Algorithmes arithmétiques pour la cryptologie — 9 Octobre 2018, Paris

Attacks on pairings (NFS)

Razvan Barbulescu
CNRS et IMJ-PRG

Three-party Diffie-Hellman

Problem

Alice, Bob and Carol use a public elliptic curve E and a pairing e with respect to a point P. Each of the participants broadcast simultaneously an information in a public channel. How can they agree on a common key ?

Joux's protocol

1. Simultaneously, each participant generates a random integer in $[0, r-1]$ and broadcasts a multiple of P:
   - Alice generates a and computes $[a]P$;
   - Bob generates b and computes $[b]P$;
   - Carol generates c and computes $[c]P$;
2. Simultaneously, each participant computes the pairing of the received information and computes the common key:
   - Alice computes $e([b]P, [c]P)^a$;
   - Bob computes $e([c]P, [a]P)^b$;
   - Carol computes $e([a]P, [b]P)^c$;

Common secret key: μ^{abc}.

Multi-linear maps

Applications

- Zero-knowledge proof;
- identity based encryption;
- short signature;
- etc.

Mathematical realization

- lattice-based maps
- elliptic curve pairings
  - in 2000 it was proposed by Sakai, Ohgishi and Kasahara and later by Joux, and key sizes were proposed based on a hypothesis;
  - in 2012 the NIST studied them for standardization and in 2013 Boneh, Franklin and Joux received the Gödel prize;
  - between 2013 and 2016 there were attacks which invalidated the key sizes;
  - currently, key sizes are being updated and new implementations are proposed.

Multi-linear maps

Applications

- Zero-knowledge proof;
- identity based encryption;
- short signature;
- etc.

Mathematical realization

- ~~lattice based maps~~ (attacks in 2016-2017)
- elliptic curve pairings
  - in 2000 it was proposed by Sakai, Ohgishi and Kasahara and later by Joux, and key sizes were proposed based on a hypothesis;
  - in 2012 the NIST studied them for standardization and in 2013 Boneh, Franklin and Joux received the Gödel prize;
  - between 2013 and 2016 there were attacks which invalidated the key sizes;
  - currently, key sizes are being updated and new implementations are proposed.

Security

Pairings security

The security of pairings based cryptosystems relies on the difficulty of

- elliptic curves discrete logarithms;
- finite fields discrete logarithm.

Embedding degree

If a paring is such that

$$E_1/\mathbb{F}_Q[r] \times E_2/\mathbb{F}_Q[r] \to (\mathbb{F}_{Q^n})^*$$

then n is called the embedding degree. If Q is prime and $n > 1$ then it is a different problem than behind DSA;

Required: DLP(curve over $\mathbb{F}_p$)$\approx$ DLP(finite field $\mathbb{F}_{p^k}$)

Discrete logarithm

Definition

Given g and g^x, find x if possible (here G is a known group of known order).

Generic algorithm

A combination of Pohlig-Hellman reduction and Pollard's rho solves DLP in a generic group G after $O(\sqrt{r})$ operations, where r is the largest prime factor of $\#G$.

Relation to pairings

A pairing $e : \langle P \rangle \times \langle P \rangle \to K(\mu)$ is safe only if

1. DLP in $E[r]$ is hard; (DLP on elliptic curves) **if** $\log_2 \#G = n$, **cost**$=2^{\frac{n}{2}}$
2. DLP in $K(\mu)$ is hard. (DLP in finite fields) **if** $\log_2 \#K(\mu) = n$, **cost**$\approx \exp(\sqrt[3]{n})$

Cryptographic sizes before 2018

Key sizes

security (bits)	key size RSA	key size ECDSA	quotient
80	1024	160	6
128	3072	256	12
256	15360	512	30

Pairings

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

Chronology of DLP in finite fields

Index Calculus

- $\mathbb{F}_p$, 1977, Adleman
- $\mathbb{F}_{2^n}$, 1982, Hellman Reyneri, use polynomials instead of numbers
- $\mathbb{F}_{p^n}$, 1994, Hellman for $n = 2$ then Adleman DeMarrais, $\mathbb{F}_{p^n} = \mathbb{Z}[\iota]/p\mathbb{Z}[\iota]$.

