Improvements on the Individual Logarithm Step in exTNFS

Yuqing Zhu[1,2], Jincheng Zhuang[1], Chang Lv[1], and Dongdai Lin[1]

[1] State Key Laboratory of Information Security, Institute of Information Engineering
Chinese Academy of Sciences, Beijing 100093, China
zhuyuqing@iie.ac.cn, zhuangjincheng@iie.ac.cn, lvchang@iie.ac.cn, ddlin@iie.ac.cn
[2] University of Chinese Academy of Sciences, Beijing 100049, China

Abstract. The hardness of discrete logarithm problem over finite fields is the foundation of many cryptographic protocols. When the characteristic of the finite field is medium or large, the state-of-art algorithms for solving the corresponding problem are the number field sieve and its variants. There are mainly three steps in such algorithms: polynomial selection, factor base logarithms computation, and individual logarithm computation. Note that the former two steps can be precomputed for fixed finite field, and the database containing factor base logarithms can be used by the last step for many times. In certain application circumstances, such as Logjam attack, speeding up the individual logarithm step is vital.
In this paper, we devise a method to improve the individual logarithm step by exploring certain subfield structure. Our technique is based on the extended tower number field sieve method and generalizes the idea used by Guillevic. The method achieves more significant improvement when the extension degree has a large proper factor. We also perform some experiments to illustrate our algorithm and confirm the result.

Keywords: Discrete logarithm problem, extended tower number field sieve, individual logarithm, smoothing phase.

1 Introduction

The discrete logarithm problem (DLP) in finite fields has played an important role in public key cryptography, firstly used to construct Diffie-Hellman key exchange protocol [9], later used as an important ingredient to build torus-based [24] and pairing-based cryptographic schemes [16,7]. The Diffie-Hellman key exchange protocol makes use of a prime field $\mathbb{F}_p$, while the torus-based and pairing-based cryptosystem make use of finite fields $\mathbb{F}_{p^n}$ and $\mathbb{F}_{q^n}$ respectively.

It has long been realized that the characteristic of the underlying finite field affects the hardness of the corresponding discrete logarithm problem. When the characteristic is small, the recent breakthrough algorithms to solve DLP run in heuristic quasi-polynomial time [3,11,12]. When the characteristic is medium to high, the state-of-art fastest algorithms are still number field sieve (NFS) and its variants. They run in heuristic $L(1/3)$ time, where

$$L_Q(\alpha, c) = \exp((c + o(1))(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}),$$

and Q is the cardinality of the field $\mathbb{F}_{p^n}$. For simplicity, we omit Q and c when there is no confusion.

The NFS-DL algorithm was firstly proposed by Gordon [10] and Schirokauer [27] as an adaptation of the NFS for factoring integers [21]. In 2006, Joux, Lercier, Smart and Vercauteren [17] presented a variant of NFS which applies to all the finite fields $\mathbb{F}_{p^n}$ of characteristic from medium to high. Let $p = L_Q(\alpha_p, c_p)$. The complexity is $L_Q(1/3, \sqrt[3]{\frac{128}{9}})$ in the medium prime case $(1/3 < c_p < 2/3)$ and $L_Q(1/3, \sqrt[3]{\frac{64}{9}})$ in the high prime case $(c_p > 2/3)$.

Briefly, NFS consists of three steps in general: polynomial selection, factor base logarithm computation, and individual logarithm computation. Note that the first two steps needs to be done only once for fixed finite field. Then one can compute logarithms of different targets based on the database of factor base elements logarithms. Also, the property of the selected polynomial affected the efficiency of the latter two steps. Further, the factor based logarithm step includes two phases: relation generation and linear algebra. The individual logarithm step includes three phases: smoothing, descent, and combination of logarithms.

1.1 Related work

Efforts have been made to improve different components of NFS-DL algorithms.

In recent years, some efficient polynomial selection methods have been proposed, such as Conjugation method [2], generalized Joux-Lercier (GJL) method [22,2], and Sarkar-Singh (SS) method [26]. They reduced the complexity in the medium prime case to $L_Q(1/3, \sqrt[3]{\frac{96}{9}})$. Especially, in the boundary case $(c_p = 2/3)$, the complexity was reduced to $L_Q(1/3, \sqrt[3]{\frac{48}{9}})$ [2]. When the characteristic has a special form [29,18] or we use multiple fields [5,23], the complexity can be further reduced.

In 2016, Kim and Barbulescu [20] presented the extended tower number field sieve (exTNFS) and achieved a new complexity in the medium prime case. When the extension degree n can factor into two coprime integers and some other conditions are satisfied, the best complexity of exTNFS in the medium prime case is $L_Q(1/3, \sqrt[3]{\frac{48}{9}})$. Later, Jeong and Kim [15] removed the coprime condition. Sarkar and Singh [25] combined the SS polynomial selection methods and exTNFS to further loosen the conditions.

Note that the polynomial selection step and factor base DL step can be computed once for a fixed finite field. If we want to compute several discrete logarithms, such as batch-DLP and delayed-target DLP, the complexity of the individual logarithm step plays an important role. For instance, the Logjam attack [1] against the real-world Diffie-Hellman key exchange protocol highlights the necessity of faster individual DL method. In Asiacrypt 2015, Guillevic [13] took advantage of the subfield structure and reduced the complexity of the smoothing phase in individual logarithm step. The improvement is significant especially when n is small.

1.2 Our contribution

In this paper, we aim at speeding up the smoothing phase further. Our method is a combination of exTNFS and generalization of Guillevic's idea. The main technique is to make full usage of the subfield structure.

Let the target finite field be $\mathbb{F}_{p^n}$ with cardinality Q. Assume m is the largest factor of n and ℓ is the largest prime factor of $\#\mathbb{F}_{p^n}^\times$. Let s be a random element in $\mathbb{F}_{p^n}$ other than in a proper subfield of $\mathbb{F}_{p^n}$ (otherwise, the DLP w.r.t s will be much easier). Let K_f be the number field where the smoothing phase will be done.

Theorem 1. *In the high prime case, i.e. $c_p > 2/3$, there exists an element* s' *in* K_f *with norm bounded by* $O(Q^{1-\frac{m}{n}})$ *such that* $\log s' \equiv \log s \mod \ell$.

Theorem 2. *In the medium prime or boundary case, i.e.* $1/3 < c_p \leq 2/3$*, there also exists an element* $\mathbf{s}'$ *in* K_f *with norm bounded by* $O(Q^{1-\frac{m}{n}})$ *such that* $\log s' \equiv \log s \mod \ell$*, if one of the following conditions holds:*

(1) there is no $k|n$ *s.t.* $p^k = L_Q(2/3)$*;*
(2) $p^m = L_Q(2/3)$*;*
(3) K_f *satisfies the conditions in Lemma 4.*

For the remaining minor case, there exists an element $\mathbf{s}'$ *with norm bounded by*

$$\begin{cases} O(Q^{1-\frac{2k}{n}}), \text{ if } \mathbb{F}_{p^n} \text{ satisfies the conditions in Lemma 3} \\ O(Q^{1-\frac{k}{n}}), \text{ otherwise} \end{cases}$$

When n is composite, the previous best result is $1 - 2/n$. Here, our result is $1 - m/n$, where m is the largest factor of n.

Remark 1. Very recently, Guillevic [14] has independently improved the individual discrete logarithm step by exploring the subfield structure. Our result is essentially the same as Guillevic's result when the characteristic is medium or large. However, there are some differences between the two methods:

- Since exTNFS performs better than traditional NFS when the extension degree is composite, we base our work on exTNFS. Guillevic's approach works also in the traditional NFS method.
- Although the basic idea of our work and Guillevic's work is to take usage of the largest subfield, the details differ. Particularly, in our work, we construct the subfield explicitly according to the exTNFS method; while in Guillevic's method, a different approach is taken to construct a polynomial basis of such subfield.

