ECC 2016

September 5–7, 2016

Extended Tower Number Field Sieve

Taechan Kim and Razvan Barbulescu

NTT Secure Platform Laboratories and CNRS, Univ Paris 6, Univ Paris 7

Discrete Logarithm Problem

Discrete Logarithm Problem (DLP)

- Let $G := \langle g \rangle$, a cyclic group of order N.
- Given g^a, find a.

DLP over generic group

- The best-known algorithm runs in time $O(\sqrt{N})$ group operations.
  e.g. Pollard's algorithm, Baby-Step-Giant-Step algorithm, ...
- The running time is exponential in $\log N$.

DLP over finite fields

- DLP over $\mathbb{F}_Q := \mathbb{F}_{p^n}$ can be solved in subexponential time complexity.
- Index-calculus-like algorithms such as Number Field Sieve, Function Field Sieve.

DLP and the Size of characteristic

DLP over small characteristic fields

- Barbulescu, Gaudry, Joux, and Thomé (2014) showed that DLP over $\mathbb{F}_{p^n}$ can be solved in quasi-polynomial time, when p is small enough compared to n.
- This is a successor of Function Field Sieve (FFS) method.

DLP over larger characteristic

- We focus on the DLP over larger characteristic fields.
- In the case of larger characteristic, most of best algorithms are based on Number Field Sieve (NFS) method.

Why do we consider DL over $\mathbb{F}_{p^n}$?

Pairings security

The security of pairings based cryptosystems relies on the difficulty of:

- elliptic curves discrete logarithms;
- finite fields discrete.

Embedding degree

If a paring is such that

$$E_1/\mathbb{F}_p[r] \times E_2/\mathbb{F}_p[r] \to \mu_r \subset (\mathbb{F}_{p^n})^*$$

then n is called the embedding degree.

Cryptographic sizes

Key sizes

security (bits)	bitsize of p^n	bitsize of $r \approx p$	quotient n
80	1024	160	6
128	3072	256	12
256	15360	512	30

Pairings

- discrete log problem over elliptic curves must be as hard as discrete log in $\mathbb{F}_{p^n}$ (under the assumption that it is as hard as factoring of the same size);
- most important cases: $2 \leq n \leq 30$;
- very fast construction (Barreto-Naehrig) at $n = 12$.

Chronology

NFS and FFS

- $\mathbb{F}_p$, '90, Gordon / Schirokauer (NFS)
- $\mathbb{F}_{p^n}$,
  - '00, Schirokauer, $\mathbb{F}_{p^n} = \mathbb{Z}[\iota]/p\mathbb{Z}[\iota]$ (TNFS)
  - '06, Joux Lercier Smart Vercauteren, modify polynomial selection (JLSV)
  - this talk, combine TNFS and JLSV: exTNFS

Previous complexity of DLP in $\mathbb{F}_Q$ when $p = L_Q(\ell_p)$

Recent improvements of NFS

After JLSV's idea, NFS has developed in recent few years, particularly in the polynomial selection step.

L_Q-notation

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

Complexity of number field sieve

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	best $\ell_p = 2/3$	$2/3 < \ell_p < 1$
NFS-JLSV	128	64	64
NFS-Conj/gJL	96	48	64
NFS-SarkarSingh	96	48	64
TNFS	none	none	64

Table : Each cell indicates m if the complexity is $L_Q(1/3, (m/9)^{1/3})$.

An anomaly

- Complexity of NFS in medium characteristic field is strictly larger than in large characteristic case.
- The best complexity is in the boundary case ($\ell_p = 2/3$).

Previous complexity of DLP in $\mathbb{F}_Q$ when $p = L_Q(\ell_p)$

Mutltiple number field sieve

Table : The complexity of each algorithms using multiple number fields (MNFS)

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	best $\ell_p = 2/3$	$2/3 < \ell_p < 1$
MNFS-JLSV	122.87	61.93	61.93
MNFS-(Conj and GJL)	89.45	45.00	61.93
MNFS-SarkarSingh	89.45	45.00	61.93
MTNFS	none	none	61.93

Special number field sieve

Table : The complexity of each algorithms used when the characteristic has a special form (SNFS)

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	$2/3 < \ell_p < 1$
SNFS-JP	64	32
STNFS	none	32

Previous complexity of DLP in $\mathbb{F}_Q$ when $p = L_Q(\ell_p)$

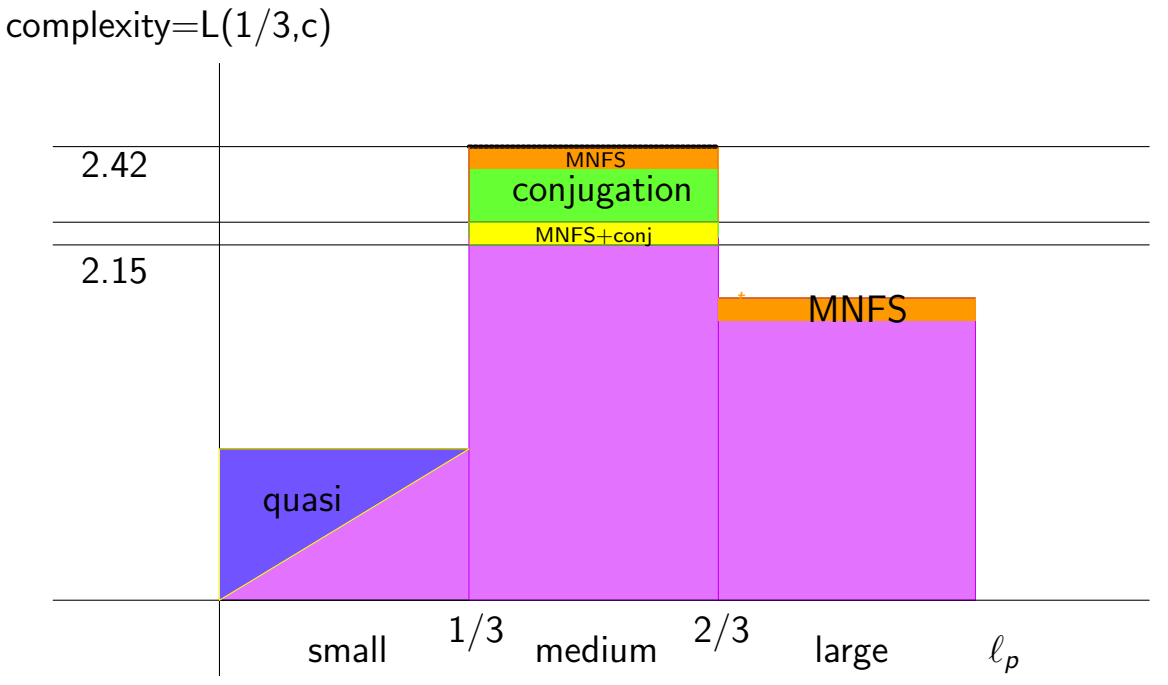


Figure : Up-to-date Complexity of DLP in $\mathbb{F}_Q$

Overview of Our Results

Our Results (extended Tower Number Field Sieve, exTNFS)

- (Idea) Combine TNFS and JLSV's method.
- (Get rid of the anomaly) When n (field extension degree) has a nontrivial factor of appropriate size,

(DLP in medium characteristic field) $\leq$ (DLP in large characteristic field)