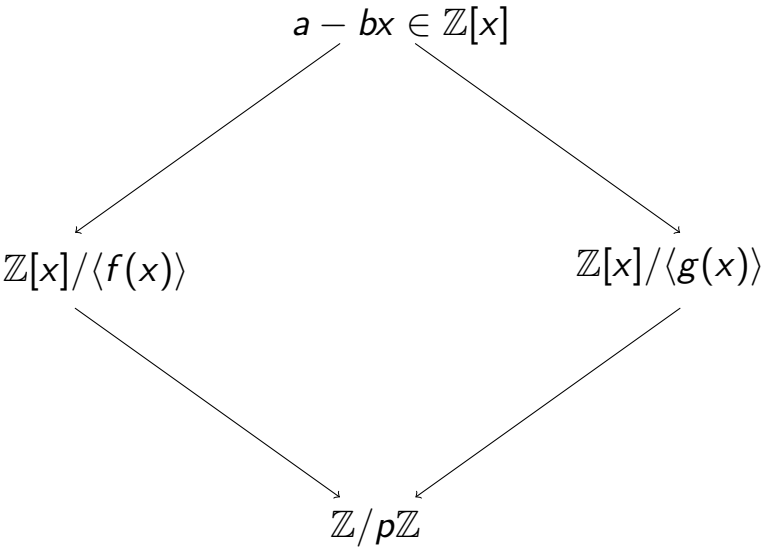
NFS and FFS

- $\mathbb{F}_p$, 1990, Gordon / Schirokauer
- $\mathbb{F}_{2^n}$, 1994, Adleman, use polynomials instead of numbers
- $\mathbb{F}_{p^n}$,
  - 2000, Schirokauer, $\mathbb{F}_{p^n} = \mathbb{Z}[\iota]/p\mathbb{Z}[\iota]$ (rehabilitated in 2015 by B., Gaudry and Kleinjung).
  - 2006, Joux Lercier Smart Vercauteren, modify polynomial selection (JLSV)
  - 2016, Kim and B., combiner TNFS and JLSV: exTNFS

The number field sieve(NFS): diagram

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

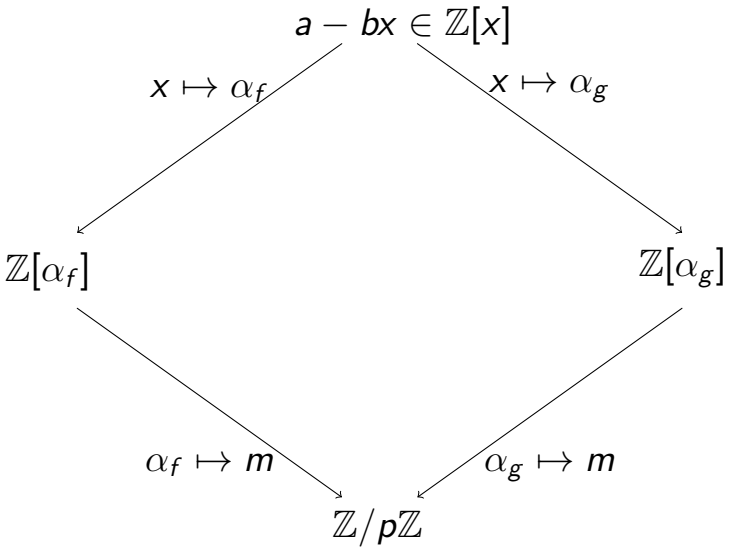
Let $f, g \in \mathbb{Z}[x]$ be two irreducible polynomials which have a common root m modulo p.



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 $\mathbb{F}_p$

$F(a,b) = \sum_{i=0}^{d} f_i a^i b^{d-i}$ where $d = \deg f$ and $G(a,b) = g_1 a + g_0 b$.

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 $F(a,b)$ and $G(a,b)$ 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.

Why is the polynomial selection important?

