Extended Tower Number Field Sieve with Application to Finite Fields of Arbitrary Composite Extension Degree

Jinhyuck Jeong[1] and Taechan Kim[2]

[1] Seoul Nationalf University, Korea
wlsyrlekd@snu.ac.kr
[2] NTT Secure Platform Laboratories, Japan
taechan.kim@lab.ntt.co.jp

Abstract. In a recent work, Kim and Barbulescu (CRYPTO 2016) proposed an algorithm, called exTNFS, that improves asymptotic complexity for the discrete logarithm problems over $\mathbb{F}_{p^n}$ in medium prime case, when the extension degree $n = \eta\kappa$ satisfies $\eta, \kappa \in \mathbb{Z}_{>1}$ and $\gcd(\eta, \kappa) = 1$. Following to this work, Sarkar and Singh (preprint) recently observed that exTNFS algorithm also admits a variant that applies when n is arbitrary composite, although their best complexity is slightly larger than that of Kim and Barbulescu.
In this article, we show that exTNFS algorithm enjoys their best complexity as well for arbitrary composite extension degree n: we show that the discrete logarithm problem over $\mathbb{F}_{p^n}$ for a medium-sized prime p and $n = \eta\kappa$, with η and $\kappa > 1$ not necessarily coprime, can be solved in time $L_{p^n}(1/3, (48/9)^{1/3})$ for a general prime p and $L_{p^n}(1/3, (32/9)^{1/3})$ for a special prime p.
The result asserts that one should be careful of choosing parameters in the pairing-based construction regarding with the best-complexity of the variant by Kim-Barbulescu whenever the embedding degree is composite.

Keywords: Discrete Logarithm Problem; Number Field Sieve; Finite Fields; Cryptanalysis

1 Introduction

Discrete logarithm problem (DLP) plays an important role in public-key cryptosytsems since its computational hardness assures the securty of the cryptosystems. The goal of the DLP over any cyclic group G of order N is to solve an element $a \in \mathbb{Z}_N$ for given a generator g of G and a random element h uniformly chosen from G satisfying $h = g^a$. Two practical choices for the group are elliptic curves and finite fields.

In this article, we focus on algorithms for the DLP over finite fields $\mathbb{F}_Q$ for a prime power $Q = p^n$. An interest in this problem is particularly motivated by pairing-based construction. A pairing is a bilinear map such that $E_1 \times E_2 \to \mathbb{F}_{p^n}$, where E_1 and E_2 are elliptic curve groups defined over $\mathbb{F}_p$ and n is called

embedding degree. The security of the pairing-based cryptosystems relies on the hardness of the elliptic curve DLP (ECDLP) and the DLP over finite fields.

In particular, algorithms for the DLP over finite fields are on a dramatic progress in a recent few years. A method based on function field sieve (FFS) yields a quasi-polynomial time attack on small characteristic fields [2]. On the other hand, a recent breakthrough on number field sieve (NFS) by Kim and Barbulescu [7] sets a new asymptotic complexity for a larger characteristic fields.

Recall the usual L_Q-notation,

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

for some constants $0 \leq \ell \leq 1$ and $c > 0$. We call the characteristic $p = L_Q(\ell_p, c_p)$ medium when $1/3 < \ell_p < 2/3$ and large when $2/3 < \ell_p \leq 1$. We are interested in the boundary case when $\ell_p = 2/3$.

The best complexity of an NFS variant by Kim and Barbulescu, called exTNFS, is $L_Q(1/3, (48/9)^{1/3})$ for medium characteristic p. The value is obtained when $n = \eta\kappa$ satisfies $\eta, \kappa > 1$, $\gcd(\eta, \kappa) = 1$ and $\kappa = \left(\frac{1}{12^{1/3}} + o(1)\right)\left(\frac{\log(Q)}{\log\log(Q)}\right)^{1/3}$. When p is of special prime, e.g. the prime in Barreto-Naehrig curve [4], one obtains a better complexity, $L_Q(1/3, (32/9)^{1/3})$.

