COMPUTING INDIVIDUAL DISCRETE LOGARITHMS FASTER IN GF(p^n)

AURORE GUILLEVIC [1,2]

[1]Institut National de Recherche en Informatique et en Automatique (INRIA)
Grace Team, Inria Saclay, France
[2]École Polytechnique/LIX
guillevic@lix.polytechnique.fr

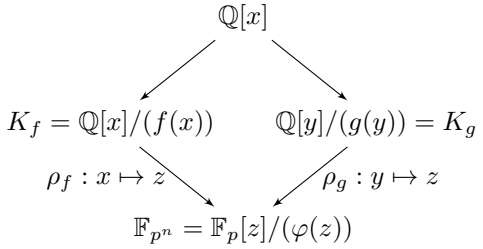
Abstract. The Number Field Sieve (NFS) algorithm is the best known method to compute discrete logarithms (DL) in large characteristic finite fields $\mathbb{F}_{p^n}$, with p large and $n \geq 1$ small. This algorithm comprises four steps: polynomial selection, relation collection, linear algebra and finally, individual logarithm computation. The first step outputs two numbers fields equipped with a map to $\mathbb{F}_{p^n}$. After the relation collection and linear algebra phases, the (virtual) logarithm of a subset of elements in each number field is known. The fourth step computes a preimage in one number field of the target element in $\mathbb{F}_{p^n}$. If one can write the target preimage as a product of elements of known (virtual) logarithm, then one can deduce the discrete logarithm of the target.

The traditional approach for the individual logarithm step can be extremely slow, and it is too slow especially for n greater than 3. Its asymptotic complexity is $L_Q[1/3, c]$ with $c \geq 1.44$. We present a new preimage computation that provides a dramatic improvement for individual logarithm computations for small n, both in practice and in asymptotic running-time: we have $L_Q[1/3, c]$ with $c = 1.14$ for $n = 2, 4$, $c = 1.26$ for $n = 3, 6$ and $c = 1.34$ for $n = 5$. Our method generalizes to any n; in particular $c < 1.44$ for the two state-of-the-art variants of NFS for extension fields.

Keywords: Discrete logarithm, finite field, number field sieve, individual logarithm.

1. Introduction

1.1. **The Number Field Sieve Algorithm for Discrete Logarithms in Finite Fields.** We recall that the NFS algorithm is made of four steps: polynomial selection, relation collection, linear algebra and finally, individual logarithm computation. This last step is mandatory to break any given instance of a discrete logarithm problem. The polynomial selection outputs two numbers fields, each equipped with a map ρ_f, ρ_g to $\mathbb{F}_{p^n}$, as shown in the following diagram. Moreover, the monic polynomial defining the finite field is $\varphi = \gcd(f, g) \bmod p$, of degree n.



Date: Preprint, May, 27th 2015.

This research was partially funded by Agence Nationale de la Recherche grant ANR-12-BS02-0001.

In the remaining of this paper, we will only use $\rho = \rho_f$ and $K = K_f$. After the relation collection and linear algebra phases, the (virtual) logarithm of a subset of elements in each number field is known. The individual logarithm step computes a preimage in one number field of the target element in $\mathbb{F}_{p^n}$. If one can write the target preimage as a product of elements of known (virtual) logarithm, then one can deduce the individual logarithm of the target. The key point of individual logarithm computation is finding a smooth enough decomposition of the target preimage.

The asymptotic running time of NFS algorithm steps are estimated with the L-function:

$$L_Q[\alpha, c] = \exp\Big(\big(c + o(1)\big)(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}\Big) \quad \text{with } \alpha \in [0,1] \text{ and } c > 0\ .$$

The α parameter measures the gap between polynomial time ($\alpha = 0$) and exponential time ($\alpha = 1$). When c is implicit, or obvious from the context, we simply write $L_Q[\alpha]$. When the complexity relates to an algorithm for a prime field $\mathbb{F}_p$, we write $L_p[\alpha, c]$.

1.2. **Previous Work on Individual Logarithm.** Many improvements for computing discrete logarithms first concerned prime fields. In 1993, Gordon [9] proposed the first version of NFS–DL algorithm for prime fields $\mathbb{F}_p$ with asymptotic complexity $L_p[1/3, 9^{1/3}]$. The previous state-of-the-art for computing discrete logarithms in prime fields was the Coppersmith, Odlyzko and Schroeppel (COS) algorithm, in $L_p[1/2, 1]$. Gordon's $L_p[1/3]$ algorithm is interesting for very large values of p, that were not yet targets for discrete logarithm computations in the nineties. Buhler, H. Lenstra and Pomerance [5] estimated the crossover point between 100 and 150 decimal digits, i.e. between 330 and 500 bits. However, with the $L_p[1/3]$ algorithm there is a new difficulty: the individual logarithm phase. The COS algorithm computes the logarithms of many "small" elements. Writing a relation between any given target element and the "small" elements of known logarithms can be done quite fast. But in the $L_p[1/3]$ algorithm, many fewer logarithms are known, because the relation collection is shorter, explaining the $L_p[1/3]$ running time instead of $L_p[1/2]$. As a drawback, the individual logarithm phase becomes quite time consuming. Since some non-small elements in the decomposition of the target have an unknown logarithm, a dedicated sieving and linear algebra phase is done for each of them. Gordon estimated the running-time of individual logarithm computation to be $L_p[1/3, 3^{2/3}]$. In 1998, Weber [17, §6] compared the NFS–DL algorithm to the COS algorithm for a 85 decimal digit prime and made the same observation about individual logarithm cost. In 2003, Joux and Lercier [11] were the first to dissociate relation collection plus linear algebra on one side and individual logarithm on the other side. They used the *special*-**q** technique to find the logarithm of medium-sized elements in the target decomposition. In 2006, Commeine and Semaev [7] analyzed the Joux–Lercier method. They obtained an asymptotic complexity of $L_p[1/3, 3^{1/3}]$ for computing individual logarithms, independent of the relation collection and linear algebra phases. In 2013, Barbulescu [2, §4, §7.3] gave a tight analysis of the individual logarithm computation for prime fields, decomposed in three steps: smoothness step, descent step and final combination of logarithms. The smoothness step has an asymptotic complexity of $L_p[1/3, 1.23]$ and the descent step of $L_p[1/3, 1.21]$. The final computation has a negligible cost.

In 2006, Joux, Lercier, Smart and Vercauteren [12] computed a discrete logarithm in a cubic extension of a prime field. They used the special-**q** descent technique again. They generalized the *rational reconstruction* of the target to extension fields. For discrete logarithms in prime fields, the target is an integer modulo p. The rational reconstruction method outputs two integers of half size compared to p, such that their quotient is equal to the target element modulo p. Finding a smooth

decomposition of the target modulo p becomes equivalent to finding a (simultaneous) smooth decomposition of two elements, each of half the size. We explain their method (that we call the JLSV fraction method in the following) for extension fields in Section 2.3. They used for their record in [12] another polynomial selection method (that we call the JLSV_0 method in the following), whose first polynomial has very small coefficients, and the second one has coefficients of size $O(p)$. Thanks to the very small coefficients of the first polynomial, their technique was useful. Their polynomial selection technique is now superseded by the JLSV_1 method [12, §2.3] for larger value of p and more recently, by the gJL and Conjugation methods [4]. As noted in [12, §3.2], the technique is useful in some practical cases, for small n. But for the JLSV_1 method and $n \geq 3$, this is already too slow. In 2008, Zajac [18] implemented the NFS-DL algorithm for computing discrete logarithms in $\mathbb{F}_{p^6}$ with p of 40 bits (12 decimal digits (dd), i.e. $\mathbb{F}_{p^6}$ of 240 bits or 74 dd). He used the methods described in [12], with a first polynomial of very small coefficients and a second one of coefficients in $O(p)$. In this case, individual logarithm was possible (see the well-documented [18, §8.4.5]). In 2013, Hayasaka, Aoki, Kobayashi and Takagi [10] computed a discrete logarithm in $\mathbb{F}_{p^{12}}$ with $p = 122663$. They also selected the two polynomials with the JLSV_0 method. We noted that all these records used the JLSV_0 polynomial selection method, so that one of them has very small coefficients (e.g. $f = x^3 + x^2 - 2x - 1$) whereas the second one has $O(p)$ coefficients. Despite the JLSV_1 method was the state-of-the-art for polynomial selection since 2006, it was never used in practice. JLSV_0 was used.