Cost of algorithms of the Index Calculus family

where norms' size is

- p in Index Calculus;
- $B^3 p^{\frac{1}{2}}$ for Gaussian integers (complexity $L_p(\frac{1}{2})$);
- $B^{d+1} p^{\frac{1}{d}}$ for NFS in $\mathbb{F}_p$ (complexity $L_p(\frac{1}{3})$);
- norms product for NFS in $\mathbb{F}_{p^n}$ when $n > 1$

Norms' product

If $f = f_d x^d + \cdots + f_1 x + f_0$ then

$$|\mathrm{N}_f(a + b\alpha_f)| = |f_d a^d + \cdots + f_1 a b^{d-1} + f_0 b^d| \leq (d+1) B^d \|f\| .$$

The bit size of the norm's product is very well approximated by
$(\deg f + \deg g) + \log_2\|f\| + \log_2\|g\|$.

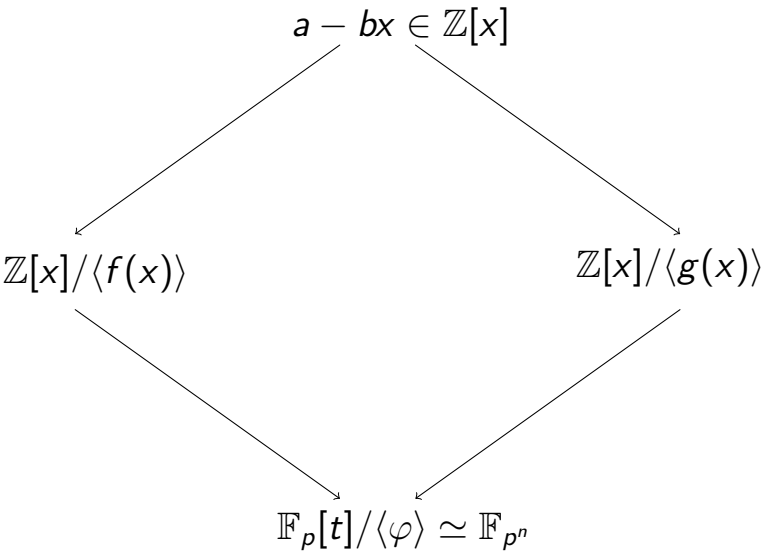
The polynomial selection task

Fix $\deg f$ and $\deg g$ as small as possible (or try all possibilities, in practice the optimal choices are ≤ 10, then find f and g of small coefficients.
Intuitively in favor of the hypothesis of 2000 : when $k \geq 2$ we have the extra condition $\min(\deg f, \deg g) \geq n$ which makes the task harder.

The idea of Joux Lercier Smart Vercauteren

Polynomial selection

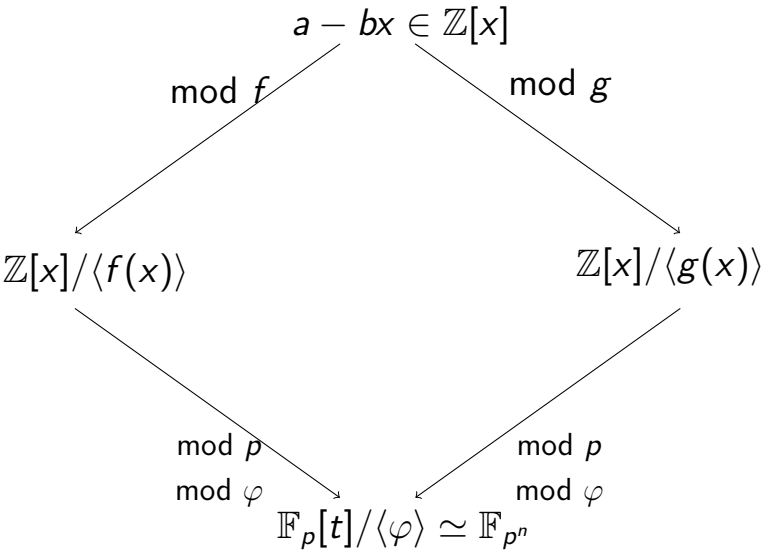
Select f and g which have a common ~~root~~ factor φ of degree n modulo p.