The rest of the paper is organized as follows. In Section 2, we introduce the extended tower number field sieve and Guillevic's work in Asiacrypt 15. In Section 3, we give the main idea of our improvement by taking advantage of the exTNFS. In Section 4, we give a careful analysis to illustrate how our method operate in different cases. In Section 5, we give some numerical experiments to illustrate our method. In Section 6, we conclude the paper.

2 Preliminaries

2.1 The extended Tower Number Field Sieve

The tower number field sieve was first introduced by [28], and then rehabilitated by [4], and extended by [20]. Here, we briefly recall the exTNFS algorithm.

Setup. Let the target field be $\mathbb{F}_Q$, where $Q = p^n$ and $p = L_Q(\alpha_p, c_p)$ with $\alpha_p > 1/3$. Assume $n = n_1 n_2$. Unlike the classical NFS algorithms, which usually involve two number fields over rational fields $\mathbb{Q}$, here in (extended) TNFS, we consider two field extensions over a number field. That is

$$\begin{tikzcd} K_f \arrow[dr, dash, "f"'] & & K_g \arrow[dl, dash, "g"] \\ & \mathbb{Q}(r) \arrow[d, dash, "h"'] & \\ & \mathbb{Q} & \end{tikzcd}$$

In this tower number field extension, $\mathbb{Q}(r)$ is a number field over $\mathbb{Q}$ by a monic irreducible polynomial h of degree n_1 with integer coefficients. K_f and K_g are two number fields above $\mathbb{Q}(r)$ defined by irreducible polynomials f and g over a ring R, where $R = \mathbb{Z}[r]/h(r)$. Compared with the classical NFS algorithms, in extended TNFS we can freely choose suitable number field $\mathbb{Q}(r)$ as the base field.

Using NFS algorithms to solve DLP in finite fields, we need to establish relations between the number fields and the target finite fields. To this end, we need that h remains irreducible modulo p such that p is inertia in R and $R/pR \cong \mathbb{F}_{p^{n_1}}$. We also need the following commutative diagram

$$\begin{tikzcd} & R[x] \arrow[dl] \arrow[dr] & \\ R[x]/\langle f(x)\rangle \arrow[dr, "\substack{\text{mod } p \\ \text{mod } \psi(x)}"'] & & R[x]/\langle g(x)\rangle \arrow[dl, "\substack{\text{mod } p \\ \text{mod } \psi(x)}"] \\ & (R/pR)[x]/\langle \psi(x)\rangle & \end{tikzcd}$$

to hold, where $\psi(x)$ is the common factor of f and g over R/pR of degree n_2. To obtain the target finite field, $(R/pR)[x]/\langle\psi(x)\rangle$ needs to be isomorphic to $\mathbb{F}_{p^n}$. In this case, $(R/pR)[x]/\langle\psi(x)\rangle$ is isomorphic to $\mathbb{F}_{p^n}$, and we can view $\mathbb{F}_{p^{n_1}}$ as $\mathbb{F}_p$ and n_2 as n comparing to the classical case.

Polynomial selection. The complexity of recent NFS algorithm and its variants highly rely on the size of the coefficients of the defining polynomials. To reduce the complexity, we have to select f, g and h with the coefficients as small as possible. To this end, we select h to be a polynomial over $\mathbb{Z}$ of degree n_1 and irreducible modulo p with coefficients of constant bound. Heuristically, we can find a suitable h with $||h||_\infty = 1$.

To select suitable f and g, which is similar to the classical case, there are several effective methods [17,22,2,26]. The Table 1 lists the results.

These results can be modified to adapt for exTNFS by replacing n by n_2 and Q by p^{n_2}. Another difference need to note is that the common factor of f and g is require to be irreducible over $\mathbb{F}_{p^{n_1}}$ other than $\mathbb{F}_p$.

For medium prime and boundary case, we can use JLSV_1 and Conjugation methods. For high prime case, we can use JLSV_2 and GJL methods. The SS is a generalization of Conjugation and GJL which relies on the existence of nontrivial subfields.

Table 1. The polynomial selection methods for NFS, where f and g are irreducible over $\mathbb{Z}$ with a common factor modulo p of degree n.

Method	$\deg f$	$\deg g$	$\|\|f\|\|_\infty$	$\|\|g\|\|_\infty$
JLSV_1[17]	n	n	$O(Q^{1/2n})$	$O(Q^{1/2n})$
$\mathrm{JLSV}_2(D \geq n)$[17]	n	D	$O(Q^{1/D+1})$	$O(Q^{1/D+1})$
Conj.[2]	$2n$	n	$O(\log p)$	$O(Q^{1/2n})$
$\mathrm{GJL}(D \geq n)$[22,2]	$D+1$	D	$O(\log p)$	$O(Q^{1/(D+1)})$
$\mathrm{SS}(e \mid n, d \geq n/e)$[26]	$e(d+1)$	de	$O(\log p)$	$O(Q^{1/e(d+1)})$

Relation collection and linear algebra. In the classical NFS, we need to sieve polynomials of degree $t-1$ in the medium prime case, where t satisfies $p^t = L_Q(2/3)$. While in the boundary or high prime case, simply taking t to be 2 is enough. The large value of t is the main reason that the complexity of NFS in the medium characteristic case is higher than that in the boundary or large characteristic case. We will give details for this in section 4.1. Thus in the exTNFS, we set n_1, the degree of h, such that $p^{n_1} \geq L_Q(2/3)$. Then we only need to sieve the polynomials of the form $a(r) + b(r)x$, where $a(r)$ and $b(r)$ are coprime polynomials in $R = \mathbb{Z}[x]/h(x)$ of degree less than n_1.

Let α_f and α_g be the roots of f and g respectively. To keep the norm of $a(r) + b(r)\alpha_f$ (resp. $a(r) + b(r)\alpha_g$) bounded by $L_Q(2/3)$, we need to set a sieving bound A for $||a||_\infty$ and $||b||_\infty$. We say that we obtain a relation if both

$$N_f(a, b) = \mathrm{Res}_r(\mathrm{Res}_x(a(r) + b(r)x, f(x)), h(r)) \text{ and}$$
$$N_g(a, b) = \mathrm{Res}_r(\mathrm{Res}_x(a(r) + b(r)x, g(x)), h(r))$$

are B-smooth for a smooth bound B. Actually, $N_f(a, b)$ (resp. $N_g(a, b)$) is equal to $\mathrm{N}_{K_f/\mathbb{Q}}(a(r) + b(r)\alpha_f)$ (resp. $\mathrm{N}_{K_g/\mathbb{Q}}(a(r)+b(r)\alpha_g)$) up to a constant. We set the factor base to consist of B-smooth prime ideals of degree one in K_f and K_g. The cardinality of the factor base is $(2 + o(1))\frac{B}{\log B}$. In practice, we can require the field K_f (resp. K_g) to have a large automorphism group which can reduce the cardinality of the factor base [17,4].

After collecting enough relations among the factor base, we can form a sparse linear system. Using Wiedemann's algorithm [30], we solve the linear equations in time $B^{2+o(1)}$ and obtain the virtual logarithms of the elements in the factor base.

Individual logarithm. To compute the logarithm of an element in $\mathbb{F}_{p^n}^\times$, in general it requires 2 phases. The first phase is smoothing phase, in which we randomize the target element s and test for $L_Q(2/3)$-smoothness with the ECM algorithm. We repeat this process until the principal ideal generated by s factors into prime ideals of small norm. Some of the prime ideals may not be in the factor base. So in the second phase, special-$\mathfrak{q}$ descent phase, we search for a relation between the prime ideal and other smaller ideals. We continue this process recursively until they all fall in the factor base.

Complexity. To achieve the optimal complexity, we usually balance the complexities of the relation collection step and the linear algebra step. The total complexity mainly depends on the sizes of the coefficients and degrees of f and g. The Table 2 lists the results.