In 2009, Joux, Lercier, Naccache and Thomé [13] proposed an attack of discrete logarithm problem in a protocol context. The relation collection is speeded-up with queries to an oracle. They wrote in [13, §B] an extended analysis of individual logarithm computation. In their case, the individual logarithm phase of the NFS-DL algorithm has a running-time of $L_Q[1/3, c]$ where $c = 1.44$ in the large characteristic case, and $c = 1.62$ in the medium characteristic case. In 2014, Barbulescu and Pierrot [1] presented a multiple number field sieve variant (MNFS) for extension fields, based on Coppersmith's ideas [8]. The individual logarithm is studied in [1, §A]. They also used a *descent* technique, for a global estimated running time in $L_Q[1/3, (9/2)^{1/3}]$, with a constant $c \approx 1.65$. Recently in 2014, Barbulescu, Gaudry, Guillevic and Morain [3, 4] announced a 160 and a 180 decimal digit discrete logarithm record in quadratic fields. They also used a technique derived from the JLSV fraction method and a special-**q** descent technique. However their technique does not scale well for larger n.

1.3. **Our Contributions.** An integer is said to be B-smooth if all its prime divisors are less than B. An ideal in a number field is said to be B-smooth if it factors into prime ideals whose norm is bounded by B. For NFS-DL in a prime field $\mathbb{F}_p$, the norm of the target preimage in the number field is bounded by p. This bound gives the running time of the individual logarithm step. Finding a smooth decomposition of the preimage and computing the individual logarithm has complexity $L_p[1/3, 3^{1/3}]$ [7] (with $3^{1/3} \simeq 1.44$), which is smaller than the complexity of relation collection and linear algebra, which is $L_p[1/3, (64/9)^{1/3}]$ (with $c = 1.92$). For NFS-DL in $\mathbb{F}_{p^n}$, the norm bound is in fact much higher. Without any improvements in preimage computation, the individual logarithm step are in $L_Q[1/3, c]$, with $c = (9/2)^{1/3} \simeq 1.65$, $3^{1/3} \simeq 1.44$, $6^{1/3} \simeq 1.82$ respectively,for the three polynomial selection methods available (JLSV_1 [12], generalized Joux–Lercier (gJL) [16, 4], Conjugation [4]). Applying the JLSV fraction method lowers the norm bound to $O(Q)$ for the gJL and the Conjugation methods. The individual logarithm in these case has complexity $L_Q[1/3, 3^{1/3}]$ as for prime fields (without the improvements of [2, §4]). However, this method is not suited for number fields generated with the

JLSV_1 method, for $n \geq 3$. In practice, we realized that this method which seems interesting and enough because of the $O(Q)$ bound, is neither enough for gJL and Conjugation method, for n greater than 3. The preimage norm is much too large, so finding a smooth factorization is too slow by an order of magnitude. This contradicts the common idea that computing the individual logarithm of an element of norm bounded by $O(Q)$ is clearly at hand once one was able to do the relation collection and linear algebra phases.

Firstly we prove a general theorem on the running-time needed to find a smooth decomposition of the norm preimage. Note that the smoothness bound $B = L_Q[2/3, \gamma]$ here is not the same as for the relation collection step, where the smoothness bound is $B_0 = L_Q[1/3, \beta_0]$.

Theorem 1.1 (Running-time of B-smooth decomposition)**.** *Let s be an element of a number field K. Assume that the norm S of s in K is bounded by $Q^e = L_Q[1, e]$. Let $B = L_Q[\alpha_B, \gamma]$. Then the optimal bound of running time for finding a B-smooth decomposition of S is $L_Q[1/3, (3e)^{1/3}]$, obtained with $\alpha_B = 2/3$ and $\gamma = (e^2/3)^{1/3}$.*

Secondly we propose a way to lift the target from the finite field to the number field, such that the norm is strictly smaller than $O(Q)$ for the gJL and Conjugation methods:

Theorem 1.2. *Let $s \in \mathbb{F}_{p^n}^*$ a random element (not in a proper subfield of $\mathbb{F}_{p^n}$). We want to compute its discrete logarithm modulo ℓ, where $\ell \mid \Phi_n(p)$. Let K be a number field given by a polynomial selection method.*

Then there exists a preimage $\bar{r}$ in K of an $r \in \mathbb{F}_{p^n}^*$, such that $\log \rho(\bar{r}) \equiv \log s \bmod \ell$ and whose norm in K is bounded by $O(Q^e)$, where Q^e equal

1. *$Q^{1-1/n}$ for the gJL and Conjugation methods;*
2. *$Q^{\frac{3}{2}-\frac{3}{2n}}$ for the JLSV_1 method;*
3. *$Q^{1-2/n}$ for the Conjugation method, if the number field has a well-chosen quadratic subfield satisfying the conditions of Lemma 4.1;*
4. *$Q^{\frac{3}{2}-\frac{5}{2n}}$ for the JLSV_1 method, if the number field has a well-chosen quadratic subfield satisfying the conditions of Lemma 4.1.*

Our method reaches the optimal bound of $Q^{\varphi(n)/n}$, with $\varphi(n)$ the Euler totient function, for $n = 2, 3, 4, 5$ and the gJL or the Conjugation method. This provides a dramatic improvement for individual logarithm computation for small n: the running-time of the first step (the smoothing step) is $L_Q[1/3, c]$ with $c = 1.14$ for $n = 2, 4$, $c = 1.26$ for $n = 3, 6$ and $c = 1.34$ for $n = 5$. It generalizes to any n, so that $c < 1.44$ for the two state-of-the-art variants of NFS for extension fields.

1.4. **Outline.** We recall in Section 2 the three polynomial selection methods involved for NFS-DL in extension fields. We also give a commonly used bound on the norm of an element in a number field. We also present a generalization of the JLSV fraction method for the two other polynomial selection methods studied in this paper. We present our main idea in Sections 3 and 4 to reduce the norm of the preimage in the number field. We give a complexity analysis of the individual logarithm phase with our method in Section 5.

2. Preliminaries

We recall the three polynomial selection methods we will study along this paper in Section 2.1. We give a common simple upper bound on the norm of an element in an number field in Section 2.2. We will need this formula to estimate a bound on the norm target and the corresponding asymptotic running-time of individual logarithm computation.

We recall now an important property of the LLL algorithm [15]. Given a lattice of $\mathbb{Z}^n$ defined by an $n \times n$ matrix L, the LLL algorithm outputs a *short* vector of the lattice, whose coefficients are bounded by

$$C \det(L)^{1/n} ,$$

where C is the LLL constant. In the remaining of this paper, we will denote by C this LLL constant.

2.1. **Polynomial Selection Methods.** Three polynomial selection methods are competitive for the initialization step of the NFS algorithm:

(1) the Joux–Lercier–Smart–Vercauteren (JLSV_1) method [12, §2.3];
(2) the generalized Joux–Lercier (gJL) method [16, 4, §2, §3.2];
(3) the Conjugation method [4, §3.3].

The gJL method has the best asymptotic running-time in the large characteristic case, while the Conjugation method holds the best one in the medium characteristic case. However for a record computation in $\mathbb{F}_{p^2}$, the Conjugation method was used [4]. Since the use in practice of each method is not fixed, we study and compare the three methods for the individual logarithm step of NFS. We recall now the construction and properties of these three methods.

2.1.1. *Joux–Lercier–Smart–Vercauteren (JLSV_1) Method.* This method was introduced in 2006. We describe it in Algorithm 1. The two polynomials f, g have degree n and coefficient size $O(p^{1/2})$. We set $\varphi = \gcd(f, g) \bmod p$ monic of degree n. We will use φ to represent the finite field extension $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(\varphi(x))$.

Algorithm 1: Polynomial selection with the JLSV_1 method [12, §2.3]

Input: p prime and n integer
Output: f, g, φ with $f, g \in \mathbb{Z}[x]$ irreducible and $\varphi = \gcd(f \bmod p, g \bmod p)$ in $\mathbb{F}_p[x]$ irreducible of degree n

Select $f_1(x), f_0(x)$, two polynomials with small integer coefficients, $\deg f_1 < \deg f_0 = n$
repeat
  choose $y \geq \lceil \sqrt{p} \rceil$
until $f = f_0 + y f_1$ *is irreducible in* $\mathbb{F}_p[x]$
$(u, v) \leftarrow$ a rational reconstruction of y modulo p
$g \leftarrow v f_0 + u f_1$
return $(f, g, \varphi = f \bmod p)$

2.1.2. *Generalized Joux–Lercier (gJL) Method.* This method was presented in Barbulescu's PhD thesis [2, §8.3] and published in [4]. An earlier publication by Matyukhin in Russian [16, §2] presents the same method. This is a generalization of the Joux–Lercier method [11] for prime fields. We sketch this method in Algorithm 2. The coefficients of g have size $O(Q^{1/(d+1)})$ and those of f have size $O(\log p)$, with $\deg g = d \geq n$ and $\deg f = d + 1$.

2.1.3. *Conjugation Method.* This method was published in [4] and used for the discrete logarithm record in $\mathbb{F}_{p^2}$, with $f = x^4 + 1$. The coefficient size of f is in $O(\log p)$ and the coefficient size of g is in $O(p^{1/2})$. It provides the best asymptotic complexity of NFS algorithm in the medium-characteristic case. We describe it in Algorithm 3.