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.



JLSV in practice

Modifications

The only modification is the polynomial selection (done in sage or magma) and the fact that in the sieve we have two non-linear polynomials.

- the implementation of Joux and Lercier was so even for $\mathbb{F}_p$;
- CADO-NFS supports two non-linear polynomials since 2014).

Records

- 2006, Joux Lercier Smart Vercauteren, $\mathbb{F}_{p^3}$, 120dd.
- 2014, Barbulescu Gaudry Guillevic Morain, $\mathbb{F}_{p^2}$, 180dd.
- 2015, Barbulescu Gaudry Guillevic Morain, $\mathbb{F}_{p^4}$, 120dd.
- 2015, Barbulescu Gaudry Guillevic Morain, $\mathbb{F}_{p^3}$ and again Guillevic, Thomé, Morain (2016) 156dd.
- 2017, Gremy, Guillevic Morain and Thomé, $\mathbb{F}_{p^6}$ using $3d$ sieving (Gremy implemented it in the nfs-hd branch of CADO-NFS since 2016) 132dd

Important tool

Theorem (Lenstra, Lenstra, Lovasz)

Let $M \in \mathcal{M}_n(\mathbb{Z})$ define a lattice. Then one can compute in polynomial time a vector of euclidean norm less than $2^{\frac{n-1}{4}} |\det M|^{\frac{1}{n}}$.

Corollary (rational reconstruction (also called continued fractions))

For any integer a and prime p one can compute two integers u and v so that

$$a \equiv \frac{u}{v} \mod p$$

and $|u|, |v| \leq 2^{\frac{1}{4}}\sqrt{p}$.

Important tool

Theorem (Lenstra, Lenstra, Lovasz)

Let $M \in \mathcal{M}_n(\mathbb{Z})$ define a lattice. Then one can compute in polynomial time a vector of euclidean norm less than $2^{\frac{n-1}{4}} |\det M|^{\frac{1}{n}}$.

Corollary (rational reconstruction (also called continued fractions))

For any integer a and prime p one can compute two integers u and v so that

$$a \equiv \frac{u}{v} \mod p$$

and $|u|, |v| \leq 2^{\frac{1}{4}}\sqrt{p}$. Proof: Apply LLL to

$$M = \begin{pmatrix} a & 1 \\ p & 0 \end{pmatrix}.$$

Indeed, the generated lattice is included in $\{(u, v) \in \mathbb{Z}^2 \mid av - u \equiv 0[p]\}$.

Polynomial selection : $\mathbf{JLSV}_1$

Raw variant

1. Select $f \in \mathbb{Z}[x]$ of degree n irreducible modulo p;
2. Set $g = f + p$.

information theory: f and g are optimal.

Practical variant

1. Take $f_0, f_1 \in \mathbb{Z}[x]$ so that $\deg f_0 = n$ and $\deg f_1 < n$.
2. Take $a \geq 2^{\frac{1}{4}}\sqrt{p}$ as small as possible so that $f := f_0 + af_1$ is irreducible modulo p.
3. Compute the rational reconstruction $a \equiv u/v \mod p$ and set $g := vf_0 + uf_1$.

justification: LLL cannot return $a/1$ as rational reconstruction.

Polynomial selection : Conjugation (part I)

Idea

- $\sqrt{3}$ in $\mathbb{F}_p$ has a representative which is larger than $2^{\frac{1}{4}}p^{\frac{1}{2}}$ so the LLL theorem cannot return the rational reconstruction

$$\sqrt{3} \equiv \sqrt{3}/1 \mod p.$$

- A polynomial $f_0 + \sqrt{3}f_1$ is not allowed but we can **conjugate** it to obtain $(f_0 + \sqrt{3}f_1)(f_0 - \sqrt{3}f_1) = f_0^2 - 3f_1^2 \in \mathbb{Z}[x]$.

Conjugation 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 $\varphi = f_0^2 - af_1^2$.
4. Compute the rational reconstruction $\sqrt{a} \equiv \frac{u}{v} \mod p$ and set $g := vf_0 + uf_1$.

