Discrete Logarithm in Medium and High Characteristic Finite Fields: The Multiple Number Field Sieve

Cécile Pierrot

Laboratoire d'Informatique de Paris 6
and Institut Mathématique de Jussieu
UPMC, Paris, France

YACC Conference, Porquerolles

Joint work with Razvan Barbulescu, Ecole Polytechnique, Palaiseau, France

The Discrete Logarithm Problem (DLP)

- Multiplicative group G generated by g :
  solving the discrete logarithm problem in G,
  is inverting the map $x \mapsto g^x$
- A hard problem in general, and used as such in cryptography
- Two families of algorithms :
  - Generic algorithms (Pollard's Rho, Pohlig-Hellman...)
  - Specific algorithms (Index Calculus)

Index Calculus Algorithms

If we want to compute Discrete Logs in G :

- Sieving Phase
  $\rightarrow$ Create a lot of sparse multiplicative relations between some (small) specific elements = the factor base

$$\prod g_i^{e_i} = \prod g_i^{e'_i} \Rightarrow \sum e_i \log(g_i) = 0$$

  $\rightarrow$ So a lot of sparse linear equations

Index Calculus Algorithms

If we want to compute Discrete Logs in G :

- Sieving Phase
  $\rightarrow$ Create a lot of sparse multiplicative relations between some (small) specific elements = the factor base

$$\prod g_i^{e_i} = \prod g_i^{e'_i} \Rightarrow \sum e_i \log(g_i) = 0$$

  $\rightarrow$ So a lot of sparse linear equations
- Linear Algebra Phase
  $\rightarrow$ Recover the Discrete Logs of the factor base

Index Calculus Algorithms

If we want to compute Discrete Logs in G :

- Sieving Phase
  $\rightarrow$ Create a lot of sparse multiplicative relations between some (small) specific elements = the factor base

$$\prod g_i^{e_i} = \prod g_i^{e_i'} \Rightarrow \sum e_i \log(g_i) = 0$$

  $\rightarrow$ So a lot of sparse linear equations
- Linear Algebra Phase
  $\rightarrow$ Recover the Discrete Logs of the factor base
- Individual Logarithm Phase
  $\rightarrow$ Recover the Discrete Logs of an arbitrary element

Sieving Phase

- How to obtain relations ?
  For all x in E, we have : $h_1(g_1(x)) = h_2(g_2(x))$.

$$
\begin{tikzcd}
 & E \arrow[dl, "g_1"'] \arrow[dr, "g_2"] & \\
E_1 \arrow[dr, "h_1"] & & E_2 \arrow[dl, "h_2"] \\
 & G &
\end{tikzcd}
$$

-

Sieving Phase

- How to obtain relations ?
  For all x in E, we have : $h_1(g_1(x)) = h_2(g_2(x))$.

$$\begin{tikzcd}
 & E \arrow[dl, "g_1"'] \arrow[dr, "g_2"] & \\
B_1 \subset E_1 \arrow[dr, "h_1"'] & & E_2 \supset B_2 \arrow[dl, "h_2"] \\
 & G &
\end{tikzcd}$$

- How to obtain "good" relations ? B_1 and B_2 two small sets.

Sieving Phase

- How to obtain relations ?
  For all x in E, we have : $h_1(g_1(x)) = h_2(g_2(x))$.

$$\begin{tikzcd}
 & E \arrow[dl, "g_1"'] \arrow[dr, "g_2"] & \\
B_1 \subset E_1 \arrow[dr, "h_1"] & & E_2 \supset B_2 \arrow[dl, "h_2"] \\
 & G &
\end{tikzcd}$$

- How to obtain "good" relations ? B_1 and B_2 two small sets.
  Factor base $=$ all the elements in G that can be written using elements of B_1 and B_2 only.

Number Field Sieve (NFS)

- Solves the DLP for finite fields $\mathbb{F}_{p^n}$ with medium to high characteristic.