Algorithm 2: Polynomial selection with the generalized Joux–Lercier method (gJL) ([4, §3.2] and [16, §2])

Input: p prime, n integer and $d \geq n$ integer
Output: f, g, φ with $f, g \in \mathbb{Z}[x]$ irreducible and $\varphi = \gcd(f \bmod p, g \bmod p)$ in $\mathbb{F}_p[x]$ irreducible of degree n

1 Choose a polynomial $f(x)$ of degree $d+1$ with small integer coefficients which has a monic irreducible factor $\varphi(x) = \varphi_0 + \varphi_1 x + \cdots + x^n$ of degree n modulo p

2 Reduce the following matrix using LLL

$$M = \begin{bmatrix} p & & & & & \\ & \ddots & & & & \\ & & p & & & \\ \varphi_0 & \varphi_1 & \cdots & 1 & & \\ & \ddots & \ddots & & \ddots & \\ & & \varphi_0 & \varphi_1 & \cdots & 1 \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\\a\end{matrix}}\right\} \deg\varphi = n \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\\a\\a\end{matrix}}\right\} d+1-n \end{matrix}$$

to get

$$\mathrm{LLL}(M) = \begin{bmatrix} g_0 & g_1 & \cdots & g_d \\ & & & \\ & & * & \\ & & & \end{bmatrix}.$$

return $(f, g = g_0 + g_1 x + \cdots + g_d x^d, \varphi)$

Algorithm 3: Polynomial selection with the Conjugation method [4, §3.3]

Input: p prime and n integer
Output: f, g, φ with $f, g \in \mathbb{Z}[x]$ irreducible and $\varphi = \gcd(f \bmod p, g \bmod p)$ in $\mathbb{F}_p[x]$ irreducible of degree n

1 **repeat**
2 Select $g_1(x), g_0(x)$, two polynomials with small integer coefficients, $\deg g_1 < \deg g_0 = n$
3 Select $P_y(Y)$ a quadratic, monic, irreducible polynomial over $\mathbb{Z}$ with small coefficients
4 **until** $P_y(Y)$ *has a root* y *in* $\mathbb{F}_p$ *and* $\varphi(x) = g_0(x) + y g_1(x)$ *is irreducible in* $\mathbb{F}_p[x]$
5 $f \leftarrow \mathrm{Res}_Y(P_y(Y), g_0(x) + Y g_1(x))$
6 $(u, v) \leftarrow$ a rational reconstruction of y
7 $g \leftarrow v g_0 + u g_1$
8 **return** (f, g, φ)

2.1.4. *Comparison.* We summarize in Table 1 the polynomial selection properties of these three methods.

2.2. **Norm Upper Bound in a Number Field.** In Section 3 we will compute the norm of an element s in a number field K_f. We will need an upper bound of this norm. Let f be an irreducible polynomial over $\mathbb{Q}$ and let $K_f = \mathbb{Q}[x]/(f(x))$ a number field. Write $s \in K_f$ as a polynomial in x: $s = \sum_{i=0}^{\deg f - 1} s_i x^i$. The norm is

TABLE 1. Properties: degree and coefficient size of the three polynomial selection methods for NFS-DL in $\mathbb{F}_{p^n}$. The coefficient sizes are in $O(X)$. To lighten the notations, we simply write the X term.

method	$\deg f$	$\deg g$	$\|\|f\|\|_\infty$	$\|\|g\|\|_\infty$
JLSV_1	n	n	$Q^{1/2n}$	$Q^{1/2n}$
gJL	$d+1>n$	$d \geq n$	$O(\log p)$	$Q^{1/(d+1)}$
Conjugation	$2n$	n	$O(\log p)$	$Q^{1/2n}$

defined by a resultant computation:

$$\mathrm{N}_{K_f/\mathbb{Q}}(s) = Res(f,s) \ . \tag{1}$$

We use Kalkbrener's bound [14, Corollary 2] for an upper bound:

$$|\operatorname{Res}(f,s)| \leq \kappa(\deg f, \deg s)||f||_\infty^{\deg s}||s||_\infty^{\deg f}, \tag{2}$$

where $\kappa(n,m) = \binom{n+m}{n}\binom{n+m-1}{n}$ and $||f||_\infty = \max_{0\leq i\leq \deg f}|f_i|$ the absolute value of the greatest coefficient. An upper bound for $\kappa(n,m)$ is $(n+m)!$. We will use the following bound in Section 3:

$$\mathrm{N}_{K_f/\mathbb{Q}}(s) \leq (\deg f + \deg s)!||f||_\infty^{\deg s}||s||_\infty^{\deg f} \ . \tag{3}$$

2.3. **Joux–Lercier–Smart–Vercauteren Fraction Method.**

Notation 2.1. Row and column indices. In the following, we will define matrices of size $d\times d$, with $d \geq n$. For ease of notation, we will index the rows and columns from 0 to $d-1$ instead of 1 to d, so that the $(i+1)$-th row at index i, $L_i = [L_{ij}]_{0\leq j\leq d-1}$, can be written in polynomial form $\sum_{j=0}^{d-1} L_{ij}x^j$, and the column index j coincides with the degree j of x^j.

Computing a preimage of small norm in the number field is a major point for efficient individual logarithm. In 2006 was proposed in [12] a method to generalize to non-prime fields the rational reconstruction method used for prime fields. For discrete logarithms in prime fields, the target is an integer modulo p. The rational reconstruction method outputs two integers of half size compared to p and such that their quotient is equal to the target element modulo p. Finding a smooth decomposition of the target modulo p becomes equivalent to finding at the same time a smooth decomposition of two elements of half size each. This is actually much faster, see [2, §4].

A generalization to extension fields is to write the target preimage as a quotient of two number field elements, each with norm of half size of the original preimage. For explaining that, we introduce some notation. We denote by s the target in the finite field $\mathbb{F}_{p^n}$ of degree n and by $\bar{s}$ a preimage (or lift) in the number field K defined by a polynomial f. Here is a first very simple preimage choice. Let $s = \sum_{i=0}^{\deg s} s_i x^i \in \mathbb{F}_{p^n}$, with $\deg s < n$ and the finite field extension defined with the polynomial φ as $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(\varphi(x))$. We lift the coefficients $s_i \in \mathbb{F}_p$ to $\bar{s}_i \in \mathbb{Z}$ then we set a preimage of s in the number field K to be

$$\bar{s} = \sum_{i=0}^{\deg s} \bar{s}_i X^i \ ,$$

with X such that $K = \mathbb{Q}[X]/(f(X))$. (We can also write $\bar{s} = \sum_{i=0}^{\deg s} \bar{s}_i \alpha^i$, with α a root of f in the number field: $K = \mathbb{Q}[\alpha]$).

Now LLL is used to obtain a quotient whose numerator and denominator have smaller coefficients. We present here the lattice used with the JLSV_1 polynomial selection method. The number field K is of degree n. We define a lattice of dimension $2n$. For the corresponding matrix, each column corresponds to a power of X; the first n columns to positive powers $1, X, X^2, \ldots, X^{n-1}$, the last n to negative powers $1^{-1}, X^{-1}, X^{-2}, \ldots, X^{-(n-1)}$.

The matrix is

$$L = \begin{array}{c} \begin{array}{cccccccc} 0 & & \ldots & n-1 & n & & \ldots & 2n-1 \end{array} \\ \begin{bmatrix} p & & & & & & & \\ & \ddots & & & & & & \\ & & & p & & & & \\ \bar{s}_0 & \ldots & & \bar{s}_{n-1} & 1 & & & \\ \vdots & & & \vdots & & & \ddots & \\ \bar{s}x^{n-1} \bmod \varphi & & & & & & & 1 \end{bmatrix} \begin{array}{c} 0 \\ \vdots \\ n-1 \\ n \\ \vdots \\ 2n-1 \end{array} \\ 2n \times 2n \end{array}$$

The first n coefficients of the output vector, $u_0, u_1, \ldots, u_{n-1}$ give a numerator u and the last n coefficients give a denominator v, so that $\bar{s} = a\frac{u(X)}{v(X)}$ with a a scalar in $\mathbb{Q}$. The coefficients u_i, v_i are bounded by

$$||u||_\infty,\ ||v||_\infty \leq Cp^{1/2}$$

since the matrix determinant is $\det L = p^n$ and the matrix is of size $2n \times 2n$. However the product of the norms of each u, v in the number field K will be much larger than the norm of the single element $\bar{s}$ because of the large coefficients of f in the norm formula. We use formula (3) to estimate this bound:

$$\mathrm{N}_{K/\mathbb{Q}}(u) \leq ||u||_\infty^{\deg f} ||f||_\infty^{\deg u} = O(p^{\frac{n}{2}} p^{\frac{n-1}{2}}) = O(p^{n-\frac{1}{2}}) = O(Q^{1-\frac{1}{2n}})$$

and the same for $\mathrm{N}_{K/\mathbb{Q}}(v)$, hence the product of the two norms is bounded by $O(Q^{2-\frac{1}{n}})$. The norm of $\bar{s}$ is bounded by $\mathrm{N}_{K/\mathbb{Q}}(\bar{s}) \leq p^n p^{\frac{n-1}{2}} = Q^{\frac{3}{2}-\frac{1}{2n}}$ which is much smaller whenever $n \geq 3$. Finding a smooth decomposition of u and v at the same time will be much slower than finding one for $\bar{s}$ directly, for large p and $n \geq 3$. This is mainly because of the large coefficients of f (in $O(p^{1/2})$).

