Logarithme discret dans les corps finis : NFS Spécial et Multiple.

Moyennes et grandes caractéristiques.

Cécile Pierrot

Laboratoire d'Informatique de Paris 6
Institut Mathématique de Jussieu & INRIA
UPMC, Paris, France
Financée par : DGA/CNRS

Journées C2 2014, Les Sept Laux

Le Problème du Logarithme Discret (DLP)

- Groupe multiplicatif G engendré par g :
  résoudre le problème du logarithme discret dans G,
  c'est inverser la fonction $x \mapsto g^x$
- Un problème difficile en général
  (et considéré comme tel en cryptographie)
- Deux familles d'algorithmes :
  - Algorithmes généraux
  - Algorithmes spécifiques

Calcul d'Indice

NFS appartient à cette famille

- Phase de Crible

  $\rightarrow$ Crée de nombreuses relations multiplicatives creuses entre certains éléments spécifiques (la base de lissité)

$$\prod (g_i)^{e_i} = \prod (g_i')^{e_i'}$$

  $\rightarrow$ Donc de nombreuses équations linéaires

- Phase d'Algèbre Linéaire

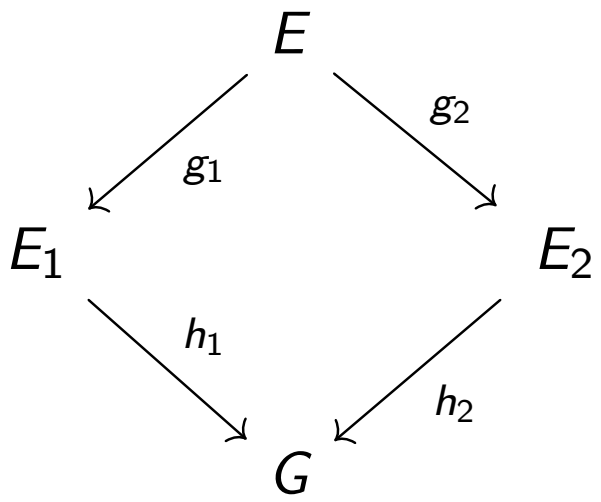
  $\rightarrow$ Retrouve les log discrets des éléments de la base de lissité

- Phase de Logarithme Individuel

  $\rightarrow$ Retrouve le log discret d'un élément arbitraire

Préliminaires à la Phase de Crible

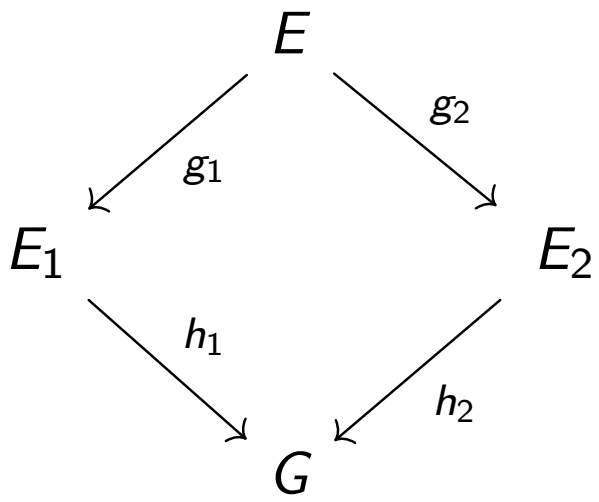
Comment obtenir des relations ?



Pour tout x appartenant à E, nous avons : $h_1(g_1(x)) = h_2(g_2(x))$.

Préliminaires à la Phase de Crible

Comment obtenir des relations ?



Pour tout x appartenant à E, nous avons : $h_1(g_1(x)) = h_2(g_2(x))$.
"Bonnes" relations = écriture via les éléments de la base de lissité uniquement.

Crible par Corps de Nombres / Number Field Sieve (NFS)

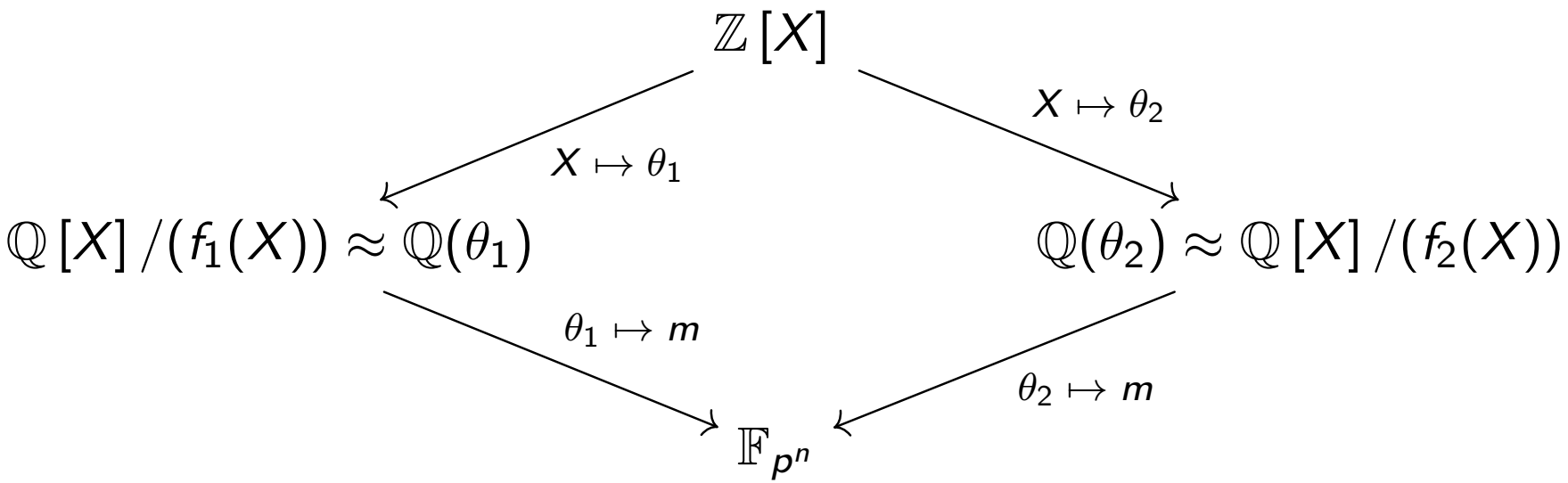
- Résout le DLP pour (tous) les corps finis $\mathbb{F}_{p^n}$ de caractéristiques moyennes ou grandes.

Crible par Corps de Nombres / Number Field Sieve (NFS)

- Résout le DLP pour (tous) les corps finis $\mathbb{F}_{p^n}$ de caractéristiques moyennes ou grandes.
- Préliminaires :
  - Trouver deux polynômes f_1 et f_2 de pgcd irréductible et de degré n modulo p.
  - Définit $\mathbb{F}_{p^n}$ comme le plus petit corps où les deux polynômes ont une racine commune.

