Extended Tower Number Field Sieve: A New Complexity for Medium Prime Case

Taechan Kim

NTT Secure Platform Laboratories
taechan.kim@lab.ntt.co.jp

Abstract. In this paper, we extend the tower number field sieve (TNFS) proposed by Barbulescu, Gaudry, and Kleinjung in Asaicrypt 2015. Our generalization based on the JLSV algorithm (by Joux, Lercier, Smart, and Vercautern, Crypto 2006) shows that one can solve the discrete logarithm over the field $\mathbb{F}_Q := \mathbb{F}_{p^n}$ in time complexity,

$$L_Q(1/3, (64/9)^{1/3}), \text{ for } p = L_Q(\ell_p) \text{ with some } \ell_p > 1/3.$$

This should be compared that the previous NFS algorithms only assures this bound either when $\ell_p > 2/3$ (the JLSV algorithm) or when p is of special form when $1/3 < \ell_p < 2/3$ (by Joux and Pierrot, Pairing 2013).

Even more, when we apply some variants (such as the multiple number field sieve or the special number field sieve) to our algorithm, then we show that the above complexity is further improved.

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

1 Introduction

The discrete logarithm problem (DLP) has been an important mathematical tool to support the security of many public key cryptosystems. For the DLP over a generic group, the best known algorithm has the exponential running time of $O(\sqrt{N})$, where N denotes the order of the group. On the other hand, if a group has special structures, then one exploits them to further leverage the computational costs. In particular, the DLP over finite fields $\mathbb{F}_Q = \mathbb{F}_{p^n}$ can be solved much more efficiently than the exponential complexity.

When the characteristic p is small compared to the extension degree n, the best known algorithm has quasi-polynomial time complexity due to Barbulescu, Gaudry, Joux, and Thomé [2].

DLP over medium/large prime cases. For larger characteristic case, most of the current best algorithms come from the number field sieve (NFS) algorithm. The NFS was first introduced by Gordon [9] targeting at the DLP over prime fields. Later, the NFS was extended to the non-prime finite field cases by Joux, Lercier,

Table 1: The complexity of each algorithms for medium/large prime characteristic cases. The left-top cell means that the JLSV algorithm has the complexity of $L_Q(1/3, (128/9)^{1/3})$ for primes $p = L_Q(\ell_p)$ with $1/3 < \ell_p < 2/3$.

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	$2/3 < \ell_p < 1$
JLSV [10]	$128/9$	$64/9$
BGGM [1]	$96/9$	$64/9$
BP [4]	$2^{13}/3^6$	$(92 + 26\sqrt{13})/27$
Pierrot [13]	$(72 + 32\sqrt{6})/15$	none
JP [11]	$\approx 64/9$	$32/9$

Smart, and Vercauteren [10]. It is further improved by many following works such as the multiple number field sieve (MNFS) by Barbulescu and Pierrot [4], the NFS with conjugation method and the generalized Joux and Lercier (gJL) method by Barbulescu, Gaudry, Guillevic, and Morain [1], and the MNFS with conjugation method and gJL method by Pierrot [13]. When p is of special form, e.g. in the case of pairing construction such as BN curves [5], the special number field sieve (SNFS) proposed by Joux and Pierrot [11] provides a better performance.

Recall the usual L_Q-notation,

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

for some constants $0 \leq \ell \leq 1$ and $c > 0$. All of the above algorithms have different complexity following by the size of the characteristic, say, medium case and large case, where we call the prime $p = L_Q(\ell_p, c_p)$ medium for $1/3 < \ell_p < 2/3$ and large for $2/3 < \ell_p < 1$.

In particular, all of them share features that the complexity for the medium prime case is slightly larger than that of the large prime case. To overview the complexity of those algorithms, we provide Table 1. The value in each cell of the table, if we denote it by C, means that the complexity of the correspond algorithm is given by $L_Q(1/3, C^{1/3})$ in the range of primes of the corresponding size. Each of the cells in the same column is listed in (almost) decreasing order (except the case between BGGM and BP in medium case, in which $96/9 < 2^{13}/3^6$).

Our Contributions. In this paper, we break out this barrier between the medium and large characteristic cases. For instance, our algorithm based on the JLSV algorithm has a complexity of $L_Q(1/3, (64/9)^{1/3})$ for *any prime p such that* $\ell_p > 1/3$. As seen in Table 1, this value is already the best among the existing algorithms in the medium case. Note that we do not restrict any form of the prime, otherwise the JP algorithm [11] requires a special form of the prime.

