High-Order Galois Automorphisms for TNFS Linear Algebra

Haetham Al Aswad[1][0000−0003−2960−8231], Cécile Pierrot[2][0000−0001−5417−7133], and Emmanuel Thomé[2][0000−0002−5669−2195]

[1] CNRS, Université de Montpellier, France
haetham.al-aswad@lirmm.fr
[2] Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
{cecile.pierrot,emmanuel.thome}@inria.fr

Abstract. The Number Field Sieve and its variants are the best-known algorithms to solve the discrete logarithm problem in finite fields. When the extension degree is composite, the Tower variant, TNFS, is the most efficient. Looking at finite fields with composite extension degrees such as 6 and 12 is motivated by pairing-based cryptography, which does not yet have a good quantum-resistant equivalent.
The two most costly steps in TNFS are the *relation collection* and *linear algebra* steps. Although the use of order-k Galois automorphisms allows one to accelerate the relation collection step by a factor of k, their use to accelerate the linear algebra step remains an open problem. In previous work, this problem is solved for $k = 2$, leveraging a quadratic acceleration factor equal to 4.
In this article, we provide a solution for $k = 6$ and $k = 12$. We propose a new construction that allows the use of a Galois automorphism of order 6 (resp. 12) in $\mathbb{F}_{p^6}$ (resp. $\mathbb{F}_{p^{12}}$), thus accelerating the linear algebra step by a factor of approximately 36 (resp. 144). Moreover, we provide a SageMath implementation of TNFS and our construction, and validate our findings on small examples.

Keywords: Cryptanalysis. Public Key Cryptography. Discrete Logarithm. Tower Number Field Sieve. Automorphisms. Schirokauer maps.

1 Introduction

Context. The discrete logarithm problem in a cyclic group $\mathbb{G}$ with a generator $g \in \mathbb{G}$ is the computational problem of finding an integer x modulo $|\mathbb{G}|$ for a given target $T \in \mathbb{G}$, such that $T = g^x$. Despite the growing interest in post-quantum cryptography, the discrete logarithm problem is still the basis of many currently deployed public-key protocols. This article deals with the discrete logarithm problem in the group of invertible elements of a finite field, $\mathbb{G} = \mathbb{F}_{p^n}^*$.

The Number Field Sieve. Excluding small-characteristic finite fields for which computation is made easier by quasi-polynomial time algorithms [4, 15, 26], the most efficient algorithm to compute discrete logarithms in finite fields is

(a variant of) the Number Field Sieve (NFS) algorithm [14, 23, 30]. All the variants of NFS have a subexponential complexity equal to $\exp((c + o(1)) \cdot (\log Q)^{1/3}(\log\log Q)^{2/3})$ where $o(1)$ tends to 0 as the finite field size Q tends to infinity and $c > 0$ is a constant that depends on the features of the target field and thus on the variant used: Special, Tower, Multiple, and potentially a combination of Special and Tower together.

The Tower variant, TNFS[3] [24, 25, 34], applies when the extension degree n is composite. Its asymptotic complexity is lower than that of NFS. De Micheli, Gaudry, and Pierrot [11] reported in 2021 the first implementation of TNFS and carried out a record computation on a 521-bit finite field with extension degree $n = 6$. One year later, Robinson [32] reported a record computation using TNFS on a 512-bit finite field of extension degree $n = 4$. These records confirm that TNFS is currently the best practical algorithm that computes discrete logarithms in finite fields of composite extension degree. Table 1 compares the performance of NFS and TNFS. Note that the two TNFS-records are approximately 100 bits larger than those carried out with NFS, and yet their costs are lower.

Year	Finite field	Bitsize of p^n	Cost in core-years	Algorithm	Work
2017	$\mathbb{F}_{p^6}$	422	26.1	NFS	[16]
2020	$\mathbb{F}_{p^6}$	423	9.3	NFS	[27]
2021	$\mathbb{F}_{p^6}$	521	2.8	TNFS	[11]
2022	$\mathbb{F}_{p^4}$	512	6.3	TNFS	[32]

Table 1: Cost in core-years of the latest discrete logarithm records on finite fields with composite extension degrees.