Diagramme Commutatif

Avec m une racine de ces polynômes dans $\mathbb{F}_{p^n}$:



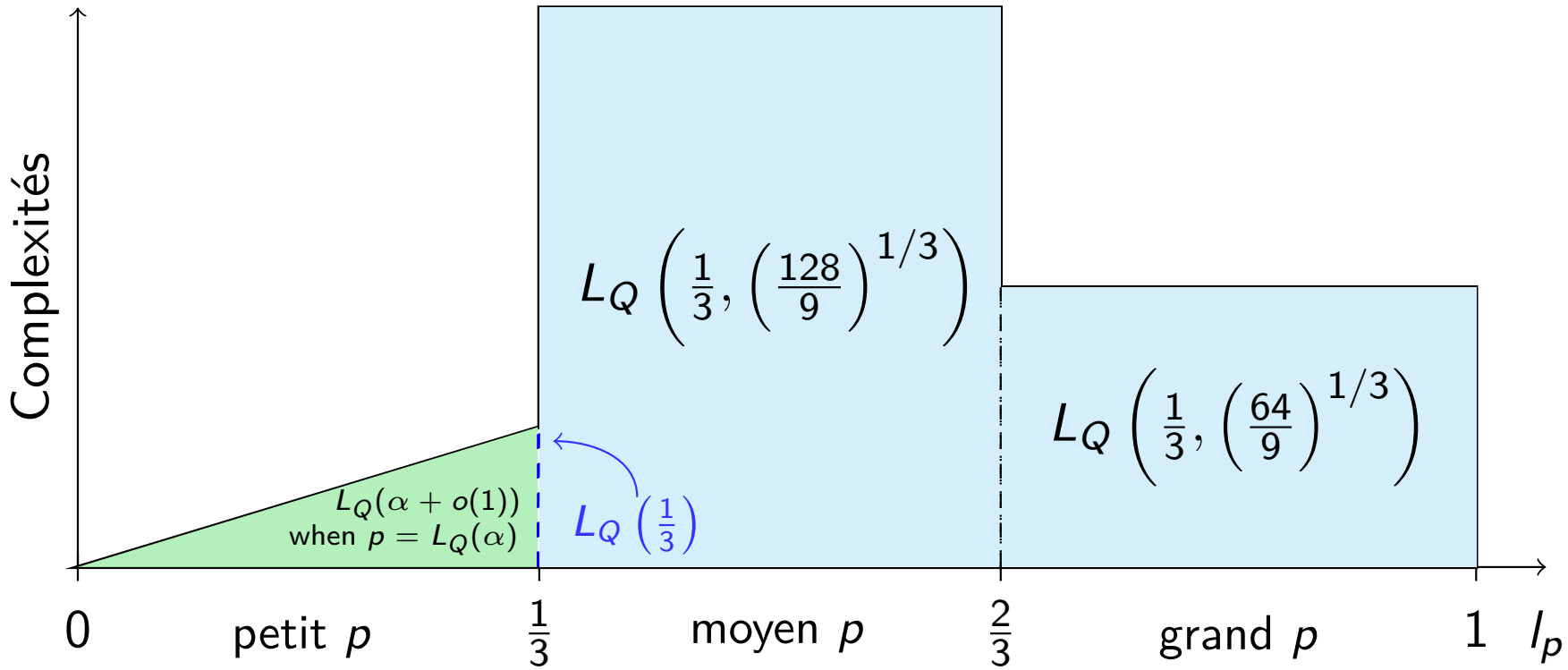
Base de lissité : objets de normes (dans les corps de nombres) plus petites qu'une certaine borne de lissité B.

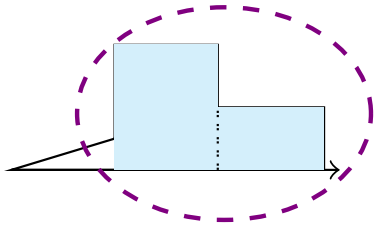
Complexités des Algorithmes par Calcul d'Indice

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

Complexités des Algorithmes par Calcul d'Indice

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





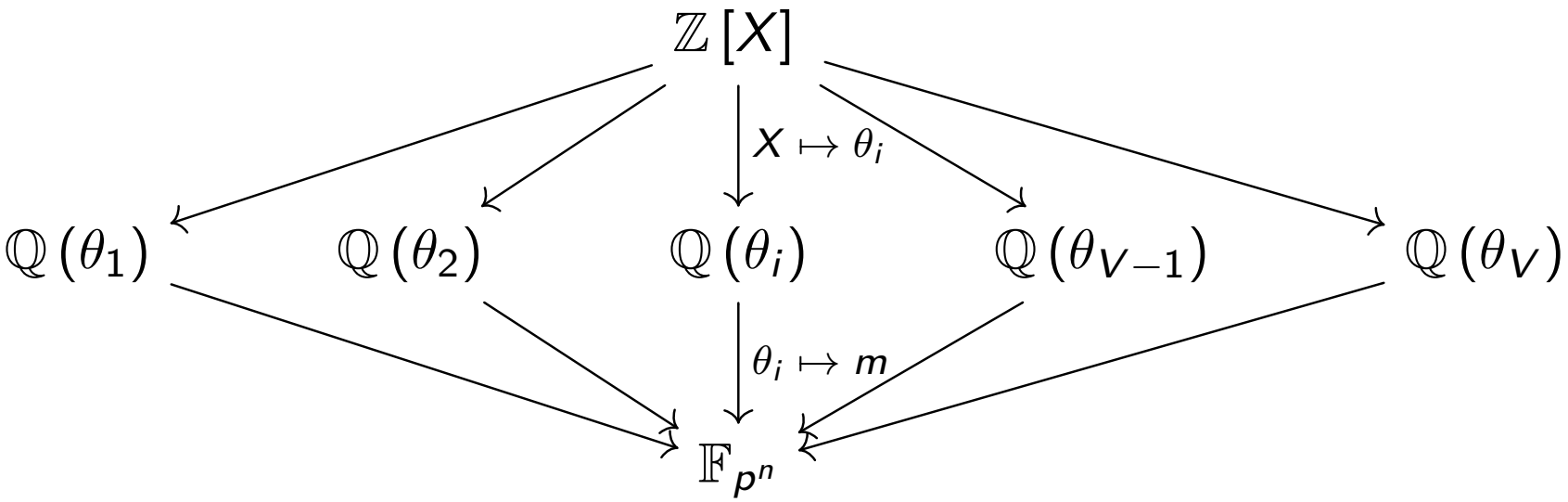
The Multiple Number Field Sieve,

- Co-écrit avec *Razvan Barbulescu*.
- Résout le DLP pour tous les corps finis $\mathbb{F}_{p^n}$ de caractéristiques moyennes et grandes.

The Special Number Field Sieve,

- Co-écrit avec *Antoine Joux*, publié à Pairing 2013.
- Résout le DLP pour certains les corps finis de caractéristiques moyennes et grandes.

