The Multiple Number Field Sieve with Conjugation Method

Cécile Pierrot

The Multiple Number Field Sieve with Conjugation Method

Cécile Pierrot*

Laboratoire d'Informatique de Paris 6
UPMC, Sorbonne Universités

August 17, 2014

Abstract

In this short paper, we propose a variant of the Number Field Sieve to compute discrete logarithms in medium characteristic finite fields. We propose an algorithm that combines two recent ideas, namely the Multiple variant of the Number Field Sieve taking advantage of a large number of number fields in the sieving phase and the Conjugation Method giving a new polynomial selection for the classical Number Field Sieve. The asymptotic complexity of our improved algorithm is $L_{p^n}(1/3, (8(9+4\sqrt{6})/15)^{1/3})$, where $\mathbb{F}_{p^n}$ is the target finite field and $(8(9+4\sqrt{6})/15)^{1/3}) \approx 2.156$. This has to be compared with the complexity of the previous state-of-the-art algorithm for medium characteristic finite fields, the Number Field Sieve with Conjugation Method, that has a complexity of approximately $L_{p^n}(1/3, 2.201)$.

1 Introduction

Public key cryptosystems are designed around computational hardness assumptions related to mathematical properties, making such protocols hard to break in practice by any adversary. Algorithmic number theory provides most of those assumptions, such as the presumed difficulty to factorize a large integer or to compute discrete logarithms in some groups. Given an arbitrary element h of a cyclic group, the discrete logarithm problem consists in recovering the exponent x of a generator g such that $g^x = h$. We focus here on the multiplicative group of the invertible elements in a finite field.

Current discrete logarithms algorithms for finite fields vary with the relative sizes of the characteristic p and the extension degree n. To be more precise, finite fields split into three families and so do the related algorithms. When p is small compared to n, the best choice is to apply the recent Quasi-Polynomial algorithm [BGJT14]. Medium and high characteristics share some properties since we use in both cases variants of the Number Field Sieve (NFS) that was first introduced to discrete logarithms computations in prime fields in 1993 by Gordon [Gor93] and then extended to all medium and high characteristic finite fields in 2006 by Joux, Lercier, Smart and Vercauteren [JLSV06]. For the past few months, discrete logarithm in finite fields has been a vivid domain and things change fast – not only for small characteristic.

In February 2014, Barbulescu and Pierrot [BP14] presented the Multiple Number Field Sieve (MNFS) that applies both in the medium and high characteristic cases. The main idea used in both cases is to go from two number fields, as in the classical NFS, to a large number of number fields, making the probability to obtain a good relation in the sieving phase higher. Yet, the sieving phase differs between medium

*This work is funded by DGA (Department of Defense, France) and CNRS.

and high characteristic, due to the fact that the parameters of the two first polynomials defining the number fields are equal in the medium case but unbalanced in the high case. Let us recall the notation $L_q(\alpha, c) = \exp(c + o(1)(\log q)^\alpha (\log\log q)^{1-\alpha})$ to be more precise about complexities, and focus on the high characteristic case. Due to unbalanced degree of the first two polynomials, the variant proposed by Barbulescu and Pierrot is dissymmetric. It means that they select in the sieving phase only elements that are small in some sense in the first number field and in at least another number field, giving to the first number field a specific role with regards to the others. With this high characteristic Multiple variant, the asymptotic complexity to compute discrete logarithms in a finite field $\mathbb{F}_{p^n}$ of characteristic $p = L_{p^n}(l_p, c)$ is the same as the complexity for factoring an integer of the same size. Namely, it is:

$$L_{p^n}\left(\frac{1}{3}, \left(\frac{2\cdot(46+13\sqrt{13})}{27}\right)^{1/3}\right).$$

In the medium case, the polynomial selection of the classical Number Field Sieve allows to construct two polynomials with same degrees and same sizes of coefficients. Making linear combination, MNFS creates then a lots of polynomials with equal parameters. Thanks to this notion of symmetry, the sieving phase of the Multiple variant consists in keeping elements that are small in any pairs of number fields, making the probability growing further.

