Improvements on the Individual Logarithm Computation for Finite Fields with Composite Extension Degrees

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
[2] University of Chinese Academy of Sciences, Beijing 100049, China
zhuyuqing@iie.ac.cn, zhuangjincheng@iie.ac.cn, lvchang@iie.ac.cn, ddlin@iie.ac.cn

Abstract. The hardness of discrete logarithm problem over finite fields is the foundation of many cryptographic protocols. The state-of-art algorithms for solving the corresponding problem are number field sieve, function field sieve and quasi-polynomial time algorithm when the characteristics of the finite field are medium to large, medium-small and small, respectively. 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 two methods to improve the individual logarithm step by exploring subfield structure when the extension degree n is composite. The first method applies to the case when the characteristic is medium to large. It is based on the extended tower number field sieve (exTNFS) and the improvement is significant when n has a large proper factor. The second one applies to any characteristic case. It is a generalization of the recent technique of Guillevic. It achieves almost optimal result and the improvement is significant when $\varphi(n)/n$ is relatively small. 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

1.1 The discrete logarithm problem

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 [10], later used as an important ingredient to build torus-based [25] and pairing-based cryptographic schemes [17,9]. 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. Denote

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

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

The state-of-art algorithms for solving the corresponding problem are number field sieve (NFS) [11,28,19,22] and function field sieve (FFS) [1,2,18,5,12] when the characteristics of the finite fields are medium to large ($p > L_Q(2/3)$) and medium-small ($L_Q(0) < p < L_Q(1/3)$), respectively. In case of small characteristic ($p = L_Q(0)$), certain algorithms [5,12,13] achieve quasi-polynomial time (QPA).

Briefly, these algorithms consist of three steps in general: polynomial selection, factor base logarithm computation, and individual logarithm computation. In polynomial selection step, two suitable polynomials are selected as a setup. The property of the selected polynomials affected the efficiency of the latter two steps. In recent years, some efficient polynomial selection methods have been proposed [23,4,27]. In factor base logarithm step, the logarithms among the factor base are computed and stored in a database. For several discrete logarithms computation, such as batch-DLP and delayed-target DLP, the polynomial selection step and factor base logarithm step can be computed only once. Then the efficiency of computing an individual logarithm will be more important. For instance, the Logjam attack [3] against the real-world Diffie-Hellman key exchange protocol highlights the necessity of faster individual DL method.

1.2   Related work

The individual logarithm step includes three phases: smoothing, descent and combination of logarithms. In smoothing phase, one randomizes the target element until it splits into several smooth elements. The complexity of this phase depends on the norm of the preimage of the target element. In Asiacrypt 2015, Guillevic [14] took advantage of the subfield of degree 1 or 2 to construct a preimage with small norm. It reduced the complexity of smoothing phase significantly when n is small.

1.3   Our contribution

In this paper, we aim at speeding up the smoothing phase further. To this end, we devise two methods to explore further the idea of using the subfield structure when the extension degree is composite.

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 corresponding number field or function field where the smoothing phase will be done.

Our first method applies to the case when the characteristic is medium to large. It is based on exTNFS.

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

Theorem 2. *In the medium characteristic 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) $p^k \neq L_Q(2/3)$ for any factor k of n with $k \neq m$;
(2) K_f satisfies the conditions in Lemma 3.

2

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

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

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 [15] 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 this method of 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.

Our second result improves the recent work of Guillevic [15], which works for any characteristic finite fields.