- Idée qui provient de la factorisation d'entiers [Cop93] et du DLP dans les corps premiers [Mat03].
- Avec m une racine commune de $f_1, \ldots, f_V$ dans $\mathbb{F}_{p^n}$:

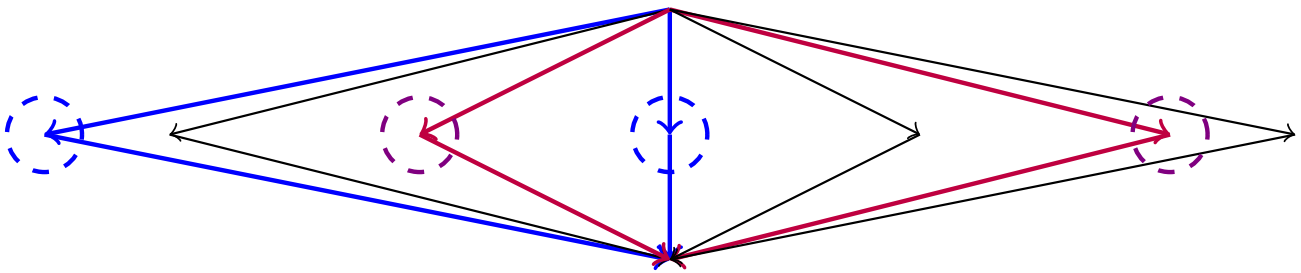


- Choix des polynômes f_1 et f_2 avec une racine commune m dans $\mathbb{F}_{p^n} \Rightarrow$ combinaison linéaire $\Rightarrow f_i = \alpha f_1 + \beta f_2$.

Moyenne VS Grande Caractéristique

Moyenne Caractéristique :

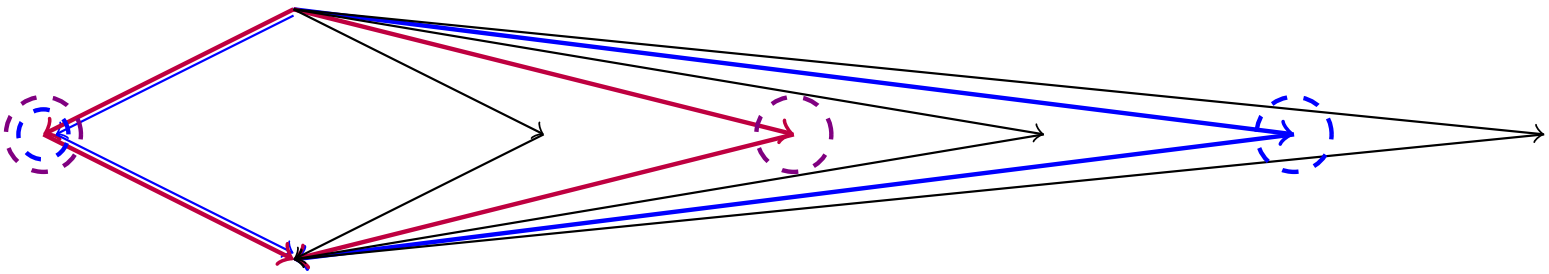
- Sélection polynomiale : f_1 et f_2 ont même degrés, même tailles de coeffs. $\Rightarrow$ même normes dans tous les $\mathbb{Q}(\theta_i)$.
- Crible : on conserve les polynômes de hauts degrés qui donnent des normes inférieures à B dans (au moins) une paire de corps de nombres.



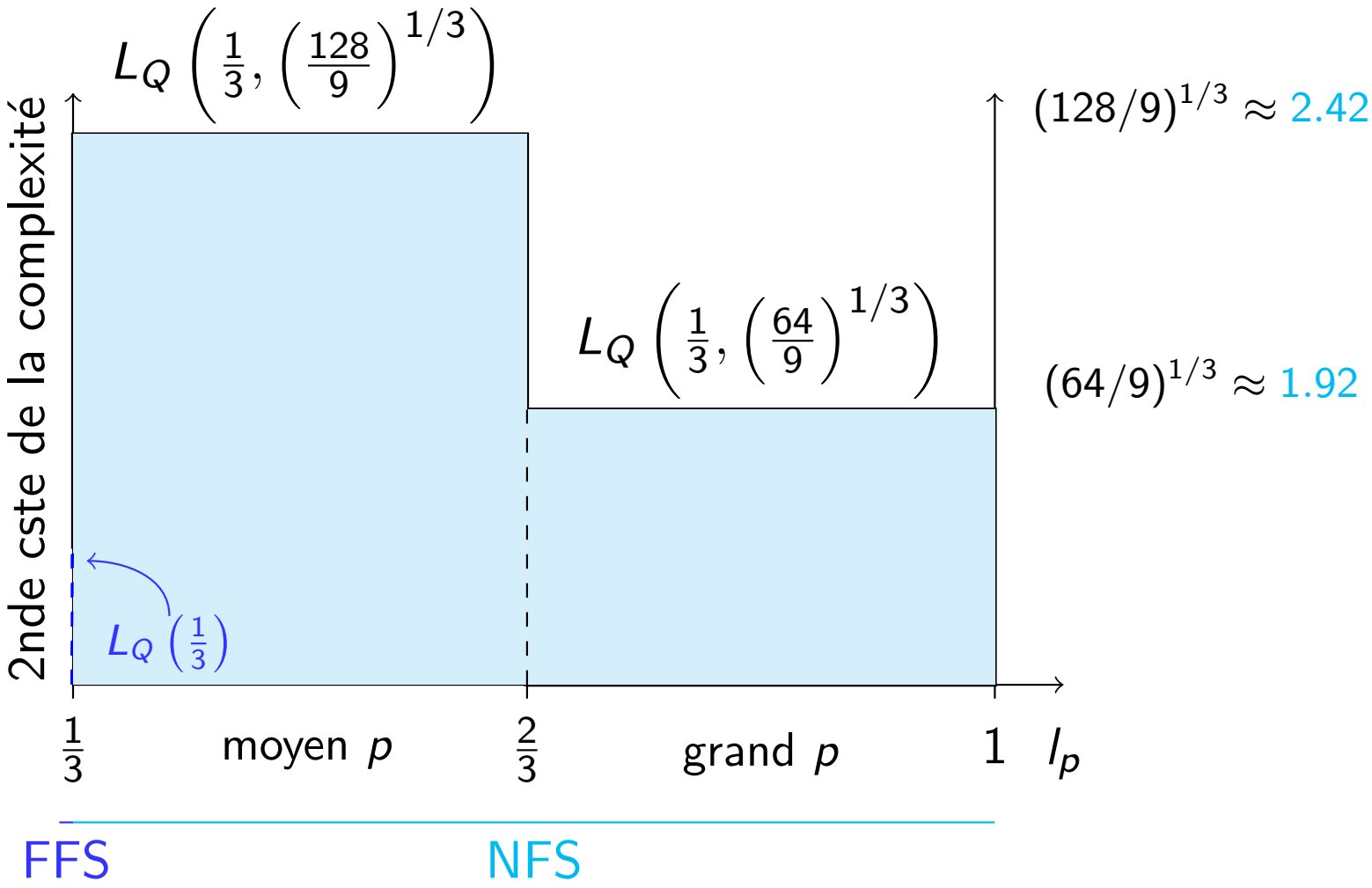
Moyenne VS Grande Caractéristique

Grande Caractéristique :