In [20], there is a requirement that n_1 and n_2 are coprime. Actually, it is not necessary. The coprime condition was raised merely to simplify the selection of f and g. Under this condition, we

Table 2. Complexity of exTNFS variants of the form $L_Q(1/3, \sqrt[3]{\frac{c}{9}})$.

algorithm	c	conditions
exTNFS-JLSV$_2$	64	$n_2 = o((\frac{\log Q}{\log\log Q})^{\frac{1}{3}})$
exTNFS-GJL	64	$n_2 \le (\frac{8}{3})^{-\frac{1}{3}}(\frac{\log Q}{\log\log Q})^{\frac{1}{3}})$
exTNFS-Conj.	48	$\alpha_p < 2/3$ or $\alpha_p = 2/3$ and $c_p < 12^{\frac{1}{3}}$ $n_2 = 12^{-\frac{1}{3}}(\frac{\log Q}{\log\log Q})^{\frac{1}{3}})$

only need to select f and g over $\mathbb{Z}$ instead of R. This coprime restriction can be removed, see [15]. Of course, one can combine the exTNFS and SS polynomial selection method, which can loosen the above conditions in some sense, see [25]. When the characteristic of the field has a special form and if we use multiple fields, we can also achieve some better results. Here we omit it. In section 4.1, we will interpret the key improvement of exTNFS in the aspect of complexity.

2.2 Guillevic's work in Asiacrypt 15

In this section, we will recall Guillevic's work in Asiacrypt 15. Computing an individual logarithm contain two phases, the smoothing phase and the descent phase. In the first phase, the element s is randomized and tested for $L(2/3)$-smooth with the ECM algorithm. Compared with the descent phase, the smoothing phase costs more time. The table in [13, Section 3.2] gave a survey of the complexities of the individual logarithm steps of NFS variants.

In [13], Guillevic gave the following lemma and demonstrated the relation between the complexity of smoothing phase and the target's norm.

Lemma 1. ([13]) *Let s be a random element in $\mathbb{F}_Q$. View s as a preimage of s in the number field K_f in the natural way. Assume the norm of s is bounded by $Q^e = L_Q(1, e)$. Denote the smoothness bound for s by $B' = L_Q(\alpha_{B'}, c_{B'})$. Then the lower bound of the expected running time for finding random k such that s^k is B'-smooth is $L_Q(1/3, (3e)^{1/3})$, where $\alpha_{B'} = 2/3$ and $c_{B'} = (e^2/3)^{1/3}$.*

According to the above lemma, the complexity of the smoothing phase is $L_Q(1/3, (3e)^{1/3})$ where e is the exponent of the norm bound. Thus, if one can reduce the norm bound of the target, one can reduce the complexity of the individual logarithm phase.

We remark that one can express s as the quotient of two polynomials, namely $s = \frac{z}{w}$, such that $||z||_\infty$ and $||w||_\infty$ are both $O(\sqrt{p})$. It doesn't change the complexity in theory when the polynomial selection method is Conjugation, GJL or SS method, but it is helpful in practice.

Guillevic [13] exploited the subfield structure of $\mathbb{F}_Q$ and improved the previous results. We describe the method in the following.

If $s, s' \in \mathbb{F}_{p^n}^{\times}$ and $s = u \cdot s'$ with u belonging to a proper subfield of $\mathbb{F}_{p^n}$, then

$$\log s \equiv \log s' \mod \ell,$$

where ℓ is the largest prime factor of $\#\mathbb{F}_{p^n}^{\times}$. This is because in practice we only consider the DLP in the multiplicative group of $\mathbb{F}_{p^n}^{\times}$ other than the groups of any proper subfields. Using this observation, we can take the leading term of s to be 1, i.e. $s = \sum_{i=0}^{n-1} s_i x^i \in \mathbb{F}_{p^n}$ with $s_{n-1} = 1$. Since s_i is $O(p)$ for $i \le n-2$ and $s_{n-1} = 1$, $||s||_\infty$ is $O(p)$. To reduce $||s||_\infty$ and achieve a lower norm, one can balance the coefficients of s.

In the JLSV$_1$ case, Guillevic formed the following lattice of dimension n.

$$L = \begin{pmatrix} p & & & \\ & \ddots & & \\ & & p & \\ s_0 & \dots & s_{n-2} & 1 \end{pmatrix}_{n\times n} \begin{array}{l} 0 \\ \vdots \\ n-2 \\ n-1 \end{array} \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} n-1 \text{ rows} \\ \}\text{coef. of } s \end{array}$$

Applying the LLL algorithm to L, one obtains a reduced element $s' = \sum_{i=0}^{n-1} s'_i x^i$ satisfying

$$\log s' \equiv \log s \mod \ell$$

and

$$||s'||_\infty \leq C p^{(n-1)/n},$$

where C is a small constant. According to [19], we have

$$|\operatorname{N}_{K_f/\mathbb{Q}}(s)| \leq (\deg f + \deg s)! ||f||_\infty^{\deg s} ||s||_\infty^{\deg f}. \tag{1}$$

Then the norm of s' satisfies

$$\operatorname{N}_{K_f/\mathbb{Q}}(s') = O\big(p^{\frac{3}{2}(n-1)}\big) = O\big(Q^{\frac{3}{2}-\frac{3}{2n}}\big).$$

In the GJL and Conjugation cases, let d_f denote the degree of f, where $d_f = d + 1 \geq n + 1$ in GJL case and $d_f = 2n$ in Conjugation case. And ψ is the common factor of f and g modulo p of degree of n. One can form the following lattice of dimension d_f.

$$L = \begin{pmatrix} p & & & & & & & \\ & \ddots & & & & & & \\ & & p & & & & & \\ s_0 & \dots & s_{n-2} & 1 & & & & \\ \psi_0 & \psi_1 & \cdots & \psi_{n-1} & 1 & & & \\ & \ddots & \ddots & & \ddots & \ddots & & \\ & & \psi_0 & \psi_1 & \cdots & \psi_{n-1} & 1 & \end{pmatrix}_{d_f\times d_f} \begin{array}{l} 0 \\ \vdots \\ n-2 \\ n-1 \\ n \\ \vdots \\ d_f-1 \end{array} \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} n-1 \text{ rows} \\ \}\text{coef. of } s \\ \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} d_f - n \text{ rows with coef. of } \psi \end{array}$$

Applying the LLL algorithm to L, one obtains a reduced element $s' = \sum_{i=0}^{n-1} s'_i x^i$ satisfying

$$\log s' \equiv \log s \mod \ell$$

and

$$||s'||_\infty \leq C p^{(n-1)/d_f},$$

where C is a small constant. The norm of s' satisfies

$$\operatorname{N}_{K_f/\mathbb{Q}}(s') = O\big(p^{n-1}\big) = O\big(Q^{1-1/n}\big).$$

Next, when n is even, Guillevic exploited the quadratic subfield to construct a preimage with small norm.

Lemma 2. ([13]) *Let $\psi(X)$ be a monic irreducible polynomial of $\mathbb{F}_p[X]$ of even degree n with a quadratic subfield $\mathbb{F}_{p^2} = \mathbb{F}_p[Y]/(A(Y))$. Moreover, assume that ψ splits over $\mathbb{F}_p[Y]/(A(Y))$ as*

$$\begin{aligned} &\psi(X) = (B(X) - Y)(B(X) - Y^p) \\ \textit{or}\ \ &\psi(X) = (B(X) - YX)(B(X) - Y^pX) \end{aligned}$$

with B monic, of degree $n/2$ and coefficients in $\mathbb{F}_p$. Let $s \in \mathbb{F}_p[X]/(\psi(X))$ a random element, $s = \sum_{i=0}^{n-1} s_i X^i$.

Then there exists $s' \in \mathbb{F}_{p^n}$,monic and of degree $n-2$ in X, and $u \in \mathbb{F}_{p^2}$, such that $s = u \cdot s'$ in $\mathbb{F}_{p^n}$.