NFS and all its variants are built around four main steps: *polynomial selection*, *relation collection*, *linear algebra*, and *individual logarithm*. Asymptotically speaking, the *relation collection* and the *linear algebra* steps are equally hard and are the two most costly steps in all NFS variants. Experimental data from discrete logarithm records shows that they are the two most costly steps in practice as well. Table 2 shows the cost of the relation collection step, the linear algebra step, and the whole computation of recent records. Although relation collection has a higher cost than linear algebra in all these records except one, it is worth emphasizing that the former parallelizes much better than the latter. Additionally, adjusting some parameters can balance the costs of these steps to a certain extent, and this strategy was followed to make the linear algebra step feasible in the 795-bit record for prime fields [9].

Composite extension degrees in cryptographic applications. Pairing-based cryptography, introduced in the early 2000s [7, 8, 22], now underpins a range of applications—for example, the Boneh–Lynn–Shacham (BLS) signature scheme [8]. Its

[3] Sometimes referred to as the extended Tower Number Field Sieve (exTNFS).

Bitsize of p^n	Finite Field	Cost in core days			Work
		Relation collection	Linear algebra	Total	
203	$\mathbb{F}_{p^{12}}$	10.5	0.28	11	[20]
324	$\mathbb{F}_{p^5}$	359	11.5	386	[16]
512	$\mathbb{F}_{p^4}$	2,195	50	2,294	[32]
521	$\mathbb{F}_{p^6}$	388	23	413	[11]
593	$\mathbb{F}_{p^3}$	3,287	5,113	8,400	[13]
595	$\mathbb{F}_{p^2}$	157	18	175	[3]
795	$\mathbb{F}_p$	876,000	228,125	1,168,000	[9]

Table 2: Costs of relation collection, linear algebra, and the whole computation in the latest discrete logarithm records with various extension degrees.

security reduces to the hardness of the discrete logarithm problem in finite fields of extension degree $n > 1$ (the embedding degree) [28]. For efficiency, only a few pairing-friendly curves are used, constraining the underlying fields. In practice, composite extension degrees are the most commonly encountered, such as $\mathbb{F}_{p^6}$ (MNT6 curves [29]) and $\mathbb{F}_{p^{12}}$ (BLS12 curves [6]). Interestingly, there are no good post-quantum candidates to replace pairing-based protocols yet.

Using Galois automorphisms to accelerate the two hardest steps in NFS. For finite fields with extension degree $n > 1$, Galois symmetries can speed up NFS and its variants. Three sub-problems arise: (i) compute some adequate (*NFS-compatible*) automorphisms of order k dividing n; (ii) use them to accelerate the relation collection by about a factor k; and (iii) use them to shrink the linear system in the linear algebra step by a factor k. Since the complexity of linear algebra is nearly quadratic due to the sparsity of the underlying matrix, solving (iii) would yield an acceleration factor for the linear algebra step as large as k^2. In [3, 38], the authors provide polynomial selection methods to construct *NFS-compatible* automorphisms for orders $k = 2, 3, 4$, and 6, and Problem (i) remains open for other orders. The solution to (ii) is studied by [3, 11, 23]. However, Problem (iii) is only solved for $k = 2$ [3, 12, 38]. It was put into practice in the latest discrete logarithm record with TNFS on $\mathbb{F}_{p^6}$ [12] and accelerated the linear algebra step by a factor of approximately 4.

Our work. We solve (i) for $k = 12$ and (iii) for $k = 6$ and $k = 12$. Specifically, our work focuses on accelerating the linear algebra step in the TNFS algorithm when applied to finite fields with extension degrees $n = 6$ and $n = 12$. First, we show using [3] a method to construct *NFS-compatible* automorphisms of order $k = n$ in these cases, i.e., $k = 6$ or $k = 12$. Second, we present a new construction that allows the use of these automorphisms to accelerate the linear algebra step in TNFS by a factor of roughly k^2. Third, we provide an implementation of TNFS in SageMath together with our construction to illustrate our findings on small-size finite fields.