Number Field Sieve (NFS)

- Solves the DLP for finite fields $\mathbb{F}_{p^n}$ with medium to high characteristic.
- Belongs to the family of Index Calculus algorithms
  $\Rightarrow$ 3 phases.

Number Field Sieve (NFS)

- Solves the DLP for finite fields $\mathbb{F}_{p^n}$ with medium to high characteristic.
- Belongs to the family of Index Calculus algorithms
  $\Rightarrow$ 3 phases.
- Preliminaries to the first phase :
  - Find two polynomials f_1 and f_2 with irreducible gcd of degree n modulo p.
  - Define $\mathbb{F}_{p^n}$ as the smallest field where the two polynomials have a common root.

Commutative Diagram

With m a root of these polynomials in $\mathbb{F}_{p^n}$:

$$\begin{tikzcd}
 & \mathbb{Z}[X] \arrow[dl, "X \mapsto \theta_1"'] \arrow[dr, "X \mapsto \theta_2"] & \\
\mathbb{Q}[X]/(f_1(X)) \approx \mathbb{Q}(\theta_1) \arrow[dr, "\theta_1 \mapsto m"] & & \mathbb{Q}(\theta_2) \approx \mathbb{Q}[X]/(f_2(X)) \arrow[dl, "\theta_2 \mapsto m"'] \\
 & \mathbb{F}_{p^n} &
\end{tikzcd}$$

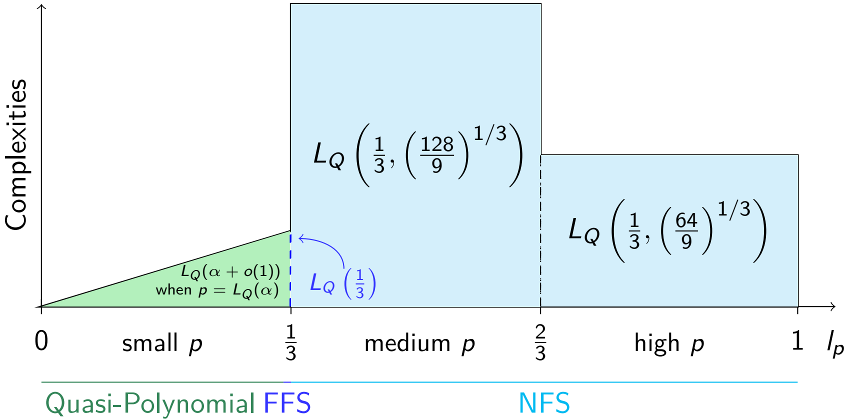
Factor base ? $B_i :=$ prime ideals (of the ring of integers) with a norm smaller than a certain smoothness bound.

Complexities

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

Complexities

- Notation : $L_Q(\alpha, c) = \exp\left(c(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}\right)$
- In $\mathbb{F}_Q$ of characteristic $p = L_Q(l_p, c)$:



The Multiple Number Field Sieve,

Joint work with *Razvan Barbulescu* (ANTS 2014). Idea from integer factorization [Coppersmith 93] and prime fields [Matyukhin 03].

The Multiple Number Field Sieve,

Joint work with *Razvan Barbulescu* (ANTS 2014). Idea from integer factorization [Coppersmith 93] and prime fields [Matyukhin 03].

Our aim is twofold :

- extend the scope of Matyukhin's variant from prime fields to all high characteristic finite fields.
- propose a variation in the medium characteristic case with a better improvement.

The Multiple Number Field Sieve,

Joint work with *Razvan Barbulescu* (ANTS 2014). Idea from integer factorization [Coppersmith 93] and prime fields [Matyukhin 03].

Our aim is twofold :

- extend the scope of Matyukhin's variant from prime fields to all high characteristic finite fields.
- propose a variation in the medium characteristic case with a better improvement.

$\Rightarrow$ Best algorithm to solve the DLP for medium and high characteristic finite fields $\mathbb{F}_{p^n}$.