2.3.1. *Application to gJL and Conjugation Method.* The method of [12] to improve the smoothness of the target norm in the number field K_f has an advantage for the gJL and Conjugation methods. First we note that the number field degree is larger than n: this is $d+1 \geq n+1$ for the gJL method and $2n$ for the Conjugation method. For ease of notation, we denote by d_f the degree of f. We define a lattice of dimension $2d_f$. Hence there is more place to reduce the coefficient size of the target $\bar{s}$.

We put p on the diagonal of the first $n-1$ rows, then $x^i\varphi(x)$ coefficients from row n to $d_f - 1$, where $0 \leqslant i < d_f - 1$ (φ is of degree n and has $n+1$ coefficients). The rows from indexd_f to $2d_f$ are filled with $X^i\bar{s} \bmod f$ (these elements have d_f

coefficients). We obtain a triangular matrix L.

$$L = \begin{bmatrix} p & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & p & & & & & & & & \\ \varphi_0 & \cdots & \varphi_{n-1} & 1 & & & & & & & \\ & \ddots & & \ddots & \ddots & & & & & & \\ & & \varphi_0 & \cdots & \varphi_{n-1} & 1 & & & & & \\ \bar{s}_0 & \ldots & \bar{s}_{n-1} & & & & 1 & & & & \\ \vdots & X^i\bar{s} \bmod f & & & & & & \ddots & & & \\ \vdots & & & & & & & & \ddots & & \\ X^{d_f-1}\bar{s} \bmod f & & & & & & & & & 1 & \end{bmatrix} \begin{matrix} 0 \\ \vdots \\ n-1 \\ n \\ \vdots \\ d_f-1 \\ d_f \\ \vdots \\ \vdots \\ 2d_f \end{matrix}$$
$$2d_f \times 2d_f$$

Since the determinant is $\det L = p^n$ and the matrix of dimension $2d_f \times 2d_f$, the coefficients obtained with LLL will be bounded by $Cp^{\frac{n}{2d_f}}$. The norm of the numerator or the denominator (with $\bar{s} = u(X)/v(X) \in K_f$) is bounded by

$$\mathrm{N}_{K_f/\mathbb{Q}}(u) \leq ||u||_\infty^{\deg f} ||f||_\infty^{\deg u} = O(p^{n/2}) = O(Q^{1/2}) \ .$$

The product of the two norms will be bounded by $O(Q)$ hence we will have the same asymptotic running time as for prime fields, for finding a smooth decomposition of the target in a number field obtained with the gJL or Conjugation method. We will show in Section 3 that we can do even better.

3. Computing a Preimage in the Number Field

Our main idea is to compute a preimage in the number field with smaller degree (less than $\deg s$) and/or of coefficients of reduced size, by using the subfield structure of $\mathbb{F}_{p^n}$. Note that we at least have one non-trivial subfield: $\mathbb{F}_p$.

Lemma 3.1. *Let $s \in \mathbb{F}_{p^n}^* = \sum_{i=0}^{\deg s} s_i x^i$, with $\deg s < n$. Let ℓ be a non-trivial divisor of $\Phi_n(p)$. Let $s' = u \cdot s$ with u in a proper subfield of $\mathbb{F}_{p^n}$. Then*

$$\log s' \equiv \log s \bmod \ell \ . \tag{4}$$

Proof. We start with $\log s' = \log s + \log u$ and since u is in a proper subfield, we have $u^{(p^n-1)/\Phi_n(p)} = 1$, then $u^{(p^n-1)/\ell} = 1$. Hence the logarithm of u modulo ℓ is zero, and $\log s' \equiv \log s \bmod \ell$. □ □

Example 3.2 (Monic preimage)**.** Let s' be equal to s divided by its leading term, $s' = \frac{1}{s_{\deg s}} s \in \mathbb{F}_{p^n}$. We have $\log s' \equiv \log s \bmod \ell$.

We assume in the following that the target s is monic since dividing by its leading term does not change its logarithm modulo ℓ.

3.1. Preimage Computation in the JLSV$_1$ Case.

Let $s = \sum_{i=0}^{n-1} s_i x^i \in \mathbb{F}_{p^n}$ with $s_{n-1} = 1$. We define a lattice of dimension n by the $n \times n$ matrix

$$L = \begin{bmatrix} p & & & \\ & \ddots & & \\ & & p & \\ \bar{s}_0 & \ldots & \bar{s}_{n-2} & 1 \end{bmatrix} \begin{matrix} 0 \\ \vdots \\ n-2 \\ n-1 \end{matrix} \begin{matrix} \Big\} \\ \Big\} \\ \Big\} \end{matrix} \begin{matrix} n-1 \text{ rows} \\ \\ \text{row } n-1 \text{ with } \bar{s} \text{ coeffs} \end{matrix}$$
$$n \times n$$

with p on the diagonal for the first $n-1$ rows (from 0 to $n-2$), and the coefficients of the monic element $\bar{s}$ on row $n-1$. Applying the LLL algorithm to M, we obtain a reduced element $\bar{r} = \sum_{i=0}^{n-1} \bar{r}_i X^i \in K_f$ such that

$$\bar{r} = \sum_{i=0}^{n-1} a_i L_i$$

with L_i the vector defined by the i-th row of the matrix and a_i a scalar in $\mathbb{Z}$. We map this equality in $\mathbb{F}_{p^n}$ with ρ. All the terms cancel out modulo p except the line with $\bar{s}$:

$$\rho(\bar{r}) \equiv \rho(a_{n-1}) \cdot \rho(\bar{s}) = u \cdot s \mod (p, \varphi)$$

with $u = \rho(a_{n-1}) \in \mathbb{F}_p$. Hence, by Lemma 3.1,

$$\log \rho(\bar{r}) \equiv \log s \bmod \ell \ . \tag{5}$$

Moreover,

$$||\bar{r}||_\infty \leq C p^{(n-1)/n} \ .$$

It is straightforward, using Inequality (3), to deduce that

$$\mathrm{N}_{K_f/\mathbb{Q}}(\bar{r}) = O\big(p^{\frac{3}{2}(n-1)}\big) = O\big(Q^{\frac{3}{2}-\frac{3}{2n}}\big) \ .$$

We note that this first simple improvement applied to the JLSV_1 construction is already better than doing nothing: in that case, $\mathrm{N}_{K_f/\mathbb{Q}}(s) = O(Q^{\frac{3}{2}-\frac{1}{2n}})$. The norm of $\bar{r}$ is smaller by a factor of size $Q^{\frac{1}{n}}$. For $n = 2$ we have $\mathrm{N}_{K_f/\mathbb{Q}}(\bar{r}) = O(Q^{\frac{3}{4}})$ and for $n = 3$, the bound is $\mathrm{N}_{K_f/\mathbb{Q}}(\bar{r}) = O(Q)$. We would like to obtain such a bound, smaller than $O(Q)$, for larger n.

3.2. **Preimage Computation in the gJL and Conjugation Cases.** Let $s = \sum_{i=0}^{n-1} s_i x^i \in \mathbb{F}_{p^n}$ with $s_{n-1} = 1$. In order to present a generic method for both the gJL and the Conjugation methods, we denote by d_f the degree of f. In the gJL case we have $d_f = d + 1 \geq n + 1$, while in the Conjugation case, $d_f = 2n$. We define the $d_f \times d_f$ matrix with p on the diagonal for the first $n-1$ rows, and the coefficients of the monic element $\bar{s}$ on row $n-1$. The rows n to d_f are filled with the coefficients of the monic polynomial $x^j \varphi$, with $0 \leq j \leq d_f - n$.

$$L = \begin{bmatrix} p & & & & & & & \\ & \ddots & & & & & & \\ & & p & & & & & \\ \bar{s}_0 & \dots & \bar{s}_{n-2} & 1 & & & & \\ \varphi_0 & \varphi_1 & \cdots & \varphi_{n-1} & 1 & & & \\ & \ddots & \ddots & & \ddots & \ddots & & \\ & & \varphi_0 & \varphi_1 & \cdots & \varphi_{n-1} & 1 & \\ \end{bmatrix}_{d_f \times d_f} \begin{matrix} 0 \\ \vdots \\ n-2 \\ n-1 \\ n \\ \vdots \\ d_f - 1 \end{matrix} \begin{matrix} \Big\} \ n-1 \text{ rows} \\ \\ \} \text{row } n-1 \text{ with } \bar{s} \text{ coeffs} \\ \Big\} \ d_f - n \text{ rows with } \varphi \text{ coeffs} \end{matrix}$$