Our main idea is based on a recent progress on the NFS by Barbulescu, Gaudry, and Kleinjung [3]. They provided an algorithm so called the tower number field sieve (TNFS) by revisiting the Schirokauer's TNFS [15]. Their

algorithm generalizes the NFS for prime field case to the NFS for prime-power field case with the following observation: Regard $\mathbb{F}_{p^\eta}$ as $(\mathbb{Z}[t]/h(t))/p(\mathbb{Z}[t]/h(t))$ for an irreducible polynomial $h \in \mathbb{Z}[t]$ of degree η. To target the field $\mathbb{F}_{p^\eta}$, one just applies arguments from the NFS algorithm for $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, replacing $\mathbb{Z}$ by R in the arguments.

Due to this construction, their analysis has an analogy with that of the NFS for prime fields, while the TNFS targets at "large" prime characteristic case in their case. Their algorithm is mathematically elegant, but the result in terms of a complexity is less impressive, since the same complexity was already known by the JLSV algorithm [10].

In this paper, we further extend this TNFS. As the TNFS algorithm has an analogy with the NFS algorithm for prime field, our extended algorithm has an analogy with the NFS algorithm for non-prime field. In a nutshell, we target a field

$$\mathbb{F}_{(p^\eta)^\kappa} = R_p[x]/k(x),$$

where $R = R/pR = \mathbb{F}_{p^\eta}$ and k is an irreducible polynomial of degree κ in $R_p[x]$. Recall that, in the case of the NFS algorithm over non-prime field, a target field can be written as $\mathbb{F}_{p^\kappa} = \mathbb{Z}_p[x]/k(x)$ by abusing the notation $\mathbb{Z}_p$ with $\mathbb{F}_p$.

Interestingly, this analogy provides a complexity analysis of the exTNFS which are quite similar to that of the NFS for "large" prime cases, while in this case we can target at the medium prime cases. As a consequence, we obtain a new complexity in the medium prime case which are the same with the state-of-art complexity in the large prime case.

2 Overview of Extended TNFS

We briefly review the TNFS [3] and provide our algorithm that extends the TNFS. Throughout this paper, we target fields $\mathbb{F}_Q$ with $Q = p^n$ for $n = \eta\kappa$, where η and κ are coprime integers. In particular, we consider the case of $p = L_Q(\ell_p)$ for some constant $\ell_p > 1/3$.

Let $h(t) \in \mathbb{Z}[t]$ be an irreducible polynomial of degree η. Define a ring $R := \mathbb{Z}[t]/h(t)$. Furthermore, we require $h(t)$ remains irreducible modulo p so that p is inert in the number field $\mathbb{Q}[t]/h(t)$ that contains a subring R. The TNFS algorithm [3] involves of selecting two irreducible polynomials f and g in $R[x]$ that shares a common root, say m, modulo pR.

The conditions on f, g, and h yield two ring homomorphisms from $R[x]/f(x)$ (resp. $R[x]/g(x)$) to $R/pR = \mathbb{F}_{p^\eta}$ by taking a root α_f (resp. α_g) of f (resp. g) to the common root m. Thus one has the commutative diagram in Figure 1. Note that, in the case of $R = \mathbb{Z}$, we get a commutative diagram in the classical NFS algorithm for prime fields.

On the other hand, let us recall a classical NFS algorithm over non-prime field, say $\mathbb{F}_{p^\kappa} = \mathbb{F}_p[x]/k(x)$ for an irreducible polynomial $k(x)$ of degree $\kappa > 1$. Polynomial selection method for most algorithms such as [10,1] require two irreducible polynomials f and g in $\mathbb{Z}[x]$ such that $k \mid \gcd(f, g)$ modulo p.

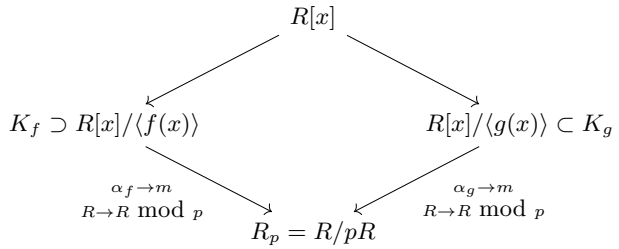

Fig. 1: Commutative diagram of TNFS with $R = \mathbb{Z}(\iota)$ and $f(m) \equiv g(m) \equiv 0 \bmod pR$. When $R = \mathbb{Z}$, it yields the NFS over prime field.