Outline of the article. We start with a description of TNFS in Section 2. Section 3 defines the Galois automorphisms that are useful in this work. Section 4 outlines the conditions and obstacles associated with using automorphisms for linear algebra acceleration, alongside a review of the relevant literature. In Section 5, we present a new construction of the diagram of NFS (via new Schirokauer maps) and we show in Section 6 that this new construction enables the acceleration of the linear algebra step by factors of 36 and 144 in finite fields of extension degrees 6 and 12, respectively. Finally, Section 7 presents our experiments that validate our findings.

2 Background

2.1 The Tower Number Field Sieve

We target a finite field $\mathbb{F}_{p^n}$, where n is composite. Let η be a non-trivial divisor of n and denote $\kappa = n/\eta$. Since the computation of a discrete logarithm in a group reduces to the case of prime-order subgroups via Pohlig-Hellman reduction, we focus on discrete logarithms modulo ℓ, a non-trivial prime divisor of $\Phi_n(p)$, where Φ_n is the n-th cyclotomic polynomial. The classical TNFS setup considers the intermediate number field $\mathcal{H} = \mathbb{Q}(\iota)$, where ι is a root of h, a polynomial of degree η over $\mathbb{Z}$ that remains irreducible modulo p. For any number field K, we let $\mathcal{O}_K$ be its ring of integers. For simplicity, we assume throughout this article that $\mathcal{O}_\mathcal{H} = \mathbb{Z}[\iota]$. This implies that h is monic.

Above $\mathcal{H}$, define two number fields $\mathcal{K}_1 = \mathcal{H}[x]/f_1(x)$ and $\mathcal{K}_2 = \mathcal{H}[x]/f_2(x)$, where f_1 and f_2 are irreducible polynomials over $\mathcal{O}_\mathcal{H}$ that share an irreducible factor φ of degree κ modulo the unique ideal $\mathfrak{p}$ over p in $\mathcal{H}$. In particular, f_1 and f_2 have degree at least κ. Let α_i be a root of f_i in $\mathcal{K}_i$ for $i = 1, 2$. Due to the conditions on the polynomials h, f_1, and f_2, we can factor the ring homomorphism from $\mathcal{O}_\mathcal{H}[x]$ to the target finite field $\mathbb{F}_{p^n}$ in two different ways, through the number fields $\mathcal{K}_1$ and $\mathcal{K}_2$. This allows us to build a commutative diagram as in Figure 3. When η and κ are coprime (which is always possible with $n = 6$ or $n = 12$), f_1 and f_2 can be defined over $\mathbb{Z}$. We make this choice for the rest of the article. To simplify the presentation, we assume that f_i is monic for $i = 1, 2$ (otherwise replace α_i by the leading coefficient times α_i).

The general framework of TNFS is common to all its variants. The *polynomial selection* step sets up the commutative diagram of Figure 3 by selecting the appropriate polynomials h, f_1, and f_2. Thereafter, by finding many small- to medium-size smooth numbers and factoring them, the *relation collection* step establishes linear relations involving prime ideals of small norms in the number fields $\mathcal{K}_1$ and $\mathcal{K}_2$. When enough equations are found, the *linear algebra* step solves the corresponding linear system. Given a target T in the finite field, the last step, called the *individual logarithm* step, uses this information to reveal the logarithm of T.

Polynomial selection. Several polynomial selection methods can be used in the TNFS context, such as the Conjugation, JLSV or Sarkar-Singh methods [3,

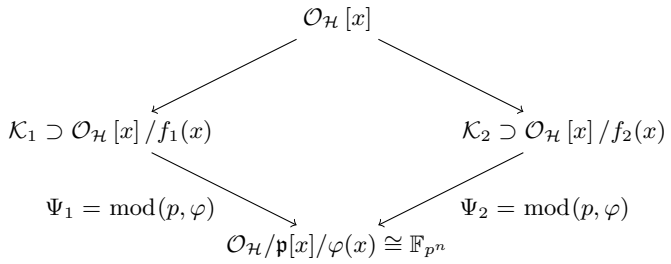


Fig. 3: Commutative diagram of Tower NFS.