Applying the LLL algorithm to L, we obtain a reduced element $\bar{r} = \sum_{i=0}^{d_f-1} \bar{r}_i X^i \in K_f$ such that $\bar{r} = \sum_{i=0}^{d_f-1} a_i L_i$ where L_i is the i-th row vector of L and a_i is a scalar in $\mathbb{Z}$. We map this equality into $\mathbb{F}_{p^n}$ with ρ. All the terms cancel out modulo (p, φ) except the one with $\bar{s}$ coefficients:

$$\rho(\bar{r}) \equiv \rho(a_{n-1}) \cdot \rho(\bar{s}) = u \cdot s \mod (p, \varphi)$$

with $u = \rho(a_{n-1}) \in \mathbb{F}_p$. Hence, by Lemma 3.1,

$$\log \rho(\bar{r}) \equiv \log s \bmod \ell \ . \tag{6}$$

Moreover,

$$||\bar{r}||_\infty \leq C p^{(n-1)/d_f} \ .$$

It is straightforward, using Inequality (3), to deduce that

$$\mathrm{N}_{K_f/\mathbb{Q}}(\bar{r}) = O\big(p^{n-1}\big) = O\big(Q^{1-1/n}\big) \ .$$

Here we obtain a bound that is *always strictly smaller* than Q for any n. In the next section we show how to improve this bound to $O\big(Q^{1-2/n}\big)$ when n is even and the number field defined by φ has a well-suited quadratic subfield.

4. Preimages of Smaller Norm with Quadratic Subfields

Reducing the degree of s can reduce the norm size in the number field for the JLSV_1 polynomial construction. We present a way to do this when n is even and the finite field $\mathbb{F}_{p^n}$ can be expressed as a degree-$n/2$ extension of a quadratic extension defined by a polynomial of a certain form. We will use this to reduce the degree for the number fields in the JLSV_1 method and to reduce the coefficient size of the preimage in all three cases.

4.1. Smaller Preimage Degree.

In this section, we prove that when n is even and $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/(\varphi(x))$ has a quadratic base field $\mathbb{F}_{p^2}$ of a certain form, from a random element $s \in \mathbb{F}_{p^n}$ with $s_{n-1} \neq 0$, we can compute an element $r \in \mathbb{F}_{p^n}$ with $r_{n-1} = 0$, and $s = u \cdot r$ with $u \in \mathbb{F}_{p^2}$. Then, using Lemma 3.1, we will conclude that $\log r \equiv \log s \bmod \ell$.

Lemma 4.1. *Let $\varphi(X)$ be a monic irreducible polynomial of $\mathbb{F}_p[X]$ of even degree n with a quadratic subfield defined by the polynomial $P_y = Y^2 + y_1 Y + y_0$. Moreover, assume that φ splits over $\mathbb{F}_{p^2} = \mathbb{F}_p[Y]/(P_y(Y))$ as*

$$\begin{aligned} & \varphi(X) = (P_z(X) - Y)(P_z(X) - Y^p) \\ \text{or} \quad & \varphi(X) = (P_z(X) - YX)(P_z(X) - Y^pX) \end{aligned}$$

with P_z monic, of degree $n/2$ and coefficients in $\mathbb{F}_p$. Let $s \in \mathbb{F}_p[X]/(\varphi(X))$ a random element, $s = \sum_{i=0}^{n-1} s_i X^i$.

Then there exists an $r \in \mathbb{F}_{p^n}$ monic and of degree $n-2$ in X, and $u \in \mathbb{F}_{p^2}$, such that $s = u \cdot r$ in $\mathbb{F}_{p^n}$.

We first give an example for $s \in \mathbb{F}_{p^4}$ then present a constructive proof.

Example 4.2. Let $P_y = Y^2 + y_1 Y + y_0$ be a monic irreducible polynomial over $\mathbb{F}_p$ and set $\mathbb{F}_{p^2} = \mathbb{F}_p[Y]/(P_y(Y))$. Assume that $Z^2 - YZ + 1$ is irreducible over $\mathbb{F}_{p^2}$ and set $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}[Z]/(Z^2 - YZ + 1)$. Let $\varphi = X^4 + y_1X^3 + (y_0+2)X^2 + y_1X + 1$ be a monic reciprocal polynomial. By construction, φ factors over $\mathbb{F}_{p^2}$ into $(X^2 - YX + 1)(X^2 - Y^pX + 1)$ and $\mathbb{F}_p[X]/(\varphi(X))$ defines a quartic extension $\mathbb{F}_{p^4}$ of $\mathbb{F}_p$. We have these two representations for $\mathbb{F}_{p^4}$:

$$\begin{array}{ccc} \mathbb{F}_{p^4} & = & \mathbb{F}_{p^2}[Z]/(Z^2 - YZ + 1) \\ | & & \\ \mathbb{F}_{p^2} & = & \mathbb{F}_p[Y]/(Y^2 + y_1Y + y_0) \\ | & & \\ \mathbb{F}_p & & \end{array}$$

and

$$\begin{array}{ccc} \mathbb{F}_{p^4} & = & \mathbb{F}_p[X]/(X^4 + y_1X^3 + (y_0+2)X^2 + y_1X + 1) \\ | & & \\ \mathbb{F}_p & & \end{array}$$

of Lemma 4.1. Two possible extension field towers are:

$$\begin{array}{l}\mathbb{F}_{p^n} = \mathbb{F}_{p^2}[Z]/(P_z(Z) - Y) \\ | \\ \mathbb{F}_{p^2} = \mathbb{F}_p[Y]/(P_y(Y)) \\ | \\ \mathbb{F}_p\end{array} \quad \text{and} \quad \begin{array}{l}\mathbb{F}_{p^n} = \mathbb{F}_{p^2}[Z]/(P_z(Z) - YZ) \\ | \\ \mathbb{F}_{p^2} = \mathbb{F}_p[Y]/(P_y(Y)) \\ | \\ \mathbb{F}_p\end{array}$$

We write s in the following representation to emphasize the subfield structure:

$$s = \sum_{i=0}^{n/2-1} (a_{i0} + a_{i1}Y)Z^i \text{ with } a_{ij} \in \mathbb{F}_p \ .$$

(1) If $\varphi = P_z(Z) - Y$ then we can divide s by $u_{LT} = a_{n/2,0} + a_{n/2,1}Y \in \mathbb{F}_{p^2}$ (the leading term in Z, i.e. the coefficient of $Z^{n/2}$) to make s monic in Z up to a subfield cofactor u_{LT}:

$$\frac{s}{u_{LT}} = \sum_{i=0}^{n/2-2} (b_{i0} + b_{i1}Y)Z^i \ + Z^{n/2-1} \ ,$$

with the coefficients b_{ij} in the base field $\mathbb{F}_p$, $b_{i0} + b_{i1}Y = (a_{i0} + a_{i1}Y)/u_{LT}$. Since $P_z(Z) = Y$ and $Z = X$ in $\mathbb{F}_{p^n}$ by construction, we replace Y by $P_z(Z)$ and Z by X to get an expression for s in X:

$$\frac{s}{u_{LT}} = \sum_{i=0}^{n/2-2} (b_{i0} + b_{i1}P_z(X))X^i + X^{n/2-1} = r(X) \ .$$

The degree in X of r is $\deg r = \deg P_z(X)X^{n/2-2} = n - 2$ instead of $\deg s = n - 1$. We set $u = 1/u_{LT}$. By construction, $u \in \mathbb{F}_{p^2}$. We conclude that $s = ur \in \mathbb{F}_{p^n}$, with $\deg r = n - 2$ and $u \in \mathbb{F}_{p^2}$.

(2) If $\varphi = P_z(Z) - YZ$ then we can divide s by $u_{CT} = a_{00} + a_{01}Y \in \mathbb{F}_{p^2}$ (the constant term in Z) to make the constant coefficient of s to be 1:

$$\frac{s}{u_{CT}} = 1 + \sum_{i=1}^{n/2-1} (b_{i0} + b_{i1}Y)X^i$$

with $b_{ij} \in \mathbb{F}_p$. Since $P_z(Z) = YZ$ and $Z = X$ in $\mathbb{F}_{p^n}$ by construction, we replace YZ by $P_z(Z)$ and Z by X to get

$$\frac{s}{u_{CT}} = 1 + \sum_{i=1}^{n/2-1} (b_{i0}X^i + b_{i1}P_z(X)X^{i-1}) = r(X) \ .$$

The degree in X of r is $\deg r = \deg P_z(X)X^{n/2-1-1} = n - 2$ instead of $\deg s = n - 1$. We set $u = 1/u_{CT}$. By construction, $u \in \mathbb{F}_{p^2}$. We conclude that $s = ur \in \mathbb{F}_{p^n}$, with $\deg r = n - 2$ and $u \in \mathbb{F}_{p^2}$.