Theorem 3. *Given a finite field of any characteristic, there exists an element $\mathbf{s}'$ in K_f with norm bounded by $O(Q^{\varphi(n)/n})$ such that $\log s' \equiv \log s \mod \ell$.*

The rest of the paper is organized as follows. In Section 2, we introduce the extended tower number field sieve and Guillevic's work at Asiacrypt 15. In Section 3, we describe our improvement by taking advantage of the exTNFS and prove Theorem 1 and Theorem 2. In Section 4, we improve Guillevic's recent work and give the proof of Theorem 3. In Section 5, we perform some numerical experiments to illustrate our two methods. In Section 6, we conclude the paper.
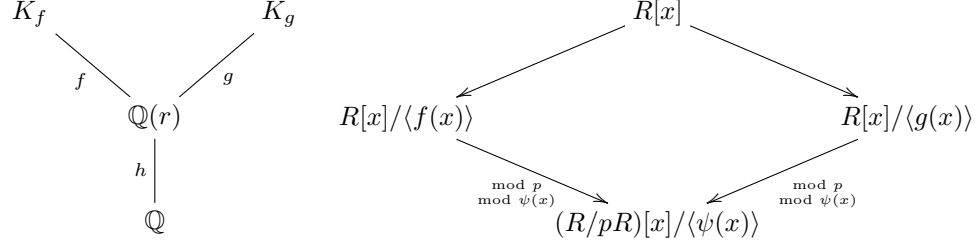
2 Preliminaries

2.1 The extended Tower Number Field Sieve

The tower number field sieve was first introduced by [29], and then rehabilitated by [6], and extended by [22]. 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 $n = n_1 n_2$. In (extended) TNFS, we consider two field extensions over a number field $\mathbb{Q}(r)$, which is defined by a monic irreducible polynomial h of degree n_1. 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 $R = \mathbb{Z}[r]/h(r)$. Moreover, we need that h remains irreducible modulo p. Then p is inertia in R and $R/pR \cong \mathbb{F}_{p^{n_1}}$. Then we have

the following commutative diagrams

$$
\begin{array}{ccc}
K_f & & K_g \\
& \searrow\,f \quad g\,\swarrow & \\
& \mathbb{Q}(r) & \\
& \downarrow\,h & \\
& \mathbb{Q} &
\end{array}
\qquad\qquad
\begin{array}{ccc}
& R[x] & \\
\swarrow & & \searrow \\
R[x]/\langle f(x)\rangle & & R[x]/\langle g(x)\rangle \\
\searrow{\scriptstyle \bmod\,p \atop \bmod\,\psi(x)} & & {\scriptstyle \bmod\,p \atop \bmod\,\psi(x)}\swarrow \\
& (R/pR)[x]/\langle \psi(x)\rangle &
\end{array}
$$

where $\psi(x)$ is the common factor of f and g over R/pR. To obtain the target finite field, the degree of $\psi(x)$ should be n_2. Hence, $(R/pR)[x]/\langle \psi(x)\rangle$ is isomorphic to $\mathbb{F}_{p^n}$.

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 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 [19,23,4,27]. Table 1 summarises the results.

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[19]	n	n	$O(Q^{1/2n})$	$O(Q^{1/2n})$
$\mathrm{JLSV}_2(D \geq n)$[19]	n	D	$O(Q^{1/D+1})$	$O(Q^{1/D+1})$
Conj.[4]	$2n$	n	$O(\log p)$	$O(Q^{1/2n})$
$\mathrm{GJL}(D \geq n)$[23,4]	$D+1$	D	$O(\log p)$	$O(Q^{1/(D+1)})$
$\mathrm{SS}(e|n, d \geq n/e)$[27]	$e(d+1)$	de	$O(\log p)$	$O(Q^{1/e(d+1)})$

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

Factor base logarithm. 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.

After collecting enough relations among the factor base, we can form a sparse linear system. Using Wiedemann's algorithm [31], 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. Table 2 summarises the results.

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	$n_2 = o\left(\left(\frac{\log Q}{\log\log Q}\right)^{\frac{1}{3}}\right)$
exTNFS-GJL	64	$n_2 \leq \left(\frac{8}{3}\right)^{-\frac{1}{3}}\left(\frac{\log Q}{\log\log Q}\right)^{\frac{1}{3}}$
exTNFS-Conj.	48	$\alpha_p < 2/3$ or $\alpha_p = 2/3$ and $c_p < 12^{\frac{1}{3}}$ $n_2 = 12^{-\frac{1}{3}}\left(\frac{\log Q}{\log\log Q}\right)^{\frac{1}{3}}$

In [22], in order to select f and g over $\mathbb{Z}$ instead of R, the degrees n_1 and n_2 are required to be coprime. This restriction can be removed, see [16]. Of course, one can combine the exTNFS and SS polynomial selection method, which can loosen the above conditions in some sense, see [26]. When the characteristic of the field has a special form [30,20] or if we use multiple fields [7,24], we can achieve better performance.