Main idea : from 2 to V number fields

- With m a root of the polynomials $f_1, \ldots, f_V$ in $\mathbb{F}_{p^n}$:

$$\begin{tikzcd}
 & & \mathbb{Z}[X] \arrow[dll] \arrow[dl] \arrow[d, "X \mapsto \theta_i"] \arrow[dr] \arrow[drr] & & \\
\mathbb{Q}(\theta_1) \arrow[drr] & \mathbb{Q}(\theta_2) \arrow[dr] & \mathbb{Q}(\theta_i) \arrow[d, "\theta_i \mapsto m"] & \mathbb{Q}(\theta_{V-1}) \arrow[dl] & \mathbb{Q}(\theta_V) \arrow[dll] \\
 & & \mathbb{F}_{p^n} & &
\end{tikzcd}$$

- Choice of polynomials f_1 and f_2 with a common root m in $\mathbb{F}_{p^n}$ $\Rightarrow$ linear combination $\Rightarrow$ for $i = 3, \ldots, V$: $f_i = \alpha_i f_1 + \beta_i f_2$ with α_i, β_i of the size of $\sqrt{V}$.

Medium VS High Characteristic

High Characteristic : extending Matyukhin's variant thanks to a polynomial selection that did not exist in 2003.

- Polynomial selection : by LLL [JLSV06].
  f_1 and f_2 have same size of coefficients but $\deg f_2 \geqslant \deg f_1$
  $\Rightarrow$ Higher norms in $\mathbb{Q}(\theta_2)$, ..., $\mathbb{Q}(\theta_V)$ than in $\mathbb{Q}(\theta_1)$.
- Sieving : keep only linear polynomials that lead to a B-smooth norm in the first number field and a B'-smooth norm in (at least) one other number field.

Medium VS High Characteristic

High Characteristic : extending Matyukhin's variant thanks to a polynomial selection that did not exist in 2003.

- Polynomial selection : by LLL [JLSV06].
  f_1 and f_2 have same size of coefficients but $\deg f_2 \geqslant \deg f_1$
  $\Rightarrow$ Higher norms in $\mathbb{Q}(\theta_2)$, ..., $\mathbb{Q}(\theta_V)$ than in $\mathbb{Q}(\theta_1)$.
- Sieving : keep only linear polynomials that lead to a B-smooth norm in the first number field and a B'-smooth norm in (at least) one other number field.

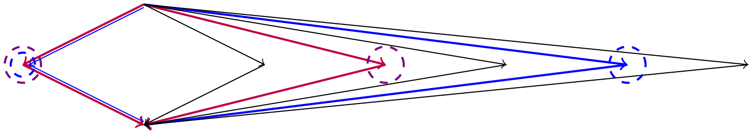
Rq : $B > B'$ i.e. more important to have a high probability of smoothness in $\mathbb{Q}(\theta_1)$ than higher probabilities in every $\mathbb{Q}(\theta_i)$.

Medium VS High Characteristic

High Characteristic : extending Matyukhin's variant thanks to a polynomial selection that did not exist in 2003.

- Polynomial selection : by LLL [JLSV06].
  f_1 and f_2 have same size of coefficients but deg $f_2 \geqslant$ deg f_1
  $\Rightarrow$ Higher norms in $\mathbb{Q}(\theta_2)$, . . . , $\mathbb{Q}(\theta_V)$ than in $\mathbb{Q}(\theta_1)$.
- Sieving : keep only linear polynomials that lead to a B-smooth norm in the first number field and a B'-smooth norm in (at least) one other number field.

Rq : $B > B'$ i.e. more important to have a high probability of smoothness in $\mathbb{Q}(\theta_1)$ than higher probabilities in every $\mathbb{Q}(\theta_i)$.