According to the lemma, if the field contains a certain quadratic subfield, we can find two preimages $s = \sum_{i=0}^{n-1} s_i x^i$ and $s' = \sum_{i=0}^{n-2} s'_i x^i$. Here, a preimage means its logarithm is congruent to the logarithm of s modulo ℓ. Then we define the following lattice

$$L = \begin{array}{ccl} \begin{pmatrix} p & & & & \\ & \ddots & & & \\ & & p & & \\ s'_0 & \dots & s'_{n-3} & 1 & \\ s_0 & \dots & s_{n-3} & s_{n-2} & 1 \end{pmatrix}_{n\times n} & \begin{matrix} 0 \\ \vdots \\ n-3 \\ n-2 \\ n-1 \end{matrix} & \begin{matrix} \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} n-2 \text{ rows} \\ \} \text{ coef. of } s' \\ \} \text{ coef. of } s \end{matrix} \end{array}$$

Using it in place of the upper-left part of the lattice in the GJL and Conjugation cases, we can find a preimage with norm $O(Q^{1-2/n})$. This improvement is significant when n is small.

3 Constructing a preimage with small norm: main idea

Assume m is the largest proper factor of n, where n is the extension degree of the finite field. In this section, we will use a tower of fields to construct a preimage with norm $O(Q^{1-m/n})$. If n is even, the best result is to reduce the norm to $O(Q^{1/2})$.

Since m is the largest proper factor of n, the largest proper subfield of $\mathbb{F}_{p^n}$ is $\mathbb{F}_{p^m}$. We set the degree of h in exTNFS to be m and the degree of ψ (the common factor of f and g over $\mathbb{F}_{p^m}$) to be $n' = n/m$. Other settings are the same as section 2.1. Let d_f and d_g denote the degrees of f and g respectively.

For $s \in \mathbb{F}_{p^n}^{\times}$, each preimage of s in K_f is $\sum_{i=0}^{n'-1} s_i(r)x^i$, where $s_i(r)$ is a polynomial in r of degree less than m. When $s_{n'-1}(r) \neq 0$, dividing each term by $s_{n'-1}(r)$, we obtain a preimage of s of the form $\sum_{i=0}^{n'-2} s_i(r)x^i + x^{n'-1}$. When $s_{n'-1}(r) = 0$, we can do the same thing to the highest nonzero term and obtain a shorter form, which is more advantageous for us to reduce the norm.

Next, we form the following lattice of dimension md_f:

$$
\begin{pmatrix}
p & & & & & & & & \\
 & \ddots & & & & & & & \\
 & & p & & & & & & \\
 & & & \ddots & & & & & \\
 & & & & p & & & & \\
 & & & & & \ddots & & & \\
 & & & & & & p & & \\
\mathbf{s_0}(\mathbf{r}) & & \dots & & \mathbf{s_{n'-2}}(\mathbf{r}) & & 1 & & \\
\mathbf{r}\mathbf{s_0}(\mathbf{r}) & & \dots & & \mathbf{r}\mathbf{s_{n'-2}}(\mathbf{r}) & & & 1 & \\
\vdots & & \vdots & & \vdots & & & & \ddots \\
\mathbf{r^{m-1}}\mathbf{s_0}(\mathbf{r}) & & \dots & & \mathbf{r^{m-1}}\mathbf{s_{n'-2}}(\mathbf{r}) & & & & & 1 \\
\boldsymbol{\psi}_\mathbf{0}(\mathbf{r}) & & \boldsymbol{\psi}_\mathbf{1}(\mathbf{r}) & & \dots & & \boldsymbol{\psi}_\mathbf{n'-1}(\mathbf{r}) & & & & 1 \\
\mathbf{r}\boldsymbol{\psi}_\mathbf{0}(\mathbf{r}) & & \mathbf{r}\boldsymbol{\psi}_\mathbf{1}(\mathbf{r}) & & \dots & & \mathbf{r}\boldsymbol{\psi}_\mathbf{n'-1}(\mathbf{r}) & & & & & 1 \\
\vdots & & \vdots & & \vdots & & \vdots & & & & & & \ddots \\
\mathbf{r^{m-1}}\boldsymbol{\psi}_\mathbf{0}(\mathbf{r}) & & \mathbf{r^{m-1}}\boldsymbol{\psi}_\mathbf{1}(\mathbf{r}) & & \dots & & \mathbf{r^{m-1}}\boldsymbol{\psi}_\mathbf{n'-1}(\mathbf{r}) & & & & & & & 1 \\
 & & \ddots & & \ddots & & & & & & \ddots & & & & \ddots \\
 & & & & \boldsymbol{\psi}_\mathbf{0}(\mathbf{r}) & & \boldsymbol{\psi}_\mathbf{1}(\mathbf{r}) & & & & & & \boldsymbol{\psi}_\mathbf{n'-1}(\mathbf{r}) & & & 1 \\
 & & & & \mathbf{r}\boldsymbol{\psi}_\mathbf{0}(\mathbf{r}) & & \mathbf{r}\boldsymbol{\psi}_\mathbf{1}(\mathbf{r}) & & & & \dots & & \mathbf{r}\boldsymbol{\psi}_\mathbf{n'-1}(\mathbf{r}) & & & & 1 \\
 & & & & \vdots & & \vdots & & & & & & \vdots & & & & & \ddots \\
 & & & & \mathbf{r^{m-1}}\boldsymbol{\psi}_\mathbf{0}(\mathbf{r}) & & \mathbf{r^{m-1}}\boldsymbol{\psi}_\mathbf{1}(\mathbf{r}) & & & & & & \mathbf{r^{m-1}}\boldsymbol{\psi}_\mathbf{n'-1}(\mathbf{r}) & & & & & & 1
\end{pmatrix}
$$

where the algebraic numbers in bold stand for the row vectors of their coordinates. Applying the LLL algorithm to the lattice, we obtain a reduced element $s' = \sum_{i=0}^{d_f-1} s'_i(r)x^i$ with

$$\log s' \equiv \log s \mod \ell.$$

Since the determinant of the lattice is $p^{m(n'-1)} = p^{n-m}$ and the dimension is md_f, we have

$$||s'||_\infty \le Cp^{\frac{n-m}{md_f}},$$

where C is a small constant. According to [19,6], we have

$$\mathrm{N}_{K_f/\mathbb{Q}}(s') = O\big(||s'||_\infty^{md_f}||f||_\infty^{md_{s'}}\big).$$

The value is

$$O\big(Q^{1-m/n}\big)$$

in Conjugation, GJL or SS case, since the coefficients of f in these cases are small. In JLSV_1 and JLSV_2 cases, they are

$$O\big(Q^{3/2-m/n}\big) \text{ and } O\big(Q^{2-m/n}\big)$$

respectively.

Thus, if there is no restriction on the degree of h, following the method above, we can construct a preimage of target element with norm $O\big(Q^{1-m/n}\big)$, where m is the largest factor of n. Especially, when n is even, we can construct a preimage with norm $O\big(Q^{1/2}\big)$. Then the complexity of the smoothing phase is reduced to $L_Q(1/3, \sqrt[3]{\frac{3}{2}})$.

However, in exTNFS, to achieve the optimal complexity, there are some restrictions on the choice of $\deg(h)$. In the next section, we will analyze the restriction on h and show how to reduce the norm to $O\big(Q^{1-m/n}\big)$ while maintain the total complexity.

4 Constructing a preimage with small norm: more details

4.1 A brief analysis to recent results about exTNFS

In this section, we revisit the relation between $\deg(h)$ and the complexity of the exTNFS algorithm to obtain the range for the choice of $\deg h$.

In exTNFS, we pick $m|n$ such that $p^m = L_Q(\alpha_q, c_q)$, where $\alpha_q \geq \frac{2}{3}$. Then $n' = \frac{1}{c_q}(\frac{\log Q}{\log\log Q})^{1-\alpha_q}$. Intuitively, we can view $q = p^m$ as a new p and n' as a new n. Other things are very similar.