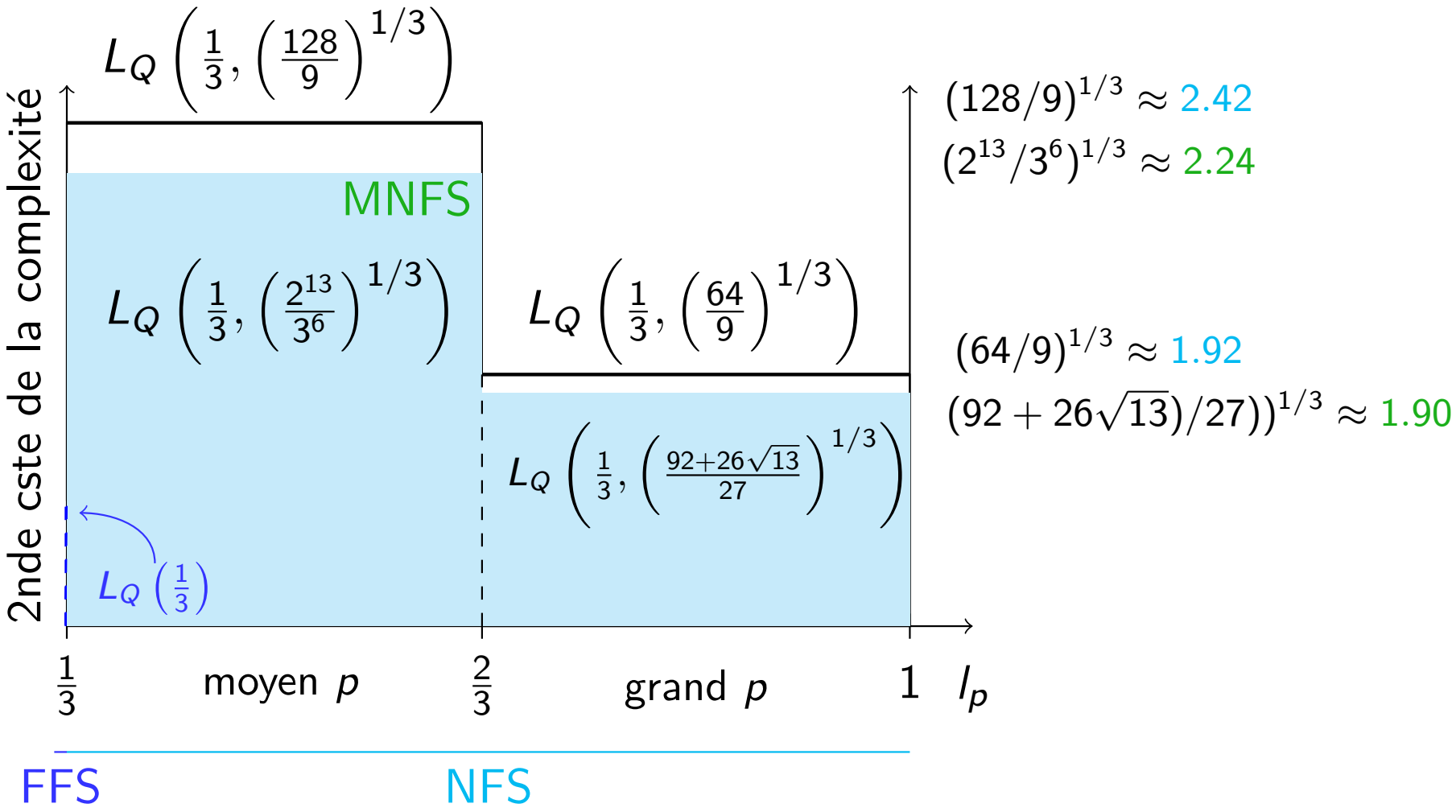
- Sélection polynomiale : f_1 et f_2 même tailles de coeffs mais $\deg f_2 \geqslant \deg f_1 \Rightarrow$ normes plus grandes dans $\mathbb{Q}(\theta_2) \ldots \mathbb{Q}(\theta_V)$.
- Crible : on conserve les polynômes de degré 1 qui donnent une norme inférieure à B dans le premier corps de hombre et une norme inférieure à B' dans (au moins) l'un des autres corps de nombres.