2.2 Guillevic's work at Asiacrypt 15

Assume the norm of the target element is bounded by $O(Q^e)$. Guillevic [14, Lemma 1] showed that the complexity of the smoothing phase is $L_Q(1/3, (3e)^{1/3})$. So, the main task is to construct a small norm preimage.

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 $s_{n-1} = 1$.

5

Let d_f denote the degree of f. 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.

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

$$d_f \times d_f$$

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. According to [21], we have

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

If the coefficient of f is small (e.g. Conjugation and GJL method), the norm of s' satisfies

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

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

Lemma 1. ([14]) *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*

$$\psi(X) = (B(X) - Y)(B(X) - Y^p)$$
$$or \ \ \psi(X) = (B(X) - YX)(B(X) - Y^p X)$$

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

$$
\begin{pmatrix}
p & & & & \\
& \ddots & & & \\
& & p & & \\
s_0' & \cdots & s_{n-3}' & 1 & \\
s_0 & \cdots & s_{n-3} & s_{n-2} & 1
\end{pmatrix}
\begin{matrix}
0 \\ \vdots \\ n-3 \\ n-2 \\ n-1
\end{matrix}
\begin{matrix}
\left.\vphantom{\begin{matrix}0\\\vdots\\n-3\end{matrix}}\right\} n-2 \text{ rows} \\
\} \text{ coef. of } s' \\
\} \text{ coef. of } s
\end{matrix}
$$

$$n \times n$$

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 Using exTNFS to construct a preimage

3.1 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 use exTNFS 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:

$$
\begin{pmatrix}
p & & & & & & & & & & & & \\
& \ddots & & & & & & & & & & & \\
& & p & & & & & & & & & & \\
& & & \ddots & & & & & & & & & \\
& & & & p & & & & & & & & \\
& & & & & \ddots & & & & & & & \\
& & & & & & p & & & & & & \\
& & & & & & & \ddots & & & & & \\
\mathbf{s_0(r)} & & \cdots & & \mathbf{s_{n'-2}(r)} & & 1 & & & & & & \\
\vdots & & \vdots & & \vdots & & & \ddots & & & & & \\
\mathbf{r^{m-1}s_0(r)} & & \cdots & & \mathbf{r^{m-1}s_{n'-2}(r)} & & & 1 & & & & & \\
\psi_0(r) & & \psi_1(r) & & \cdots & & & & \psi_{n'-1}(r) & 1 & & & \\
\vdots & & \vdots & & & & & & \vdots & & \ddots & & \\
\mathbf{r^{m-1}\psi_0(r)} & \mathbf{r^{m-1}\psi_1(r)} & & & \cdots & & & & \mathbf{r^{m-1}\psi_{n'-1}(r)} & & 1 & & \\
& \ddots & & & \ddots & & & & & \ddots & & \ddots & \\
& & \psi_0(r) & & \psi_1(r) & & \cdots & & \psi_{n'-1}(r) & & 1 & & \\
& & \vdots & & \vdots & & \vdots & & \vdots & & & \ddots & \\
& & \mathbf{r^{m-1}\psi_0(r)} & & \mathbf{r^{m-1}\psi_1(r)} & & \cdots & & \mathbf{r^{m-1}\psi_{n'-1}(r)} & & & & 1
\end{pmatrix}
$$

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

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

where C is a small constant. According to [21,8], we have

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

The value is

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

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

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

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 $O(Q^{1-m/n})$, where m is the largest factor of n. Especially, when n is even, we can construct a preimage with norm $O(Q^{1/2})$. 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 $\deg(h)$. Thus we first briefly recall the complexity analysis about exTNFS, then we can finish the proof of Theorem 1 and Theorem 2.