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	best $\ell_p = 2/3$	$2/3 < \ell_p < 1$
NFS-JLSV	128	64	64
NFS-Conj/gJL	96	48	64
NFS-SarkarSingh	96	48	64
TNFS	none	none	64

Table : Each cell indicates m if the complexity is $L_Q(1/3, (m/9)^{1/3})$. When n has a nontrivial factor of appropriate size

Overview of Our Results

Our Results (extended Tower Number Field Sieve, exTNFS)

- (Idea) Combine TNFS and JLSV's method.
- (Get rid of the anomaly) When n (field extension degree) has a nontrivial factor of appropriate size,

(DLP in medium characteristic field) $\leq$ (DLP in large characteristic field)

$p = L_Q(\ell_p)$	best $1/3 < \ell_p < 2/3$	$\ell_p = 2/3$	$2/3 < \ell_p < 1$
exTNFS-JLSV	64	64	64
exTNFS-Conj/gJL	48 (best)	48	64
exTNFS-SarkarSingh	48 (best)	48	64
TNFS	none	none	64

Table : Each cell indicates m if the complexity is $L_Q(1/3, (m/9)^{1/3})$. When n has a nontrivial factor of appropriate size

DLP in $\mathbb{F}_Q = \mathbb{F}_{p^n}$ when n is composite with good factors

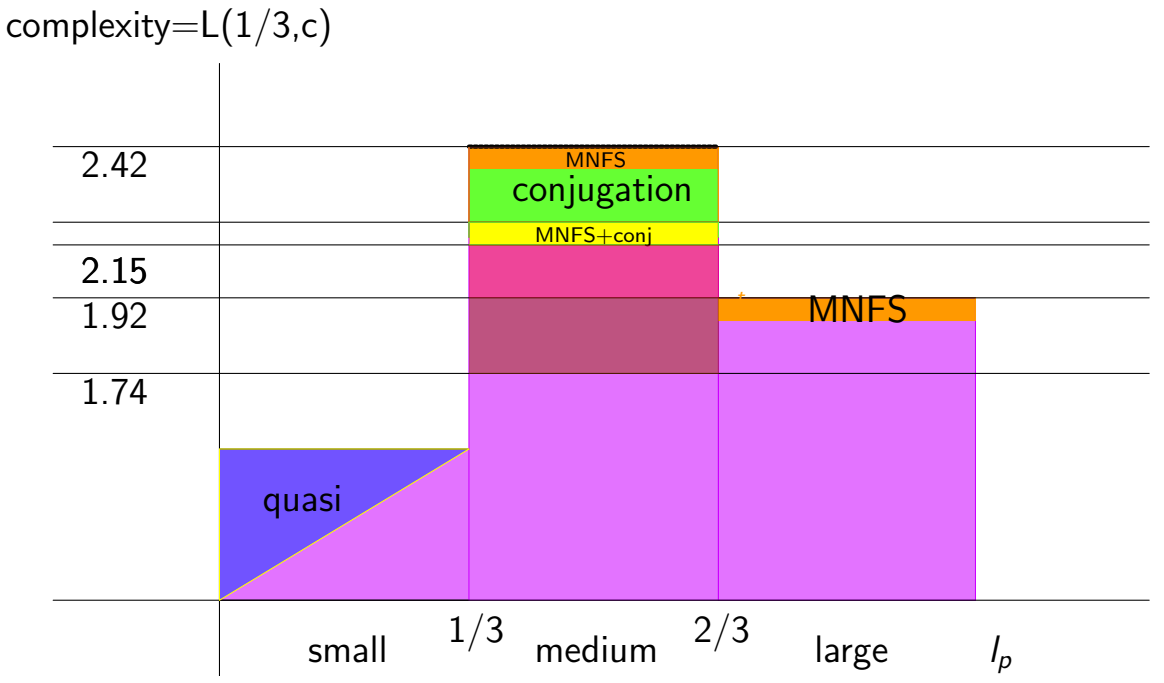


Figure : A New Complexity of DLP in $\mathbb{F}_Q$

DLP in $\mathbb{F}_Q = \mathbb{F}_{p^n}$ when n is composite with good factors

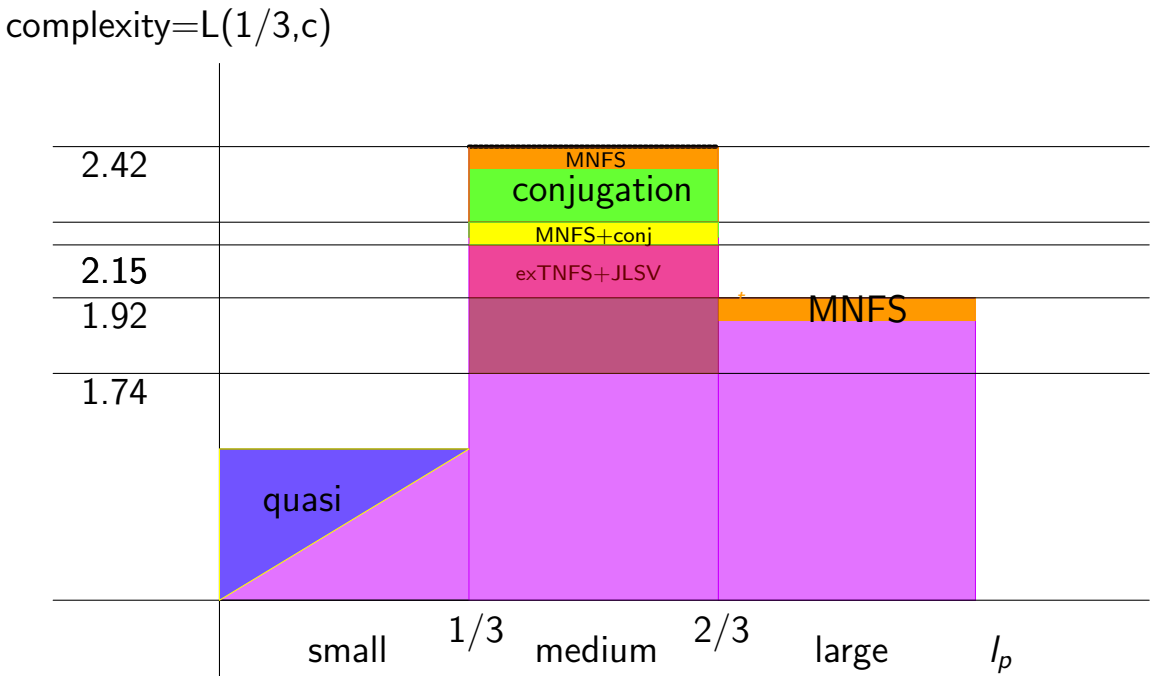


Figure : A New Complexity of DLP in $\mathbb{F}_Q$

DLP in $\mathbb{F}_Q = \mathbb{F}_{p^n}$ when n is composite with good factors

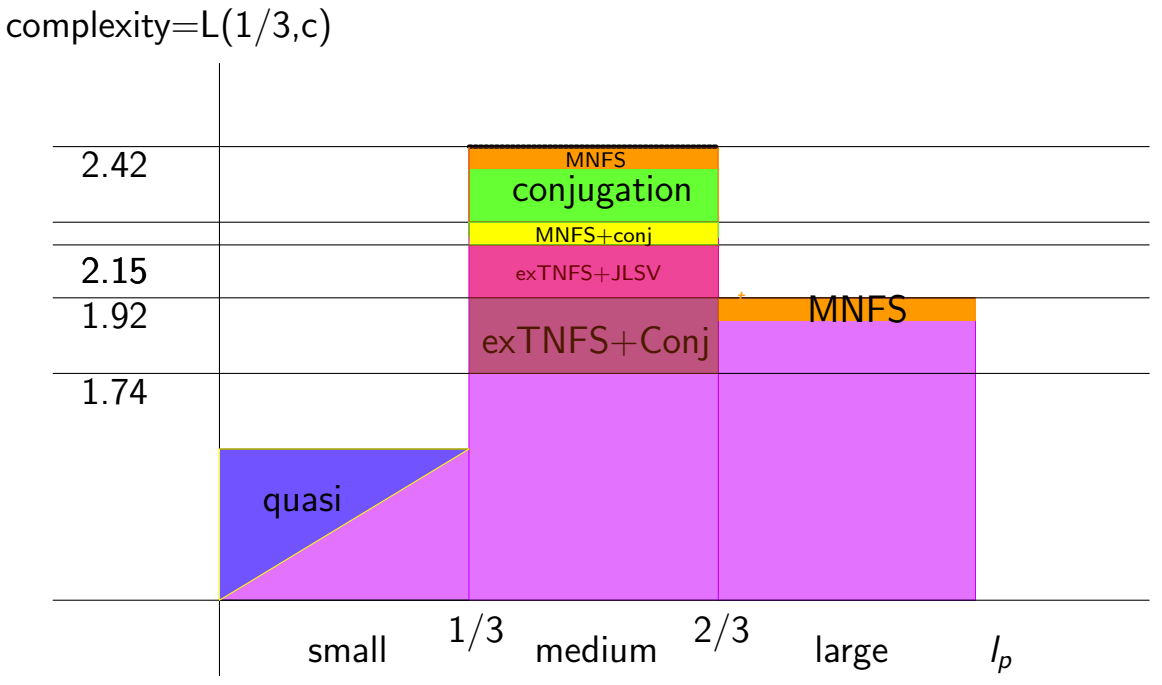


Figure : A New Complexity of DLP in $\mathbb{F}_Q$

New complexity of DLP in $\mathbb{F}_Q$ when $p = L_Q(\ell_p)$

Multiple number field sieve

Table : The complexity of each algorithms using multiple number fields (MNFS)

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	best $\ell_p = 2/3$	$2/3 < \ell_p < 1$
MNFS-JLSV	122.87	61.93	61.93
MNFS-(Conj and GJL)	89.45	45.00	61.93
MNFS-SarkarSingh	89.45	45.00	61.93
MTNFS	none	none	61.93

Special number field sieve

Table : The complexity of each algorithms used when the characteristic has a special form (SNFS)

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	$2/3 < \ell_p < 1$
SNFS-JP	64	32
STNFS	none	32

New complexity of DLP in $\mathbb{F}_Q$ when $p = L_Q(\ell_p)$