□ □

Now we apply the technique described in Section 3.1 to reduce the coefficient size of r in the JLSV$_1$ construction. We have $r_{n-1} = 0$ and we assume that $r_{n-2} = 1$. We define the lattice by the $(n-1) \times (n-1)$ matrix

$$L = \begin{bmatrix} p & & & \\ & \ddots & & \\ & & p & \\ \bar{r}_0 & \dots & \bar{r}_{n-3} & 1 \end{bmatrix} \begin{matrix} 0 \\ \vdots \\ n-3 \\ n-2 \\ n-1 \times n-1 \end{matrix} \begin{matrix} \Big\} \ n-2 \text{ rows} \\ \\ \\ \} \text{row } n-2 \text{ with } \bar{r} \text{ coeffs} \end{matrix}$$

After reducing the lattice with LLL, we obtain an element $\overline{rr}$ whose coefficients are bounded by $Cp^{\frac{n-2}{n-1}}$. The norm of $\overline{rr}$ in the number field K_f constructed with the JLSV$_1$ method is

$$\mathrm{N}_{K_f/\mathbb{Q}}(\overline{rr}) = O(p^{\frac{3}{2}n-2-\frac{1}{n-1}}) = O(Q^{\frac{3}{2}-\frac{2}{n}-\frac{1}{n(n-1)}}) \ .$$

This is better than the previous $O\big(Q^{\frac{3}{2}-\frac{3}{2n}}\big)$ case: the norm is smaller by a factor of size $O\big(Q^{\frac{1}{2}n+\frac{1}{n(n-1)}}\big)$. For $n=4$, we obtain $\mathrm{N}_{K_f/\mathbb{Q}}(\overline{rr}) = O\big(Q^{\frac{11}{12}}\big)$, which is strictly less than $O(Q)$.

We can do even better by re-using the element $\bar{r}$ of degree $n-2$ and the given one s of degree $n-1$, and combining them.

4.2. **Smaller Preimage Norm.** First, suppose that the target element $s = \sum_{i=0}^{n-1} s_i x^i$ satisfies $s_{n-1} = 0$ and $s_{n-2} = 1$. After what we have seen above, it is tempting to simply define the n-dimensional lattice

$$L = \begin{bmatrix} p & & & & \\ & \ddots & & & \\ & & p & & \\ \bar{s}_0 & \dots & \bar{s}_{n-3} & 1 & \\ & \bar{s}_0 & \dots & \bar{s}_{n-3} & 1 \end{bmatrix}_{n-1\times n-1} \begin{matrix} 0 \\ \vdots \\ n-3 \\ n-2 \\ n-1 \end{matrix} \begin{matrix} \Big\} \\ \\ \\ \} \text{ row } n-2 \text{ with } \bar{s} \text{ coeffs} \\ \} \text{ row } n-1 \text{ with } x\bar{s} \text{ coeffs} \end{matrix} \ n-2 \text{ rows}$$

After LLL reduction, we obtain an element $\bar{r} = \sum_{i=0}^{n-1} a_i L_i$. We map this equality to $\mathbb{F}_{p^n}$ and get

$$\rho(\bar{r}) = (a_{n-2} + a_{n-1}x)s \ .$$

But there is no reason for $(a_{n-2} + a_{n-1}x)$ to be in a proper subfield of $\mathbb{F}_{p^n}$ so we cannot apply Lemma 3.1 to this equation.

Note that we still can define the lattice

$$L = \begin{bmatrix} p & & & & \\ & \ddots & & & \\ & & p & & \\ \bar{s}_0 & \dots & \bar{s}_{n-3} & 1 & \\ 0 & \dots & \dots & 0 & p \end{bmatrix}_{n-1\times n-1} \begin{matrix} 0 \\ \vdots \\ n-3 \\ n-2 \\ n-1 \end{matrix} \begin{matrix} \Big\} \\ \\ \\ \} \text{ row } n-2 \text{ with } \bar{s} \text{ coeffs} \\ \} \text{ row } n-1 \text{ with } p \end{matrix} \ n-2 \text{ rows}$$

but this is a straightforward generalization of Section 3.1 for s of any degree and the norm bound is the same.

The observation we made is that we can define a lattice whose vectors, once mapped to $\mathbb{F}_{p^n}$, are either 0 (so vectors are sums of multiples of p and φ) or are multiples of the initial target s, satisfying Lemma 3.1. The above r of degree $n-2$ is a good candidate. The initial s also. If there is no initial s of degree $n-1$, then simply take at random any u in a proper subfield of $\mathbb{F}_{p^n}$ which is not $\mathbb{F}_p$ itself and set $s = u \cdot r$. Then s will have $s_{n-1} \neq 0$. Then define the lattice

$$L = \begin{bmatrix} p & & & & \\ & \ddots & & & \\ & & p & & \\ \bar{r}_0 & \dots & \bar{r}_{n-3} & 1 & \\ \bar{s}_0 & \dots & \bar{s}_{n-3} & \bar{s}_{n-2} & 1 \end{bmatrix}_{n\times n} \begin{matrix} 0 \\ \vdots \\ n-3 \\ n-2 \\ n-1 \end{matrix} \begin{matrix} \Big\} \\ \\ \\ \} \text{ row } n-2 \text{ with } \bar{r} \text{ coeffs} \\ \} \text{ row } n-1 \text{ with } \bar{s} \text{ coeffs} \end{matrix} \ n-2 \text{ rows}$$

and use it in place of the lattices of Section 3.1 or 3.2. We summarize the coefficient and norm bounds in Table 2. For ease of reading, we omit the $O(\cdot)$ notation.

4.3. **Examples for Small n and p of 180 Decimal Digits (dd).**

TABLE 2. Norm bound of the reduced element $\overline{rr}$ in the number field K when φ satisfies the conditions of Lemma 4.1.

method	$\|\|\overline{rr}\|\|_\infty$	$\mathrm{N}_{K_f/\mathbb{Q}}(\overline{rr})$
JLSV_1	$p^{\frac{n-2}{n}}$	$Q^{\frac{3}{2}-\frac{5}{2n}}$
gJL	$p^{\frac{n-2}{d+1}}$	$Q^{1-\frac{2}{n}}$
Conjugation	$p^{\frac{n-2}{2n}}$	$Q^{1-\frac{2}{n}}$

4.3.1. *Example for $n = 2$, Conjugation Method.* We take the parameters of the record in [4]: p is a 90 decimal digit (300 bit) prime number, and f, φ are computed with the Conjugation method. We choose a target s from the decimal digits of exp(1).

$$\begin{aligned} p &= 314159265358979323846264338327950288419716939937510582097494459230781640628620899877709223 \\ f &= x^4 + 1 \\ \varphi &= x^2 + 1077815130958230186669898831022443948094122976438953490974106325080494553766987846916995 93x + 1 \\ s &= 271828182845904523536028747135319858432320810108854154561922818073323375769498574988743 14x \\ &\quad + 958880662507673263211420165757531990227722354115265486848084409739492084711947246810906 92 \end{aligned}$$

We first compute $s' = \frac{1}{s_0}s$ then reduce

$$L = \begin{bmatrix} p & 0 & 0 & 0 \\ s'_0 & 1 & 0 & 0 \\ 1 & \varphi_1 & 1 & 0 \\ 0 & 1 & \varphi_1 & 1 \end{bmatrix}$$

then $\mathrm{LLL}(L)$ produces $\bar{r}$ of degree 3 and coefficient size $O(p^{1/4})$. Actually LLL outputs four short vectors, hence we get four small candidates for $\bar{r}$, each of norm $\mathrm{N}_{K_f/\mathbb{Q}}(\bar{r}) = O(p) = O(Q^{1/2}) = O(Q^{\varphi(n)/n})$, i.e. 90 dd. To slightly improve the smoothness search time, we can compute linear combinations of these four reduced preimages.

$$\begin{aligned} &360339728645720582847 1x^3 + 136790355536430097110 78x^2 + 557746247085194895659 4x + 856176942703613067714 \\ &921946132448219081489 3x^3 - 449817579633385492601 3x^2 + 895775002549467382219 8x + 111788824169113006040 9 \\ &282683909446241831417 02x^3 + 569966674122622538525 9x^2 - 178019404032168663329 11x + 544843224771048269684 8 \\ &335216279294146314006 0x^3 + 321258501223569290228 7x^2 - 557063651808475912551 3x + 469265082905446625423 27 \end{aligned}$$

The norm of the first element is

$$\mathrm{N}_{K_f/\mathbb{Q}}(\bar{r}) = 213988280295201686111690452803024284348669666570970757613375980707604853409486778001629 21$$

of 90 decimal digits, as expected.