23, 33]. Each method yields different degrees and coefficient sizes for h, f_1, and f_2, which influence the performance of the algorithm. Based on the recent records [11,32], the Conjugation method seems to perform best in practice, and Barbulescu et al. [3] show how to construct adequate automorphisms using this method. Therefore, we consider this method only.

Conjugation method for polynomial selection [3]. First, a polynomial h is chosen such that $\deg h = \eta$, the coefficients of h are small integers, and h remains irreducible modulo p. Second, a quadratic irreducible polynomial μ over $\mathbb{Z}$ with small coefficients is selected, which possesses a root ρ modulo p. Third, two polynomials g_0 and g_1 with small integer coefficients are chosen under the condition that $\deg(g_1) < \deg(g_0) = \kappa$ and $\varphi := g_0 + \rho g_1$ is irreducible modulo p. The polynomial f_1 is defined as $f_1 := \mathrm{Res}_Y(\mu(Y), g_0 + Y g_1)$, and f_2 is defined as $f_2 := v g_0 + u g_1$, where $\frac{u}{v} \equiv \rho \pmod p$ is a rational reconstruction of ρ. Given that $f_1 \equiv 0 \pmod{(p, \varphi)}$ and $f_2 \equiv v\varphi \pmod p$, both share φ as an irreducible factor modulo p. Their respective degrees are 2κ and κ.

Relation collection. The goal of the relation collection step is to select, among the set of polynomials $\phi(x, \iota) \in \mathcal{O}_{\mathcal{H}}[x]$ at the top of Figure 3, the candidates that yield a relation. A relation is found if for both $i \in \{1, 2\}$, the polynomial $\phi(x, \iota)$ maps to a principal fractional $\mathcal{O}_{\mathcal{K}_i}$-ideal in $\mathcal{K}_i$ that is B_i-*smooth* for some predefined bound B_i. Most often the search space for relation collection consists of linear polynomials $\phi(x, \iota) = a(\iota) - b(\iota)x \in \mathcal{O}_{\mathcal{H}}[x]$. The ideals that occur in the factorizations in $\mathcal{O}_{\mathcal{K}_1}$ and $\mathcal{O}_{\mathcal{K}_2}$ constitute the factor basis $\mathcal{F}$. More precisely, we define $\mathcal{F}$ as the disjoint union $\mathcal{F} = \mathcal{F}_1 \sqcup \mathcal{F}_2$ with, for $i = 1, 2$:

$$\mathcal{F}_i(B_i) = \{\text{prime ideals of } \mathcal{O}_{\mathcal{K}_i} \text{ of norm} \leq B_i \text{ and inertia degree 1 over } \mathcal{O}_{\mathcal{H}}\}.$$

An ideal $(a(\iota) - b(\iota)\alpha_i)$ is B_i-smooth if and only if its norm $\mathcal{N}_i(a(\iota) - b(\iota)\alpha_i)$ is B_i-smooth for $i \in \{1, 2\}$, where $\mathcal{N}_i$ defines the absolute algebraic norm in $\mathcal{K}_i$ (i.e., over $\mathbb{Q}$). Working with absolute norms enables efficient sieving algorithms. The relation collection stops when we have enough relations to construct a system of linear equations that may be full rank. The unknowns are the *virtual logarithms* of the ideals of the factor basis. A virtual logarithm map is a linear map with values in $\mathbb{Z}/\ell\mathbb{Z}$, which we define in §2.2.

Linear algebra. A nice feature of the linear system created is that the number of non-zero coefficients per row is very small. This allows us to use sparse linear algebra algorithms in $\mathbb{Z}/\ell\mathbb{Z}$ such as the Wiedemann algorithm [37] or Coppersmith's block Wiedemann algorithm [10], which allows partial parallelization. The output of this step is a kernel vector corresponding to virtual logarithms of the ideals in the factor basis.