However, their variant cannot be applied to a composite n such that $\gcd(\eta, \kappa) \neq 1$, e.g. a prime power. Recently, Sarkar and Singh observed that exTNFS method can be applied even when n is arbitrary composite [9]. The best complexity of their variant is achieved by $L_Q(1/3, (64/9)^{1/3})$ when n is a power of 2.

In this paper, we show that the exTNFS actually easily can be extended to the case when n is arbitrary composite, while maintaining their best complexity. Precisely, we propose an algorithm that solves the DLP over $\mathbb{F}_Q = \mathbb{F}_{p^n}$ for an arbitrary composite $n = \eta\kappa$ such that $\kappa = \left(\frac{1}{12^{1/3}} + o(1)\right)\left(\frac{\log(Q)}{\log\log(Q)}\right)^{1/3}$ in time $L_Q(1/3, (48/9)^{1/3})$. Note that our variant already has a better complexity than Sarkar-Singh's variant, furthermore, the same complexity holds even when n is not a power of 2. As before, if p is a special prime, then the complexity reduces to $L_Q(1/3, (32/9)^{1/3})$.

2 Extended TNFS

2.1 Setting

Throughout this paper, we target fields $\mathbb{F}_Q$ with $Q = p^n$ where $n = \eta\kappa$ such that $\eta, \kappa \neq 1$ and the characteristic p is medium or large, i.e. $\ell_p > 1/3$. Unlike the exTNFS by Kim and Barbulescu [7], we don't require the coprimality condition of η and κ.

A main idea of our work with them is that we take the coefficients of $f(x)$ and $g(x)$ fully from R not restricted to $\mathbb{Z}$. It makes us possible to remove the gcd condition on the factors of the extension degree n. A similar approach is recently discussed by Sarkar and Singh [9].

We briefly review how to select polynomials in exTNFS algorithm. Basically, we follow the commutative diagram by Kim and Barbulescu (Fig. 1). First we select a polynomial $h(t) \in \mathbb{Z}[t]$ of degree η which is irreducible modulo p. We put $R := \mathbb{Z}[t]/h(t) = \mathbb{Z}(\iota)$ and note that $R/pR \simeq \mathbb{F}_{p^\eta}$. Then we select two polynomials f and g with coefficients in R whose reductions modulo p have a common factor $k(x)$ of degree κ which is irreducible over $\mathbb{F}_{p^\eta}$.

The conditions on f, g and h yield two ring homomorphisms from $R[x]/f(x)$ (resp. $R[x]/g(x)$) to $(R/pR)/k(x) = \mathbb{F}_{p^{\eta\kappa}}$: in order to compute the reduction of a polynomial in $R[x]$ modulo p then modulo $k(x)$ one can start by reducing modulo f (resp. g) and continue by reducing modulo p and then modulo $k(x)$. The result is the same if we use f as when we use g. Thus one has the commutative diagram in Figure 1 which is a generalization of the classical diagram of NFS.

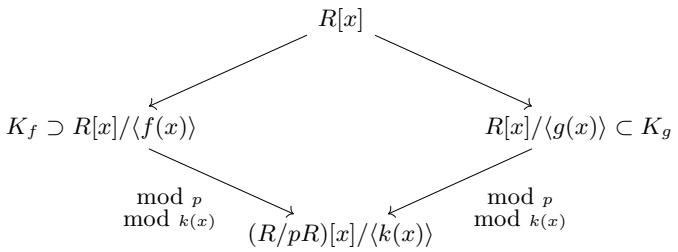

Fig. 1: Commutative diagram of exTNFS. We can choose f and g to be irreducible polynomials over R such that $k = \gcd(f, g) \bmod p$ is irreducible over $R/pR = \mathbb{F}_{p^\eta}$.

After the polynomial selection, the exTNFS algorithm proceeds as all the variants of NFS, following the same steps: relations collection, linear algebra and individual logarithm. Most of these steps are very similar to the TNFS algorithms as we shall explain below.