For a more general analysis, we assume we sieve polynomials of degree $t-1$, denoted by $\phi(x) = a_0(r) + a_1(r)x + \cdots + a_{t-1}(r)x^{t-1}$. We set the smooth bound $B = L_Q(1/3, c_b)$ and the sieving bound A such that $A^{mt} = L_Q(1/3, c_a)$. Since $p^m \geq L_Q(2/3)$, the degree of f and g should be compared with $(\frac{\log Q}{\log\log Q})^{\frac{1}{3}}$. We let $d = c_d(\frac{\log Q}{\log\log Q})^{\frac{1}{3}}$. In the relation collection step, we will sieve different $\phi(x)$ within the sieving bound A. It costs A^{mt} time. The cardinality of the factor base is about $(2+o(1))\frac{B}{\log B}$. It follows that the linear algebra step will cost about B^2 time. To balance the complexities of the first two steps, we need

$$A^{mt} = B^2. \tag{2}$$

To collect enough relations, we need obtain at least B relations in the first step, namely

$$A^{mt}\mathcal{P} = B, \tag{3}$$

where $\mathcal{P}$ denote the probability to collect a relation of a random polynomial ϕ.

The probability to collect a relation relies on the norms of ϕ both in K_f and K_g. We let

$$\begin{aligned} N_f(\phi) &= \mathrm{Res}_r(\mathrm{Res}_x(\phi(x), f(x)), h(r)) \text{ and} \\ N_g(\phi) &= \mathrm{Res}_r(\mathrm{Res}_x(\phi(x), g(x)), h(r)). \end{aligned}$$

According to [19,6], similar to [4,20], we have

$$\begin{aligned} |N_f(\phi)\cdot N_g(\phi)| &\leq C(m,t,d_f,d_g)||f||_\infty^{m(t-1)}A^{md_f}||g||_\infty^{m(t-1)}A^{md_g} \\ &= C(m,t,d_f,d_g)(||f||_\infty||g||_\infty)^{m(t-1)}A^{m(d_f+d_g)}, \end{aligned}$$

where $C(m,t,d_f,d_g)$ is a function in m,t,d_f and d_g with value negligible to $L_Q(2/3)$. In conjugation, GJL or SS method, which are the recent best polynomial selection methods, the coefficients of f are $O(\log p)$ and those of g are $O(p^{n'/d_f})$. For a more general result, we assume the coefficients of g are $O(p^{n'/n_g})$, where n_g is compared with d_f. Thus, we have

$$\begin{aligned} |N_f(\phi)\cdot N_g(\phi)| &\leq (||g||_\infty)^{m(t-1)}A^{m(d_f+d_g)}, \\ &= Q^{\frac{t-1}{n_g}}A^{mtd\frac{d_f+d_g}{td}}, \\ &= L_Q(2/3, \frac{(t-1)d}{c_d n_g})L_Q(2/3, \frac{c_a c_d(d_f+d_g)}{td}), \\ &= L_Q(2/3, \frac{(t-1)d}{c_d n_g} + \frac{c_a c_d(d_f+d_g)}{td}). \end{aligned}$$

According to [8], $\mathcal{P}$, the B-smooth probability satisfies

$$1/\mathcal{P} = L_Q(1/3, \frac{1}{3c_b}\cdot(\frac{(t-1)d}{c_d n_g} + \frac{c_a c_d(d_f+d_g)}{td})).$$

According to Equation (2) and (3), we obtain

$$c_a = 2c_b,$$

and

$$B = 1/\mathcal{P}.$$

Thus combining above equations, we have

$$\begin{aligned} 3c_b^2 &= \frac{(t-1)d}{c_d n_g} + \frac{2c_b c_d(d_f + d_g)}{td} \\ &\geq 2\sqrt{2c_b \frac{t-1}{t}\frac{d_f + d_g}{n_g}}. \end{aligned}$$

It follows that $9c_b^3 \geq 8\frac{t-1}{t}\frac{d_f+d_g}{n_g}$. Hence the total complexity is

$$L_Q(1/3, 2c_b) = L_Q(1/3, \sqrt[3]{\frac{c}{9}}),$$

where

$$c = 72c_b^3 \geq 64\frac{t-1}{t}\frac{d_f+d_g}{n_g}.$$

In classic NFS, we can achieve the analogous result by similar deduction. Let's first pay attention to the term $\frac{t-1}{t}$. Here in exTNFS, we can let $t = 2$ to achieve the best result provided $p^m \geq L_Q(2/3)$. However in classic NFS, when $p < L_Q(2/3)$, t will be much bigger and $\frac{t-1}{t}$ will be close to 1. This is the key improvement of exTNFS in the aspect of complexity.

For the term $\frac{d_f+d_g}{n_g}$, it depends on the polynomial selection methods. When $p^m = L_Q(2/3)$, the best result is $\frac{3}{2}$ achieved by Conjugation or SS method. In this case, the total complexity is $L_Q(1/3, \sqrt[3]{\frac{48}{9}})$. However, when $p^m > L_Q(2/3)$ we cannot apply Conjugation method. The Table 1 shows the minimal value for $\frac{d_f+d_g}{n_g}$ is 2 achieved by GJL or SS method. Then the total complexity is $L_Q(1/3, \sqrt[3]{\frac{64}{9}})$.

Based on the analysis above, in the rest of the paper we only discuss the Conjugation, GJL and SS polynomial selection methods, since they are more efficient. When $p^m = L_Q(2/3)$, we use Conjugation and SS methods. When $p^m > L_Q(2/3)$, we use GJL and SS methods.

Also, the analysis can be applied to special NFS and its variants, since their essential advantages are that we can select polynomials with smaller coefficients due to the special form of the characteristic.

4.2 Reducing the norm in different cases

Let's go back to the remaining problem in section 3. We deal with it in two main cases. Let m be the largest proper factor of n.

Case 1 $p^m = L_Q(2/3)$ or there is no factor k of n such that $p^k = L_Q(2/3)$.

In this case, when $p^m \geq L_Q(2/3)$, we follow the strategy in the previous section. We can reduce the norm to $O\big(Q^{1-m/n}\big)$ while maintaining the total complexity. When $p^m < L_Q(2/3)$, we claim that m must be equal to 1 and n is a prime. Since $p \geq L_Q(1/3)$ and $p^n = L_Q(1)$, if n is composite, then $p^m \geq p^{\sqrt{n}} \geq L_Q(2/3)$, which yields a contradiction. Thus when $p^m < L_Q(2/3)$, m is equal to 1. We can use the trivial subfield $\mathbb{F}_p$ to reduce the norm to $O\big(Q^{1-m/n}\big)$.

Case 2 There is a factor k of n such that $p^k = L_Q(2/3)$ and $p^m > L_Q(2/3)$.

Let $q = p^k$ and $n'' = n/k$. In this case, we need to set $\deg(h)$ to be k, and f, g to have a common irreducible factor ψ of degree n'' over $\mathbb{F}_q$. Then we can achieve the $L_Q(1/3, \sqrt[3]{\frac{48}{9}})$ complexity by exTNFS algorithm. Note that, in this case, if we use the subfield $\mathbb{F}_q$, we can only reduce the norm to $O\big(Q^{1-k/n}\big)$ other than $O\big(Q^{1-m/n}\big)$.

Firstly, we give a generalized version of the Lemma 2 to obtain a slightly better result.

Lemma 3. *Assume there is a proper subfield $\mathbb{F}_{q^\lambda} = \mathbb{F}_q[Y]/A(Y)$ of $\mathbb{F}_{q^{n''}}$ with $\lambda > 1$ such that ψ splits over $\mathbb{F}_{q^\lambda}$ as*

$$\psi(X) = \prod_{i=0}^{\lambda-1}(B(X) - Y^{q^i}),$$

where $B(X)$ is a polynomial of degree n''/λ with coefficients in F_q. Let $s = \sum_{i=0}^{n''-1} s_i X^i$ be a random element in $\mathbb{F}_q[X]/\psi(X)$. We can find an element s' in $\mathbb{F}_q[X]/\psi(X)$ of degree at most $n''-2$ satisfying $s = u \cdot s'$ with $u \in \mathbb{F}_{q^\lambda}$.

