a generator of subgroup of cardinality N, and determine the factor base discrete logarithm with respect to that element in the subgroup. We have verified the conjecture for all the prime power q less than 307.

Theorem 7. *Assume that the conjecture is true. We can find a generator of the subgroup of cardinality N of $\mathbb{F}^*_{q^{2(q-1)}}$, and compute the discrete logarithms of linear factors with respect to the generator in time $\tilde{O}(q^{1+\theta})$.*

Proof. Assuming that for any basis B of lattice $\mathcal{L}_1$, we have the Smith Normal Form transformation $D = S_1 B S_2$, where D is the Smith Normal Form of lattice $\mathcal{L}_1$, and S_1, S_2 are corresponding transformations with respect to B. Then it is easy to verify that the last column of S_2 are the ratio of the discrete logarithms of

$$X + \frac{g^q - g}{A - 1}, X + \frac{g^q - g}{Ag^q - g}, \cdots, X + \frac{g^q - g}{Ag^{kq} - g^k}, \cdots, X + \frac{g^q - g}{Ag - g^q}$$

over $\mathbb{Z}/NZ$ respectively.

Assuming that the last row of S_2^{-1} is $(e'_0, e'_1, \cdots, e'_q)$, one may verify that $\langle \prod_{i=0}^{q} (X + \frac{g^q - g}{Ag^{kq} - g^k})^{e'_k} \rangle$ contains the subgroup of $(\mathbb{F}_{q^{2(q-1)}})^*$ of order N. With the ratio, it is easy to calculate the discrete logarithms of $X + \frac{g^q - g}{Ag^{kq} - g^k}$ $(k = 0, 1, \cdots, q)$ with respect to the generator. And the discrete logarithm of other elements in the factor base can be obtained through relation (4).

Two $q \times q$ matrices can be multiplied in $O(q^\theta)$ arithmetic operations. According to [6, 7, 20], θ is less than 2.373. The cost of computing the Smith Normal Form is $O(q^\theta)$([18]). Furthermore, with Optimized CW-like algorithms [6, 7, 20], the complexity of computing the inverse of S_2 is also bounded by $O(q^\theta)$ arithmetic operations. In our case, the arithmetic operations are additions and multiplications in $\mathbb{Z}/N\mathbb{Z}$, each has bit complexity $\tilde{O}(q)$. □

3.1 Other Eigenvalues of M over $\mathbb{C}$

Theorem 6 states that $N | \det(\mathcal{L}_1) | N^{q+1}$. We conjecture that $\det(\mathcal{L}_1)$ is in fact N, so qualitatively the determinant of an N-ary lattice derived from $\tilde{M_1} - I$ should be small. In this subsection, we show that the determinant of $M_i - I$ over $\mathbb{C}$ is indeed small.

Theorem 8. *For $1 \le i \le q-2$, the complex norm of the determinant of $M_i - I$ is not zero, and it is no larger than $(\sqrt{q} + 1)^{q+1}$.*

Note that the determinant is in general not a rational integer, but a cyclotomic integer in $\mathbb{Z}[\zeta_{q-1}]$. In our view, it provides a strong supporting evidence of the conjecture. The theorem follows easily from the statement that the eigenvalues of M_i ($1 \le i \le q-2$) have complex norm $\sqrt{q}$, which we prove in this subsection. First we compute the eigenvalue of G_i for $i \ne 0$.

Lemma 1. *Acting on any subspace* $\mathbb{C}[x]/(x^{q+1}-\zeta_{q-1}^{i})(1 \le i \le q-2)$, *all of the eigenvalues of* G_i *have complex norm* $\sqrt{q}$.

Proof. We can factor $x^{q+1}-\zeta_{q-1}^{i}$ completely over $\mathbb{C}$, and by Chinese Remainder Theorem,

$$\mathbb{C}[x]/(x^{q+1}-\zeta_{q-1}^{i}) \cong \bigoplus_{j=0}^{q} \mathbb{C}[x]/(x-\zeta_{q^2-1}^{j(q-1)+i}),$$

where $\zeta_{q^2-1} = e^{2\pi \mathbf{i}/(q^2-1)}$. In each component, G is a multiplication by a constant, thus the eigenvalue of G is equal to

$$\sum_{\alpha\in\mathbb{F}_q} \zeta_{q^2-1}^{(j(q-1)+i)\log_g(g+\alpha)} = \sum_{\alpha\in\mathbb{F}_q} \mu_j(g+\alpha),$$

where μ_j is a multiplicative character from $\mathbb{F}_{q^2}^{*}$ to $\mathbb{C}$ by sending g to $\zeta_{q^2-1}^{j(q-1)+i}$. The Lemma follows from the next lemma. □

Lemma 2. *Let* μ *be a multiplicative character for* $\mathbb{F}_{q^2}$ *that is not trivial over* $\mathbb{F}_q^{*}$, *we have* $|\sum_{\alpha\in\mathbb{F}_q} \mu(g+\alpha)| = \sqrt{q}$.