Yet, few months later, in August 2014, Barbulescu, Gaudry, Guillevic and Morain detailed in a preprint [BGGM14] some practical improvements for the classical Number Field Sieve. They gave besides a new polynomial selection method that has a nice theoretical interest too since it leads to the best asymptotic heuristic complexity known in the medium characteristic case, overpassing the one given in [BP14] that was the current state-of-the-art algorithm in this case until this month. This new polynomial selection also called Conjugation Method permits to create one polynomial with a *small* degree and *high* coefficients and another one with *high* degree and constants coefficients. Finally, the authors obtain the asymptotic complexity:

$$L_{p^n}\left(\frac{1}{3}, \left(\frac{96}{9}\right)^{1/3}\right).$$

We propose here to adapt the Multiple variant to this very recent algorithm. At first sight, one could fear that the parameters of the two polynomials given with the Conjugation Method could act as a barrier, since their unbalanced features differ from the ones used in the medium characteristic case of [BP14]. Moreover, following the high characteristic dissymmetric sieving phase of [BP14] and creating the remaining polynomials with linear combination would mean spreading both *high* coefficients and *high* degrees on the polynomials defining the various number fields. This clearly would not be a good idea, since all the NFS-based algorithms require to create elements with small norms. However, remarking that this Conjugation Method may allow the selection of more than two polynomials, it is possible to astutely set up the remaining polynomials. Indeed, the idea is to try to keep the advantage of this kind of *balanced dissymetry* brought by the two polynomials with *small*-degree-*high*-coefficients/*high*-degree-*small*-coefficients.

We explain in Section 2 how to take advantage of this remark to construct a dissymetric Multiple Number Field Sieve. The asymptotic complexity analysis is given in Section 3. In a nutshell, the Multiple Number Field Sieve with Conjugation Method (MNFS-CM) becomes the best current algorithm to compute discrete logarithms in medium characteristic finite fields since it has complexity:

$$L_{p^n}\left(\frac{1}{3}, \left(\frac{8\cdot(9+4\sqrt{6})}{15}\right)^{1/3}\right).$$

This has to be compared with the complexity given in [BGGM14]. Our second constant is such that $\left(8\,(9+4\sqrt{6})/15\right)^{1/3} \approx 2.156$ whereas $(96/9)^{1/3} \approx 2.201$.

2 Combining the Multiple variant of the Number Field Sieve with the Conjugation Method

Let $\mathbb{F}_{p^n}$ denote the finite field we target, p its characteristic and n the extension degree relatively to the base field. We propose an algorithm to compute discrete logarithms in $\mathbb{F}_{p^n}$ as soon as p can be written as $p = L_{p^n}(l_p, c_p)$ with $1/3 \leqslant l_p < 2/3$. In this case we say that the characteristic has medium size. In Section 2.1 we explain how to represent the finite field and to construct the polynomials that define the large number of number fields we need. In Section 2.2 we give details about the variant of the Multiple Number Field Sieve we propose to follow.

2.1 Polynomial Selection

Basic idea: large numbers of polynomials with a common root in $\mathbb{F}_{p^n}$

To compute discrete logarithms in $\mathbb{F}_{p^n}$, all algorithms based on the Number Field Sieve start by choosing two polynomials f_1 and f_2 with integers coefficients such that the greatest common divisor of these polynomials has an irreducible factor of degree n over the base field. If m denote a common root of these two polynomials in $\mathbb{F}_{p^n}$ and $\mathbb{Q}(\theta_i)$ denote the number field $\mathbb{Q}[X]/(f_i(X))$ for each $i = 1, 2$, *i.e.* θ_i is a root of f_i in $\mathbb{C}$, then we are able to draw the commutative diagram of Figure 1.