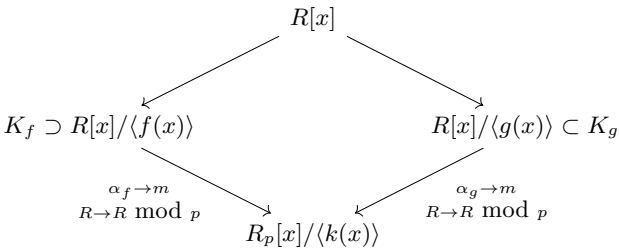

Fig. 2: Commutative diagram of exTNFS with $R = \mathbb{Z}(\iota)$ and $R_p = R/pR$. When $R = \mathbb{Z}$, it yields the diagram for NFS over non-prime field. When $k(x) = x - m$, it yields the diagram for TNFS.

In our extended TNFS, we consider two irreducible polynomials f and g in $R[x]$, where R is the ring defined as before. At this stage, we let $k(x) \in R_p[x] = \mathbb{F}_{p^\eta}[x]$ be irreducible of degree κ and we impose the conditions such that k divides both f and g modulo pR.

Let $R_p := R/pR$. By the above conditions on f, g, h, and k, there exist two ring homomorphisms from $R[x]/f(x)$ (resp. $R[x]/g(x)$) to $R_p[x]/k(x) = \mathbb{F}_Q$. Each of homomorphism maps the root α_f (resp. α_g) of f (resp. g) to $m \in R_p$, where m denotes a root of $k(x)$ modulo pR. See the commutative diagram given in Figure 2. When $R = \mathbb{Z}$, it yields the digram in the classical NFS for target field $\mathbb{F}_{p^\kappa}$. When $k(x) = x - m$ for a common root m of f and g, it simply provides the diagram for the TNFS as in Figure 1.

As in [1], we take the coefficients of f or g from $\mathbb{Z}$, not in R itself, but we keep considering f and g as polynomials in $R[x]$. Denote K_f (resp. K_g) by the number field defined by f (resp. g) over the field $\mathbb{Q}[t]/h(t)$. We consider $R[x]/f(x)$ (resp. $R[x]/g(x)$) as a subring of K_f (resp. K_g). In the case of exTNFS, these conditions on f and g further ask the coefficients of k to be in $\mathbb{Z}_p$, instead of $R_p = \mathbb{F}_{p^\eta}$.

Afterwards, the exTNFS algorithm proceeds as usual. It comprises of polynomial selection, relation collection, linear algebra step, and individual logarithm

phase. Most of these steps are quite similar to the TNFS algorithms as we shall explain below.

3 Detailed Descriptions

3.1 Polynomial Selection

As described before, we take f and g from $\mathbb{Z}[x]$, but in the following analysis we keep considering them as in $R[x]$. Then the previous condition on $k \in R_p[x]$ implies that k should be an irreducible polynomial in $R_p[x]$ with coefficients in $\mathbb{Z}_p$ satisfying that $k \mid \gcd(f, g) \pmod{p}$. Recall that $R_p = \mathbb{F}_{p^\eta}$, where $\deg(k) = \kappa$ is coprime to η. Since any irreducible polynomial over $\mathbb{F}_p$ of degree κ is also irreducible over $\mathbb{F}_{p^\eta}$ for $\gcd(\eta, \kappa) = 1$, we are free to choose k from any irreducible polynomial over $\mathbb{F}_p$.

For our purpose, one can use any polynomial selection method as in the NFS algorithm for large prime cases [10,1,13]. To fix ideas, we take polynomials f and g following by the JLSV algorithm [10].

JLSV algorithm. We briefly describe the polynomial selection in the JLSV algorithm for the large prime characteristic case ([10], Sec 3.2). One first chooses a monic polynomial $f_0(x)$ of degree κ, and has small coefficients. Set an integer $W \sim p^{1/(D+1)}$, where D (the precise value will be determined later) will be $D := \deg(g) \geq \kappa$. Then we define $f(x) := f_0(x + W)$. Take the coefficients of $g(x)$ by the LLL reduction output of the lattice L defined by the columns:

$$L := (p \cdot \mathbf{x^0}, \ldots, p \cdot \mathbf{x}^\kappa, \mathbf{f(x)}, \mathbf{xf(x)}, \ldots, \mathbf{x^{D+1-\kappa} f(x)}).$$

Here, $\mathbf{f(x)}$ denotes a vector by its coefficients for a polynomial f. Finally, we set $k = f$ and we have $\|f\|_\infty \approx \|g\|_\infty \approx p^{\kappa/(D+1)}$, where $\|f\|_\infty$ denotes the absolute value of the largest coefficient of f.