Note that if μ is trivial over $\mathbb{F}_{q^2}$, we have $\sum_{\alpha\in\mathbb{F}_q}\mu(g+\alpha) = q$. If μ is not trivial over $\mathbb{F}_{q^2}^{*}$ but is trivial over $\mathbb{F}_q^{*}$, then $\sum_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q}\mu(g\beta+\alpha) = 0$. On the other hand

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q}\mu(g\beta+\alpha) &= \sum_{\alpha\in\mathbb{F}_q}\mu(\alpha) + \sum_{\beta\in\mathbb{F}_q^{*}}\sum_{\alpha\in\mathbb{F}_q}\mu(g\beta+\alpha)\\ &= q-1+(q-1)\sum_{\alpha\in\mathbb{F}_q}\mu(g+\alpha),\end{aligned}$$

hence we have $\sum_{\alpha\in\mathbb{F}_q}\mu(g+\alpha) = -1$. This gives another way to explain the eigenvalues of G_0.

Proof. Observe that for any two pairs $(\alpha_1,\beta_1) \ne (\alpha_1,\beta_1)$ in $\mathbb{F}_q^2$, where $\alpha_1 \ne \beta_1$ and $\alpha_2 \ne \beta_2$, we have $(g+\alpha_1)/(g+\beta_1) \ne (g+\alpha_2)/(g+\beta_2)$. So the map from $\mathbb{F}_q^2 - \{(a,a)|a\in\mathbb{F}_q\}$ to $\mathbb{F}_{q^2}$ that sends (α,β) to $(g+\alpha)/(g+\beta)$ is an injection, where the image is $\mathbb{F}_{q^2}-\mathbb{F}_q$, so we have

$$\begin{aligned}&(\sum_{\alpha\in\mathbb{F}_q}\mu(g+\alpha))(\sum_{\alpha\in\mathbb{F}_q}\mu^{-1}(g+\alpha))\\ =&q+\sum_{\alpha\in\mathbb{F}_q,\beta\in\mathbb{F}_q,\alpha\ne\beta}\mu((g+\alpha)/(g+\beta))\\ =&q+\sum_{\gamma\in\mathbb{F}_{q^2}-\mathbb{F}_q}\mu(\gamma)\\ =&q+\sum_{\gamma\in\mathbb{F}_{q^2}}\mu(\gamma)-\sum_{\gamma\in\mathbb{F}_q}\mu(\gamma)\\ =&q\end{aligned}$$

□

Note that

$$\begin{aligned}\sum_{\alpha\in\mathbb{F}_q}\mu^q(g+\alpha) &= \sum_{\alpha\in\mathbb{F}_q}\mu((g+\alpha)^q)\\ &= \sum_{\alpha\in\mathbb{F}_q}\mu(g^q+\alpha)\\ &= \sum_{\alpha\in\mathbb{F}_q}\mu(S-g+\alpha)\\ &= \mu(-1)\sum_{\alpha\in\mathbb{F}_q}\mu(g+\alpha).\end{aligned}$$

So these sums come in pairs. We have the following conclusion about the eigenvalues of M:

Theorem 9. *For M in any subspace $\mathbb{C}[x]/(x^{q+1}-\zeta_{q-1}^i)(1\le i\le q-2)$, all of the eigenvalues of M_i have complex norm $\sqrt{q}$.*

Proof. With the consideration of Theorem 3, $T\mid_{\mathbb{C}[x]/(x^{q-1}-\zeta_{q-1}^i)}$ is a unitary transformation under the basis $1, x, \cdots, x^q$. On the other hand, by Lemma 1, $\frac{1}{\sqrt{q}}G\mid_{\mathbb{C}[x]/(x^{q-1}-\zeta_{q-1}^i)}$ is also a unitary matrix under that basis. It can be diagonalized by the unitary matrix $\tilde{U}=(\mu_j(g^k))(j,k\in[q])$, where μ_j is a multiplicative character from $\mathbb{F}_{q^2}^*$ to $\mathbb{C}$ satisfying $\mu_j(g^{1+q})=\zeta_{q-1}^i$.