Individual discrete logarithm. The final step consists in finding the discrete logarithm of one or several target elements. This step is subdivided into two substeps: a smoothing step and a descent step. The smoothing step is an iterative process where the target element is randomized until the randomized value lifted back to one of the number fields $\mathcal{K}_i$ is B_i'-smooth for a smoothness bound $B_i' > B_i$, for $i = 1$ or 2. The second step consists in decomposing every factor of the lifted value, in our case prime ideals with norms less than a smoothness bound B_i', into elements of the factor basis for which we now know the virtual logarithms. This eventually makes it possible to reconstruct the discrete logarithm of the target element. TNFS differs from NFS in this step as there exist improvements for the smoothing step when the target finite field has proper subfields [2, 18].

2.2 Schirokauer and virtual logarithm maps

This section follows the presentation in [36]. For an arbitrary number field K, let $\mathcal{O}_K$ be its ring of integers, $\mathcal{O}_K^\times$ its unit group, and $\mu_K \subset \mathcal{O}_K^\times$ the group of roots of unity. The Dirichlet unit theorem states that

$$\mathcal{O}_K^\times \simeq \mu_K \times \mathbb{Z}^{r_K},$$

where r_K is the *unit rank* of K. A $\mathbb{Z}$-basis of the non-torsion part (i.e., $\mathbb{Z}^{r_K}$) is called a *system of fundamental units*. Because we are interested in computing discrete logarithms modulo large ℓ, we safely assume the following:

Assumption 1. *All number fields K considered are such that* $\mathrm{disc}(\mathcal{O}_K)$ *and* $\#\,\mathrm{Cl}(\mathcal{O}_K)$ *are coprime to ℓ, and $[\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^\ell : \mathbb{F}_\ell] = r_K$. Furthermore, we consider only number field extensions $K \subset L$ such that $(\mathcal{O}_L^\times)^\ell \cap \mathcal{O}_K^\times \subset (\mathcal{O}_K^\times)^\ell$. (In other words, fundamental units in K do not gain ℓ-th roots once lifted to L.)*

We drop the i subscripts and consider $\mathcal{K}$ one of the two number fields of Figure 3, with $\mathcal{O} = \mathcal{O}_\mathcal{K}$ its ring of integers, and r its unit rank. Let $\mathcal{F}$ be the factor basis in $\mathcal{K}$, and let Γ be the group of $\mathcal{F}$-units[4] in $\mathcal{K}$, that is

$$\Gamma := \{\phi \in \mathcal{K}^* \mid (\phi) \text{ factors in } \mathcal{F}\}.$$

Looking at Γ modulo ℓ-th powers, we have the following statement.

[4] All references to S-units assume that the set of places that is considered is implicitly extended to contain infinite places as well.

Proposition 2 (Structure of Γ/Γ^ℓ). *Let $\mathcal{K}$, $\mathcal{O}$, r, $\mathcal{F}$, Γ be as above. Let $\mathcal{I}$ be the group of fractional ideals that completely factor in $\mathcal{F}$. For any integer ℓ that is coprime to $\#\operatorname{Cl}(\mathcal{O}_\mathcal{K}) \cdot \#\mu_\mathcal{K}$, we have the isomorphism*

$$\Gamma/\Gamma^\ell \simeq \mathcal{O}^\times/(\mathcal{O}^\times)^\ell \times \mathcal{I}/\mathcal{I}^\ell,$$

with basis $\{u_1, \ldots, u_r\} \cup \mathcal{F}/\mathcal{F}^\ell$, where $\{u_1, \ldots, u_r\}$ is a system of fundamental units of $\mathcal{K}$ considered modulo $(\mathcal{O}^\times)^\ell$. In particular, $\dim(\Gamma/\Gamma^\ell) = r + |\mathcal{F}|$.

Proof. This follows mostly from the Dirichlet-Chevalley-Hasse unit theorem [21, Theorem 8.2]. A proof is given in Section 8 for completeness.

Schirokauer maps. By Proposition 2, fundamental units (with ideal factorization) would give explicit coordinates for Γ/Γ^ℓ, but computing them is hard. Schirokauer maps [35] circumvent this, under an additional hypothesis.