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

Polynomial selection : Conjugation (part II)

Example

Discrete logarithm in $\mathbb{F}_{p^2}$ of 180 decimal digits Consider DLP in $\mathbb{F}_{p^2}$ where $p = \lfloor \pi \cdot 10^{89} \rfloor + 14905741$

- GJL : $f = x^4 + x - 1$ and

$$\begin{aligned} g \;=\; & 559473469462407609487884994103807929466175004x^3 \\ & +798666418503298564339720923046088783814641 21x^2 \\ & +523914868396455299702960744004261593029990 66x \\ & -140985078126918434544107335150321349526616620. \end{aligned}$$

- Conjugation : $f = x^4 + 1$ and

$$\begin{aligned} g \;=\; & 448225077249286433565160965828828303618362474x^2 \\ & -296061099084763680469275137306557962657824623x \ ; \\ & 448225077249286433565160965828828303618362474. \end{aligned}$$

$\mathbb{F}_{p^2}$ (Conjugation) was 160 times faster than $\mathbb{F}_p$ (GJL)

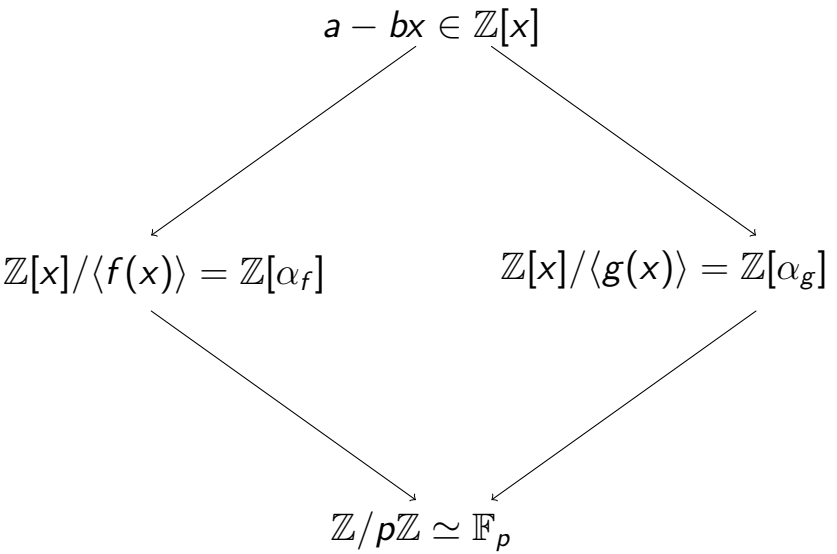
Domain of application

- $N_f = E^{2n}$ and $N_g = E^n(p^n)^{\frac{1}{2n}}$ instead of $E^d N^{\frac{1}{d+1}}$ and $EN^{\frac{1}{d+1}}$ for the prime case;
- 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.

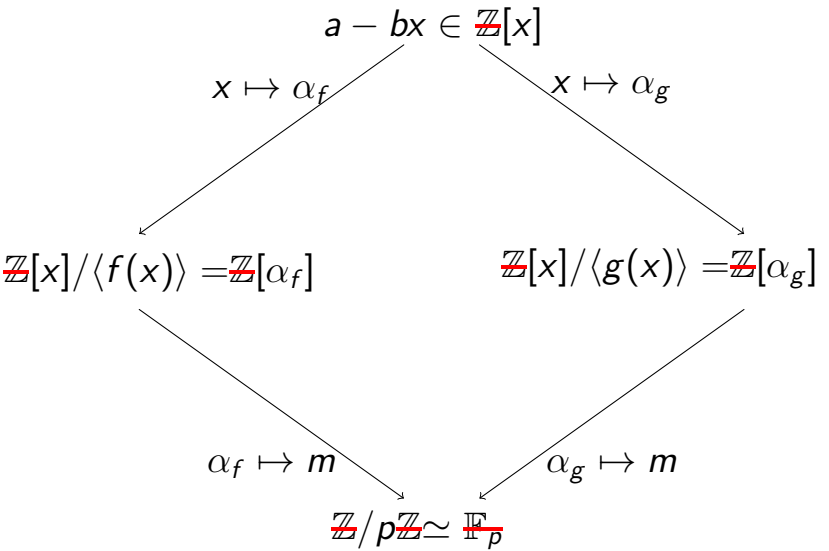


TNFS diagram

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 k such that p is inert in its number field $\mathbb{Q}(\iota)$; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.