Choice of h. Now we are left to select an irreducible polynomial $h(t)$ of degree η to define a ring $R = \mathbb{Z}[t]/h(t)$. We also require that h remains irreducible modulo p. We select the coefficients of h to be small so that $\|h\|_\infty = O(1)$. Heuristically, one can find such polynomials after η trials, since the probability of irreducibility modulo p is $\approx 1/\eta$. For more rigorous description on the existence of such polynomials, refer to [3] for details.

3.2 Relation Collection

As usual, we say that we obtain a relation when two principal ideals each of which is generated by the image of a polynomial $r(x) \in R[x]$ in K_f or K_g simultaneously factor into prime ideals of norm less than a value B (will be determined later).

Throughout this section, to fix ideas, we only consider the cases of f-side, but it also readily applies to the case of g-side.

Factor base. In particular, we only consider linear polynomials of form $r(x) = a - bx$ as in the case of the TNFS. It helps us to deal with only prime ideals of degree 1 as a factor base element (except a few ideals that divides the discriminants).

The following proposition [7, Lemma 2.3.9] is a simple generalization of Lemma 10.5.1 in [6] which was restated in [3, Proposition 1].

Proposition 1 ([3], Proposition 1.). *Let $\mathbb{Q}(\iota) = \mathbb{Q}[t]/h(t)$ be a number field and $\mathcal{O}_\iota$ be its ring of integers. Let f be an irreducible polynomial in $\mathcal{O}_\iota[x]$ and α denotes one of its roots. We consider the extension number field $K_f := \mathbb{Q}(\iota, \alpha)$. Denote $\mathcal{O}_f$ by its ring of integers. Let $\mathfrak{D}$ be a prime ideal in K_f lying over a prime ideal $\mathfrak{q} \subseteq \mathcal{O}_\iota$. If $\mathfrak{D}$ divides the ideal $(a - b\alpha) \subset K_f$ for any coprime elements $a, b \in \mathcal{O}_\iota$, then either $\mathfrak{q}$ divides the index $[\mathcal{O}_f : \mathcal{O}_\iota[\alpha]]$ or*

$$\mathfrak{D} = \langle \mathfrak{q}, \alpha - \gamma \rangle,$$

where γ is an element in $\mathbb{Q}(\iota)$ such that $\gamma \equiv a/b \pmod{\mathfrak{q}}$.

As a consequence of this proposition, we keep only the ideals of degree 1 in the factor bases of each side. We define the factor base for f for a smoothness bound B (will be determined later) by

$$\mathcal{F}_f(B) = \left\{ \langle \mathfrak{q}, \alpha - \gamma \rangle : \begin{array}{l} \mathfrak{q} \text{ is a prime in } \mathbb{Q}(\iota) \text{ lying over prime} \\ p \leq B \text{ and } f(\gamma) \equiv 0 \pmod{\mathfrak{q}} \end{array} \right\}.$$

We define $\mathcal{F}_g(B)$ similarly. As usual, we have to deal with the case when $\mathfrak{q}$ divides the index ideal $[\mathcal{O}_f : \mathcal{O}_\iota[\alpha]]$ separately. To do this, we add the ideals above $Disc(f)$ and the ideals above the leading coefficients to the factor base for f, and similarly for g. See [3] for details.

Finally, we write the set of all the factor base elements for both side by $\mathcal{F}$. By the prime number theorem, we again make an usual heuristic arguments that $\#\mathcal{F} \approx 2(B/\log B)$. In our analysis, we approximate $\#\mathcal{F} = L_Q(1/3, \beta)$ for some $\beta > 0$.

Estimation of the norm size. Once the factor base is fixed, we search for relations by testing the smoothness of $N_{K_f/\mathbb{Q}}(a - b\alpha_f)$ for $a, b \in R = \mathbb{Z}(\iota)$. For this, we first estimate the size of the norm.

Let $a(t), b(t) \in \mathbb{Z}[t]$ be polynomials of at most degree $\eta - 1$. Denote A by an absolute bound on the coefficients of $a(t)$ and $b(t)$. We introduce the following lemma derived in [3].