3.2 A brief analysis to recent results about exTNFS

There are lots of analysis to the complexity of the classical NFS whenever the characteristic is medium or large. Here we summarize the results of recent selection methods (GJL, Conj. and SS). One of their similarities is that they all set the coefficients of one polynomial to be small.

Let Q denote the cardinality of the target field and d_f (resp. d_g) denote the degree of f (resp. g) as before. Assume we sieve degree $t-1$ polynomials of the form $a_0 + a_1 x + \cdots + a_{t-1} x^{t-1}$. Suppose the coefficients of f is small and the coefficients of g are bounded by $O(Q^{1/n_g})$. One can check n_g is compared with d_f.

Then the best complexity will have a uniform formula

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

where

$$c = 64 \frac{t-1}{t} \frac{d_f + d_g}{n_g}.$$

This result can be directly generalized to suit for exTNFS when we alter n_g to represent the coefficients of g are bounded by $O(p^{n_2/n_g})$. Moreover, it also suits for special NFS.

From the above formula, we can see that the optimal case is $t = 2$. This can be achieved only when $p^{n_1} > L_Q(2/3)$, where n_1 is the degree of h. For the term $\frac{d_f+d_g}{n_g}$, it depends on the polynomial selection methods. When $p^{n_1} = L_Q(2/3)$, the best result is $\frac{3}{2}$ achieved by Conjugation or SS method. Then the best complexity is $L_Q(1/3, \sqrt[3]{\frac{48}{9}})$. When $p^{n_1} > L_Q(2/3)$ we cannot apply Conjugation method. The minimal value for $\frac{d_f+d_g}{n_g}$ is 2 achieved by GJL or SS method. Then the total complexity is $L_Q(1/3, \sqrt[3]{\frac{64}{9}})$, which is larger than the former case.

Thus it is sufficient to consider the case that there is $k|n$ such that $p^k = L_Q(2/3)$.

8

3.3 Reducing the norm in different cases

As before, let m be the largest proper factor of n.

If the characteristic is large, i.e. $p > L_Q(2/3)$, there is no problem. Thus we only need to consider the medium and boundary case. If $p^k \neq L_Q(2/3)$ for any factor k of n with $k \neq m$, then we can set $\deg(h)$ to be m.

For the remaining case, $\deg(h)$ should be $k < m$ and p^k is about $L_Q(2/3)$. Let $q = p^k$ and $n'' = n/k$. In this case, we need to set f, g to have a common irreducible factor ψ of degree n'' over $\mathbb{F}_q$. Note that, in this case, if we use the subfield $\mathbb{F}_q$, we can only reduce the norm to $O(Q^{1-k/n})$ other than $O(Q^{1-m/n})$.

Firstly, we give a generalized version of the Lemma 1 to obtain a slightly better result.

Lemma 2. *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.

$$\mathbb{F}_{q^{n''}} = \mathbb{F}_q[X]/\psi(X) = \mathbb{F}_q[X,Y]/(A(Y), B(X) - Y)$$

$$\Big|$$

$$\mathbb{F}_{q^\lambda} = \mathbb{F}_q[Y]/A(Y)$$

$$\Big|$$

$$\mathbb{F}_q$$

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 $\frac{n''}{\lambda}(\lambda - 1) + \frac{n''}{\lambda} - 2 = n'' - 2$. $\qquad\square$

9

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 $O(Q^{1-2k/n})$.

Next, we will show if some requirements for K_f can be met, we can construct a preimage with norm $O(Q^{1-m/n})$. 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 3. *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 $O(Q^{1-m/n})$.*

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

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

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 $y^i x^j$. 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 $O(Q^{1-m/n})$. $\qquad\square$

Example. We consider the finite field $\mathbb{F}_{p^{30}}$, where $p = $ 39614081257132168796771975177. 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 $f = \text{Res}_Y(Y^2 + 1, x^6 - 1 - x^3 Y) = x^{12} - x^6 + 1$. 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 3 are all satisfied.