4.3.2. *Example for $n = 3$, gJL Method.* We take p of 60 dd (200 bits) so that $\mathbb{F}_{p^3}$ has size 180 dd (600 bits) as above. We took p a prime made of the 60 first decimal digits of π. We constructed f, φ, g with the gJL method described in [4].

$$\begin{aligned} p &= 314159265358979323846264338327950288419716939937510582723487 \\ f &= x^4 - x + 1 \\ \varphi &= x^3 + 227138144243642333129902287795664772043667053260089299478579 x^2 \\ &\quad + 126798022201426805402186761110440110121157863791585328913565 x \\ &\quad + 863983091574414435397918995177883881848539630718471155526 38 \\ g &= 287767088987135456608033317246385224990821439 1x^3 + 609951652432557506082184162014047061886340388 1x^2 \\ &\quad - 101235332348344733160532896231657564372672984 03x + 202907337179191496597604128420820845026712055 6 \\ s &= 271828182845904523536028747135319858432320810108854154561922x^2 \\ &\quad + 281807332337576949857498874314095888066250767326321142016575x \\ &\quad + 753199022772235411526548684808589516264937392972591398598 75 \end{aligned}$$

We set $s' = \frac{1}{s_2}s$. The lattice to be reduced is

$$L = \begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ s'_0 & s'_1 & 1 & 0 \\ \varphi_0 & \varphi_1 & \varphi_2 & 1 \end{bmatrix}$$

then LLL(L) computes four short vectors $\bar{r}$ of degree 3, of coefficient size $O(p^{1/2})$, and of norm size $\mathrm{N}_{K_f/\mathbb{Q}}(\bar{r}) = O(p^2) = O(Q^{2/3}) = O(Q^{\varphi(n)/n})$.

$$\begin{aligned}
&159774930637505900093909307018x^3 + 165819631832105094449987774814x^2 + 177828199322419553601266354904x - 159912786936943488400590389195 \\
&136583029354520905232412941048x^3 - 521269847225531188433352927453x^2 + 322722415562853671586868492721x + 255238068915917937217884608875 \\
&118289007598934068726663000266x^3 + 499013489972894059858543976363x^2 - 105084220861844155797015713666x + 535978811382585906107397024241 \\
&411603890054539500131474313773x^3 - 240161030577722451131067159670x^2 - 373289346204280810310169575030x - 389720783049275894296185820094
\end{aligned}$$

The norm of the first element is

$$\mathrm{N}_{K_f/\mathbb{Q}}(\bar{r}) = 997840136509677868374734441582077227769466501519927620849763845265357390584602475858356409809239812991892769866071779$$

of 117 decimal digits (note that $\frac{2}{3}180 = 120$ dd).

4.3.3. *Example for $n = 4$, $JLSV_1$ Method.*

$$\begin{aligned}
p &= 3141592653589793238462643383279502884199800 11 \\
\ell &= 4934802200544679309417245499938075567665114324793283480273169881952175564988477281978006 1 \\
f = \varphi &= x^4 + x^3 + 7089815403622064109316 2x^2 + x + 1 \\
g &= 1019160964270671715678 72x^4 + 1019160964270671715678 72x^3 + 2208063288740498985510 11x^2 \\
&\quad + 1019160964270671715678 72x + 1019160964270671715678 72 \\
s &= 2718281828459045235360287471353198584323208 10x^3 + 1088541545619222818073323375769498574988743 14x^2 \\
&\quad + 9588806625076732632114201657575319902277223 5x + 4115265486848084409739492084712758839195201 8
\end{aligned}$$

We set $s' = \frac{1}{s_3}s$. The subfield simplification for s gives

$$r = x^2 + 1349691223972631029797432269152823554001619 11x + 1046424406499377563685457653347410492071210 11 \ .$$

We reduce the lattice defined by

$$L = \begin{bmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ r_0 & r_1 & 1 & 0 \\ s'_0 & s'_1 & s'_2 & 1 \end{bmatrix}$$

then LLL(L) produces these four short vectors of degree 3, coefficient size $O(p^{1/2})$, and norm $\mathrm{N}_{K_f/\mathbb{Q}}(\overline{rr}) = O(p^{\frac{7}{2}}) = O(Q^{7/8})$ (smaller than $O(Q)$).

$$\begin{aligned}
&58429619971492637519 46x^3 + 2907368273308610113 76x^2 - 5618779793817086743792x + 1092494800287557029045 \\
&16408426439031611753 59x^3 + 1555259026913188958957 5x^2 - 4425488394163838271378x - 5734086421794811858814 \\
&64506869065045253748 53x^3 + 1376877124265095739941 9x^2 + 1061758394423409088057 9x + 1626161707916779758091 2 \\
&16929135804139878865391x^3 + 6981855717048102583 44x^2 + 1279930041101224611407 9x - 2278728269871806528415 7
\end{aligned}$$

The norm of the first element is

$$\begin{aligned}
\mathrm{N}_{K_f/\mathbb{Q}}(\overline{rr}) = \ & 1452143929217271115166861110413357998278729994931024260194421897764500704952 7 \backslash \\
& 0123656021783074136945302749067576757516984664647990043605467452102146421782 85
\end{aligned}$$

of 155 decimal digits (with $\frac{7}{8}180 = 157.5$).

5. Asymptotic Complexities

In this section, we prove Theorem 1.1. First, we need a result on smoothness probability. We recall the definition of B-smoothness already stated in Section 1.3: An integer S is B-smooth if and only if all its prime divisors are less than or equal to B. We also recall that the L-notation widely used for sub-exponential asymptotic complexities:

$$L_Q[\alpha, c] = \exp\Big(\big(c + o(1)\big)(\log Q)^{\alpha}(\log\log Q)^{1-\alpha}\Big) \quad \text{with } \alpha \in [0,1] \text{ and } c > 0 \ .$$

The Canfield–Erdős–Pomerance [6] theorem provides a useful result to measure smoothness probability:

Theorem 5.1 (B-smoothness probability)**.** *For an integer S bounded by $L_Q[\alpha_S, \sigma]$ and a smoothness bound $B = L_Q[\alpha_B, \beta]$, the probability that S is B-smooth is*

$$\Pr(S \textit{ is } B\textit{-smooth}) = L_Q\left[\alpha_S - \alpha_B, -(\alpha_S - \alpha_B)\frac{\sigma}{\beta}\right] \ . \tag{7}$$

We prove now the Theorem 1.1 that states the running-time of individual logarithm when the norm of the target in a number field is bounded by $O(Q^e)$.

of Theorem 1.1. From Theorem 5.1, the probability that S bounded by $Q^e = L_Q[1, e]$ is B-smooth with $B = L_Q[\alpha_B, \gamma]$ is $\Pr(S \text{ is } B\text{-smooth}) = L_Q\big[1-\alpha_B, -(1-\alpha_B)\frac{e}{\gamma}\big]$. We assume that a B-smoothness test with ECM takes time $L_B[1/2, 2^{1/2}] = L_Q[\frac{\alpha_B}{2}, (2\gamma\alpha_B)^{1/2}]$. The running-time for finding a B-smooth decomposition of S is the ratio of the time per test (ECM cost) to the B-smoothness probability of S:

$$L_Q\Big[\frac{\alpha_B}{2}, (2\gamma\alpha_B)^{1/2}\Big] L_Q\Big[1-\alpha_B, (1-\alpha_B)\frac{e}{\gamma}\Big] \ .$$

We optimize first the α value, so that $\alpha \leq 1/3$ (that is, not exceeding the α of the two previous steps of the NFS algorithm):

$$\max(\alpha_B/2, 1-\alpha_B) \leq \frac{1}{3} \ .$$

This gives the system

$$\begin{cases} \alpha_B \leq 2/3 \\ \alpha_B \geq 2/3 \end{cases}$$

So we conclude that

$$\alpha_B = \frac{2}{3} \ . \tag{8}$$

The running-time for finding a B-smooth decomposition of S is therefore

$$L_Q\Big[1/3, \Big(\frac{4}{3}\gamma\Big)^{1/2} + \frac{e}{3\gamma}\Big] \ . \tag{9}$$

The minimum of the function $(\frac{4}{3}\gamma)^{1/2} + \frac{e}{3\gamma}$ is $(3e)^{1/3}$, corresponding to $\gamma = (e^2/3)^{1/3}$, which yields our optimal running time:

$$L_Q\Big[1/3, (3e)^{1/3}\Big] \ .$$

□ □

This result should be compared with the running time of $L_Q[\frac{1}{3}, (\frac{9}{2})^{1/3}]$ for the JLSV$_1$ method ($e = 3/2$) computed by Barbulescu and Pierrot [1, Appendix A], and the running time of $L_Q[\frac{1}{3}, 3^{1/3}]$ for prime fields ($e = 1$) computed by Commeine and Semaev [7, §4.1].

TABLE 3. Running-time to compute a B-smooth decomposition of S bounded by Q^e, for some values of e in $[1/3, 3]$ and $B = L_Q[2/3, (e^2/3)^{1/3}]$.