Lemma 1 ([3], Theorem 3.). *Let h and f be monic irreducible polynomials over $\mathbb{Z}$ of respective degrees η and $\kappa := \deg(f)$. Let $K_f := \mathbb{Q}(\iota, \alpha)$ be the composition field as defined in Proposition 1, where ι and α are respective roots of h and f. Let $a(t), b(t) \in \mathbb{Z}[t]$ be polynomials of at most degree $\eta - 1$ with $\|a\|_\infty, \|b\|_\infty \leq A$. Then we have*

$$|N_{K_f/\mathbb{Q}}(a(\iota) - b(\iota)\alpha_f)| < A^{\eta \cdot \kappa} \|f\|_\infty^\eta \|h\|_\infty^{\kappa \cdot (\eta - 1)} C(\eta, \kappa), \tag{1}$$

where $C(\eta, \kappa) = (\eta + 1)^{(3\kappa+1)\eta/2} (\kappa + 1)^{3\eta/2}$.

Remark that we conditioned on h and f to be monic in Lemma 1. However, this is just to avoid some technicalities, and we simply overcome the issue by adding a few prime ideals that divide the leading coefficient to the factor base. See [3]. For the simplicity, we keep assuming the polynomials are monic.

Turning to our interest. To fix idea, we approximate the value $D := \deg(g) \geq \kappa$ by,

$$D = c_D \left(\frac{\log Q}{\log \log Q} \right)^{1/3}.$$

Let us evaluate $\|h\|_\infty = O(1)$ and the values of $\|f\|_\infty, \|g\|_\infty \approx p^{\kappa/(D+1)}$ coming from the JLSV polynomial selection (Section 3.1) to Equation 1. Then we get

$$|N_{K_f/\mathbb{Q}}(a - b\alpha_f)| < \left(A^{\eta\kappa}(p^{\frac{\kappa}{D+1}})^\eta\right)^{1+o(1)} = \left(E^\kappa P^{\frac{\kappa}{D+1}}\right)^{1+o(1)}, \tag{2}$$

and

$$|N_{K_g/\mathbb{Q}}(a - b\alpha_g)| < \left(A^{\eta D}(p^{\frac{\kappa}{D+1}})^\eta\right)^{1+o(1)} = \left(E^D P^{\frac{\kappa}{D+1}}\right)^{1+o(1)}, \tag{3}$$

where we set $E := A^\eta$ and $P := |R_p| = p^\eta$.

In our analysis, we assumed that the contribution of $C(\eta, D)$ (thus, so $C(\eta, \kappa)$) is negligible. It is equivalent to ask the value of $C(\eta, D)$ to be strictly smaller than $L_Q(2/3)$, or, the expression for η is strictly less than $\left(\frac{\log Q}{\log \log Q}\right)^{1/3}$. It is also equivalent to $P = L_Q(\ell_P)$ for some $\ell_P > 2/3$.

It is remarkable that the above expressions for the norms are the same for the large prime case [10, Appendix A.3.], where $P = p$ and $\kappa = n$. Recall that the TNFS algorithm had a similar analogy with the NFS for the prime field case.

Virtual logarithms. From a relation, we deduce a linear relation in terms of Schirokauer's virtual logarithms [14]. For this, it is simpler to work with $K_f = \mathbb{Q}(\theta)$ for a primitive element θ in K_f. Since the arguments in our exTNFS does not change from that of the TNFS, we simply refer to [3] for further details.

3.3 Complexity Analysis

In this section, we analyze the complexity of the main phase of the algorithm. It is analogous to that of the NFS for large prime cases (e.g. [10, Appendix A.3.]).

In our case, the size of the search space for pairs $(a, b) \in R^2$ is E^2. We collect approximately B linear relations of virtual logarithms to solve the logarithms of the factor base elements. The cost for linear algebra step is thus of B^2. To minimize the cost, we set

$$E = B = L_Q(1/3, \beta) \text{ for some } \beta > 0.$$

From Equation (2) and (3), the product of the norms is bounded by $\left(E^{D+\kappa} P^{\frac{2\kappa}{D+1}}\right)^{1+o(1)} = \left(E^{D+\kappa} Q^{\frac{2}{D+1}}\right)^{1+o(1)}$. When $P = L_Q(\ell_P)$ for $\ell_P > 2/3$, then the contribution by κ becomes negligible to D (recall that $Q = P^\kappa$) and we have

$$\text{(absolute value of the product of norms)} = L_Q(2/3, \beta c_D + 2/c_D),$$

which is minimized to $L_Q\big(2/3, 2\sqrt{2\beta}\big)$ at $c_D = \sqrt{2/\beta}$.