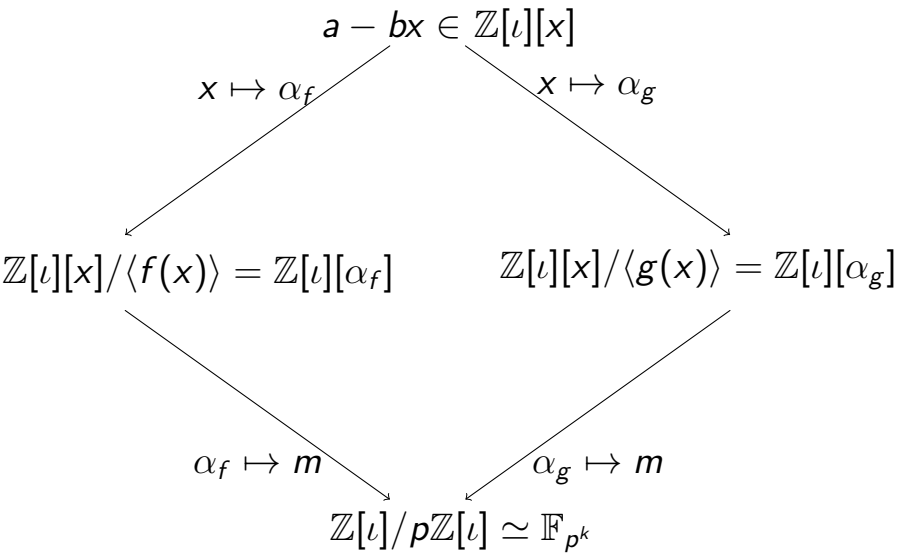


TNFS diagram

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

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 k such that p is inert in its number field $\mathbb{Q}(\iota)$; we have $\mathbb{Z}[\iota]/p\mathbb{Z}[\iota] \simeq \mathbb{F}_{p^k}$.



Relation collection

Reminder of NFS

Enumerate pairs (a, b) in $\mathbb{Z} \times \mathbb{Z}$ without common divisors such that $F(a, b)$ and $G(a, b)$ are B-smooth for a parameter B.

TNFS

- Enumerate pairs (a, b) in $\mathbb{Z}[\iota] \times \mathbb{Z}[\iota]$ without common divisors such that $\mathrm{N}_{\mathbb{Q}(\iota)/\mathbb{Q}}(F(a, b))$ and $\mathrm{N}_{\mathbb{Q}(\iota)/\mathbb{Q}}(G(a, b))$ are B-smooth for the same parameter B as in NFS.
- In particular for the first example, we enumerate $(a, b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ and search those where

$$(\mathrm{Re}F(a, b))^2 + (\mathrm{Im}F(a, b))^2 \text{ and } (\mathrm{Re}G(a, b))^2 + (\mathrm{Im}G(a, b))^2$$

  are B-smooth.

Relation collection

Reminder of NFS

Enumerate pairs (a, b) in $\mathbb{Z} \times \mathbb{Z}$ without common divisors such that $F(a, b)$ and $G(a, b)$ are B-smooth for a parameter B.