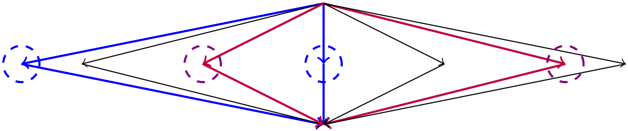


Medium VS High Characteristic

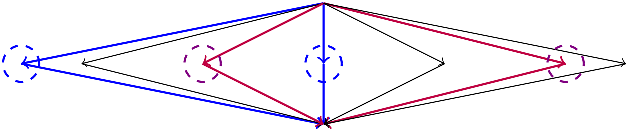
Medium Characteristic : balancing the roles of the number fields.

- Polynomial selection : continued fraction method [JLSV06].
  f_1 of degree n, irreducible modulo p and such that :
  $$f_1 = g + c \cdot h$$
  where g and h are polynomials with small coeff and $c \approx \sqrt{p}$.
  Continued fraction gives : $c \equiv a/b \mod p$ with $a, b \approx \sqrt{p}$.
  $$f_2 \equiv bf_1 \mod p$$
  $\Rightarrow$ f_1 and f_2 have same degree and same size of coeff
  $\Rightarrow$ same norms for all $\mathbb{Q}(\theta_i)$.
- Sieving : keep only high degree polynomials that lead to B-smooth norms in (at least) a pair of number fields.

Particularities of the Medium Characteristic Case



Particularities of the Medium Characteristic Case

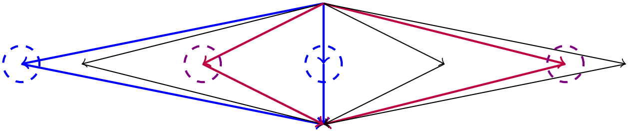


- Benefits of symmetry :

	NFS	MNFS
Number of number fields	2	V
Size of the factor base	$2B$	VB
Probability of a good relation	$\mathcal{P}$	$\mathcal{P}\frac{V(V-1)}{2} \approx \mathcal{P}\frac{V^2}{2}$

$\Rightarrow$ Quadratic gain in the probability : offers the possibility to lower the time of the sieving and to choose a better smoothness bound B.

Particularities of the Medium Characteristic Case



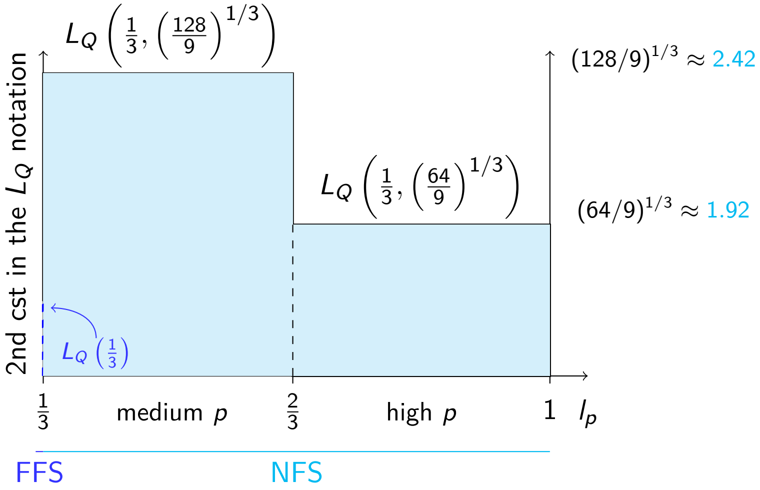
- Benefits of symmetry :

	NFS	MNFS
Number of number fields	2	V
Size of the factor base	$2B$	VB
Probability of a good relation	$\mathcal{P}$	$\mathcal{P}\frac{V(V-1)}{2} \approx \mathcal{P}\frac{V^2}{2}$