Norm bound	$Q^{1/3}$	$Q^{1/2}$	$Q^{2/3}$	$Q^{4/5}$	Q	$Q^{3/2}$	Q^2	Q^3
running-time constant c in $L_Q[\frac{1}{3}, c]$	1	$(\frac{3}{2})^{1/3}$	$2^{1/3}$	$\frac{12}{5}^{1/3}$	$3^{1/3}$	$\frac{9}{2}^{1/3}$	$6^{1/3}$	$9^{1/3}$
constant $c = (3e)^{1/3}$	1.00	1.14	1.26	1.34	1.44	1.65	1.82	2.08

5.1. **Running-Time of Special-q Descent.** The second step of the individual logarithm computation is the *special-***q** *descent*. This consists in computing the logarithms of the medium-sized elements in the factorization of the target in the number field. This step is very technical and we refer to Joux–Lercier–Naccache-Thomé [13, §B], Commeine and Semaev [7, §4.3], Barbulescu and Pierrot [1, §A], and Barbulescu [2, §7.3] for an analysis. They claim that this is possible to tune parameters so that the running time is in $L_Q[1/3, \delta]$ with δ strictly less than the constant involved in the running time of finding a B-smooth decomposition of the target. Since we considerably lowered this constant to $c = (3e)^{1/3}$, more work is needed to find whether we still have $\delta < c$. The third and final step of individual logarithm computation is very fast. It combines all the logarithms computed before, to get the final discrete logarithm of the target. It seems that now the special-**q** descent is clearly the bottleneck of the individual logarithm computation.

6. Conclusion

We give in Table 4 an upper bound for the norm of s in a number field K_f for three polynomial selection methods: the JLSV_1 method, the generalized Joux–Lercier method and the Conjugation method, and the complexity of finding a B-smooth decomposition of $\text{N}_{K_f/\mathbb{Q}}(s)$.

TABLE 4. Properties of polynomials and norm estimate for the three polynomial selection methods, with $s = \sum_{i=0}^{\deg s} s_i x^i \in \mathbb{F}_{p^n}^*$ and assuming that $\deg s = n - 1$.

polynomial select.	JLSV_1[12, §2.3]	gJL[16, 4]	Conjugation[4]
$\deg f$	n	$d + 1 \geq n + 1$	$2n$
$\|\|f\|\|_\infty$	$O(p^{1/2})$	$O(\log p)$	$O(\log p)$
$\text{Norm}_{K_f/\mathbb{Q}}(s)$	$p^{\deg s/2}\|\|s\|\|_\infty^n$	$\|\|s\|\|_\infty^{d+1}$	$\|\|s\|\|_\infty^{2n}$
nothing	$Q^{3/2-1/(2n)}$	$Q^{1+1/n}$	Q^2
[12] and §2.3	Q^2	Q	Q
This work, 3.1, 3.2	$Q^{3/2-3/(2n)}$	$Q^{1-1/n}$	$Q^{1-1/n}$
This work, 4.2	$Q^{3/2-5/(2n)}$	$Q^{1-2/n}$	$Q^{1-2/n}$

Finally, we give our practical results for small n in Table 5, where there are the most dramatic improvements. We obtain the optimal norm size of $Q^{\varphi(n)/n}$ for $n = 2, 3, 5$ with the gJL method and also for $n = 4$ with the Conjugation method.

Acknowledgements. Many thanks to François Morain, Pierrick Gaudry and Ben Smith for their helpful comments.

TABLE 5.

polynomial select.	JLSV_1[12, §2.3]	gJL[16, 4]	Conjugation[4]
$n = 2$			
Norm bound	$Q^{3/4}$, § 3.1	$Q^{1/2}$, § 3.2	
running time, c	$\left(\frac{9}{4}\right)^{1/3} = 1.31$	$\left(\frac{3}{2}\right)^{1/3} = 1.14$	
$n = 3$			
Norm bound	Q § 3.1	$Q^{2/3}$, § 3.2	
running time, c	$3^{1/3} = 1.44$	$2^{1/3} = 1.26$	
$n = 4$			
Norm bound	$Q^{7/8}$, § 4.2	$Q^{3/4}$, § 3.2	$Q^{1/2}$, § 4.2
running time, c	$\left(\frac{21}{8}\right)^{1/3} = 1.38$	$\left(\frac{9}{4}\right)^{1/3} = 1.31$	$\left(\frac{3}{2}\right)^{1/3} = 1.14$
$n = 5$			
Norm bound	$Q^{6/5}$, § 3.1	$Q^{4/5}$, § 3.2	
running time, c	$\left(\frac{18}{5}\right)^{1/3} = 1.53$	$\left(\frac{12}{5}\right)^{1/3} = 1.34$	
$n = 6$			
Norm bound	$Q^{13/12}$, § 4.2	$Q^{5/6}$, § 3.2	$Q^{2/3}$, § 4.2
running time, c	$\left(\frac{13}{4}\right)^{1/3} = 1.48$	$\left(\frac{5}{2}\right)^{1/3} = 1.36$	$2^{1/3} = 1.26$

REFERENCES

[1] R. Barbulescu and C. Pierrot. The multiple number field sieve for medium- and high-characteristic finite fields. *LMS Journal of Computation and Mathematics*, 17:230–246, 1 2014. `http://journals.cambridge.org/article_S1461157014000369`.

[2] Razvan Barbulescu. *Algorithmes de logarithmes discrets dans les corps finis*. PhD thesis, Université de Lorraine, 2013.

[3] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain. Discrete logarithms in GF(p^2) — 180 digits, 2014. Announcement available at the NMBRTHRY archives.

[4] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain. Improving NFS for the discrete logarithm problem in non-prime finite fields. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 129–155. Springer, 2015.

[5] J.P. Buhler, Jr. Lenstra, H.W., and Carl Pomerance. Factoring integers with the number field sieve. In ArjenK. Lenstra and Jr. Lenstra, HendrikW., editors, *The development of the number field sieve*, volume 1554 of *Lecture Notes in Mathematics*, pages 50–94. Springer Berlin Heidelberg, 1993.

[6] E. R. Canfield, P. Erdös, and C. Pomerance. On a problem of Oppenheim concerning "factorisatio numerorum". *J. Number Theory*, 17(1):1–28, 1983.

[7] An Commeine and Igor Semaev. An algorithm to solve the discrete logarithm problem with the number field sieve. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography*, volume 3958 of *Lecture Notes in Computer Science*, pages 174–190. Springer, 2006.

[8] Don Coppersmith. Modifications to the number field sieve. *Journal of Cryptology*, 6(3):169–180, 1993.

[9] Daniel M. Gordon. Discrete logarithms in GF(p) using the number field sieve. *SIAM J. Discrete Math*, 6:124–138, 1993.

[10] Kenichiro Hayasaka, Kazumaro Aoki, Tetsutaro Kobayashi, and Tsuyoshi Takagi. An experiment of number field sieve for discrete logarithm problem over gf(p 12). In Marc Fischlin and Stefan Katzenbeisser, editors, *Number Theory and Cryptography*, volume 8260 of *Lecture Notes in Computer Science*, pages 108–120. Springer Berlin Heidelberg, 2013.

[11] A. Joux and R. Lercier. Improvements to the general number field for discrete logarithms in prime fields. *Math. Comp.*, 72(242):953–967, 2003.

[12] A. Joux, R. Lercier, N. Smart, and F. Vercauteren. The number field sieve in the medium prime case. In *Advances in Cryptology–CRYPTO 2006*, volume 4117 of *Lecture Notes in Comput. Sci.*, pages 326–344. Springer, 2006.

[13] Antoine Joux, Reynald Lercier, David Naccache, and Emmanuel Thomé. Oracle-assisted static Diffie-Hellman is easier than discrete logarithms. In Matthew G. Parker, editor, *12th IMA International Conference on Cryptography and Coding*, volume 5921 of *Lecture Notes in Computer Science*, pages 351–367, Cirencester, UK, December 15–17, 2009. Springer, Berlin, Germany.

[14] M. Kalkbrener. An upper bound on the number of monomials in determinants of sparse matrices with symbolic entries. *Mathematica Pannonica*, 73:82, 1997.

[15] A.K. Lenstra, Jr. Lenstra, H.W., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[16] D. Matyukhin. Effective version of the number field sieve for discrete logarithms in the field GF(p^k) (in Russian). *Trudy po Discretnoi Matematike*, 9:121–151, 2006. `http://m.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=tdm&paperid=144&option_lang=eng`.

[17] Damian Weber. Computing discrete logarithms with quadratic number rings. In Kaisa Nyberg, editor, *Advances in Cryptology – EUROCRYPT'98*, volume 1403 of *Lecture Notes in Computer Science*, pages 171–183, Espoo, Finland, May 31 – June 4, 1998. Springer, Berlin, Germany.

[18] Pavol Zajac. *Discrete Logarithm Problem in Degree Six Finite Fields*. PhD thesis, Slovak University of Technology, 2008.