Definition 3 (Usual definition of a Schirokauer map). *Consider notations as above. A Schirokauer map on Γ/Γ^ℓ is an $\mathbb{F}_\ell$-linear map $\Gamma/\Gamma^\ell \longrightarrow (\mathbb{Z}/\ell\mathbb{Z})^r$.*

Construction of a Schirokauer map. Schirokauer [35] gives a construction of a non-trivial such map. Write $\mathcal{K} = \mathbb{Q}[X]/(F)$ with $F \in \mathbb{Q}[X]$ irreducible and monic, and $\operatorname{disc}(F)$ coprime to ℓ. Consider the decomposition of F modulo ℓ into irreducible distinct factors: $F = \prod_j F_j \bmod \ell$. By the Chinese remainder theorem, we have the ring isomorphisms:

$$\mathcal{O}/\ell\mathcal{O} \simeq \mathbb{F}_\ell[X]/(F) \simeq \prod_j \mathbb{F}_\ell[X]/(F_j).$$

Define $Q := \operatorname{lcm}\left(\ell^{\deg(F_j)} - 1\right)$ and consider $x \in \Gamma \cap \mathcal{O}$. By the above isomorphism, we have $x^Q \equiv 1 \pmod{\ell\mathcal{O}}$. Further, lifting the congruence modulo $\ell^2\mathcal{O}$, we get $x^Q \equiv 1 + \ell \cdot P(x) \pmod{\ell^2\mathcal{O}}$ for some $P \in \mathbb{Z}[X]$ with degree bounded by $\deg(F) - 1$. We define the maps

$$\mathbf{A} : \begin{cases} \Gamma/\Gamma^\ell \longrightarrow \mathcal{O} \\ x \longmapsto \frac{x^Q - 1}{\ell}, \end{cases} \qquad \overline{\mathbf{A}} : \begin{cases} \Gamma/\Gamma^\ell \longrightarrow \mathbb{F}_\ell[X]/(F) \simeq \mathbb{F}_\ell^d \\ x \longmapsto \mathbf{A}(x) \bmod \ell\mathcal{O}. \end{cases} \tag{1}$$

As far as we know, for large ℓ, all practically computable Schirokauer map constructions (including ours presented in later sections) are based on the map $\mathbf{A}$.

The Schirokauer map used in the literature $\Lambda : \Gamma/\Gamma^\ell \to (\mathbb{Z}/\ell\mathbb{Z})^r$ is *defined* over an element x as the first r coefficients (or any r independent integer linear combinations of them) of $\overline{\mathbf{A}}(x)$. This provides a linear map that is computable in polynomial time. While the map Λ is non-trivial, there is no efficient way to test whether it is non-trivial enough, in the sense of the assumption:

Assumption 4. *Λ has maximal rank on $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell$.*

Under Assumption 4, Proposition 2 implies that every $\phi \in \Gamma/\Gamma^\ell$ can be uniquely represented as

$$\phi \leftrightarrow \left((\Lambda(\phi)_i)_{i=1}^r , (\operatorname{val}_\mathfrak{p}(\phi))_{\mathfrak{p} \in \mathcal{F}} \right). \tag{2}$$

In other words, $\mathcal{B}^\dagger = (\Lambda(\cdot)_i) \sqcup (\operatorname{val}_\mathfrak{p}(\cdot))_{\mathfrak{p} \in \mathcal{F}}$ is a basis of the dual $(\Gamma/\Gamma^\ell)^\dagger$.

Virtual logarithm maps. Consider $\mathcal{K}_1$ and $\mathcal{K}_2$ from Figure 3 with Γ_i and a Schirokauer map Λ_i on each side, such that Assumption 4 holds.