Multiple number field sieve

Table : The complexity of each algorithms using multiple number fields (MNFS)

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	best $\ell_p = 2/3$	$2/3 < \ell_p < 1$
MexTNFS-JLSV	61.93	61.93	61.93
MexTNFS-(Conj and GJL)	45.00	45.00	61.93
MexTNFS-SarkarSingh	45.00	45.00	61.93
MTNFS	none	none	61.93

Special number field sieve

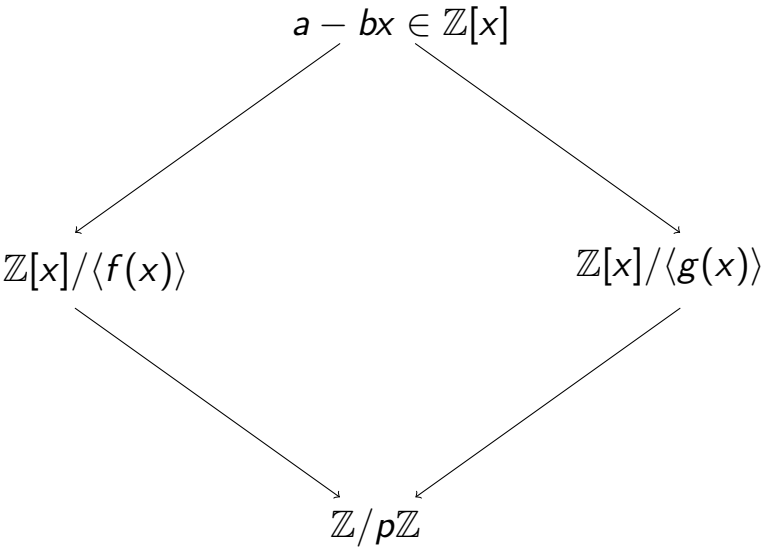
Table : The complexity of each algorithms used when the characteristic has a special form (SNFS)

$p = L_Q(\ell_p)$	$1/3 < \ell_p < 2/3$	$2/3 < \ell_p < 1$
SexTNFS-JP	32	32
STNFS	none	32

The number field sieve(NFS): diagram

NFS for DLP in $\mathbb{F}_p$

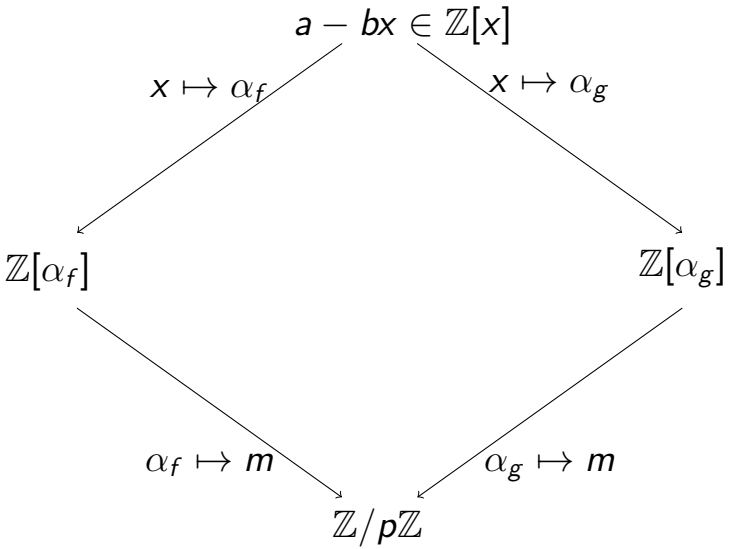
Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.



The number field sieve(NFS): diagram

NFS for DLP in $\mathbb{F}_p$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.



The NFS algorithm for $\mathbb{F}_p$

Input a finite field $\mathbb{F}_p$, two elements t (generator) and s
Output $\log_t s$

The NFS algorithm for $\mathbb{F}_p$

Input a finite field $\mathbb{F}_p$, two elements t (generator) and s
Output $\log_t s$

1: (Polynomial selection) Choose two polynomials f and g in $\mathbb{Z}[x]$ which have a common root modulo p;

The NFS algorithm for $\mathbb{F}_p$

Input a finite field $\mathbb{F}_p$, two elements t (generator) and s
Output $\log_t s$

1: (Polynomial selection) Choose two polynomials f and g in $\mathbb{Z}[x]$ which have a common root modulo p;

2: (Sieve) Collect relatively prime pairs (a, b) such that the norms $N_f(a - b\alpha_f)$ and $N_g(a - b\alpha_g)$ are B-smooth (for a parameter B);

The NFS algorithm for $\mathbb{F}_p$

Input a finite field $\mathbb{F}_p$, two elements t (generator) and s
Output $\log_t s$

1: (Polynomial selection) Choose two polynomials f and g in $\mathbb{Z}[x]$ which have a common root modulo p;

2: (Sieve) Collect relatively prime pairs (a, b) such that the norms $N_f(a - b\alpha_f)$ and $N_g(a - b\alpha_g)$ are B-smooth (for a parameter B);

3: Write a linear equation for each pair (a, b) found in the Sieve stage.