2.2 Detailed Descriptions

Polynomial Selection

Choice of h We have to select a polynomial $h(t) \in \mathbb{Z}[x]$ of degree η which is irreducible modulo p and whose coefficients are as small as possible. As in TNFS we try random polynomials h with small coefficients and factor them in $\mathbb{F}_p[t]$ to test irreducibility. Heuristically, one succeeds after η trials and since $\eta \leq 3^\eta$ we expect to find h such that $\|h\|_\infty = 1$. For a more rigorous description on the existence of such polynomials one can refer to [3].

Next we select f and g in $R[x]$ which have a common factor $k(x)$ modulo p of degree κ which remains irreducible over $\mathbb{F}_{p^\eta} = R/pR$. We choose such polynomials based on a generalized Conjugation method. In a recent work [9], Sarkar and Singh considered a generalization of gJL method but a generalization

of Conjugation method and the case of special prime were not discussed. As exTNFS with Conj provides a better complexity than exTNFS with gJL, our approach is superior to Sarkar and Singh's variant using generalized gJL method.

Generalized Conjugation method We describe a polynomial selection method called generalized Conjugation method (gConj method). It generalizes the Conjugation method described in [7,1]. First, one chooses two bivariate polynomials $g_1(t,x)$ and $g_0(t,x)$ in $\mathbb{Z}[t,x]$ of form

$$g_1(t,x) = g_{1,0}(t) + g_{1,1}(t)x + \cdots + g_{1,\kappa-1}(t)x^{\kappa-1}$$

and

$$g_0(t,x) = g_{0,0}(t) + g_{0,1}(t)x + \cdots + g_{0,\kappa}(t)x^{\kappa},$$

where $g_{i,j}(t) \in \mathbb{Z}[t]$ are polynomials with small coefficients in $\mathbb{Z}$ and of degree less than or equal to $\eta-1$. Note that if ι denotes a root of $h(t)$ over the algebraic closure of $\mathbb{F}_p$, then $g_0(\iota,x)$ and $g_1(\iota,x)$ are polynomials over $\mathbb{F}_{p^\eta} = \mathbb{F}_p(\iota) = \mathbb{F}_p[t]/h(t)$ (in this paper, we abuse the notation of ι for a root of h both in $\mathbb{C}$ and algebraic closure of $\mathbb{F}_p$).

Next one chooses a quadratic, monic, irreducible polynomial $\mu(x) \in \mathbb{Z}[x]$ with small coefficients. If $\mu(x)$ has a root δ modulo p and $g_0(\iota,x) + \delta g_1(\iota,x)$ is irreducible over $\mathbb{F}_{p^\eta}$, then set $k(x) = g_0(\iota,x) + \delta g_1(\iota,x) \in \mathbb{F}_{p^\eta}[x]$. Otherwise, one repeats the above steps until such g_1, g_0, and δ are found. Once it has been done, find u and v such that $\delta \equiv u/v \pmod p$ and $u, v \leq O(\sqrt{p})$ using rational reconstruction. Finally, we set $f(t,x) = \mathrm{Res}_Y(\mu(Y), g_0(t,x) + Y g_1(t,x))$ and $g(t,x) = v g_0(t,x) + u g_1(t,x)$. By construction we have

- $\deg_x(f) = 2\kappa$ and $\|f\|_\infty = \max\{f_{i,j}\} = O(1)$;
- $\deg_x(g) = \kappa$ and $\|g\|_\infty = \max\{g_{i,j}\} = O(\sqrt{p}) = O(Q^{\frac{1}{2\eta\kappa}})$.

The bound on $\|f\|_\infty$ depends on the number of polynomials $g_0 + \delta g_1$ tested before we find one which is irreducible over $\mathbb{F}_{p^\eta}$. Heuristically this happens on average after κ trials. Since there are $3^{2\eta\kappa} > \kappa$ choices of $g_0(t,x)$ and $g_1(t,x)$ of norm 1 (here, the norm means the maximum size of its integer coefficients) we have $\|f\|_\infty = O(1)$.

We give some examples in the followings.