Based the above discussion, we obtain the validity of Theorem 1 and Theorem 2.

4 Finding preimage with norm of exponent $\varphi(n)/n$

4.1 Guillevic's recent work

Very recently, Guillevic [15] improved the result of [14]. Guillevic exploited the primitive element of the finite field to construct a polynomial basis of the largest proper subfield. With the basis of the subfield, a preimage with smaller degree can be constructed by linear algebra. Concretely, assume s is the target element in the finite field and $\{1, u, u^2, \cdots, u^{m-1}\}$ is a polynomial basis of the largest proper subfield. Then $s, us, u^2s, \cdots, u^{m-1}s$ are different elements in the field and with the same logarithm modulo ℓ. Reducing the matrix generated by the m elements, we obtain a row-echelon form and the first row represents a degree $n - m$ element. Using this matrix, following the similar tragedy in previous section, we can construct a preimage with norm bounded by $O(Q^{1-\frac{m}{n}})$.

4.2 Further improvement

Based on the fact that a primitive element can be easily found, we can fully use the subfield to construct a preimage with the norm about $Q^{\varphi(n)/n}$. Assume the extension degree n is

$$n = \prod_{i \in I} p_i^{e_i},$$

where p_i is the distinct prime factor of n and $e_i \geq 1$. Let $n_i = n/p_i$. Then each proper subfield of $\mathbb{F}_{p^n}$ is contained in one of the subfields $\mathbb{F}_{p^{n_i}}$. We will use the these fields to construct a preimage with the norm about $Q^{\varphi(n)/n}$.

Assume the target element is s. Let $\{1, u_i, u_i^2, \cdots, u_i^{n_i-1}\}$ be a polynomial basis of $\mathbb{F}_{p^{n_i}}$. Firstly we reduce the following matrix

$$(s, u_1 s, u_1^2 s, \cdots, u_1^{n_1-1} s, \cdots, u_i s, u_i^2 s, \cdots, u_i^{n_i-1} s, \cdots)^T$$

to get a row-echelon form. The first several rows may be zero, and the rank of the matrix is $n - \varphi(n)$. Removing the zero rows, we define the derived matrix to be M.

Then we form the following $d_f \times d_f$ lattice

$$\begin{pmatrix} p & & & & & & & & \\ & \ddots & & & & & & & \\ & & p & & & & & & \\ M_{1,1} & \cdots & M_{1,\varphi(n)} & 1 & & & & & \\ \vdots & \ddots & & \ddots & \ddots & & & \\ M_{n-\varphi(n),1} & & \cdots & & M_{n-\varphi(n),n-1} & 1 & & \\ \psi_0 & \psi_1 & \psi_2 & \cdots & & & 1 & \\ & \ddots & \ddots & \ddots & & & & \ddots & \\ & & \psi_0 & \psi_1 & & \psi_2 & \cdots & & 1 \end{pmatrix}$$

where $\psi = x^n + \psi_{n-1}x^{n-1} + \cdots + \psi_0$ is the degree n irreducible factor of f modulo p. Using LLL algorithm to reduce the lattice, we can obtain a preimage s' with coefficients about $p^{\varphi(n)/d_f}$. Thus its norm would be around $p^{\varphi(n)} = Q^{\varphi(n)/n}$ when the coefficient f is small.

This result is almost optimal and valid for any characteristic. We also remark that this method is compatible with the former method based on the exTNFS.

5 Numerical Experiments

In this section, we give some numerical experiments to reduce the norm of the preimage. The former two examples follow our first method that is based on exTNFS. The latter two examples use the second method that improves the recent result of Guillevic.