The NFS algorithm for $\mathbb{F}_p$

Input a finite field $\mathbb{F}_p$, two elements t (generator) and s
Output $\log_t s$

1: (Polynomial selection) Choose two polynomials f and g in $\mathbb{Z}[x]$ which have a common root modulo p;

2: (Sieve) Collect relatively prime pairs (a, b) such that the norms $N_f(a - b\alpha_f)$ and $N_g(a - b\alpha_g)$ are B-smooth (for a parameter B);

3: Write a linear equation for each pair (a, b) found in the Sieve stage.

4: (Linear algebra) Solve the linear system to find (virtual) logarithms of the prime ideals of norm less than B;

The NFS algorithm for $\mathbb{F}_p$

Input a finite field $\mathbb{F}_p$, two elements t (generator) and s
Output $\log_t s$

1: (Polynomial selection) Choose two polynomials f and g in $\mathbb{Z}[x]$ which have a common root modulo p;

2: (Sieve) Collect relatively prime pairs (a, b) such that the norms $N_f(a - b\alpha_f)$ and $N_g(a - b\alpha_g)$ are B-smooth (for a parameter B);

3: Write a linear equation for each pair (a, b) found in the Sieve stage.

4: (Linear algebra) Solve the linear system to find (virtual) logarithms of the prime ideals of norm less than B;

5: (Individual logarithm) Write $\log_t s$ in terms of the previously computed logs.

The polynomial selection is important

Size of norms

- If we sieve all pairs a, b so that $|a|, |b| \leq E$, the sieving cost is E^2.
- Let $K_f = \mathbb{Q}(\alpha_f) = \mathbb{Q}[x]/f(x)$. Then, (ignoring some negligible factors) we have

$$N_f := |N_{K_f/\mathbb{Q}}(a - b\alpha_f)| \leq E^{\deg(f)}\|f\|.$$

- If we reduce N_f and N_g, we can obtain relations with better probability (we can reduce the work!!).

Polynomial selection for $\mathbb{F}_p$: Base-m method

Put $m = \lfloor p^{\frac{1}{d+1}} \rfloor$ and write $p = f_d m^d + f_{d-1} m^{d-1} + \cdots f_1 m + f_0$ in base m and put

- $f = f_d x^d + \cdots + f_1 x + f_0$;
- $g = x - m$.

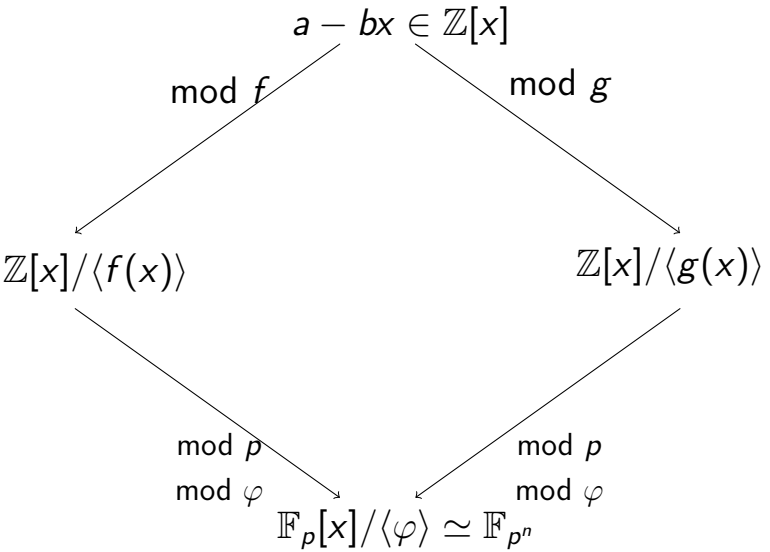
From the choice, we have

$$N_f \leq p^{1/(d+1)} E^d \text{ and } N_g \leq p^{1/(d+1)} E.$$

The idea of Joux Lercier Smart Vercauteren

Polynomial selection

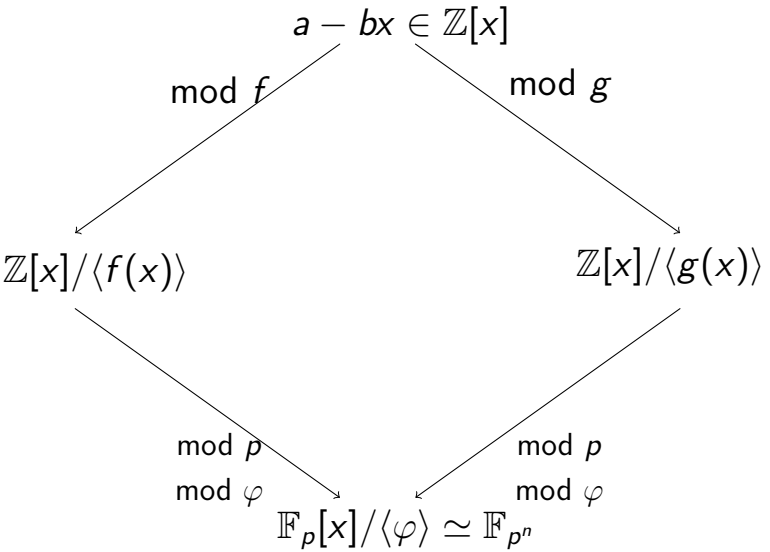
Select f and g which have a common ~~root~~ factor φ of degree n modulo p.



The idea of Joux Lercier Smart Vercauteren

Polynomial selection

Select f and g which have a common ~~root~~ factor φ of degree n modulo p.



Polynomial selection : conjugation method

Algorithm

1. Take $f_0, f_1 \in \mathbb{Z}[x]$ so that $\deg f_0 = n$ and $\deg f_1 < n$.
2. Take $a < p$ non-square so that $\sqrt{a}$ exists in $\mathbb{F}_p$ and $\varphi := f_0 + \sqrt{a} f_1$ is irreducible modulo p.
3. Set $f = f_0^2 - a f_1^2$.
4. Compute the rational reconstruction of $\sqrt{a}$ modulo p: u/u and set $g := u f_0 + v f_1$.

justification: f and g share the factor φ modulo p.