Example 1. We target a field $\mathbb{F}_{p^4}$ for $p \equiv 7 \bmod 8$ prime. For example, we take $p = 1000010903$. If we choose $h(t) = t^2 + 1$ then $h \bmod p$ is irreducible over $\mathbb{F}_p$. Consider $R = \mathbb{Z}(\iota) = \mathbb{Z}[t]/h(t)$ and $\mathbb{F}_{p^2} = \mathbb{F}_p(\iota) = \mathbb{F}_p[t]/h(t)$. Choose an irreducible polynomial $\mu(x) = x^2 - 2 \in \mathbb{Z}[x]$ with small coefficients. It has a root $\sqrt{2} = 219983819 \in \mathbb{F}_p$. We take $k(x) = (x^2 + \iota) + \sqrt{2}x \in \mathbb{F}_{p^2}[x]$ and $f(x) = (x^2 + \iota + \sqrt{2}x)(x^2 + \iota - \sqrt{2}x) = x^4 + (2\iota - 2)x^2 + 1 \in R[x]$. Then we find $u, v \in \mathbb{Z}$ such that $u/v \equiv \sqrt{2} \bmod p$ where their order are of $\sqrt{p}$. Now we take $g(x) = v(x^2 + \iota) + ux = 25834(x^2 - \iota + 2) + 18297 \in R[x]$. One easily checks that f and g are irreducible over R and k is irreducible over $\mathbb{F}_{p^2}$ so that they are suitable for exTNFS algorithm.

Example 2. Now we target a field $\mathbb{F}_{p^9}$. Choose an irreducible polynomial $h(t) = t^3 + t + 1 \in \mathbb{Z}[t]$ such that it still remains prime modulo p. Again, we take $p = 1000010903$ for example. Choose $h(t) = t^3 + t + 1 \in \mathbb{Z}[t]$ which remains irreducible modulo p. Let $R = \mathbb{Z}(\iota) = \mathbb{Z}[t]/h(t)$ and $\mathbb{F}_{p^3} = \mathbb{F}_p(\iota) = \mathbb{F}_p[t]/h(t)$. We set $\mu(x) = x^2 - 3$. Compute u and v such that $u/v \equiv \sqrt{3} \bmod p$. Then the polynomials $k(x) = (x^3 + \iota) + \sqrt{3}x \in \mathbb{F}_{p^3}[x]$, $f(x) = (x^3 + \iota)^2 - 3x^2 \in R[x]$ and $g(x) = v(x^3 + \iota) + ux \in R[x]$ satisfy the conditions of polynomial selection for exTNFS algorithm.

Algorithm 1 Polynomial selection with the generalized Conjugation method (gConj)

Input: p prime and $n = \eta\kappa$ integer such that $\eta, \kappa > 1$
Output: f, g, k, h with $h \in \mathbb{Z}[t]$ irreducible of degree η, and $f, g \in R[x]$ irreducible over $R = \mathbb{Z}[t]/h\mathbb{Z}[t]$, and $k = \gcd(f \bmod p, g \bmod p)$ in $\mathbb{F}_{p^\eta} = \mathbb{F}_p[t]/h(t)$ irreducible of degree κ

Choose $h \in \mathbb{Z}[t]$, irreducible of degree η such that p is inert in $\mathbb{Q}[t]/h(t)$
repeat
  Select $g_{0,0}(t), \ldots, g_{0,\kappa-1}(t)$, polynomials of degree $\leq \eta - 1$ with small integer coefficients;
  Select $g_{1,0}(t), \ldots, g_{1,\kappa'-1}(t)$, polynomials of degree $\leq \eta - 1$, and $g_{0,\kappa'}(t)$, a constant polynomial with small integer coefficients, for an integer $\kappa' < \kappa$;
  Set $g_0(t, x) = x^\kappa + \sum_{i=0}^{\kappa-1} g_{0,i}(t)x^i$ and $g_1(t, x) = \sum_{i=0}^{\kappa'} g_{1,i}(t)x^i$;
  Select $\mu(x)$ a quadratic, monic, irreducible polynomial over $\mathbb{Z}$ with small coefficients;
until $\mu(x)$ has a root δ modulo p and $k(x) = g_0(\iota, x) + \delta g_1(\iota, x)$ is irreducible in $\mathbb{F}_{p^\eta}[x]$;
$(u, v) \leftarrow$ a rational reconstruction of δ;
$f \leftarrow \mathrm{Res}_Y(\mu(Y), g_0(\iota, x) + Y g_1(\iota, x))$;
$g \leftarrow vg_0(\iota, x) + ug_1(\iota, x)$;
return (f, g, k, h)