Proof. The proof is similar. We set the tower of fields as follows.

$$\begin{array}{c}
\mathbb{F}_{q^{n''}} = \mathbb{F}_q[X]/\psi(X) = \mathbb{F}_q[X,Y]/(A(Y), B(X) - Y) \\
\Big| \\
\mathbb{F}_{q^\lambda} = \mathbb{F}_q[Y]/A(Y) \\
\Big| \\
\mathbb{F}_q
\end{array}$$

We represent s as

$$s = \sum_{i=0}^{n''/\lambda-1} c_i(Y)X^i.$$

with $c_i(Y)$ of degree in Y at most $\lambda - 1$. Dividing s by $c_{n''/\lambda-1}(Y)(\in \mathbb{F}_{q^\lambda})$, we obtain

$$\frac{s}{c_{n''/\lambda-1}(Y)} = \sum_{i=0}^{n''/\lambda-2} d_i(Y)X^i + X^{n''/\lambda-1},$$

with $d_i(Y)$ of degree at most $\lambda - 1$. Substituting Y with $B(X)$, we obtain the right hand side is

$$\sum_{i=0}^{n''/\lambda-2} d_i(B(X))X^i + X^{n''/\lambda-1},$$

which is of degree at most $\frac{n''}{\lambda}(\lambda-1)+\frac{n''}{\lambda}-2=n''-2$. $\square$

Following the lemma, if the field has certain form, we can construct a preimage of degree at most $n''-2$. Then we can apply the LLL algorithm to obtain a preimage of norm $O\big(Q^{1-2k/n}\big)$.

Next, we will show if some requirements for K_f can be met, we can construct a preimage with norm $O\big(Q^{1-m/n}\big)$.

Note that since k, the degree of h, satisfies $p^k=L_Q(2/3)$, we should use Conjugation method or SS method for polynomial selection. For simplicity, we consider the Conjugation method case while the other case is similar. In this case, the degree of f is $2n/k=2n''$.

Lemma 4. *Let $K_f=\mathbb{Q}(r)[X]/f(X)=\mathbb{Q}(r,x)$. Assume there is a subfield $\mathbb{Q}(r,y)\subseteq K_f$ of index $2n'$ such that the coefficients of the minimal polynomials of y over $\mathbb{Q}(r)$ and x over $\mathbb{Q}(r,y)$ are both small, i.e. are bounded by $O(\log p)$. Let s be a random element in $\mathbb{F}_{p^n}$. We can construct a preimage of s in K_f with norm $O\big(Q^{1-m/n}\big)$.*

Proof. Under this condition, we can view K_f as the extension field of $\mathbb{Q}(r,y)$ by adding x and $\mathbb{Q}(r,y)$ as the extension field of $\mathbb{Q}(r)$ by adding y. Every element s in K_f can also be expressed as

$$\tilde{s}=\sum_{i=0}^{n'-1}\tilde{s}_i(r,y)x^i$$

where we use $\tilde{s}$ to denote s in this expression. Note that, although $\tilde{s}$ and s are the same element in K_f, $||\tilde{s}||_\infty$ and $||s||_\infty$ are totally different.

Since the coefficients of the minimal polynomials of x and y are small, one can check the norm of s will be

$$\mathrm{N}_{K_f/\mathbb{Q}}(s)=\mathrm{N}_{K_f/\mathbb{Q}}(\tilde{s})=O\big(||\tilde{s}||_\infty^{md_f}\big),$$

whose form is the same as before.

Now, let $\tilde{s}\in K_f$ be a preimage of an element in $\mathbb{F}_Q$. Assume $\tilde{s}=\sum_{i=0}^{n'-1}\tilde{s}_i(r,y)x^i$ with $\tilde{s}_{n'-1}(r,y)\neq 0$. We divide each term by $\tilde{s}_{n'-1}(r,y)$, and obtain

$$\tilde{s'}=\sum_{i=0}^{n'-1}\tilde{s'}_i(r,y)x^i+x^{n'-1}.$$

We can view it as a polynomial in x and y with coefficients in r. Then we can construct a vector whose components are the coefficients of y^ix^j. If we use the vector to replace the corresponding row of the lattice in section 3 and change the expression of ψ, then we can form a new lattice. Applying the LLL algorithm to the lattice, we can obtain a preimage $\tilde{s''}$ with

$$||\tilde{s''}||_\infty\leq Cp^{\frac{n-m}{md_f}}.$$

Thus the norm of $\tilde{s''}$ is bounded by $O\big(Q^{1-m/n}\big)$. $\square$

We give an example in which the condition are satisfied. We consider the finite field $\mathbb{F}_{p^{30}}$, where $p=3961408125713216879677197517$7. The largest proper factor of 30 is 15. If we set $\deg(h)=5$, we should set $\deg(f)=12$ in Conjugation method. Since 5 and 12 are coprime, it is sufficient to select f over $\mathbb{Z}$. Firstly, we choose two small coefficients polynomial x^6-1 and x^3. Next, we choose the irreducible polynomial Y^2+1 over $\mathbb{Z}$ which has a root modulo p. Let $f = \mathrm{Res}_Y(Y^2+1, x^6-1-x^3Y) = x^12-x^6+1$. One can check f is irreducible over $\mathbb{Z}$ and thus has a degree 6 irreducible factor modulo p. Let y be a root of the equation y^3-3y+1. One can check f splits into 3 irreducible factor over $\mathbb{Q}(y)$. One of the factor is x^4+yx^2+1 with small coefficients. Hence in this example, the conditions in Lemma 4 are all satisfied.

We summarize the results in the Table 4.2.

Table 3. The norm bound of the preimage and the complexity of the smoothing phase. The polynomial selection method we use is Conjugation, GJL or SS method depending on the target field. Assume m is the largest factor of n.

Conditions	Norm bound	Smoothing phase $L_Q(\frac{1}{3}, c)$ c in this work
$p^m = L_Q(2/3)$ or no $k\|n$ s.t. $p^k = L_Q(2/3)$	$Q^{1-m/n}$	$(3(1-\frac{m}{n}))^{1/3}$
otherwise if K_f has a certain form	$Q^{1-m/n}$	$(3(1-\frac{m}{n}))^{1/3}$
else if $\mathbb{F}_{p^n}$ has a certain form	$Q^{1-2k/n}$	$(3(1-\frac{2k}{n}))^{1/3}$
the left case	$Q^{1-k/n}$	$(3(1-\frac{k}{n}))^{1/3}$

Our method is a generalization of the method in [13] and is advanced when n is composite and not very small. Especially, when n has large proper factor (or equivalently small proper factor), our method is very efficient. For example, when $2|n$, we can reduce the complexity of the smoothing phase to $L_Q(\frac{1}{3}, \sqrt[3]{\frac{3}{2}} \approx 1.14)$.

5 Numerical Experiments

In this section, we give some numerical experiments to illustrate the validity of our method. For $n = 2, 3, 4$ or 5, our results are the same as those in [13]. Here we give examples for $n = 6$ and $n = 12$.

5.1 Examples for $\mathbb{F}_{p^6}$

Example 1 for $n = 6$ with GJL method. We take a random prime number p of about 100-bit (30 decimal digit), and $n = 6$. The size of the field $\mathbb{F}_{p^6}$ is about 180 decimal digits (dd). Since largest proper factor of n is 3, we set h to be a polynomial of degree 3 with small coefficients and irreducible modulo p. Let r be a root of h. We take f to be a degree 4 irreducible polynomial over $\mathbb{Z}$ with small integer coefficients. Moreover we require that f has a degree 2 irreducible factor ψ

modulo p. Since 2 and 3 are prime, ψ is still irreducible over $\mathbb{F}_{p^3}$. At last we pick a random s in $\mathbb{F}_{p^6}$.

$$
\begin{aligned}
p =& 1267650600228229401496703205653 \\
h =& r^3 - r^2 + 1 \\
f =& x^4 + 1 \\
\psi =& x^2 + 266892166039080060530265635980 \\
g =& 81918998706487x^2 + 1122915792871022 \\
s =& (770996322275293048913407867893r^2 + 176890373159319570424980826427r + 1160569386245587035814582189227)x \\
& + 935836514622535375852962122149r^2 + 707940155816471541960680236692r + 203370792026598947471097543375
\end{aligned}
$$

with p a 31 dd prime number and p^6 of 181 dd.