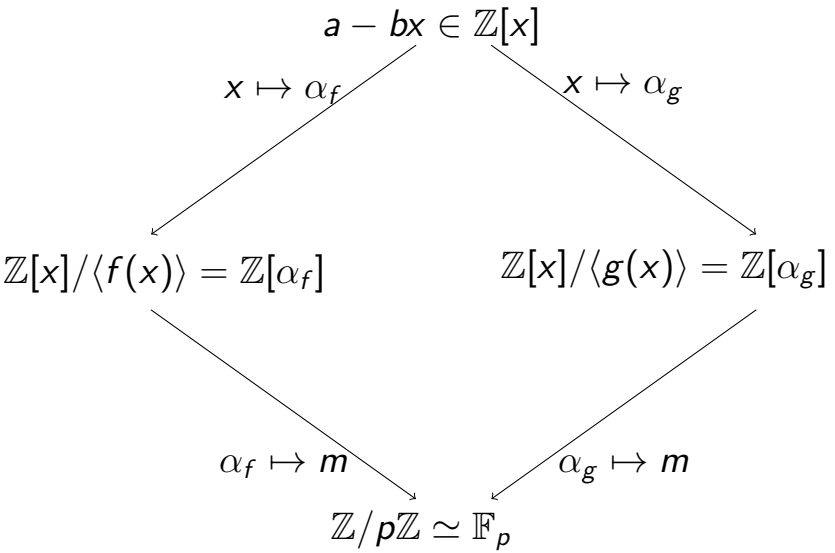
New complexity

When $n = \frac{1}{12}^{\frac{-1}{3}} (\frac{\log p^n}{\log\log p^n})^{\frac{1}{3}}$ the complexity is $L_{p^n}(1/3, \sqrt[3]{48/9})$ instead of $\geq L_{p^n}(1/3, \sqrt[3]{64/9})$

TNFS diagram

NFS for DLP in $\mathbb{F}_p$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

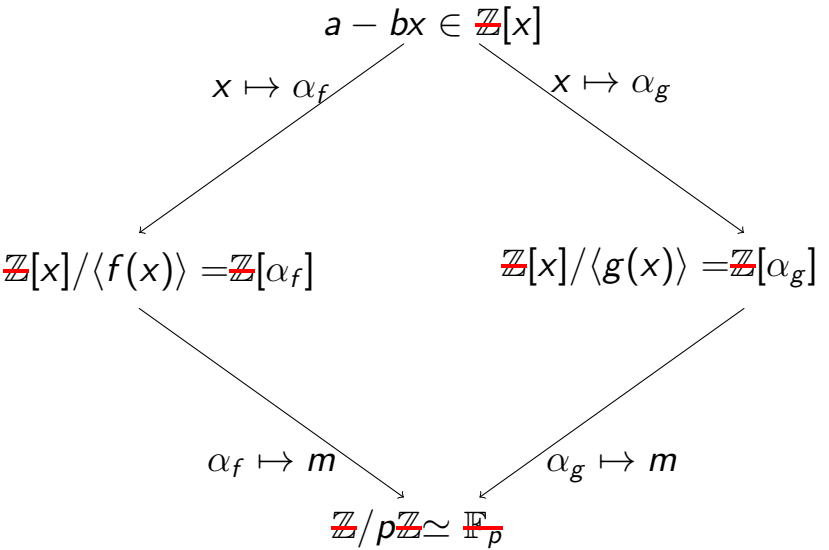


TNFS diagram

NFS for DLP in $\mathbb{F}_p$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

Let $h \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n such that p is inert in its number field $\mathbb{Q}(\iota)$; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^n}$.

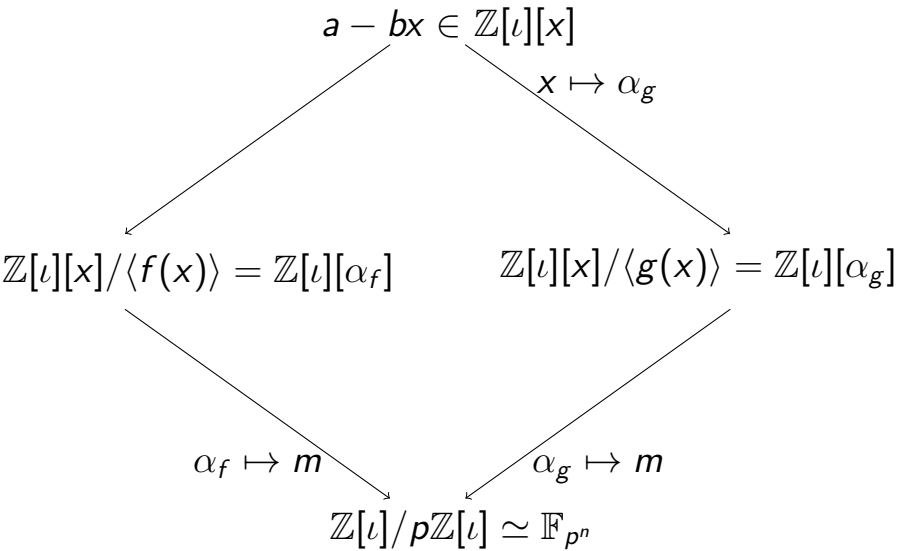


TNFS diagram

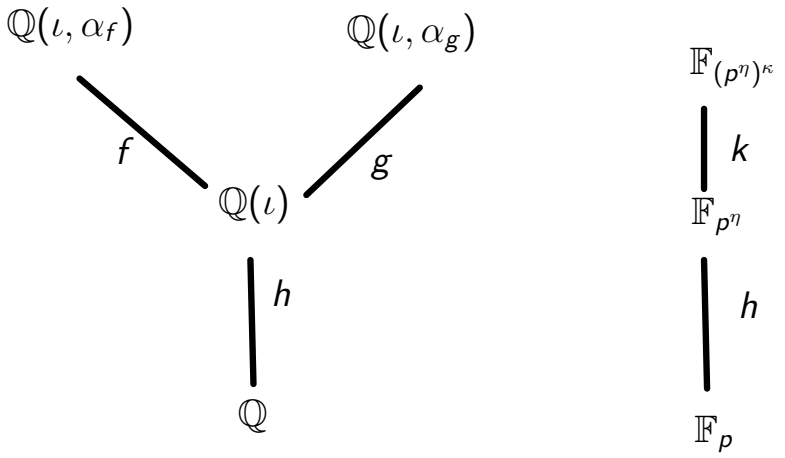
NFS for DLP in $\mathbb{F}_{p^n}$

Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.

Let $h \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n such that p is inert in its number field $\mathbb{Q}(\iota)$; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^n}$.



The extended TNFS

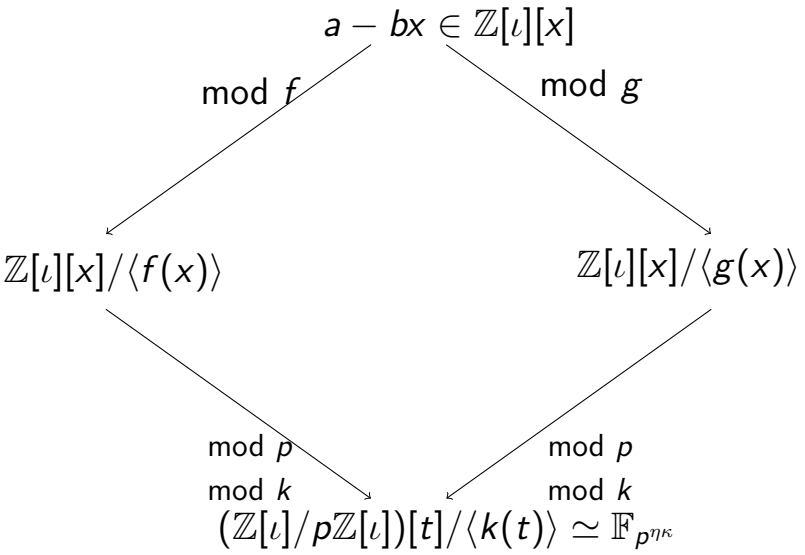


exTNFS algorithm

constraints: $n = \eta\kappa$ with $\gcd(\eta, \kappa) = 1$

1. select h as in TNFS for $\mathbb{F}_{p^\eta}$;
2. select f and g as for $\mathbb{F}_{p^\kappa}$ (e.g. JLSV, Conjugation, GJL, ...); put $k = \gcd(f \bmod p, g \bmod p)$;
3. continue the algorithm as for TNFS.