5.1 Examples using the first method

Example 1 ($n = 6$ 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 $\mathbb{F}_{p^6}$.

$$p = 1267650600228229401496703205653$$
$$h = r^3 - r^2 + 1$$
$$f = x^4 + 1$$
$$\psi = x^2 + 266892166039080060530265635980$$
$$g = 81918998706487x^2 + 1122915792871022$$
$$s = \left(770996322275293048913407867893r^2 + 17689037315931957042498082\,6427r + 1160569386245587035814582189227\right)x$$
$$+ 935836514622535375852962122149r^2 + 707940155816471541960680236692r + 203370792026598947471097543375$$

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

$$\begin{pmatrix}
p & & & & & & & & & & & \\
& p & & & & & & & & & & \\
& & p & & & & & & & & & \\
\mathbf{s_0'} & & & 1 & & & & & & & & \\
\mathbf{rs_0'} & & & & 1 & & & & & & & \\
\mathbf{r^2 s_0'} & & & & & 1 & & & & & & \\
\mathbf{\psi_0} & & & & & & 1 & & & & & \\
\mathbf{r\psi_0} & & \mathbf{0} & & & & & 1 & & & & \\
\mathbf{r^2\psi_0} & & & & & & & & 1 & & & \\
& & & \mathbf{\psi_0} & & & & & & 1 & & \\
& & & \mathbf{r\psi_0} & & \mathbf{0} & & & & & 1 & \\
& & & \mathbf{r^2\psi_0} & & & & & & & & 1
\end{pmatrix}$$

The returned short element s'' is

$$(-654596r^2 - 25066478r + 8079577)x^3 + (7089818r^2 + 1960648r + 1047289)x^2 +$$
$$(5995809r^2 - 9170200r - 9594102)x + 26292350r^2 - 7675630r + 1535300,$$

with coefficient at most 8 dd. Its norm is

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

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

Example 2 ($n = 12$ with Conjugation 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. 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 $f = \text{Res}_Y(Y^2 + r + 1, x^2 + Y)$. Then f is irreducible over R have an irreducible factor $\psi(x) = x^2 - y$ over $\mathbb{F}_{p^6}$.

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

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

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

We form the lattice

$$\begin{pmatrix} p & & & & & & & & & \\ & \ddots & & & & & & & & \\ & & p & & & & & & & \\ \mathbf{s'_0} & & 1 & & & & & & & \\ \vdots & & & \ddots & & & & & & \\ \mathbf{r^5 s'_0} & & & & 1 & & & & & \\ \psi_0 & & & & & 1 & & & & \\ \vdots & & & \mathbf{0} & & & \ddots & & & \\ \mathbf{r^5 \psi_0} & & & & & & & 1 & & \\ & & & & & \psi_0 & & & 1 & \\ & & & & & \vdots & & \mathbf{0} & & \ddots \\ & & & & & \mathbf{r^5 \psi_0} & & & & 1 \end{pmatrix}$$

and use LLL algorithm to reduce the lattice and the returned short element s'' is

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

with coefficient at most 4 dd. Its norm is

$$\mathrm{N}_{K_f/\mathbb{Q}}(s'') = {\scriptstyle 431379348639129770256541609523642067259116541169361721928445464826512738568148819622317334695 51,}$$

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

5.2 Examples using the second method

Example 3 ($n = 6$ with JSLV$_1$ method). For the sake of comparison, we take the same setting of [15, Example.4]. Let $p = 314159265358979323846434359$ a 85-bit prime. f and g are degree 6

irreducible polynomials defined by JLSV$_1$ method as follows.

$$f = x^6 - 11209975711932x^5 - 28024939279845x^4 - 20x^3 + 28024939279830x^2 + 11209975711938x + 1$$

$$g = 5604994576830x^6 + 20986447533158x^5 - 31608799819555x^4 - 112099891536600x^3 - 52466118832895x^2$$
$$+ 12643519927822x + 5604994576830.$$

The target element s in $\mathbb{F}_p[x]/(f(x))$ is

$$642770498858150816216245x^5 + 162400524326938996131777738x^4 + 450939028378094990902013x^3$$
$$+ 386837435944575764759144x^2 + 820975591360212920808122x + 327950288419716939937510 50.$$

$x + 3$ is a generator of the finite field. We find a polynomial basis $\{1, u, u^2\}$ for the subfield $\mathbb{F}_{p^3}$ and a polynomial basis $\{1, v\}$ for the subfield $\mathbb{F}_{p^2}$, where $u = (x+3)^{p^3+1}$ and $v = (x+3)^{p^4+p^2+1}$.