TNFS

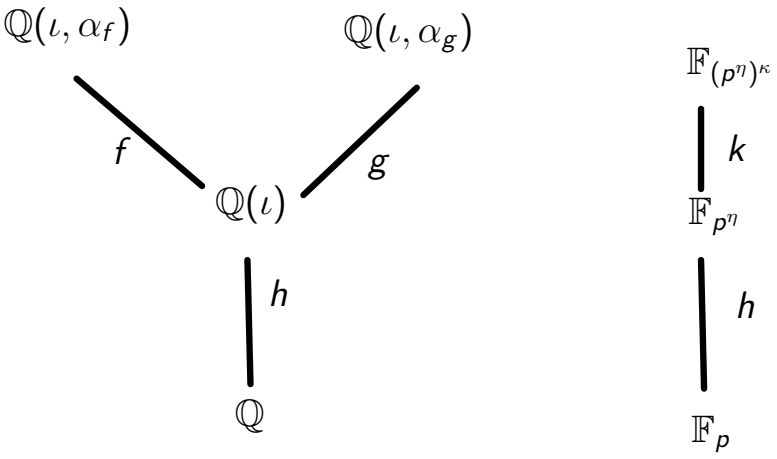
- Enumerate pairs (a, b) in $\mathbb{Z}[\iota] \times \mathbb{Z}[\iota]$ without common divisors such that $\mathrm{N}_{\mathbb{Q}(\iota)/\mathbb{Q}}(F(a, b))$ and $\mathrm{N}_{\mathbb{Q}(\iota)/\mathbb{Q}}(G(a, b))$ are B-smooth for the same parameter B as in NFS.
- In particular for the first example, we enumerate $(a, b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ and search those where

$$(\mathrm{Re}F(a, b))^2 + (\mathrm{Im}F(a, b))^2 \text{ and } (\mathrm{Re}G(a, b))^2 + (\mathrm{Im}G(a, b))^2$$

  are B-smooth.

We collect smooth values of polynomials with $2n$-variables.

The extended TNFS (Kim B. 2016)

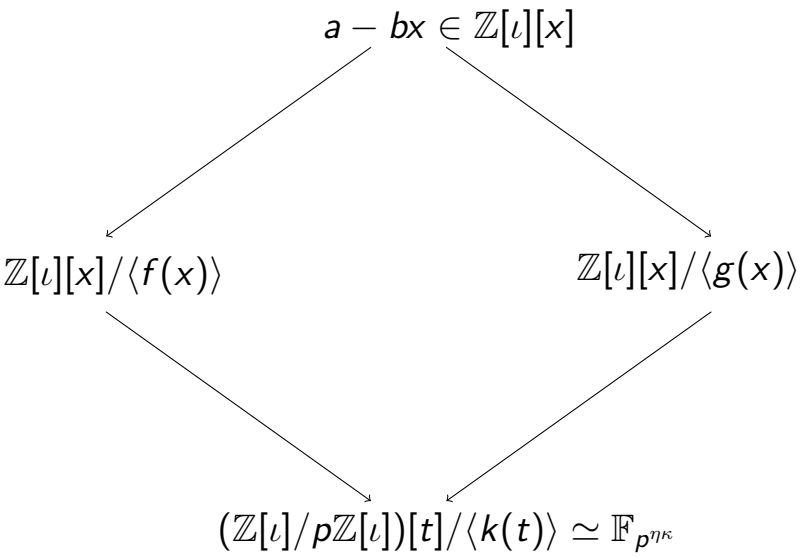


exTNFS algorithm

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 $\mathbb{F}_{p^\kappa}$; put $k = \gcd(f \bmod p, g \bmod p)$;
3. continue the algorithm as for TNFS.