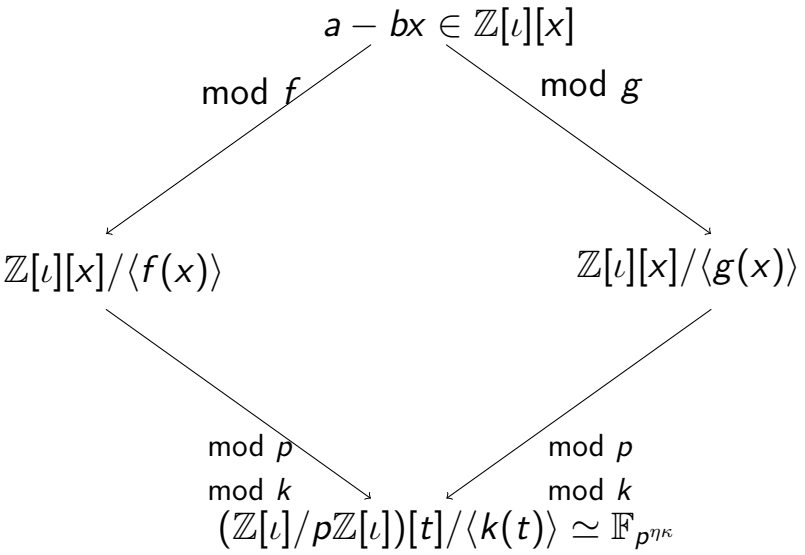
exTNFS diagram



Explication

- f and g are chosen from $\mathbb{Z}[x]$ but viewed as $\mathbb{Z}[\iota][x]$.
- k is irreducible over $\mathbb{F}_p$ and, since $\gcd(\eta, \kappa) = 1$, it is automatically irreducible over $\mathbb{F}_{p^\eta}$.

exTNFS diagram



Explication

- f and g are chosen from $\mathbb{Z}[x]$ but viewed as $\mathbb{Z}[\iota][x]$.
- k is irreducible over $\mathbb{F}_p$ and, since $\gcd(\eta, \kappa) = 1$, it is automatically irreducible over $\mathbb{F}_{p^\eta}$.

Size of norms

Complexity analysis

In the complexity analysis of the NFS, the size of the norm, $N_{K_f/\mathbb{Q}}(a - b\alpha_f)$ plays an important role, where $K_f = \mathbb{Z}[x]/f(x)$ or $K_f = \mathbb{Z}[\iota][x]/f(x)$ in (ex)TNFS.

Size of norms: Classical NFS

Let $K_f = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/f(x)$ and $|a|, |b| \leq E$. Then, we have

$$|N_{K_f/\mathbb{Q}}(a - b\alpha)| \leq (E^{\deg(f)}\|f\|)^{1+o(1)}$$

Size of norms

Complexity analysis

In the complexity analysis of the NFS, the size of the norm, $N_{K_f/\mathbb{Q}}(a - b\alpha_f)$ plays an important role, where $K_f = \mathbb{Z}[x]/f(x)$ or $K_f = \mathbb{Z}[\iota][x]/f(x)$ in (ex)TNFS.

Size of norms: Classical NFS

Let $K_f = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/f(x)$ and $|a|, |b| \leq E$. Then, we have

$$|N_{K_f/\mathbb{Q}}(a - b\alpha)| \leq (E^{\deg(f)}\|f\|)^{1+o(1)}$$

Size of norms: (ex)TNFS

Let $K_f = \mathbb{Q}(\iota, \alpha) = \mathbb{Q}(\iota)[x]/f(x)$ and $\mathbb{Q}(\iota) = \mathbb{Q}[t]/h(t)$. And let

$$a = \sum_{k=0}^{n-1} a_k \iota^k \text{ and } \sum_{k=0}^{n-1} b_k \iota^k$$

with a_k and b_k bounded in absolute value by $A = E^{1/n}$ so that we enumerate the same number of candidates as in NFS. Then, we have

$$|N_{K_f/\mathbb{Q}}(a - b\alpha)| \leq E^{\deg(f)}\|f\|^{\eta} L_{p^n}(2/3, o(1)),$$

when $\|h\| = O(1)$ and $p = L_{p^n}(\ell_p, c)$ for $\ell_p > 1/3$.

Size of norms

Complexity analysis

In the complexity analysis of the NFS, the size of the norm, $N_{K_f/\mathbb{Q}}(a - b\alpha_f)$ plays an important role, where $K_f = \mathbb{Z}[x]/f(x)$ or $K_f = \mathbb{Z}[\iota][x]/f(x)$ in (ex)TNFS.

Size of norms: Classical NFS

Let $K_f = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/f(x)$ and $|a|, |b| \leq E$. Then, we have

$$|N_{K_f/\mathbb{Q}}(a - b\alpha)| \leq (E^{\deg(f)}\|f\|)^{1+o(1)}$$

Size of norms: (ex)TNFS

Let $K_f = \mathbb{Q}(\iota, \alpha) = \mathbb{Q}(\iota)[x]/f(x)$ and $\mathbb{Q}(\iota) = \mathbb{Q}[t]/h(t)$. And let

$$a = \sum_{k=0}^{n-1} a_k \iota^k \text{ and } \sum_{k=0}^{n-1} b_k \iota^k$$

with a_k and b_k bounded in absolute value by $A = E^{1/n}$ so that we enumerate the same number of candidates as in NFS. Then, we have

$$|N_{K_f/\mathbb{Q}}(a - b\alpha)| \leq E^{\deg(f)}\|f\|^{\eta}\, \cancel{L_{p^n}(2/3, o(1))},$$

when $\|h\| = O(1)$ and $p = L_{p^n}(\ell_p, c)$ for $\ell_p > 1/3$.

Examples with JLSV$_2$ method

NFS with target field $\mathbb{F}_{p^\kappa}$

- $f, g \in \mathbb{Z}[x]$ chosen by JLSV$_2$ method.

Degree, and size of coefficients in JLSV$_2$

- $\deg(f) = \kappa$ and $\|f\| = p^{\kappa/(D+1)}$;
- $\deg(g) = D \geq \kappa$ and $\|g\| = p^{\kappa/(D+1)}$.

From our choice of the polynomials, (classical case)

- $|N_{\mathbb{Q}(\alpha_f)/\mathbb{Q}}(a - b\alpha_f)| \leq (E^{\deg(f)}\|f\|)^{1+o(1)} = (p^{\kappa/(D+1)}E^\kappa)^{1+o(1)}$
- $|N_{\mathbb{Q}(\alpha_g)/\mathbb{Q}}(a - b\alpha_g)| \leq (E^{\deg(g)}\|g\|)^{1+o(1)} = (p^{\kappa/(D+1)}E^D)^{1+o(1)}$

Examples with JLSV$_2$ method

TNFS with target field $\mathbb{F}_{(p^\eta)^\kappa}$

- $f, g \in \mathbb{Z}[x]$ chosen by JLSV$_2$ method same as before.
- Choose $h \in \mathbb{Z}[x]$ of degree η with small coefficients.