Firstly, we reduce the matrix $(s, us, u^2s, vs)^T$ and obtain

$$M = \begin{pmatrix} 17226645327834538783496360 & 19577486147226702425658904 & 1 & 0 & 0 & 0 \\ 76214575295663291763876 77 & 26472271339135481991455467 & 75613294594517441159399 6 & 1 & 0 & 0 \\ 1344387891444430538215117 0 & 20154192696520575351979551 & 14302472262579398892259522 & 11707887538852257161192089 & 1 & 0 \\ 103738016569731364064693 82 & 17554204256890502823332899 & 8453621569611458736380137 & 46584786083727753102306 77 & 22768000008168991745859386 & 1 \end{pmatrix}.$$

Then we use LLL algorithm to reduce the following lattice

$$\begin{pmatrix} p & 0 & 0 & 0 & 0 & 0 \\ 0 & p & 0 & 0 & 0 & 0 \\ M_{11} & M_{12} & 1 & 0 & 0 & 0 \\ M_{21} & \cdots & M_{23} & 1 & 0 & 0 \\ M_{31} & \cdots & & M_{34} & 1 & 0 \\ M_{41} & \cdots & & & M_{45} & 1 \end{pmatrix}$$

and the returned short element s' is

$$142941457x^5 + 47837420x^4 + 111161458x^3 + 50825839x^2 - 118396416x - 95953753.$$

Its norm is

$$\mathrm{N}_{K_f/\mathbb{Q}}(s') = 767148278194626644031284903464853782272054374996164829769754158482911452562929180814544762898891244091221390096821 7.$$

It is a 328-bit number which is smaller than that in [14, Example.4].

Example 4 ($n = 12$ with GJL method). To show our method can reduce the norm to about $Q^{\varphi(n)/n}$, we take an example of $\mathbb{F}_{p^{12}}$. Let $p = 1125899906842679$ a 51-bit prime. We take the irreducible polynomial $x^{15} - x^3 + 1$ to be f. It has a degree 12 irreducible factor ψ modulo p. Then we random pick a target element s in $\mathbb{F}_p[x]/(\psi(x))$. The settings are listed in the following.

$$f = x^{15} - x^3 + 1$$
$$\psi = x^{12} + 694944321654605x^9 + 631892778678733x^6 + 14223930429323x^3 + 465607407774785$$
$$s = 231653230892563x^{11} + 220784742484639x^{10} + 983886361605666x^9 + 64431543852012x^8$$
$$+ 554606661641025^7 + 1020037578605352x^6 + 1061970849476224x^5 + 91082849083538x^4$$
$$+ 42855528549150x^3 + 303578170201214x^2 + 51539418925611x + 262805301891464$$

One can check $x + 2$ is a generator of the finite field. We find a polynomial basis $\{1, u, u^2, u^3, u^4, u^5\}$ for the subfield $\mathbb{F}_{p^6}$ and a polynomial basis $\{1, v, v^2, v^3\}$ for the subfield $\mathbb{F}_{p^4}$, where $u = (x+2)^{p^6+1}$ and $v = (x+2)^{p^8+p^4+1}$.

Firstly, we reduce the matrix $(s, us, \cdots, u^5 s, vs, v^2 s, v^3 s)^T$ and obtain a 9×12 row-echelon matrix with the first row is all zero, since the rank should be $12 - \varphi(12) = 8$. We remove the first row and let the new matrix to be M. Then we use LLL algorithm to reduce the following lattice

$$\begin{pmatrix} p & & & & & & \\ & \ddots & & & & & \\ & & p & & & & \\ & & & M & & & \\ & & & & \psi & & \\ & & & & & \ddots & \\ & & & & & & x^2\psi \end{pmatrix}$$

and the returned short element s' is

$$5109x^{13} - 4682x^{12} + 10441x^{11} + 2824x^{10} - 1909x^9 + 10885x^8 - 1905x^7 - 2973x^6 - 4705x^5$$
$$+ 7151x^4 + 4518x^3 + 3643x^2 - 4143x + 358.$$

Its norm is

$$\mathrm{N}_{K_f/\mathbb{Q}}(s') = 1439768313850579370382358429776202443240536235483268049124154579,$$

which is a 210-bit number. Its size is about $1/3$ of the size of the finite field.