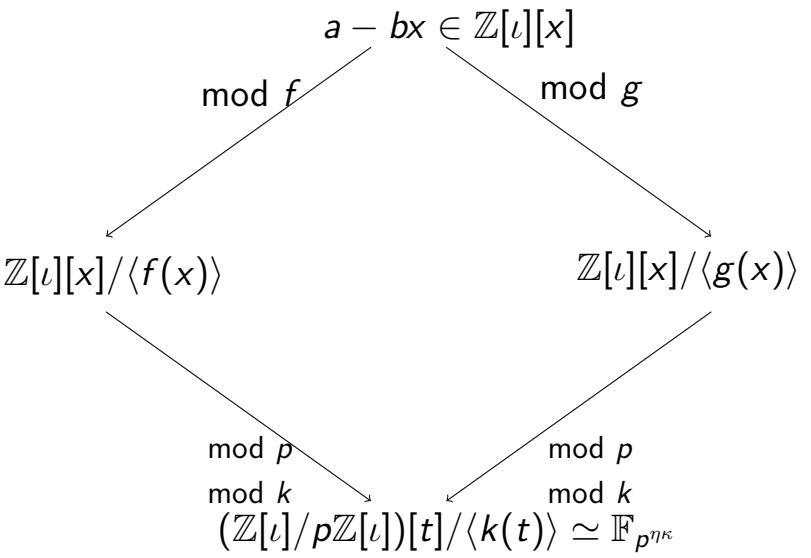
exTNFS diagram



Explication

k is irreducible over $\mathbb{F}_p$ and, since $\gcd(\eta, \kappa) = 1$, it is automatically irreducible over $\mathbb{F}_{p^\eta}$.

exTNFS diagram

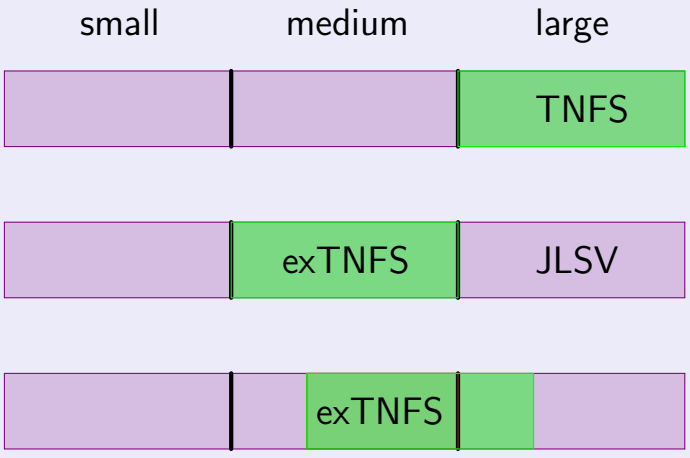


Explication

k is irreducible over $\mathbb{F}_p$ and, since $\gcd(\eta, \kappa) = 1$, it is automatically irreducible over $\mathbb{F}_{p^\eta}$.

exTNFS with Conjugation

From Kim to Barbulescu



exTNFS with Conjugation method

- idea: exTNFS can be used to extend to the left any case of NFS
- complexity: the best case of NFS is when $p = L_{p^n}(1/3, 12^{\frac{1}{3}})$ and one uses the Conjugation method

Theorem

If $n = \eta\kappa$, $\gcd(\eta, \kappa) = 1$ *and* $\kappa = 12^{-\frac{1}{3}}$ *then DLP can be solved in time* $L_{p^n}(1/3, \sqrt[3]{48/9})$.

The case of p of polynomial form and k composite : SexTNFS

Method when $p = \Pi(u)$

1. Enumerate polynomials S of degree $\leq n-1$ until $x^n + S(x) - u$ is irreducible modulo p;
2. return $g = x^n + S(x) - u$ and $f = \Pi(x^n + S(x))$

Correction: $f(x) - p = \Pi(x^n + S(x)) - \Pi(u) = (x^n + S(x) - u)(\cdots)$.

Size of norms

The product of norms, which must be small, has size

$$E^{n(d+1)} Q^{\frac{1}{nd}},$$

where E and Q are given.

exTNFS + Joux-Pierrot = SexTNFS

Updated key sizes

Barbulescu-Duquesne 2018

- 128 bits of security:

family of pairings	old bit sizes	new bit sizes
Barreto-Baehrig (BN)	3072	5534
Barreto-Lynn-Scott k=12 (BLS12)	3072	5530
Kachisa-Schaefer-Scott k=16 (KSS16)	3072	5281
Kachisa-Schaefer-Scott k=18 (KSS18)	3072	6401

- 192 bits of security:

family of pairings	old bit sizes	new bit sizes
Kachisa-Schaefer-Scott k=18 (KSS18)	8192	12200
Barreto-Lynn-Scott k=24 (BLS24)	8192	13300

- 256 bits of security:

family of pairings	old bit sizes	new bit sizes
Kachisa-Schaefer-Scott k=18 (KSS18)	15360	27000
Barreto-Lynn-Scott k=24 (BLS24)	15360	27000

Depending on the feasability of quantum computer, pairings might be abandoned.