Let $\mathcal{P}$ denote the probability that the product of the norms factors into primes less than B. Using Canfield-Erdös-Pomerance theorem, we have

$$\mathcal{P} = L_Q(1/3, -2/3\sqrt{2/\beta}).$$

Since we want to have $E^2 \cdot \mathcal{P} = B$, we take $1/\mathcal{P} = B$. It yields the value of $\beta = (8/9)^{1/3}$. Thus the total cost for the main phase becomes

$$L_Q(1/3, 2\beta) = L_Q(1/3, (64/9)^{1/3}),$$

where $(64/9)^{1/3} \approx 1.923$. Recall that our complexity analysis has carried out under the condition that

$$p = L_Q(\ell_p, c_p) \text{ for some } \ell_p > 1/3.$$

This should be compared that a previous state-of-art algorithm in the medium characteristic case, the MNFS with conjugation method [13], has a complexity of $L_Q(1/3, 2.156)$. Moreover, this already has a similar complexity with the SNFS in the same case, which applies only for special prime case. Furthermore, using many variants, we show that the complexity can be reduced further in Section 4.

The choice of parameters. Throughout this section, we assumed that $p = L_Q(\ell_p)$ for $\ell_p > 1/3$, conditioned on that

$$P = p^\eta = L_Q(\ell_P) \text{ for some } \ell_P > 2/3,$$

for κ to be negligible to D, and

$$\eta = c_\eta \left(\frac{\log Q}{\log\log Q}\right)^{\ell_\eta} \text{ for some } \ell_\eta < 1/3,$$

for $C(\eta, D)$ to be negligible to $L_Q(2/3)$.

This can be done as follows: From $P = L_Q(\ell_P) = L_Q(\ell_p + \ell_\eta)$, these two requirements are equivalent to $2/3 - \ell_p < \ell_\eta < 1/3$. Since $\ell_p > 1/3$ (i.e. $1/3 > 2/3 - \ell_p$), one can always select a real number ℓ_η between $2/3 - \ell_p$ and $1/3$.

4 Variants.

The case of the SNFS. In the case of the prime p is of a special form, we apply Joux and Pierrot's SNFS method [11] to our exTNFS. This includes the case appears in the pairing constructions (e.g. BN curve [5], Freeman curve [8]), but it generally applies to any case satisfying that

$$p = \Pi(u) \text{ for some } u,$$

where $\Pi(x)$ is a polynomial of degree λ of small coefficients.

In the case, our exTNFS selects two polynomials similarly as in Joux and Pierrot's algorithm. Let $h(t) \in \mathbb{Z}[t]$ be an irreducible polynomial of degree η, still irreducible modulo p, and of small coefficients. Choose $k(x)$ an irreducible polynomial of degree κ over $\mathbb{F}_p$, but viewed as a polynomial over $R_p = \mathbb{F}_{p^\eta}$ similarly before. Note that k is still irreducible over R_p since $\gcd(\kappa, \eta) = 1$. Let $f = k$ be of form

$$f(x) = k(x) = x^\kappa + S(x) - u,$$

where the coefficients of S are chosen from $\{-1, 0, 1\}$ and $p = \Pi(u)$. Choose g such that

$$g(x) = \Pi(x^\kappa + S(x)).$$

Then, we deduce that $k \mid g \bmod pR$.

Applying Lemma 1, we obtain the product of norm bounded by

$$|N_{K_f/\mathbb{Q}}(a - b\alpha_f)| \cdot |N_{K_g/\mathbb{Q}}(a - b\alpha_g)| < \left(E^{(\lambda+1)\kappa} P^{1/\lambda}\right)^{1+o(1)},$$

where $E = A^\eta$ and $P = p^\eta$ as before.

Set $\kappa\lambda = \left(\frac{2\log Q}{3\log\log Q}\right)^{1/3}$. Following the analysis by Joux and Pierrot [11, Section 6.3.], instead of p by P, we obtain the overall complexity given by

$$L_Q(1/3, (32/9)^{1/3})$$

conditioned on that $P = L_Q(\ell_P)$ for $\ell_P > 2/3$. As before, the condition translates to $\ell_p > 1/3$. See the end of Section 3.3.