Degree, and size of coefficients in JLSV$_2$

- $\deg(f) = \kappa$ and $\|f\| = p^{\kappa/(D+1)}$;
- $\deg(g) = D \geq \kappa$ and $\|g\| = p^{\kappa/(D+1)}$.

From our choice of the polynomials, (TNFS case)

- $|N_{\mathbb{Q}(\iota,\alpha_f)/\mathbb{Q}}(a - b\alpha_f)| \leq (E^{\deg(f)}\|f\|^\eta)^{1+o(1)} = ((p^\eta)^{\kappa/(D+1)}E^\kappa)^{1+o(1)}$
- $|N_{\mathbb{Q}(\iota,\alpha_g)/\mathbb{Q}}(a - b\alpha_g)| \leq (E^{\deg(g)}\|g\|^\eta)^{1+o(1)} = ((p^\eta)^{\kappa/(D+1)}E^D)^{1+o(1)}$

exTNFS with JLSV$_2$

exTNFS with JLSV$_2$

- use of JLSV$_2$: complexity $L_{p^n}(1/3, \sqrt[3]{64/9})$ instead of $L_{p^n}(1/3, \sqrt[3]{96/9})$.
- We take E as in JLSV$_2$ for attacking $\mathbb{F}_{P^\kappa}$ (for a prime $P \approx p^\eta$) and get the same norm size as for $\mathbb{F}_{p^\kappa}$.
- We constraint the condition $\kappa = o\left(\left(\frac{\log Q}{\log\log Q}\right)^{1/3}\right)$ that is equivalent to ask $P \approx p^\eta$ to be large.

exTNFS with Conjugation method

exTNFS with Conjugation

- We take f and g as in Conjugation method for attacking $\mathbb{F}_{P^\kappa}$ (for a prime $P \approx p^\eta$) and get the same norm size as for $\mathbb{F}_{P^\kappa}$.
- The best case of NFS with conjugation is when $p = L_{p^n}(1/3, 12^{\frac{1}{3}})$. It translates to the condition $p^\eta = L_{p^n}(1/3, 12^{\frac{1}{3}})$ in the exTNFS case.

Theorem

One solve the DLP over $\mathbb{F}_{p^n} = \mathbb{F}_{p^{\eta\kappa}}$ such that

- $\kappa = 12^{-1/3}\left(\frac{\log(p^n)}{\log\log(p^n)}\right)^{1/3}$
- p is medium or $p = L_Q(1/3, c_p)$ with $c_p \leq 12^{1/3}$.

in time complexity

$$L_{p^n}(1/3, (48/9)^{1/3}).$$

Variants

MNFS

- use multiple number fields (instead of those of f and g);
- best complexity $L_{p^n}(1/3, 1.71)$.

SNFS

- used when p has a special form (most pairing-friendly construction comes in this case), e.g. Barreto-Naehrig pairings;
- selection of f and g as in Joux-Pierrot variant for large characteristic;
- Theorem: when p is large or medium SNFS has complexity $L_{p^n}(1/3, \sqrt[3]{32/9})$ (instead of $L_{p^n}(1/3, \sqrt[3]{64/9})$ in medium case previously).

Keysizes update (1/2)

Current keysizes

- The same recommended key sizes for pairings and RSA:

"An RSA modulus N and a finite field $\mathbb{F}_{p^n}$ therefore offer about the same level of security if N and p^n are of the same order of magnitude." by Lenstra.

- The current key sizes: derived from the complexity $L_{p^n}(1/3, \sqrt[3]{64/9})$.

Key sizes update: when p is of general form

- The best complexity: $L_Q(1/3, \sqrt[3]{48/9})$.
- New size of Q_{new} should be increased by a factor $64/48 \approx 1.33$ from:

$$L_{Q_{\text{new}}}(1/3, \sqrt[3]{48/9}) = L_{Q_{\text{old}}}(1/3, \sqrt[3]{64/9})$$

Keysizes update (2/2)

SNFS: when p is of special form (e.g. BN curves)

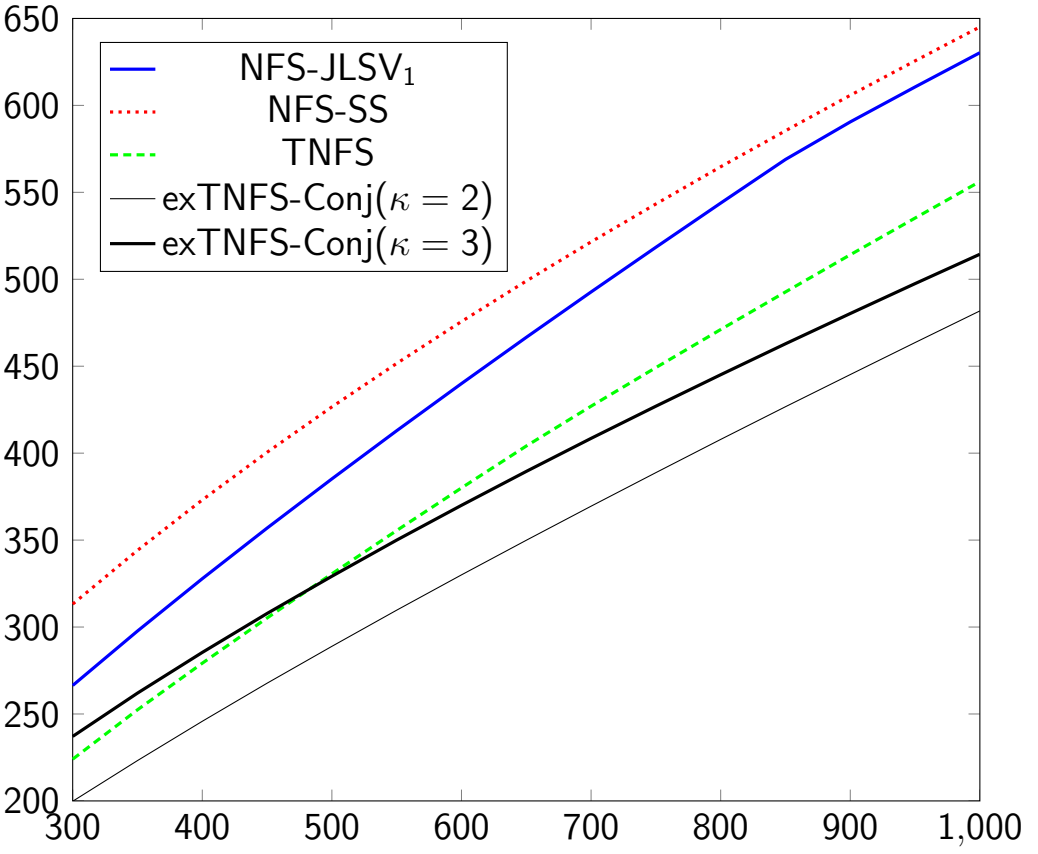
- The previous best complexity (by Joux-Pierrot's SNFS): $L_Q(1/3, \sqrt[3]{32/9})$ when p is large and $L_Q(1/3, \sqrt[3]{64/9})$ when p is medium.
- BN curves with embedding degree $n = 12$: considered as medium case, the key derived from $L_Q(1/3, \sqrt[3]{64/9})$.