Definition 5 (Virtual logarithm). *A virtual logarithm map is a pair of $\mathbb{F}_\ell$-linear forms $\mathrm{vlog}_i : \Gamma_i/\Gamma_i^\ell \longrightarrow \mathbb{Z}/\ell\mathbb{Z}$ for $i = 1, 2$, such that for all $\phi \in \mathcal{O}_\mathcal{H}[x]$ that project to $\phi_1 \in \Gamma_1$ and $\phi_2 \in \Gamma_2$, we have*

$$\mathrm{vlog}_1 \phi_1 = \mathrm{vlog}_2 \phi_2. \tag{3}$$

The goal of relation collection and linear algebra is to compute a virtual logarithm map. The relation collection step assembles numerous constraints of the form given by Equation (3). We now see why these constraints lead to a linear system whose solution reveals our virtual logarithm map.

Assumption 4 provides us with a basis $\mathcal{B}_i^\dagger$ of $(\Gamma_i/\Gamma_i^\ell)^\dagger$, for $i = 1, 2$. Determining a virtual logarithm map amounts to decomposing $(\mathrm{vlog}_1, \mathrm{vlog}_2)$ along $(\mathcal{B}_1^\dagger, \mathcal{B}_2^\dagger)$. Put differently, let us do the thought exercise of considering the bidual bases $\mathcal{B}_i^\ddagger = \left((\lambda_{i,j})_{j=1}^{r_i}, (\mathfrak{p}^*)_{\mathfrak{p}\in\mathcal{F}_i}\right)$ for $i = 1, 2$. Elements of these bases are elements of Γ_i/Γ_i^ℓ. The $\lambda_{i,j}$ form a system of generators of $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell$. The $\mathfrak{p}^*$ are associated to ideals $\mathfrak{p}$ but they are of different nature. The "virtual logarithms" are the unknowns $\mathrm{vlog}_i(\lambda_{i,j})$ and $\mathrm{vlog}_i(\mathfrak{p}^*)$ in the equation below.

$$\begin{aligned} &\sum_{i=1}^{r_1} \Lambda_1(\phi_1)_i \cdot \mathrm{vlog}_1 \lambda_{1,i} + \sum_{\mathfrak{p}\in\mathcal{F}_1} \mathrm{val}_\mathfrak{p}(\phi_1) \cdot \mathrm{vlog}_1 \mathfrak{p}^* \\ =&\sum_{i=1}^{r_2} \Lambda_2(\phi_2)_i \cdot \mathrm{vlog}_2 \lambda_{2,i} + \sum_{\mathfrak{p}\in\mathcal{F}_2} \mathrm{val}_\mathfrak{p}(\phi_2) \cdot \mathrm{vlog}_2 \mathfrak{p}^*. \end{aligned} \tag{4}$$

For notational ease, we will henceforth shorten the $\mathfrak{p}^*$ notation to simply $\mathfrak{p}$, and let $\mathrm{vlog}\,\mathfrak{p}$ actually mean $\mathrm{vlog}\,\mathfrak{p}^*$. The important caveat is that this depends on Λ. Furthermore, we will use the shorthand $\mathrm{vlog}\,\boldsymbol{\Lambda}$ (resp. $\mathrm{vlog}\,\boldsymbol{\mathcal{F}}$) to denote the r- (resp. $|\mathcal{F}|$-) dimensional vector $(\mathrm{vlog}\,\lambda_1, \ldots, \mathrm{vlog}\,\lambda_r)$ (resp. $(\mathrm{vlog}\,\mathfrak{p})_{\mathfrak{p}\in\mathcal{F}}$). Finally, for $\phi \in \Gamma$, we implicitly project modulo Γ^ℓ and write $\mathrm{vlog}\,\phi$ and $\Lambda(\phi)$. Following these notations, $\mathrm{vlog}\,\phi$ is also

$$\mathrm{vlog}\,\phi = \Lambda(\phi) \cdot \mathrm{vlog}\,\boldsymbol{\Lambda} + (\mathrm{val}_\mathfrak{p}\,\phi)_{\mathfrak{p}\in\mathcal{F}} \cdot \mathrm{vlog}\,\boldsymbol{\mathcal{F}}. \tag{5}$$

Remark 6. A virtual logarithm map is not something we *choose*. It is merely the map that defines the unknowns in the linear system that we solve. In particular, since the connection from $\mathfrak{p}$ to $\mathfrak{p}^*$ that we discussed above depends on the Schirokauer map Λ, we like to say that the virtual logarithm map depends on Λ. In this article, we constrain the solution of our linear system—and thus the virtual logarithm map—to satisfy specific properties that accelerate the linear algebra step. In turn, these properties can only be met if the Schirokauer maps (Λ_1, Λ_2) fulfill certain conditions.