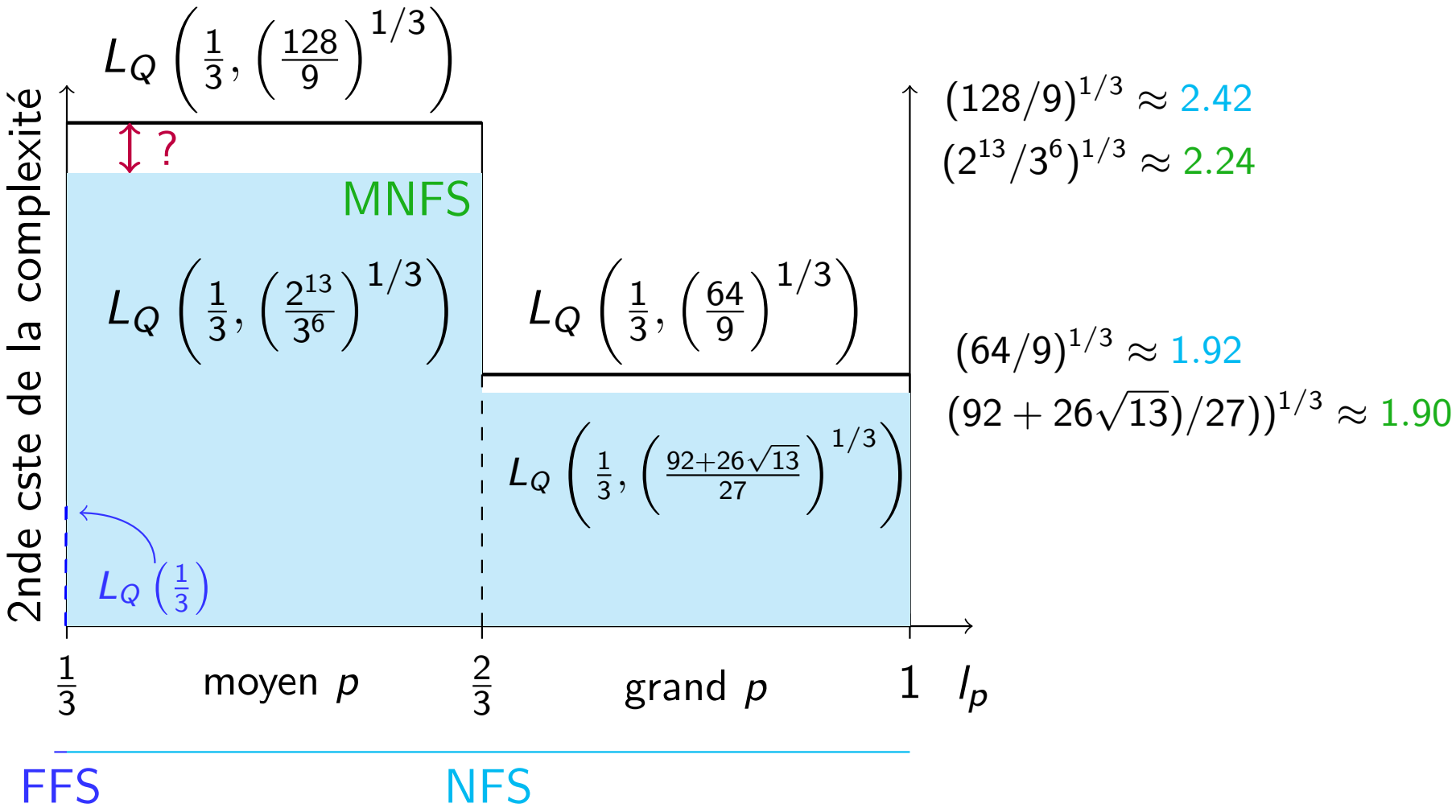
Complexités asymptotiques : NFS



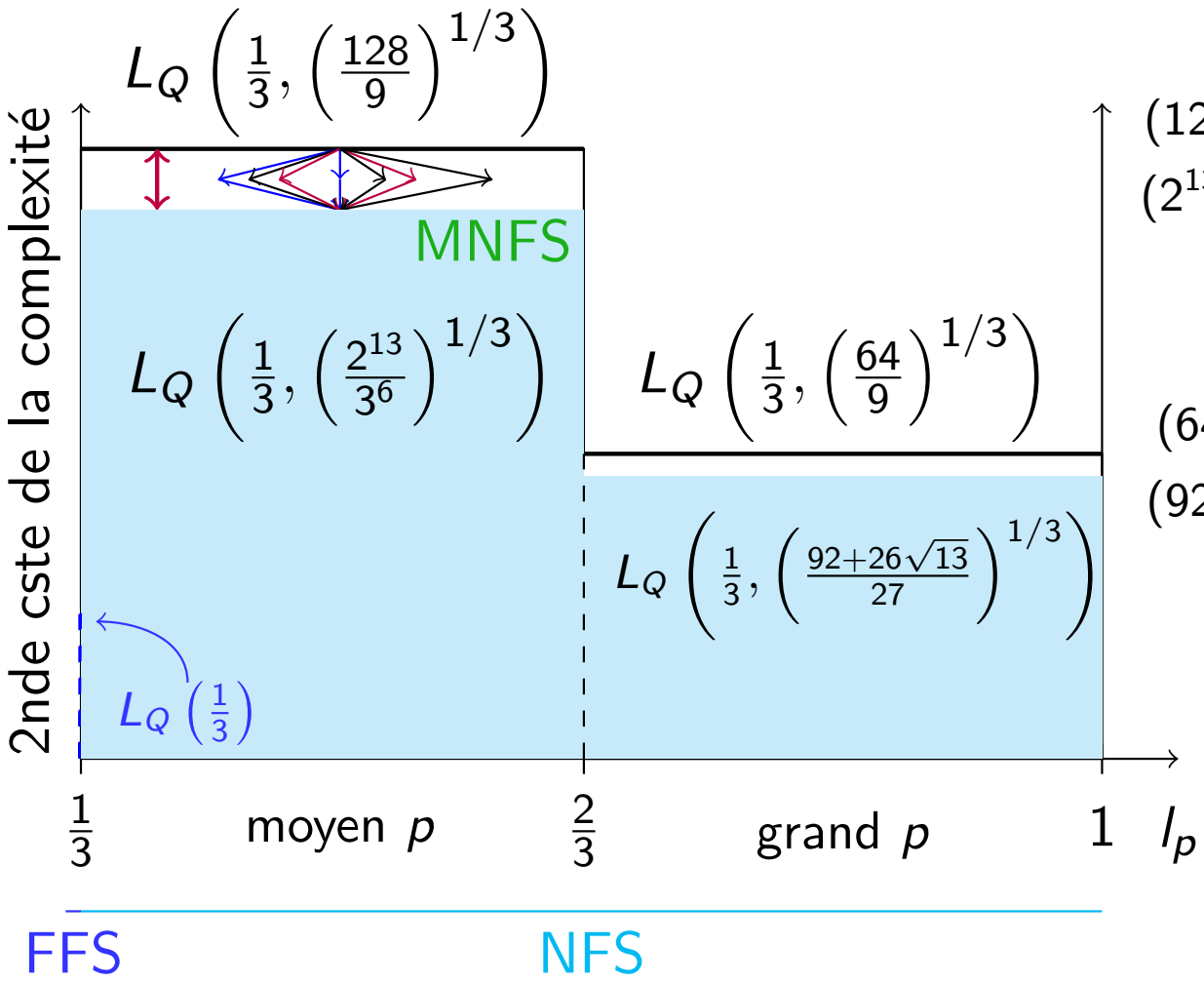
Complexités asymptotiques : NFS et MNFS



Complexités asymptotiques : NFS et MNFS



Complexités asymptotiques : NFS et MNFS



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

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

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

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

Corps finis de caractéristique creuse

The Special Number Field Sieve in $\mathbb{F}_{p^n}$
Application to Pairing-Friendly Constructions.

- Résout le DLP pour (certains) corps finis $\mathbb{F}_{p^n}$ de caractéristique moyenne à grande.

Corps finis de caractéristique creuse

The Special Number Field Sieve in $\mathbb{F}_{p^n}$
Application to Pairing-Friendly Constructions.

- Résout le DLP pour (certains) corps finis $\mathbb{F}_{p^n}$ de caractéristique moyenne à grande.
- Certains ? $\Rightarrow$ meilleurs polynômes lorsque p est spécial.

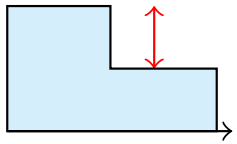
Corps finis de caractéristique creuse

The Special Number Field Sieve in $\mathbb{F}_{p^n}$
Application to Pairing-Friendly Constructions.

- Résout le DLP pour (certains) corps finis $\mathbb{F}_{p^n}$ de caractéristique moyenne à grande.
- Certains ? $\Rightarrow$ meilleurs polynômes lorsque p est spécial.
- Dès lors que $p = P(u)$ où P a petit degré et petits coeffs u petit (en comparaison avec p) $\Rightarrow$ représentation creuse.
- Application aux corps finis liés aux couplages (MNT ou courbes de Barreto-Naehrig...)