Relation Collection The elements of $R = \mathbb{Z}[t]/h(t)$ can be represented uniquely as polynomials of $\mathbb{Z}[t]$ of degree less than $\deg h$.

We proceed as in TNFS and enumerate all the pairs $(a, b) \in \mathbb{Z}[t]^2$ of degree $\leq \eta - 1$ such that $\|a\|_\infty$, $\|b\|_\infty \leq A$ for a parameter A to be determined. We say that we obtain a relation for the pair (a, b) if

$$N_f(a, b) := \mathrm{Res}_t(\mathrm{Res}_x(a(t) - b(t)x, f(x)), h(t)) \text{ and}$$
$$N_g(a, b) := \mathrm{Res}_t(\mathrm{Res}_x(a(t) - b(t)x, g(x)), h(t))$$

are B-smooth for a parameter B to be determined (an integer is B-smooth if all its prime factors are less than B). If ι denotes a root of h in R our enumeration is equivalent to putting linear polynomials $a(\iota) - b(\iota)x$ in the top of the diagram

of Figure 1. One can generalize exTNFS to the case where one puts non-linear polynomials $r(x) \in R[x]$ of degree $\tau - 1$ in the diagram.

For each pair (a, b) one obtains a linear equation where the unknowns are logarithms of elements of the factor base as in the classical variant of NFS for discrete logarithms. Other than the polynomial selection step, our algorithm is basically the same with the description of the exTNFS algorithm. For full description of the algorithm, refer to [7].

3 Complexity

From now on, we often abuse the notation for a bivariate polynomial $f(t, x)$ in $\mathbb{Z}[t, x]$ and a polynomial $f(x) = f(\iota, x)$ in $R[x]$ for $R = \mathbb{Z}[\iota]$. Unless stated, $\deg(f)$ denotes both the degree of $f(x) \in R[x]$ and the degree of $f(t, x) \in \mathbb{Z}[t, x]$ with respect to x. The norm of $f(x) \in R[x]$, denoted by $\|f\|_\infty$, is defined by the maximum of the absolute value of the integer coefficients of $f(t, x)$ where f is considered as $f(x) = f(\iota, x) \in R[x]$.

We need the following lemma that can be found in [7, Lemma 2].

Lemma 1 ([7], Lemma 2.). *Let h be an irreducible polynomial over $\mathbb{Z}$ of degree η and f be an irreducible polynomial over $\mathbb{Z}[\iota]$ of degree $\deg(f)$. Let ι (resp. α) be a root of h (resp. f) in its number field and set $K_f := \mathbb{Q}(\iota, \alpha)$. Let $A > 0$ be a real number and T an integer such that $2 \leq T \leq \deg(f)$. For each $i = 0, \ldots, \deg(f) - 1$, let $a_i(t) \in \mathbb{Z}[t]$ be polynomials of degree $\leq \eta - 1$ with $\|a_i\|_\infty \leq A$.*

1. *We have*

$$\left|N_{K_f/\mathbb{Q}}\Big(\sum_{i=0}^{T-1} a_i(\iota)\alpha^i\Big)\right| < A^{\eta \deg(f)} \|f\|_\infty^{(T-1)\eta} \|h\|_\infty^{(T+\deg(f)-1)(\eta-1)} D(\eta, \deg(f)),$$

   where $D(\eta, \kappa) = \big((2\kappa-1)(\eta-1)+1\big)^{\eta/2} (\eta+1)^{(2\kappa-1)(\eta-1)/2} \big((2\kappa-1)!\eta^{2\kappa}\big)^{\eta}$.
2. *Assume in addition that $\|h\|_\infty$ is bounded by an absolute constant H and that $p = L_Q(\ell_p, c)$ for some $\ell_p > 1/3$ and $c > 0$. Then*

$$N_f(a, b) \leq E^{\deg(f)} \|f\|_\infty^\eta L_Q(2/3, o(1)), \tag{1}$$

   where $E = A^\eta$

The above formula remains the same when we restrict the coefficients of f to be integers.