Key sizes update for special p

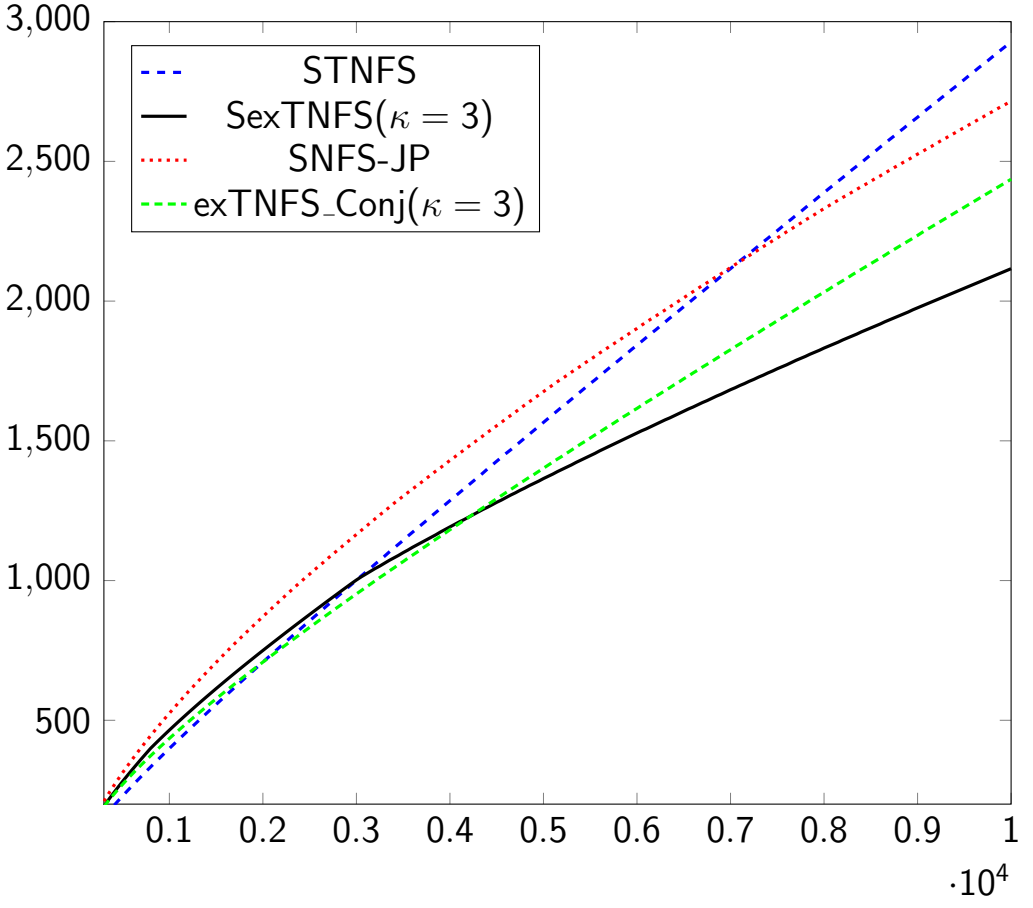
- New best complexity (SexTNFS): $L_Q(1/3, \sqrt[3]{32/9})$ in either case.
- The size of Q_{new} should be increased by twice from:

$$L_{Q_{\text{new}}}(1/3, \sqrt[3]{32/9}) = L_{Q_{\text{old}}}(1/3, \sqrt[3]{64/9}).$$

Precise comparison for $\mathbb{F}_{p^6}$



Precise comparison for $\mathbb{F}_{p^{12}}$ when p is Barreto-Naehrig



Recent developments: n splits into non-coprime factors

Complexities

1. Sarkar and Singh (eprint 2016/485): when n is a power of 2, the complexity is

$$L_{p^n}(1/3, (64/9)^{1/3}) \text{ instead of } L_{p^n}(1/3, (96/9)^{1/3}).$$

2. Jeong and Kim (eprint 2016/526): when n has any nontrivial factor with appropriate size, the best complexities are the same as the best case of exTNFS:

$$L_{p^n}(1/3, (48/9)^{1/3}) \ (p\text{: general}) \text{ or } L_{p^n}(1/3, (32/9)^{1/3}) \ (p\text{: special}).$$

3. Ideas: allow to choose f and g from $\mathbb{Z}[\iota][x]$ instead of $\mathbb{Z}[x]$.

DLP in $\mathbb{F}_Q = \mathbb{F}_{p^n}$ when n is composite

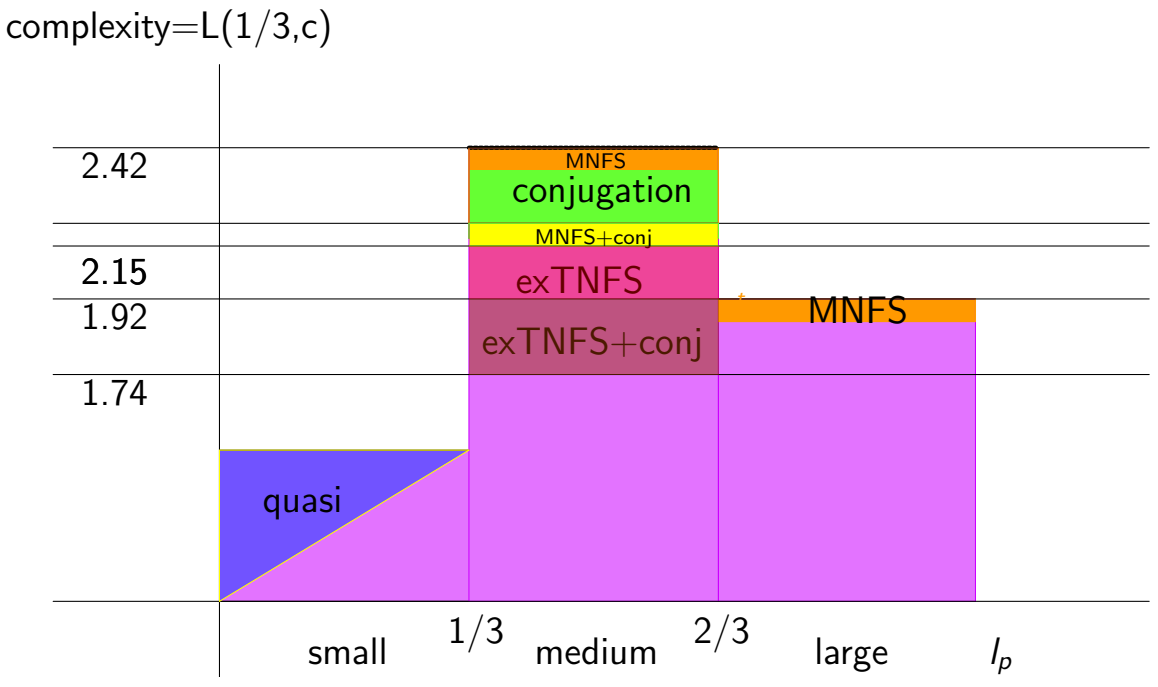


Figure : A New Complexity of DLP in $\mathbb{F}_Q$

The extended tower number field sieve. Crypto 2016. eprint 2015/505