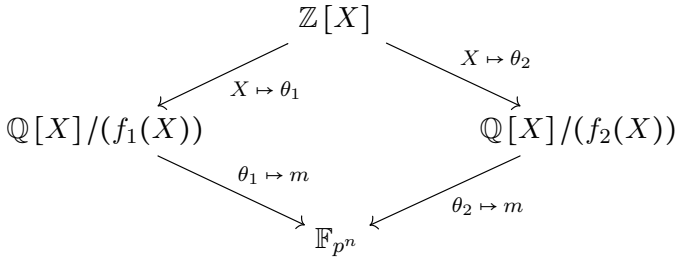

Figure 1: Commutative diagram of NFS.

Since the Multiple variant of NFS require to have a large number of number fields, let say V number fields, then we have to construct $V-2$ other polynomials that share the same common root m in $\mathbb{F}_{p^n}$. The commutative diagram that is the cornerstone of all Multiple Number Field Sieve is then:

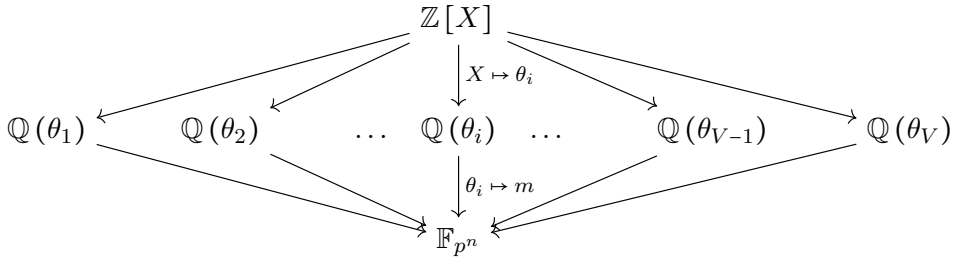

Figure 2: Commutative diagram of Multiple variant of NFS

Settings: Construction of V polynomials with the Conjugation Method

We start with the Conjugation Method given in [BGGM14, Paragraph 6.3] to construct the first two polynomials. The idea is as follows.

We create two stand-in polynomials g_a and g_b in $\mathbb{Z}[X]$ with small coefficients such that $\deg g_a = n$ and $\deg g_b < n$. We search then for a polynomial $X^2 + uX + v$, where u and v are integers of constant sizes, that is irreducible over $\mathbb{Z}[X]$ and has its roots λ and λ' in $\mathbb{F}_p$. Since we seek for a degree n irreducible polynomial over $\mathbb{F}_p[X]$ to construct the finite field, we keep the polynomial $X^2 + uX + v$ if either $g_a + \lambda g_b$ or $g_a + \lambda' g_b$ is irreducible over $\mathbb{F}_p[X]$. When we have found such parameters, we choose our first polynomial $f_1 \in \mathbb{Z}[X]$ such that:

$$f_1 = g_a^2 - u g_a g_b + v g_b^2.$$

Equivalently, f_1 is defined in [BGGM14] as equal to $\mathrm{Res}_Y(Y^2+uY+v, g_a(X)+Y g_b(X))$. Since λ and λ' are roots of X^2+uX+v in $\mathbb{F}_p$, we have that $f_1 \equiv g_a^2-(\lambda+\lambda')g_a g_b+\lambda\lambda' g_b^2 \mod p$. In other words, $f_1 \equiv (g_a+\lambda g_b)(g_a+\lambda' g_b) \mod p$. Thus we have a polynomial f_1 of degree $2n$ with coefficients in $O(1)$ that is divisible by $g_a + \lambda g_b$ in $\mathbb{F}_p[X]$.

Let us construct the next two polynomials. Thanks to continued fractions we can write:

$$\lambda \equiv \frac{a}{b} \equiv \frac{a'}{b'} \mod p$$

where a, b, a' and b' are of the size of $\sqrt{p}$. We underline that these two reconstructions (a, b) and (a', b') of λ are linearly independent over $\mathbb{Q}$. We set then:

$$f_2 = b g_a + a g_b \quad \text{and} \quad f_3 = b' g_a + a' g_b.$$

Note that the Conjugation Method ends with the selection of f_1 and f_2 and does not use the second reconstruction. It is clear that both f_2 and f_3 have degree n and coefficients of size $\sqrt{p}$. Furthermore, we notice that $f_2 \equiv b(g_a + \lambda g_b) \mod p$ and similarly $f_3 \equiv b'(g_a + \lambda g_b) \mod p$, so they share a common root with f_1 in $\mathbb{F}_{p^n}$.