Choix des Polynômes

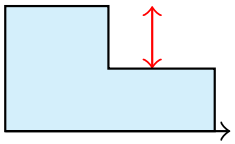
Paramètres qui régissent la complexité de NFS :



- Degré des polynômes sur lesquels on crible.
- Degré des polynômes f_1 et f_2 et taille de leurs coefficients.

Choix des Polynômes

Paramètres qui régissent la complexité de NFS :

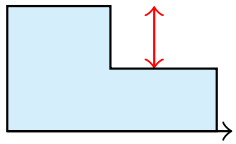
- Degré des polynômes sur lesquels on crible. 
- Degré des polynômes f_1 et f_2 et taille de leurs coefficients.

Nouvelle construction (SNFS) :

- Construction unique que p soit moyen ou grand.

Choix des Polynômes

Paramètres qui régissent la complexité de NFS :



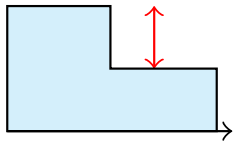
- Degré des polynômes sur lesquels on crible.
- Degré des polynômes f_1 et f_2 et taille de leurs coefficients.

Nouvelle construction (SNFS) :

- Construction unique que p soit moyen ou grand.
- $f_1(x) = h(x) - u$ avec h de degré n et à petits coeffs tel que f_1 soit irréductible sur $\mathbb{F}_p$.
- $f_2(x) = P(h(x))$ de degré $n \cdot \deg(P)$ et à petits coeffs

Choix des Polynômes

Paramètres qui régissent la complexité de NFS :



- Degré des polynômes sur lesquels on crible.
- Degré des polynômes f_1 et f_2 et taille de leurs coefficients.

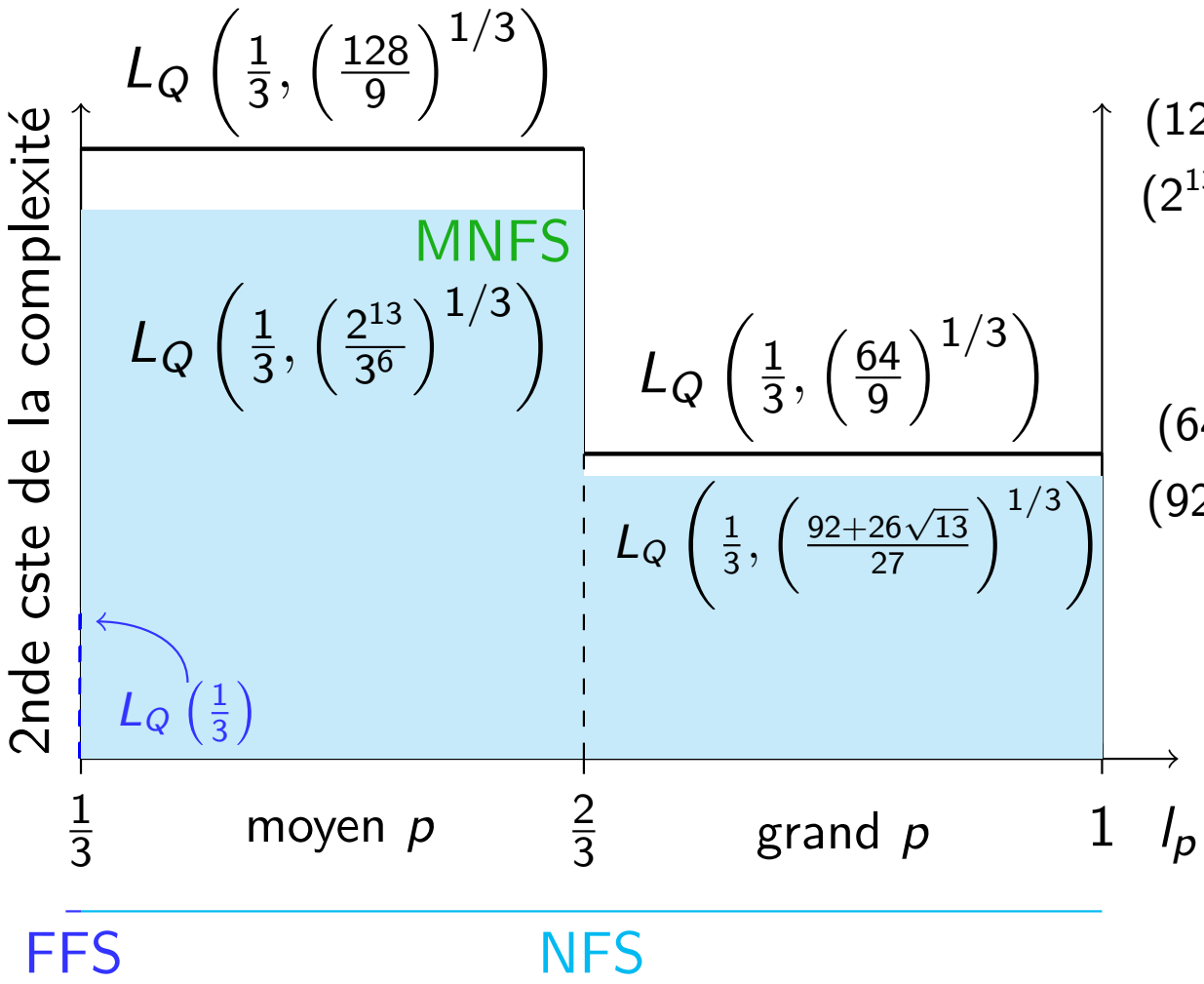
Nouvelle construction (SNFS) :

- Construction unique que p soit moyen ou grand.
- $f_1(x) = h(x) - u$ avec h de degré n et à petits coeffs tel que f_1 soit irréductible sur $\mathbb{F}_p$.
- $f_2(x) = P(h(x))$ de degré $n \cdot \deg(P)$ et à petits coeffs

$$f_2(X) = P(f_1(X) + u) \equiv P(u) = p,$$

où $\equiv$ représente l'équivalence $\bmod f_1(X)$.
$\Rightarrow \text{pgcd}(f_1, f_2)$ est de degré n et irréductible sur $\mathbb{F}_p$.