Proof. The proof can be found in [7].

3.1 exTNFS-gConj

We propose here a variant of NFS which combines exTNFS with generalized Conjugation method of polynomial selection. Since our polynomial selection is done over R not $\mathbb{Z}$, we can work with $n = \eta\kappa$ even when $\gcd(\eta, \kappa) \neq 1$. As we shall observe, the bound of the norms remains the same with exTNFS-Conj. It yields the same complexity as before.

Theorem 1 (exTNFS with gConj method). *(under the classical NFS heuristics) If $Q = p^n$ is a prime power such that*

- $p = L_Q(\ell_p, c_p)$ *with* $1/3 < \ell_p \leq 2/3$;
- $n = \eta\kappa$ *such that* $\eta, \kappa \neq 1$ *and* $\kappa = \left(\frac{1}{12^{1/3}} + o(1)\right)\left(\frac{\log(Q)}{\log\log(Q)}\right)^{1/3}$,

then the discrete logarithm over $\mathbb{F}_Q$ can be solved in $L_Q(1/3, (48/9)^{1/3})$.

Proof. Evaluating the values coming from the Conjugation method (Section 2.2) in Equation (1), we have

$$|N_f(a,b)| < E^{2\kappa} L_Q(2/3, o(1)), \tag{2}$$
$$|N_g(a,b)| < E^{\kappa}(p^{\kappa\eta})^{1/(2\kappa)} L_Q(2/3, o(1)). \tag{3}$$

When we combine Equations (2) and (3) we obtain

$$|N_f(a,b)| \cdot |N_g(a,b)| < E^{3\kappa} Q^{(1+o(1))/(2\kappa)}.$$

But this is Equation (5) in [1] when $\tau = 2$ (the parameter τ is written as t in [1], the number of coefficients of the sieving polynomial r). The rest of the computations are identical as in point 3. of Theorem 1 in [1], so

$$\text{complexity(exTNFS-gConj)} = L_Q(1/3, (48/9)^{1/3}).$$

4 Variants

4.1 The case when p has a special form (SexTNFS)

A generalized polynomial selection method also admits a variant for special prime. It includes the primes that are used for pairing-based construction. The previous SexTNFS by Kim and Barbulescu cannot be applied to pairing-friendly fields with prime power embedding degree, such as Kachisa-Schaefer-Scott curve [6] $p = (u^{10} + 2u^9 + 5u^8 + 48u^6 + 152u^5 + 240u^4 + 625u^2 + 2398u + 3125)/980$ of embedding degree 16. For a given integer d, an integer p is d-SNFS if there exists an integer u and a polynomial $\Pi(x)$ with integer coefficients so that

$$p = \Pi(u),$$

$\deg \Pi = d$ and $\|\Pi\|_\infty$ is bounded by an absolute constant.

We consider the case when $n = \eta\kappa$, $\gcd(\eta, \kappa) = 1$ with $\kappa = o\left(\left(\frac{\log Q}{\log\log Q}\right)^{1/3}\right)$ and p is d-SNFS. In this case our exTNFS selects h, f and g so that

– h is a polynomial over $\mathbb{Z}$ and irreducible modulo p, $\deg h = \eta$ and $\|h\|_\infty = O(1)$;
– f and g are two polynomials with coefficients from $R = \mathbb{Z}[\iota]$, have a common factor $k(x)$ modulo p which is irreducible over $R/pR = \mathbb{F}_{p^n} = \mathbb{F}(\iota)$ of degree κ.