6 Conclusion

In this work, we improve the individual logarithm computation in finite fields with composite degrees in two ways. In the first way, when the characteristic is medium to large, we use the exTNFS to explicitly construct a subfield and find a preimage of the target element with norm bounded by $O(Q^{1-m/n})$ in most cases. The second method generalizes Guillevic's recent work which works for any characteristic finite fields. We use the primitive element to construct all the proper subfields to construct a preimage with norm $O(Q^{\varphi(n)/n})$. The two methods are compatible. Also we give experimental results to confirm our theoretical results. Due to our results, when $\varphi(n)/n$ is relatively small, the complexity of the smoothing phase will be highly reduced and even 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. Adleman, L.M.: The function field sieve. In: ANTS. pp. 108–121 (1994)
2. Adleman, L.M., Huang, M.A.: Function field sieve method for discrete logarithms over finite fields. Inf. Comput. 151, 5–16 (1999)
3. 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)

4. 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)

5. 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)

6. Barbulescu, R., Gaudry, P., Kleinjung, T.: The tower number field sieve. In: Advances in Cryptology–ASIACRYPT 2015, pp. 31–55. Springer (2014)

7. 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)

8. Bistritz, Y., Lifshitz, A.: Bounds for resultants of univariate and bivariate polynomials. Linear Algebra and its Applications 432(8), 1995–2005 (2010)

9. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. SIAM J. Comput. 32(3), 586–615 (2003)

10. Diffie, W., Hellman, M.E.: New directions in cryptogrphy. IEEE Transactions on Information Theory 22(6), 644–654 (1976)

11. Gordon, D.M.: Discrete logarithms in $GF(p)$ using the number field sieve. SIAM Journal on Discrete Mathematics 6(1), 124–138 (1993)

12. Granger, R., Kleinjung, T., Zumbrägel, J.: On the powers of 2. Cryptology ePrint Archive, Report 2014/300 (2014)

13. Granger, R., Kleinjung, T., Zumbrägel, J.: On the discrete logarithm problem in finite fields of fixed characteristic. arXiv:1507.01495v1 (2015)

14. 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)

15. Guillevic, A.: Faster individual discrete logarithms in non-prime finite fields with the NFS and FFS algorithms. Cryptology ePrint Archive, Report 2016/684 (2016)

16. 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)

17. Joux, A.: A one round protocol for tripartite Diffie-Hellman. J. Cryptology 17(4), 263–276 (2004)

18. Joux, A., Lercier, R.: The function field sieve in the medium prime case. In: EUROCRYPT. pp. 254–270 (2006)

19. 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)

20. 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)

21. Kalkbrener, M.: An upper bound on the number of monomials in determinants of sparse matrices with symbolic entries. Mathematica Pannonica 73, 82 (1997)

22. 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)

23. 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)

24. 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)

25. Rubin, K., Silverberg, A.: Torus-based cryptography. In: Advances in Cryptology - CRYPTO 2003. pp. 349–365 (2003)

26. 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)

27. 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)

28. 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)

29. Schirokauer, O.: Using number fields to compute logarithms in finite fields. Mathematics of Computation 69(231), 1267–1283 (2000)
30. Semaev, I.: Special prime numbers and discrete logs in finite prime fields. Mathematics of computation 71(237), 363–377 (2002)
31. Wiedemann, D.H.: Solving sparse linear equations over finite fields. Information Theory, IEEE Transactions on 32(1), 54–62 (1986)