Taking $s' = \frac{1}{s_1}s$, we have

$$
s' = x + 903148587808476041011875748734r^2 + 1258489317074214699144650431856r + 922893237103555904448793411796.
$$

We use LLL algorithm to reduce the lattice

$$
\begin{pmatrix}
p &&&&&&&&&&& \\
& p &&&&&&&&&& \\
&& p &&&&&&&&& \\
\mathbf{s'_0} &&& 1 &&&&&&&& \\
\mathbf{rs'_0} &&&& 1 &&&&&&& \\
\mathbf{r^2s'_0} &&&&& 1 &&&&&& \\
\boldsymbol{\psi_0} &&&&&& 1 &&&&& \\
\mathbf{r}\boldsymbol{\psi_0} &&& \mathbf{0} &&&& 1 &&&& \\
\mathbf{r^2}\boldsymbol{\psi_0} &&&&&&&& 1 &&& \\
&&& \boldsymbol{\psi_0} &&&&&& 1 && \\
&&& \mathbf{r}\boldsymbol{\psi_0} &&& \mathbf{0} &&&& 1 & \\
&&& \mathbf{r^2}\boldsymbol{\psi_0} &&&&&&&& 1
\end{pmatrix}
$$

The returned short element s'' is

$$
\begin{aligned}
&(-654596r^2 - 25066478r + 8079577)x^3 + (7089818r^2 + 1960648r + 1047289)x^2 + \\
&(5995809r^2 - 9170200r - 9594102)x + 26292350r^2 - 7675630r + 1535300,
\end{aligned}
$$

with coefficient at most 8 dd. Its norm is

$$
\mathrm{N}_{K_f/\mathbb{Q}}(s'') = 4248798334960557244412392769828417173736921202329989260540205222267760951710588002882574241
$$

which is a 91 dd number. Its length is about $91/181 \approx 0.502$ of that of p^6, as expect.

Example 2 for $n = 6$ with Conjugation method. We take another random prime number p of about 30 dd. We select h in the same way. Let r be a root of h. Using Conjugation method. We take a degree 2 irreducible polynomial Y^2+1 which has a root y modulo p. Let $f = \mathrm{Res}_Y(Y^2+1, x^2+Y)$.

Then f is irreducible over $\mathbb{Z}$ and has an irreducible factor $\psi(x) = x^2 - y$ over $\mathbb{F}_p$.

$$
\begin{aligned}
p =& 7170914684772626399787694948453 \\
h =& r^3 + r + 1 \\
f =& x^4 + 1 \\
\psi =& x^2 + 294838925512229337898309576527 \\
g =& 966642759457218x^2 + 2497301836054577 \\
s =& (2767660019267865248076151275104r^2 + 357970798563045003813528394260r + 6311123219907587664235529021977)x \\
& + 2234776892532612450942592349739r^2 + 5963032404036223471843728113344r + 2280716845436119385331170350884
\end{aligned}
$$

with p a 31 dd prime number and p^6 of 186 dd.

Taking $s' = \frac{1}{s_1}s$, we have

$$
s' = x + 6829187035664634928218051355972r^2 + 2356513401811425063371831680423x + 7055298630876009777096508302136.
$$

Since ψ doesn't have degree 1 term, we form a similar lattice in Example 1. Here we omit it. We use LLL algorithm to reduce the lattice and the returned short element s'' is

$$
\begin{aligned}
&(-243030r^2 - 1609858r - 14170476)x^3 + (17026360r^2 + 19611969r + 40385280)x^2 + \\
&(-21368270r^2 - 25460768r + 45578231)x + 4785869r^2 - 5442349r - 3676839,
\end{aligned}
$$

with coefficient at most 8 dd. Its norm is

$$
\mathrm{N}_{K_f/\mathbb{Q}}(s'') = 9408692079257501461183742234523910224598901984786177574687834188371565707188019033831132562049,
$$

which is a 94 dd number. Its length is $94/186 \approx 0.505$ of that of p^6.

5.2 Examples for $\mathbb{F}_{p^{12}}$

Example 3 for $n = 12$ with GJL method. In this example, we consider the case for $n = 12$. We want to take a 600-bit finite field. Then the characteristic p will be about 15 dd. The largest proper factor of n is 6, we set h to be a polynomial of degree 6 with small coefficients and irreducible modulo p. Let r be a root of h and R be the ring $\mathbb{Z}[r]$. We take f to be a degree 4 irreducible polynomial over R with small coefficients. Moreover we require that f has degree 2 irreducible factor ψ over $\mathbb{F}_{p^6}$. At last, we randomly pick an element s in $\mathbb{F}_{p^6}$.

$$
\begin{aligned}
p =& 2251799813685269 \\
h =& r^6 + r - 1 \\
f =& x^4 + r \\
\psi =& x^2 + 1993972645314362r^5 + 2014524994046034r^4 + 775349557393539r^3 + 2239410057339674r^2 + 1611508501046572r + 723760306664988 \\
s =& (664609958516367r^5 + 696970620962968r^4 + 772196105657867r^3 + 663786159251904r^2 + 1018587115350r + 871785303785789)x \\
& + 1254825522464853r^5 + 163391769589048r^4 + 1440697992754427r^3 + 833042729041497r^2 + 1146684997003032r + 2084950047673640
\end{aligned}
$$

with p a 16 dd prime number and p^{12} of 185 dd. Here we omit the expression of g, since our computation doesn't involve g.

Taking $s' = \frac{1}{s_1}s$, we have

$$s' = x + 234049405977480r^5 + 1765403141103884r^4 + 630709406564539r^3 + 176355858132932r^2 + 1701204684849980r + 1626756316867936.$$

We use LLL algorithm to reduce the lattice

$$\begin{pmatrix}
p & & & & & & & & & \\
 & \ddots & & & & & & & & \\
 & & p & & & & & & & \\
\mathbf{s_0'} & & & 1 & & & & & & \\
\vdots & & & & \ddots & & & & & \\
\mathbf{r^5 s_0'} & & & & & 1 & & & & \\
\psi_{\mathbf{0}} & & & & & & 1 & & & \\
\vdots & & \mathbf{0} & & & & & \ddots & & \\
\mathbf{r^5}\psi_{\mathbf{0}} & & & & & & & & 1 & \\
 & & \psi_{\mathbf{0}} & & & & & & & 1 \\
 & & \vdots & & \mathbf{0} & & & & & \ddots \\
 & & \mathbf{r^5}\psi_{\mathbf{0}} & & & & & & & 1
\end{pmatrix}$$

The returned short element s'' is

$(-7r^5 - 2614r^4 - 222r^3 + 4628r^2 + 312r - 709)x^3 + (-4300r^5 - 4266r^4 + 3920r^3 + 1798r^2 + 707r - 2828)x^2 +$
$(2175r^5 + 562r^4 - 2736r^3 + 1424r^2 + 101r + 4279)x + 1177r^5 + 1899r^4 + 1716r^3 + 2547r^2 + 617r - 4199$

with coefficient at most 4 dd. Its norm is

$$\mathrm{N}_{K_f/\mathbb{Q}}(s'') = 372487549410149008233968185650362611811865648277418284310197911695670133050753371949466198397479,$$

which is a 96 dd number. Its length is $96/185 \approx 0.519$ of that of p^{12}.