We choose such polynomials using the method of Joux and Pierrot [5]. Find a bivariate polynomial S of degree $\kappa - 1$ w.r.t. x such that

$$S(t, x) = S_0(t) + S_1(t)x + \cdots + S_{\kappa-1}(t)x^{\kappa-1} \in \mathbb{Z}[t, x],$$

where $S_i(t)$'s have their coefficients in $\{-1, 0, 1\}$ and are of degree $\leq \eta - 1$. We further require that $k(\iota, x) = x^\kappa + S(\iota, x) - u$ is irreducible over $\mathbb{F}_{p^n}$ modulo p. Since the proportion of irreducible polynomials in $\mathbb{F}_q$ (q: a prime power) of degree κ is $1/\kappa$ and there are $3^{\eta\kappa}$ choices we expect this step to succeed. Then we set

$$\begin{cases} g = x^\kappa + S(\iota, x) - u \\ f = \Pi(x^\kappa + S(\iota, x)). \end{cases}$$

If f is not irreducible over $R[x]$, which happens with small probability, start over. Note that g is irreducible modulo p and that f is a multiple of g modulo p. More precisely, as in [5], we choose $S(t, x)$ so that the number of its terms is approximately $O(\log n)$. Since $3^{\log n} > \kappa$, this allows us enough chance to get an irreducible polynomial g. The size of the largest integer coefficient of f comes from the part $S(t, x)^d$ and it is bounded by $\sigma^d = O\left((\log n)^d\right)$, where σ denotes the number of the terms in $S(t, x)$. By construction we have:

– $\deg(g) = \kappa$ and $\|g\|_\infty = u = p^{1/d}$;
– $\deg(f) = \kappa d$ and $\|f\|_\infty = O((\log n)^d)$.

We inject these values in Equations (1) and obtain

$$\begin{aligned} |N_f(a, b)| &\leq E^{\kappa d} L_Q(2/3, o(1)) \\ |N_g(a, b)| &\leq E^\kappa P^{1/d} L_Q(2/3, o(1)), \end{aligned}$$

where $E := A^\eta$ and $P := |R/pR| = p^\eta$. We recognize the size of the norms in the analysis by Joux and Pierrot [5, Section 6.3.], so we obtain the same complexity as in their paper, and we proved the following:

Theorem 2 (SexTNFS with arbitrary composite n). *If $Q = p^n$ is a prime power such that*

– *p is d-SNFS prime and $p = L_Q(\ell_p, c_p)$ with $1/3 < \ell_p$;*
– *$n = \eta\kappa$ such that $\eta, \kappa \neq 1$;*

then the discrete logarithm over $\mathbb{F}_Q$ can be solved in $L_Q(1/3, (32/9)^{1/3})$.

4.2 The multiple polynomial variants (MexTNFS-gConj)

One can also accelerate the complexity of exTNFS with generalized Conjugation method using multiple polynomial variants. The description is similar to the previous multiple variant of NFS: choose a polynomial $\mu(x) \in \mathbb{Z}[x]$, that is irreducible, quadratic, has small coefficients, and has a root δ modulo p. As before, choose $k = g_0 + \delta g_1 \in \mathbb{F}_{p^\eta}[x]$ and set $f = Res_Y(\mu(Y), g_0 + Y g_1) \in R[x]$, where g_0 and g_1 are polynomials in $R[x]$. This time, we find two pairs of integers (u, v) and (u', v') using rational reconstrucion such that

$$\delta \equiv u/v \equiv u'/v' \bmod p,$$

where we require (u, v) and (u', v') are linearly independent over $\mathbb{Q}$ and the integers u, v, u', v' are all of the size of $\sqrt{p}$.