Complexités asymptotiques : NFS et MNFS



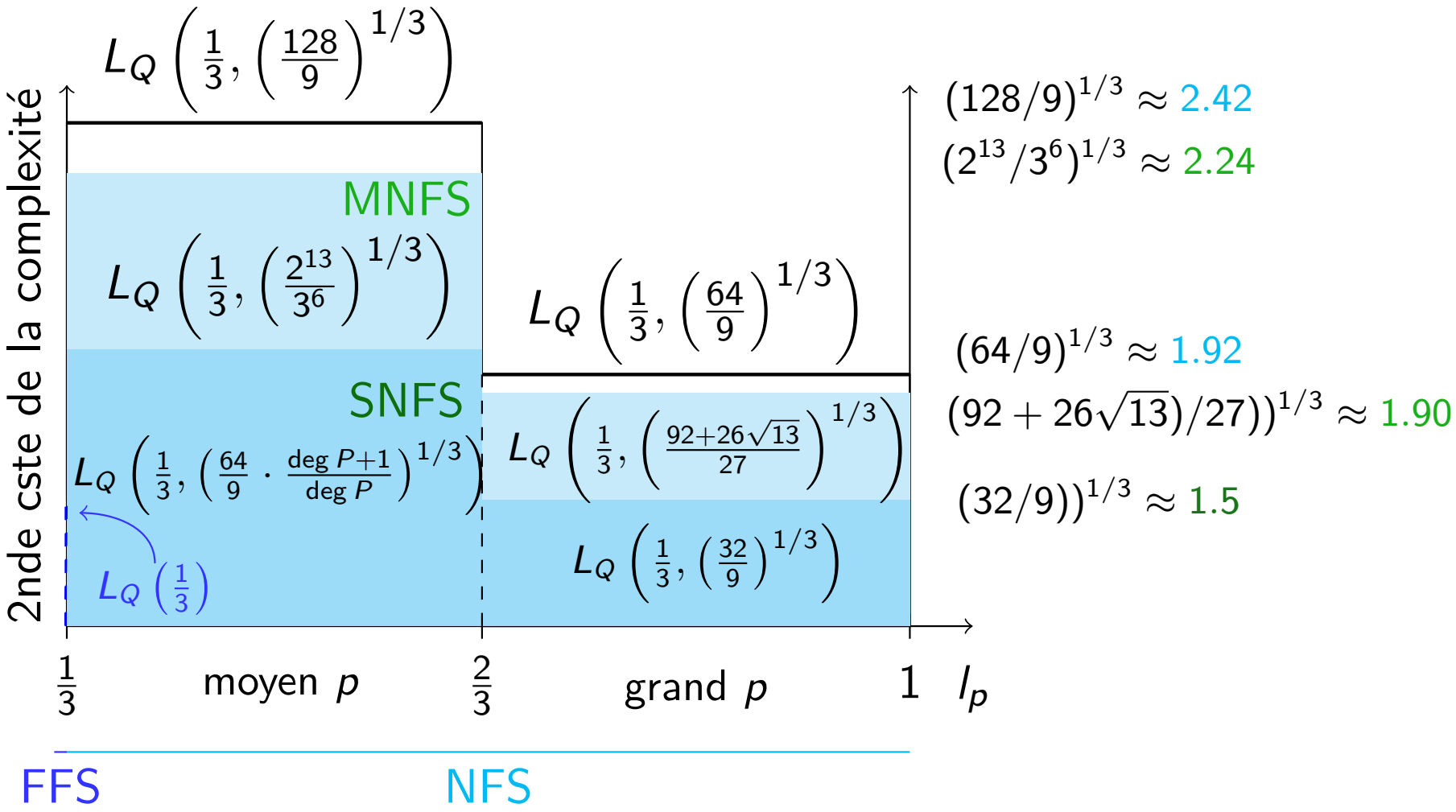
$(128/9)^{1/3} \approx 2.42$

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

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

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

Complexités asymptotiques : NFS, MNFS et SNFS



Merci pour votre attention !

An Example ?

- The Barreto-Naehrig family is optimal for a 128 bits security level with :
  $P(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1$
  $R(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1$
  $Y(x) = 6x^2 + 4x + 1$
- Choose u such that $P(u)$ and $R(u)$ are primes and of convenient size. For $u = \lfloor 2^{62.5} \rfloor + 54525$ we have :

$$E : Y^2 = X^3 + 3$$

over $\mathbb{F}_{6513305019599253805152425835527202156406008609274450191912835466146347850408 3}$.

- MOV Attack : $E[R(u)] \times E[R(u)] \to \mathbb{F}_{p^{12}}$

Consequences for pairing-friendly constructions ?

- The best choice ? Balance DLPs !
  $\Rightarrow \sqrt{p} = L_{p^n}(1/3, \gamma) \Leftrightarrow p = L_{p^n}(1/3, 2\gamma)$
- Complexities in this boundary case ?
  - Before : $L_{p^n}(1/3, c^{1/3})$ with $c > 128/9$
  - New analysis of NFS : $c = 128/9$
  - SNFS : $c = (64/9) \cdot (\deg P + 1)/(\deg P)$
- Consequences :
  - Correct a mistake about generation of pairing-friendly curves (confusion Discrete Logs in high characteristic $\approx$ factorisation)
  - Confirm the current choices of parameters.

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

Generic Algorithms

- Pohlig-Hellman :
  Given a group G of order $\prod p_i^{e_i}$,
  reduces the DLP in G to DLPs in groups of prime order p_i.
- Baby Step/Giant Step, Pollard's rho :
  - Baby Step/Giant Step : Let $T = \lceil \sqrt{p} \rceil$
    1. Create list $a, a/g, \cdots, a/g^{T-1}$
    2. Create list $1, g^T, g^{2T}, \cdots, g^{T(T-1)}$
    3. Find collision
  - Pollard's rho : improved memoryless algorithm.

  $\Rightarrow$ Discrete logs in G of prime order p in $O(\sqrt{p})$ operations.

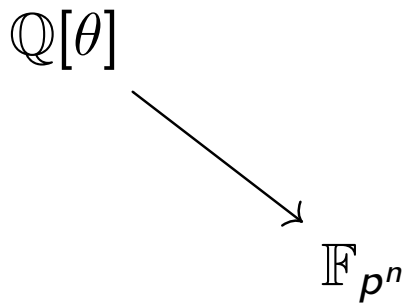
Choice of Polynomials

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)