Example 4 for $n = 12$ with Conjugation method. We take n, p, h the same as Example 3. We use Conjugation method to select another f. We take the degree 2 irreducible polynomial $Y^2 + r + 1$ over R which has a root y modulo p. Let $f = \mathrm{Res}_Y(Y^2 + r + 1, x^2 + Y)$. Then f is irreducible over R have an irreducible factor $\psi(x) = x^2 - y$ over $\mathbb{F}_{p^6}$.

$$\begin{aligned}
p =& 2251799813685269 \\
h =& r^6 + r - 1 \\
f =& x^4 + r + 1 \\
\psi =& x^2 + 1393011884796690r^5 + 59969310637491r^4 + 919511363925453r^3 + 1390071113864919r^2 + 527241010054474r + 206790248742725 \\
s =& (675688506111714r^5 + 71129290300099r^4 + 557484538944572r^3 + 1005641832848766r^2 + 1890428537462931r + 1965692533792037)x \\
& + 939495520213432r^5 + 2062172030826571r^4 + 497471116144056r^3 + 2030726831698333r^2 + 1437854873482680r + 1015489052888070.
\end{aligned}$$

Taking $s' = \frac{1}{s_1}s$, we have

$$s' = x + 1393011884796690x^5 + 59969310637491x^4 + 919511363925453x^3 + 1390071113864919x^2 + 527241010054474x + 206790248742725.$$

We form a similar lattice in Example 3 and use LLL algorithm to reduce the lattice and the returned short element s'' is

$$(659r^5 + 1992r^4 + 4052r^3 - 955r^2 - 2736r - 924)x^3 + (-1727r^5 + 45r^4 - 1026r^3 + 378r^2 + 4423r - 2048)x^2 + (64r^5 + 2363r^4 + 757r^3 - 268r^2 - 1412r - 2056)x + 2352r^5 - 981r^4 - 2777r^3 + 2597r^2 + 1979r - 3266$$

with coefficient at most 4 dd. Its norm is

$$\mathrm{N}_{K_f/\mathbb{Q}}(s'') = 43137934863912977025654160952364206725911654116936172192844546482651273856814881962231733469551,$$

which is a 95 dd number. Its length is $95/185 \approx 0.514$ of that of p^{12}.

We summarize our experimental results in the following table.

Table 4. The experimental results.

Extension degree	experiments	exponent of the target's norm Q^e	ideal values in [13]
$n = 6$	1	0.502	2/3
	2	0.505	
$n = 12$	3	0.519	5/6
	4	0.514	

Our experimental values are close to the theoretical value 1/2, which is better than the values in [13].

6 Conclusion

In this work, we improve the individual logarithm computation in NFS-DL algorithm by combining the exTNFS and generalizing Guillevic's idea to explore subfield structure. Our method can construct a preimage of the target element with norm $O(Q^{1-m/n})$ in most cases when the characteristic is medium to large. Also we give experimental results to confirm our theoretical results. Due to our results, when n has relatively large proper factor, the complexity of the smoothing phase will be reduced below that of special-$\mathfrak{q}$ phase. Then the key to further reduce the complexity of the individual logarithm step may turn to find new improvements on the special-$\mathfrak{q}$ phase.

References

1. Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J.A., Heninger, N., Springall, D., Thomé, E., Valenta, L., et al.: Imperfect forward secrecy: How Diffie-Hellman fails in practice. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. pp. 5–17. ACM (2015)
2. Barbulescu, R., Gaudry, P., Guillevic, A., Morain, F.: Improving NFS for the discrete logarithm problem in non-prime finite fields. In: Advances in Cryptology–EUROCRYPT 2015, pp. 129–155. Springer (2015)
3. Barbulescu, R., Gaudry, P., Joux, A., Thomé, E.: A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: Advances in Cryptology - EUROCRYPT 2014. pp. 1–16 (2014)

4. Barbulescu, R., Gaudry, P., Kleinjung, T.: The tower number field sieve. In: Advances in Cryptology–ASIACRYPT 2015, pp. 31–55. Springer (2014)
5. Barbulescu, R., Pierrot, C.: The multiple number field sieve for medium-and high-characteristic finite fields. LMS Journal of Computation and Mathematics 17(A), 230–246 (2014)
6. Bistritz, Y., Lifshitz, A.: Bounds for resultants of univariate and bivariate polynomials. Linear Algebra and its Applications 432(8), 1995–2005 (2010)
7. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. SIAM J. Comput. 32(3), 586–615 (2003)
8. Canfield, E.R., Erdös, P., Pomerance, C.: On a problem of oppenheim concerning factorisatio numerorum. Journal of Number Theory 17(1), 1–28 (1983)
9. Diffie, W., Hellman, M.E.: New directions in cryptogrphy. IEEE Transactions on Information Theory 22(6), 644–654 (1976)
10. Gordon, D.M.: Discrete logarithms in $GF(p)$ using the number field sieve. SIAM Journal on Discrete Mathematics 6(1), 124–138 (1993)
11. Granger, R., Kleinjung, T., Zumbrägel, J.: On the powers of 2. Cryptology ePrint Archive, Report 2014/300 (2014)
12. Granger, R., Kleinjung, T., Zumbrägel, J.: On the discrete logarithm problem in finite fields of fixed characteristic. arXiv:1507.01495v1 (2015)
13. Guillevic, A.: Computing individual discrete logarithms faster in $GF(p^n)$ with the NFS-DL algorithm. In: Advances in Cryptology–ASIACRYPT 2015, pp. 149–173. Springer (2015)
14. Guillevic, A.: Faster individual discrete logarithms in non-prime finite fields with the nfs and ffs algorithms. Cryptology ePrint Archive, Report 2016/684 (2016)
15. Jeong, J., Kim, T.: Extended tower number field sieve with application to finite fields of arbitrary composite extension degree. Cryptology ePrint Archive, Report 2016/526 (2016)
16. Joux, A.: A one round protocol for tripartite diffie-hellman. J. Cryptology 17(4), 263–276 (2004)
17. Joux, A., Lercier, R., Smart, N., Vercauteren, F.: The number field sieve in the medium prime case. In: Advances in Cryptology-CRYPTO 2006, pp. 326–344. Springer (2006)
18. Joux, A., Pierrot, C.: The special number field sieve in $\mathbb{F}_{p^n}$, Application to pairing-friendly constructions. In: 6th International Conference on Pairing-based Cryptography, Pairing 2013. vol. 8365, pp. 45–61. Springer International Publishing (2013)
19. Kalkbrener, M.: An upper bound on the number of monomials in determinants of sparse matrices with symbolic entries. Mathematica Pannonica 73, 82 (1997)
20. Kim, T., Barbulescu, R.: Extended tower number field sieve: A new complexity for the medium prime case. In: Advances in Cryptology–CRYPTO 2016. Springer (2016)
21. Lenstra, A.K., Jr., H.W.L., Manasse, M.S., Pollard, J.M.: The number field sieve. In: Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA. pp. 564–572 (1990)
22. Matyukhin, D.V.: Effective version of the number field sieve for discrete logarithm in a field $GF(p^k)$. Trudy po Diskretnoi Matematike 9, 121–151 (2006)
23. Pierrot, C.: The multiple number field sieve with Conjugation and Generalized Joux-Lercier methods. In: Advances in Cryptology–EUROCRYPT 2015, pp. 156–170. Springer (2015)
24. Rubin, K., Silverberg, A.: Torus-based cryptography. In: Advances in Cryptology - CRYPTO 2003. pp. 349–365 (2003)
25. Sarkar, P., Singh, S.: A generalisation of the Conjugation method for polynomial selection for the extended tower number field sieve algorithm. Cryptology ePrint Archive, Report 2016/537 (2016)
26. Sarkar, P., Singh, S.: New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields. In: Advances in Cryptology – EUROCRYPT 2016, pp. 429–458. Springer (2016)
27. Schirokauer, O.: Discrete logarithms and local units. Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 345(1676), 409–423 (1993)
28. Schirokauer, O.: Using number fields to compute logarithms in finite fields. Mathematics of Computation 69(231), 1267–1283 (2000)

29. Semaev, I.: Special prime numbers and discrete logs in finite prime fields. Mathematics of computation 71(237), 363–377 (2002)
30. Wiedemann, D.H.: Solving sparse linear equations over finite fields. Information Theory, IEEE Transactions on 32(1), 54–62 (1986)