Next we set $f_1 = f$, $f_2 = vg_0 + ug_1$ and $f_3 = v'g_0 + u'g_1$ and select other $V - 3$ irreducible polynomials $f_i := \mu_i f_2 + \nu_i f_3$ where $\mu_i = \sum_{j=0}^{\eta-1} \mu_{i,j} \iota^j$ and $\nu_i = \sum_{j=0}^{\eta-1} \nu_{i,j} \iota^j$ are elements of $R = \mathbb{Z}[t]/h\mathbb{Z}[t]$ such that $\|\mu_i\|_\infty, \|\nu_i\|_\infty \leq V^{\frac{1}{2\eta}}$ where $V = L_Q(1/3, c_v)$ is a parameter which will be selected later. Denote α_i a root of f_i for $i = 1, 2, \ldots, V$.

By construction, we have:

- $\deg(f_1) = 2\kappa$ and $\|f_1\|_\infty = O(1)$;
- $\deg(f_i) = \kappa$ and $\|f_i\|_\infty = V^{\frac{1}{2\eta}} (p^{\eta\kappa})^{1/(2\kappa)}$ for $2 \leq i \leq V$.

As before, evaluating these values into Equation (1), we obtain:

$$|N_{f_1}(a, b)| < E^{2\kappa} L_Q(2/3, o(1))$$
$$|N_{f_i}(a, b)| < E^{\kappa} (p^{\kappa\eta})^{\frac{1}{2\kappa}} L_Q(2/3, o(1)) \text{ for } 2 \leq i \leq V.$$

We emphasize that $\left(V^{1/(2\eta)}\right)^\eta = V^{1/2} = L_Q(2/3, o(1))$.

Then, one can proceed the computation identical to [8]. When $P = p^\eta = L_Q(2/3, c_P)$ such that $c_P > (\frac{7+2\sqrt{13}}{6})^{1/3}$ and τ is the number of coefficients of the enumerated polynomials r, then the complexity obtained is $L_Q(1/3, C(\tau, c_P))$ where

$$C(\tau, c_P) = \frac{2}{c_P \tau} + \sqrt{\frac{20}{9(c_P\tau)^2} + \frac{2}{3} c_P (\tau - 1)}.$$

The best case is when $c_P = (\frac{56+24\sqrt{6}}{12})^{1/3}$ and $\tau = 2$ (linear polynomials):

$$\text{complexity(best case of MexTNFS-gConj)} = L_Q\left(1/3, \frac{3 + \sqrt{3(11 + 4\sqrt{6})}}{\left(18(7 + 3\sqrt{6})\right)^{1/3}}\right),$$

where the second constant being approximated by 1.71.

Acknowledgement. The authors would like to thank Razvan Barbulescu and Jung Hee Cheon for their valuable comments.

References

1. R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain. Improving NFS for the discrete logarithm problem in non-prime finite fields. In *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *Lecture Notes in Comput. Sci.*, pages 129–155, 2015.
2. R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Comput. Sci.*, pages 1–16, 2014.
3. R. Barbulescu, P. Gaudry, and T. Kleinjung. The Towed Number Field Sieve. In *Advances in Cryptology – ASIACRYPT 2015*, volume 9453 of *Lecture Notes in Comput. Sci.*, pages 31–55, 2015.
4. P. S. L. M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography – SAC 2005*, volume 9566 of *Lecture Notes in Comput. Sci.*, pages 319–331, 2005.
5. A. Joux and C. Pierrot. The special number field sieve in $\mathbb{F}_{p^n}$ – application to pairing-friendly constructions. In *Pairing-Based Cryptography - Pairing 2013*, volume 8365 of *Lecture Notes in Comput. Sci.*, pages 45–61, 2013.
6. E. J. Kachisa, E. F. Schaefer, and M. Scott. Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. In *Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings*, pages 126–135, 2008.
7. T. Kim and R. Barbulescu. Extended Tower Number Field Sieve: A New Complexity for Medium Prime Case. In *Advances in Cryptology – CRYPTO 2016*.
8. C. Pierrot. The multiple number field sieve with conjugation and generalized Joux-Lercier methods. In *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *Lecture Notes in Comput. Sci.*, pages 156–170, 2015.
9. P. Sarkar and S. Singh. A general polynomial selection method and new asymptotic complexities for the tower number field sieve algorithm. *IACR Cryptology ePrint Archive*, 2016:485, 2016.