We finally set for all i from 4 to V:

$$f_i = \alpha_i f_2 + \beta_i f_3$$

with α_i and β_i of the size of $\sqrt{V}$. Thanks to linear combination, for all $2 \leqslant i \leqslant V$, f_i has degree n, coefficients of size $\sqrt{p}$ and is divisible by $g_a + \lambda g_b$ in $\mathbb{F}_p[X]$.

2.2 A dissymmetric Multiple Number Field Sieve

As any Index Calculus algorithm, the variant we propose follows three phases: the sieving phase, in which we create lots of relations involving only a small set of elements, the factor base ; the linear algebra, to recover the discrete logarithms of the elements of the factor base ; and the individual logarithm phase, to compute the discrete logarithm of an arbitrary element of the finite field.

We propose to sieve as usual on high degree polynomials $\phi(X) = a_0 + \cdots + a_{t-1}X^{t-1}$ with coefficients of size bounded by S. Let us recall that, given an integer y, an integer x is called *y-smooth* if it can be written as a product of factors less than y. We collect then all polynomials such that, first, the norm of $\phi(\theta_1)$ is B-smooth and, second, there exists (at least) one number field $\mathbb{Q}(\theta_i)$ with $i \geqslant 2$ in which the norm $\phi(\theta_i)$ is B'-smooth. In other simpler words, we create relations thanks to polynomials that cross over the diagram of Figure 3 in two paths: the one on the left side of the drawing and (at least) another one among those on the right. If we set that the factor base consists in the union of all the prime ideals in the rings of integers that have a B-or-B'-smooth norm, the smoothness bound depending on the number field, then we keep only relations that involve these factor base elements.

After the same post-processing as in [JLSV06] or as detailed in [BGGM14] more recently, each such polynomial ϕ yields a linear equation between "logarithms of ideals" coming from two number fields. Hence, from each relation we obtain a linear equation where the unknowns are the logarithms of ideals. Let us remark that by construction each equation involves few unknowns only.

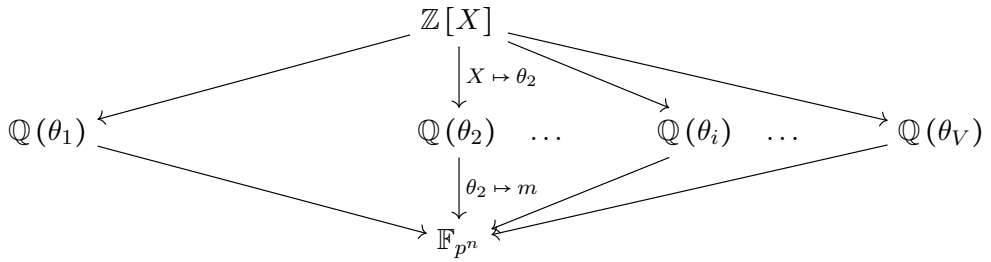

Figure 3: Commutative diagram for the dissymmetric Multiple Number Field Sieve with Conjugation Method

The sparse linear algebra and individual logarithm phases run exactly as in the classical Number Field Sieve of [JLSV06]. Even if there exists a specific way to manage the last phase with a multiple variant as detailed in [BP14], taking advantage of the large number of number fields again, we do not consider it here. In fact, the runtime of the classical individual logarithm phase is already negligible with regards to the total runtime of the algorithm, as proved by Barbulescu and Pierrot in their article.

3 Asymptotic Complexity Analysis

Let us fix the notations and write the extension degree n and the characteristic p of the target finite field $\mathbb{F}_Q$ as:

$$n = \frac{1}{c_p}\left(\frac{\log Q}{\log\log Q}\right)^{1-l_p} \quad \text{and} \quad p = \exp(c_p(\log Q)^{l_p}(\log\log Q)^{1-l_p})$$

with $1/3 \leqslant l_p < 2/3$. The parameters that take part in the heuristic asymptotic complexity analysis of our Multiple Number Field Sieve with Conjugation Method are the sieving bound S, the degree of the polynomials we are sieving over $t-1$, the number of number fields V, the smoothness bound B related to the first number field and the smoothness bound B' related to the others number fields. The analysis works by optimizing the total runtime of the sieving and linear algebra phases while complying with two constraints.