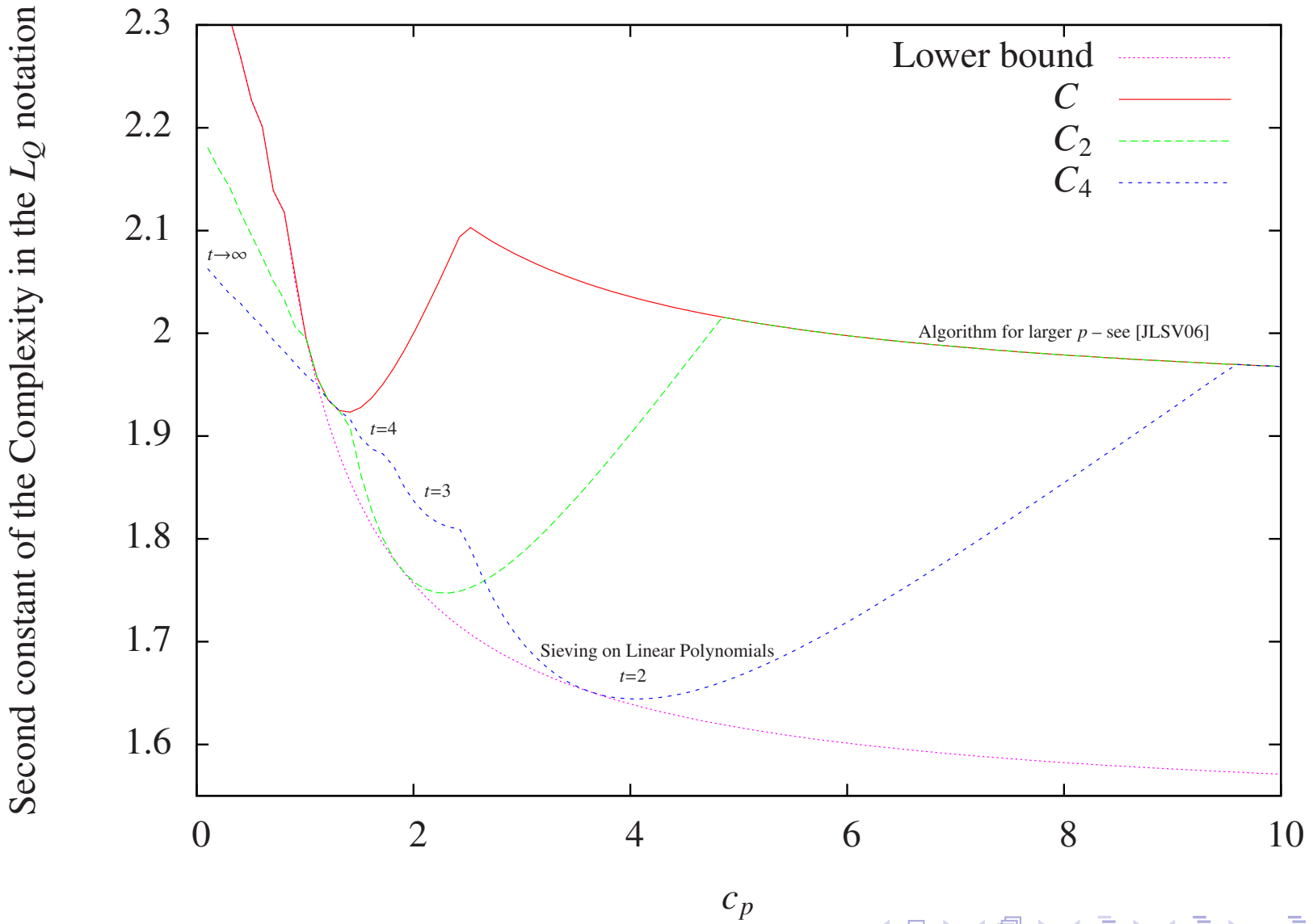
Some Obstructions Coming from Number Fields and its Solutions

How to go down ?



- 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.

SNFS Complexities for the boundary case $p = L_{p^n}(2/3, c_p)$



SNFS Asymptotic Complexities

$p = L_{p^n}(l_p, c_p)$	NFS	SNFS
medium characteristic p $1/3 \leqslant l_p < 2/3$	$L_{p^n}\left(\frac{1}{3}, \left(\frac{128}{9}\right)^{1/3}\right)$	$L_{p^n}\left(\frac{1}{3}, \left(\frac{64}{9}.\frac{\deg P + 1}{\deg P}\right)^{1/3}\right)$
high characteristic p $2/3 < l_p$	$L_{p^n}\left(\frac{1}{3}, \left(\frac{64}{9}\right)^{1/3}\right)$	$L_{p^n}\left(\frac{1}{3}, \left(\frac{32}{9}\right)^{1/3}\right)$ $*$

$*$. As soon as $\deg(P) = \frac{1}{n}\left(\frac{2\log Q}{3\log\log Q}\right)^{1/3}$

Consequences for pairing-friendly constructions ?

- The best choice ? Balance DLPs !
  $\Rightarrow \sqrt{p} = L_{p^n}(1/3) \Leftrightarrow p = L_{p^n}(1/3)$
- Complexities in this boundary case ?
  - Before : $L_{p^n}(1/3, c^{1/3})$ with $c > 128/9$
  - New analysis of NFS : $c = 128/9$? ?
  - SNFS : $c = (64/9) \cdot (\deg P + 1)/(\deg P)$

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

- Until now [NFS by JLSV 2006] :
  - Computing the norm of h in $\mathbb{Q}[X]/f(X)$ is computing the resultant :
    $|\det \mathrm{Sylv}(h, f)| = |\sum_{\sigma_j \in \mathrm{S}_D} \mathrm{sign}(\sigma_j) \prod_{k=1}^{D} \mathrm{Sylv}_{k,\sigma_j(k)}|$.
  - Can be upper bounded by :

$$\Theta \|f\|^{\deg h} \|h\|^{\deg f}$$

with Θ = number of permutations with non zero contributions in the sum.

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

- Until now [NFS by JLSV 2006] :
  - Computing the norm of h in $\mathbb{Q}[X]/f(X)$ is computing the resultant :
    $|\det \mathrm{Sylv}(h, f)| = |\sum_{\sigma_j \in \mathrm{S}_D} \mathrm{sign}(\sigma_j) \prod_{k=1}^{D} \mathrm{Sylv}_{k,\sigma_j(k)}|$.
  - Can be upper bounded by :

$$\Theta \|f\|^{\deg h} \|h\|^{\deg f}$$

    with Θ = number of permutations with non zero contributions in the sum.
  - When $p > L_{p^n}(1/3)$, Θ was negligible, but no more in the boundary case : $\Rightarrow$ complexity raises.

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

- Until now [NFS by JLSV 2006] :
  - Computing the norm of h in $\mathbb{Q}[X]/f(X)$ is computing the resultant :
    $|\det \mathrm{Sylv}(h, f)| = |\sum_{\sigma_j \in \mathrm{S}_D} \mathrm{sign}(\sigma_j) \prod_{k=1}^{D} \mathrm{Sylv}_{k,\sigma_j(k)}|$.
  - Can be upper bounded by :

$$\Theta \|f\|^{\deg h} \|h\|^{\deg f}$$

    with Θ = number of permutations with non zero contributions in the sum.
  - When $p > L_{p^n}(1/3)$, Θ was negligible, but no more in the boundary case : $\Rightarrow$ complexity raises.
- Now : new bound on $\Theta \Rightarrow$ negligible again $\Rightarrow$ restore the analysis $\Rightarrow$ extend the 128/9 to this boundary case.

What about the quasi-polynomial algorithm ?

- Algorithm in $\exp(O(\log q \log k))$ for $\mathbb{F}_{q^k}$.
  Id est : in $n^{O(\log n)}$ where n is the bitsize of the cardinality of the field.
  More precisely, for $\mathbb{F}_{q^k}$, if q can be written as $q = L_{q^k}(c)$, the complexity is in $L_{q^k}(c + o(1))$.
- How ? Modification in the descent phase.
- Really works ? No implementation at the moment.