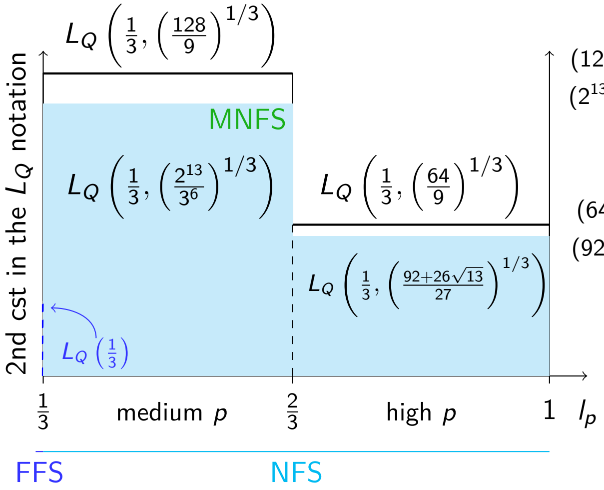
$\Rightarrow$ Quadratic gain in the probability : offers the possibility to lower the time of the sieving and to choose a better smoothness bound B.

- Asymptotically, the complexity is optimal when $B = V^3$.

Asymptotic Complexities : NFS



Asymptotic Complexities : MNFS



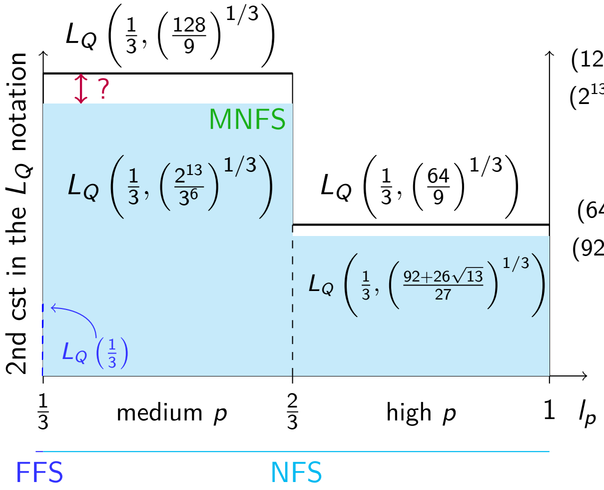
$(128/9)^{1/3} \approx 2.42$

$(2^{13}/3^6)^{1/3} \approx 2.24$

$(64/9)^{1/3} \approx 1.92$

$(92 + 26\sqrt{13})/27))^{1/3} \approx 1.90$

Asymptotic Complexities : MNFS



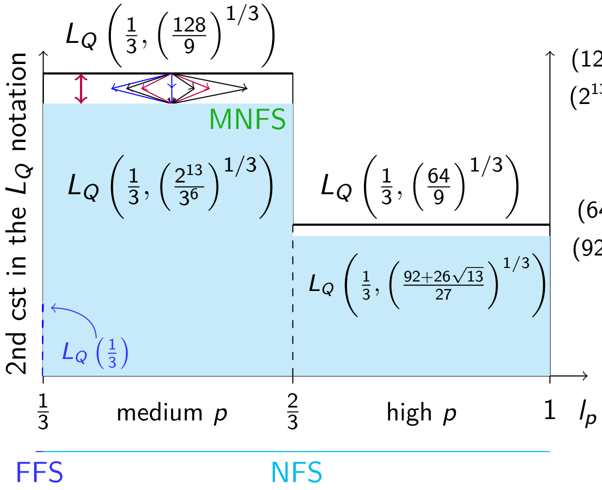
$(128/9)^{1/3} \approx 2.42$

$(2^{13}/3^6)^{1/3} \approx 2.24$

$(64/9)^{1/3} \approx 1.92$

$(92 + 26\sqrt{13})/27))^{1/3} \approx 1.90$

Asymptotic Complexities : MNFS



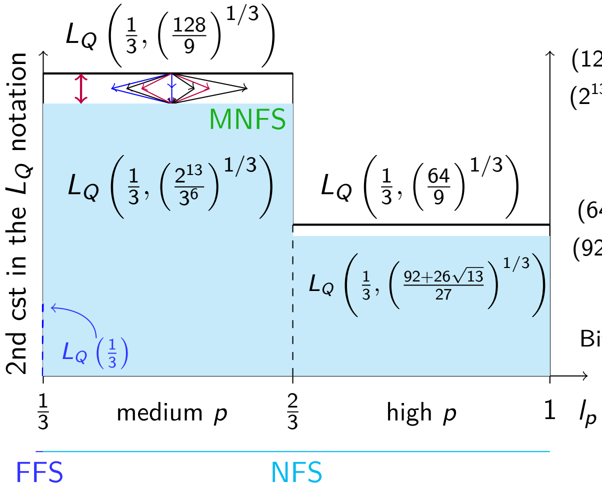
$(128/9)^{1/3} \approx 2.42$

$(2^{13}/3^6)^{1/3} \approx 2.24$

$(64/9)^{1/3} \approx 1.92$

$(92 + 26\sqrt{13})/27))^{1/3} \approx 1.90$

Asymptotic Complexities : MNFS



$(128/9)^{1/3} \approx 2.42$

$(2^{13}/3^6)^{1/3} \approx 2.24$

$(64/9)^{1/3} \approx 1.92$

$(92 + 26\sqrt{13})/27))^{1/3} \approx 1.90$

Bitsize ratio : $2 \rightarrow 1.63$

The take away slide

As a dessert * :

MNFS gave the opportunity to write an analysis of the folklore fact that the runtime of the individual logarithm phase is negligible with respect to the total runtime of NFS.

*. You know, the kind of dessert that seems nice when you order it but feels really heavy once you already have eaten too much.

Thank you for your attention !

Extension of NFS in the boundary case $p = L_{p^n}(1/3)$