The case of the MNFS. Choose f_1 and f_2 followed by the JLSV algorithm as described earlier (in terms of the previous notations, $f_1 = f$ and $f_2 = g$). We select other $V - 2$ irreducible polynomials as linear combinations of f_1 and f_2 of coefficients bounded by $\sqrt{V}$. Denote α_i by a root of f_i for $i = 1, 2, \ldots, V$. As before, we have the norms bounded by

$$|N_{K_{f_1}/\mathbb{Q}}(a - b\alpha_1)| < \left(E^\kappa P^{\kappa/(D+1)}\right)^{1+o(1)},$$

and

$$|N_{K_{f_i}/\mathbb{Q}}(a - b\alpha_i)| < \left(E^D P^{\kappa/(D+1)}\right)^{1+o(1)} \text{ for } 2 \le i \le V.$$

We choose $\kappa = \frac{1}{c_P}\left(\frac{\log Q}{\log\log Q}\right)^{1-c_P}$, $D = c_D\left(\frac{\log Q}{\log\log Q}\right)^{1/3}$, and $E = L_Q(1/3, c_E c_P)$. When $\ell_P > 2/3$, we get $E^\kappa = L_Q(\ell)$ for $\ell < 2/3$.

Replaced with p by P in the analysis by Barbulescu and Pierrot [4, Section 5.3.], we deduce the complexity of exTNFS using the MNFS in the medium characteristic case,

$$L_Q\left(1/3, \left(\frac{92 + 26\sqrt{13}}{27}\right)^{1/3}\right).$$

Similarly before, the condition $\ell_P > 2/3$ translates to $\ell_p > 1/3$.

5 Conclusion

In this paper, we extend the TNFS which was recently revisited by Barbulescu, Gaudry, and Kleinjung [3]. Our results shows that the DLP over medium characteristic field, which was believed to be harder before, is not so harder than the case of large characteristic field. Precisely, the complexity of our extended TNFS does not depend on the size of the characteristic, whenever $p = L_Q(\ell_p)$ for $\ell_p > 1/3$. Consequently, in the world of DLP over finite fields, we only have two separate cases, small characteristic case (when $\ell_p < 1/3$) and large characteristic case (when $\ell_p > 1/3$).

References

1. R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain. Improving NFS for the discrete logarithm problem in non-prime finite fields. In Oswald and Fischlin [12], pages 129–155.
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 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, pages 1–16, 2014.
3. R. Barbulescu, P. Gaudry, and T. Kleinjung. The Towed Number Field Sieve. In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, to appear*, LNCS. Springer, 2015.
4. R. Barbulescu and C. Pierrot. The multiple number field sieve for medium- and high-characteristic finite fields. *LMS Journal of Computation and Mathematics*, 17:230–246, 2014.
5. P. S. L. M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers*, pages 319–331, 2005.
6. H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag New York, Inc., New York, NY, USA, 1993.
7. H. Cohen. *Advanced topics in computational number theory*. Graduate texts in mathematics. Springer, New York, N.Y., Berlin, Heidelberg,, 2000.
8. D. Freeman. Constructing pairing-friendly elliptic curves with embedding degree 10. In *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, pages 452–465, 2006.
9. D. M. Gordon. Discrete logarithms in gf(p) using the number field sieve. *SIAM J. Discret. Math.*, 6(1):124–138, Feb. 1993.
10. A. Joux, R. Lercier, N. P. Smart, and F. Vercauteren. The number field sieve in the medium prime case. In C. Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*, pages 326–344. Springer, 2006.
11. A. Joux and C. Pierrot. The special number field sieve in $\mathfrak{O}_{\mathrm{p}^{\mathrm{n}}}$ - application to pairing-friendly constructions. In *Pairing-Based Cryptography - Pairing 2013 - 6th International Conference, Beijing, China, November 22-24, 2013, Revised Selected Papers*, pages 45–61, 2013.

12. E. Oswald and M. Fischlin, editors. *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*. Springer, 2015.
13. C. Pierrot. The multiple number field sieve with conjugation and generalized joux-lercier methods. In Oswald and Fischlin [12], pages 156–170.
14. O. Schirokauer. Discrete logarithms and local units. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 345(1676):409–423, 1993.
15. O. Schirokauer. Using number fields to compute logarithms in finite fields. *Math. Comput.*, 69(231):1267–1283, 2000.