Balancing the cost of the two first phases

We first require that the runtime of the sieving phase S^t equals the cost of the linear algebra. Since the linear system of equations we obtain is sparse, the cost of the linear algebra is asymptotically $(B + VB')^2$. Similarly to balancing the runtime of the two phases, we require that $B = VB'$. Thus, leaving apart the constant 4 that is clearly negligible with regards to the sizes of the parameters, the first constraint can be written as:

$$S^t = B^2. \tag{1}$$

Balancing the number of equations with the number of unknows

To be able to do the linear algebra phase correctly, we require that the number of unknows, that is approximately B, is equal to the number of equations produced in the sieving phase. If we note $\mathcal{P}$ the probability that a polynomial give a good relation then we want to have $S^t\mathcal{P} = B$. Combining it with the constraint (1), it leads to:

$$B = 1/\mathcal{P}.$$

Evaluating the probability of smoothness

To evaluate the probability $\mathcal{P}$ we need to recall some tools about norms in number fields. For $f_i \in \mathbb{Z}[X]$ an irreducible polynomial, θ_i a complex root of f_i, and for any polynomial $\phi \in \mathbb{Z}[X]$, the norm $\mathrm{N}(\phi(\theta))$ satisfies $\mathrm{Res}(\phi, f_i) = \pm l_i^{\deg \phi}\, \mathrm{N}(\phi(\theta))$, where l_i is the leading coefficient of f_i. Since we treat l_i together with small primes, we make no distinction in smoothness estimates between norms and resultants. If $\|f_i\|_\infty$ denotes the largest coefficients of f_i in absolute value then we have the upper bound on the resultant:

$$|\mathrm{Res}(\phi, f_i)| \leq (\deg f_i + \deg \phi)! \cdot \|f_i\|_\infty^{\deg \phi} \cdot \|\phi\|_\infty^{\deg f_i}.$$

Thus, recalling that f_1 is of degree $2n$ and has constant coefficients and that every other polynomials f_i has degree n and coefficients of the size $\sqrt{p}$, we obtain that the norm of a polynomial ϕ in the sieving is bounded by S^{2n} in the first number field and by $S^n p^{t/2}$ in every other number fields.

To evaluate the probability of smoothness of this norms with regards to B and B', the main tool is the following theorem:

Theorem 1 (Canfield, Erdős, Pomerance [CEP83])**.** *Let $\psi(x, y)$ denote the number of positive integers up to x which are y-smooth. If $\epsilon > 0$ and $3 \leq u \leq (1-\epsilon)\log x/\log\log x$, then $\psi(x, x^{1/u}) = xu^{-u+o(u)}$.*

Yet, this result under this form is not very convenient. If we write the two integers x and y with the L_q-notation, we obtain a more helpful corollary:

Corollary 1. *Let $(\alpha_1, \alpha_2, c_1, c_2) \in [0,1]^2 \times [0,\infty)^2$ be four reals such that $\alpha_1 > \alpha_2$. Let $\mathcal{P}$ denote the probability that a random positive integer below $x = L_q(\alpha_1, c_1)$ splits into primes less than $y = L_q(\alpha_2, c_2)$. Then we have $\mathcal{P}^{-1} = L_q\left(\alpha_1 - \alpha_2, (\alpha_1 - \alpha_2)c_1 c_2^{-1}\right)$.*

So we would like to express both norms and sieving bounds with the help of this notation. As usual, we set:

$$t = \frac{c_t}{c_p}\left(\frac{\log Q}{\log\log Q}\right)^{2/3-l_p}, \quad S^t = L_Q(1/3, c_s c_t), \quad B = L_Q(1/3, c_b) \quad \text{and} \quad V = L_Q(1/3, c_v).$$