- We want to upper-bound the resultant : $|\det \mathrm{Sylv}(h,f)| \leqslant \Theta \|f\|^{\deg h} \|h\|^{\deg f}$ with $\Theta =$ number of permutations with non zero contributions in the sum.
- Θ ? Let deg $(h) = n$ and deg $(f) = t$.
  Before : $\Theta \leqslant n^t t^n$. Kalkbrener gives : $\Theta \leqslant \binom{n+t}{n} \cdot \binom{n+t-1}{t}$.
  Because of the following inequalities :

$$\begin{aligned}
\binom{n+t}{n} \cdot \binom{n+t-1}{t} &= \frac{n}{n+t} \left(\frac{(n+t)!}{n!t!} \right)^2 \\
&\leq \frac{n}{n+t} \left(\frac{(n+1)\cdots(n+t)}{t!} \right)^2 \\
&\leq \frac{n}{n+t} \left(\prod_{i=1}^{t} \frac{(n+i)}{i} \right)^2 \\
&\leq \frac{n}{n+t} \prod_{i=1}^{t} \left(\frac{n}{i} + 1 \right)^2
\end{aligned}$$

we obtain that $\Theta \leqslant (n+1)^{2t}$.

Choice of Polynomials

Previously (NFS) :

- For medium p : f_1 irreducible of degree n over $\mathbb{F}_p$ and $f_2 = f_1 + p$
  Small degrees but high coeffs for f_2
- For high p : based on lattice reduction of $(f_1, Xf_1, \cdots, X^{d-n}f_1, p, Xp, \cdots, X^d p)$
  $\Rightarrow$ f_2 is a multiple of f_1 modulo p but with smaller coeffs
  f_1 with not too small coeffs (otherwise we get trivial multiples)

Some Obstructions Coming from Number Fields and its Solutions

How to go down ?

$$\begin{tikzcd} \mathbb{Q}[\theta] \arrow[dr] & \\ & \mathbb{F}_{p^n} \end{tikzcd}$$

- No unique factorization over elements $\Rightarrow$ we consider ideals in the ring of integers of $\mathbb{Q}[\theta]$.
- Ideals are not principal $\Rightarrow$ we (virtually) raise them to the power of the class number of $\mathbb{Q}[\theta]$.
- Generators are not unique $\Rightarrow$ Schirokauers maps.