Thus we have that $GT/\sqrt{q}$ is a unitary transformation([12]), which implies our conclusion. □

Corollary 3. *The determinant of the linear system $M_i\oplus M_{q-1-i}$ is q^{q+1}.*

With a direct deduction, we obtain the following theorem:

Theorem 10. *Let $f(x)$ be the characteristic polynomial of M, we have:*

$$f(x)=\begin{cases}(x-q)(x^2-1)^{\frac{q}{2}}h(x), & q \textit{ is even;}\\ (x-q)(x^2-1)^{\frac{q-1}{2}}(x\pm 1)h(x), & q \textit{ is odd,}\end{cases}$$

where $h(x)$ is a polynomial in $\mathbb{Z}[x]$ with degree q^2-q-2, all of whose roots have complex norm $\sqrt{q}$.

4 Concluding Remarks

In this work we focus on provability of the recent ground-breaking algorithm on the discrete logarithm over small characteristic finite fields. We feel that the Kummer case can be tackled using the current techniques, so we concentrate on this interesting case. We design a more efficient algorithm to solve the factor base discrete logarithm, and reduce the correctness of algorithm to a conjecture on the determinant of a simple lattice. We leave the proof of the conjecture as an open problem.

References

1. Adleman, L.: A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In: FOCS. pp. 55–60. IEEE Computer Society (1979)
2. Adleman, L.: The function field sieve. In: Adleman, L., Huang, M. (eds.) ANTS. LNCS, vol. 877, pp. 108–121. Springer (1994)
3. Barbulescu, R., Gaudry, P., Joux, A., Thomé, E.: A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: Nguyen, P., Oswald, E. (eds.) Advances in Cryptology - EUROCRYPT 2014. LNCS, vol. 8441, pp. 1–16. Springer (2014)
4. Cheng, Q., Wan, D., Zhuang, J.: Traps to the BGJT-algorithm for discrete logarithms. LMS Journal of Computation and Mathematics 17, 218–229 (2014)
5. Chung, F.: Diameters and eigenvalues. Journal of American Mathematical Society 2(2), 187–196 (1989)
6. Davie, A., Stothers, A.: Improved bound for complexity of matrix multiplication. Proceedings of the Royal Society of Edinburgh: Section A Mathematics 143, 351–369 (2013)
7. Gall, F.: Powers of tensors and fast matrix multiplication. In: Nabeshima, K., Nagasaka, K., Winkler, F., Szántó, Á. (eds.) ISSAC 2014. pp. 296–303. ACM (2014)
8. Göloglu, F., Granger, R., McGuire, G., Zumbrägel, J.: On the function field sieve and the impact of higher splitting probabilities. In: Canetti, R., Garay, J. (eds.) Advances in Cryptology - CRYPTO 2013. LNCS, vol. 8043, pp. 109–128. Springer (2013)
9. Granger, R., Kleinjung, T., Zumbrägel, J.: On the powers of 2. Cryptology ePrint Archive, Report 2014/300 (2014)
10. Granger, R., Kleinjung, T., Zumbrägel, J.: On the discrete logarithm problem in finite fields of fixed characteristic. Cryptology ePrint Archive, Report 2015/685 (2015)
11. Hansen, T., Mullen, G.: Primitive polynomials over finite fields. Mathematics of Computation 59(200), 639–643 (1992)
12. Hohn, F.: Elementary matrix algebra. Courier Corporation (2013)
13. Huang, M., Narayanan, A.: Finding primitive elements in finite fields of small characteristic. arXiv:1304.1206 (2013)
14. Joux, A.: Faster index calculus for the medium prime case application to 1175-bit and 1425-bit finite fields. In: Johansson, T., Nguyen, P. (eds.) Advances in Cryptology - EUROCRYPT 2013. LNCS, vol. 7881, pp. 177–193. Springer (2013)
15. Joux, A.: A new index calculus algorithm with complexity L(1/4+o(1)) in small characteristic. In: Lange, T., Lauter, K., Lisonek, P. (eds.) Selected Areas in Cryptography - SAC 2013. LNCS, vol. 8282, pp. 355–379. Springer (2013)
16. Joux, A., Pierrot, C.: Improving the polynomial time precomputation of frobenius representation discrete logarithm algorithms - simplified setting for small characteristic finite fields. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014. LNCS, vol. 8873, pp. 378–397. Springer (2014)
17. Pohlig, S., Hellman, M.: An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Transactions on Information Theory 24(1), 106–110 (1978)
18. Storjohann, A.: Near optimal algorithms for computing smith normal forms of integer matrices. In: Engeler, E., Caviness, B., Lakshman, Y. (eds.) ISSAC 1996. pp. 267–274. ACM (1996)

19. Wan, D.: Generators and irreducible polynomials over finite fields. Mathematics of Computation 66(219), 1195–1212 (1997)
20. Williams, V.: Multiplying matrices faster than Coppersmith-Winograd. In: STOC. pp. 887–898. ACM (2012)