With this in hands, the first constraint can be rewritten as:

$$c_s c_t = 2c_b \tag{2}$$

We apply besides the Theorem 1 to reformulate the other constraint. Let us note $L_Q(1/3, p_r)$ (respectively $L_Q(1/3, p_{r'})$) the probability to get a B-smooth norm in the first number field (respectively a B'-smooth norm in at least one other number field). The second constraint becomes $c_b = -(p_r + p_{r'})$. Using equation (2), the constants in the probabilities can be written as:

$$p_r = \frac{-2c_s}{3c_b} = \frac{-2(2/c_t)c_b}{3c_b} \qquad \text{and} \qquad p_{r'} = c_v - \frac{(2/c_t)c_b + c_t/2}{3(c_b - c_v)}.$$

That leads to require $c_b = -(-4/(3c_t) + c_v - (4c_b + c_t^2)/(6c_t(c_b - c_v)))$ and afterwards $6c_t(c_b^2 - c_v^2) = 8(c_b - c_v) + 4c_b + c_t^2$. Finally we would like to have:

$$(6c_t)c_b^2 - 12c_b - 6c_t c_v^2 + 8c_v - c_t^2 = 0 \tag{3}$$

Optimizing the asymptotic complexity

We recall that the complexity of our algorithm is given by the cost of the linear algebra $L_Q(1/3, 2c_b)$, since we equalize the runtime of the sieving and linear algebra phases. Hence we look for minimizing c_b under the above constraint (3). The method of Lagrange multipliers indicates that c_b, c_v and c_t have to be solutions of the following system:

$$\begin{cases} 2 + \lambda(12c_t c_b - 12) = 0 \\ \lambda(-12c_v c_t + 8) = 0 \\ \lambda(6c_b^2 - 6c_v^2 - 2c_t) = 0 \end{cases}$$

with $\lambda \in \mathbb{R}^*$. From the second row we obtain $c_t = 2/(3c_v)$ and from the third one we get $c_b = (c_v^2 + 2/(9c_v))^{1/2}$. Together with equation (3), it gives the equation in one variable: $405c_v^6 + 126c_v^3 - 1 = 0$. We deduce that $c_v = ((3\sqrt{6} - 7)/45)^{1/3}$ and we recover $c_b = ((9 + 4\sqrt{6})/15)^{1/3}$. Finally, the heuristic asymptotic complexity of the Multiple Number Field Sieve with Conjugation Method is:

$$L_Q\left(\frac{1}{3}, \left(\frac{8 \cdot (9 + 4\sqrt{6})}{15}\right)^{1/3}\right)$$

This has to be compared with the Number Field Sieve with Conjugation Method proposed in [BGGM14] that has complexity $L_Q(1/3, (96/9)^{1/3})$. Our second constant is $(8(9 + 4\sqrt{6})/15)^{1/3} \approx 2.156$, whereas $(96/9)^{1/3} \approx 2.201$.

References

[BGGM14] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain. Improvements to the number field sieve for non-prime finite fields. INRIA Hal Archive, Report 01052449, 2014.

[BGJT14] Razvan Barbulescu, Pierrick Gaudry, Antoine Joux, and Emmanuel Thomé. A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In *EUROCRYPT*, pages 1–16, 2014.

[BP14] Razvan Barbulescu and Cécile Pierrot. The multiple number field sieve for medium and high characteristic finite fields. *LMS Journal of Computation and Mathematics*, 17:230–246, 2014.

[CEP83] Earl Rodney Canfield, Paul Erdös, and Carl Pomerance. On a problem of Oppenheim concerning factorisatio numerorum. *Journal of Number Theory*, 17:1–28, 1983.

[Gor93] Daniel M. Gordon. Discrete logarithms in GF(p) using the number field sieve. 6(1):124–138, 1993.

[JLSV06] Antoine Joux, Reynald Lercier, Nigel P. Smart, and Frederik Vercauteren. The number field sieve in the medium prime case. In *CRYPTO 2006*, volume 4117, pages 326–344, 2006.