Remark 7. In practice, it is fairly common (albeit a bit wasteful) to use more than r coordinates for a Schirokauer map. This leads to a system that is underdetermined, but it is not a problem since all resulting maps work just as well.

3 TNFS automorphisms

The following extends the definition of [12].

Definition 8 (TNFS automorphism). *Consider $\mathbb{F}_{p^n}, \mathcal{K}_1, \mathcal{K}_2$ as in Figure 3. A TNFS automorphism is a pair of $\mathbb{Q}$-automorphisms $(\sigma_1, \sigma_2) \in \mathrm{Aut}_{\mathbb{Q}}(\mathcal{K}_1) \times \mathrm{Aut}_{\mathbb{Q}}(\mathcal{K}_2)$ fulfilling two conditions:*

- *Both are Frobenius automorphisms: they fix a degree-n prime ideal $\mathfrak{p}_i$ over p in $\mathcal{O}_{\mathcal{K}_i}$.*
- *Both project to the same Frobenius: there exists $\overline{\sigma} \in \mathrm{Gal}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)$ such that for all $(\phi_1, \phi_2) \in \mathcal{O}_{\mathcal{H}}[x]/(f_1) \times \mathcal{O}_{\mathcal{H}}[x]/(f_2)$:*

$$\Psi_1\left(\sigma_1(\phi_1)\right) = \overline{\sigma}\left(\Psi_1(\phi_1)\right) \quad \textit{and} \quad \Psi_2\left(\sigma_2(\phi_2)\right) = \overline{\sigma}\left(\Psi_2(\phi_2)\right),$$

  where (Ψ_1, Ψ_2) are the projection morphisms from Figure 3.

We emphasize that the most restrictive condition is the first one. The second one follows by raising σ_1 and σ_2 to appropriate powers. We often restrict the point of view to one of the fields, in which case we refer to "a TNFS automorphism on $\mathcal{K}$" as one of σ_1 and σ_2 in the above setup.

Construction of Galois automorphisms with the Conjugation method. When a TNFS setup targeting a field $\mathbb{F}_{p^n}$ is considered, the largest automorphism order we can hope for is $k = n$. To meet that goal, it is sufficient to choose the three polynomials h, f_1, and f_2 such that $\mathcal{H}$ has an automorphism of degree η that we term σ_h, and each of the fields $\mathcal{L}_i := \mathbb{Q}[x]/(f_i)$ has an automorphism of degree κ denoted as σ_{f_i} for $i = 1, 2$. Indeed, since η and κ are coprime, for $i = 1, 2$, the automorphism σ_i of $\mathcal{K}_i$ defined by the joint action of σ_h and σ_{f_i} has order $\eta \times \kappa = n$. In [3], the authors provide choices of g_0 and g_1 for the Conjugation method presented in §2.1 that provide automorphisms of $\mathcal{L}_1$ and $\mathcal{L}_2$ of orders equal to 2, 3, 4 and 6. Table 4 presents these choices.

To minimize norms in the number fields, h is usually chosen such that $\|h\|_\infty \leq 1$. Combined with the constraint of having an explicit automorphism of order η, this restricts the choice drastically. For reference, Table 5 lists several choices for h. It is easy to form alternative choices along the same lines, for those degrees or other degrees. However, not all degrees provide candidates with small coefficients. More generally, as observed in [19], there is a positive proportion of the primes p that are inert in none of the corresponding number fields: for such primes, we have to loosen the constraint on $\|h\|_\infty$. Except for the case $\eta = 3$ for which the requirement that h be cyclic imposes $\|h\|_\infty \geq 2$ anyway (see Table 5), we did not encounter this unfortunate situation in our experiments (see §7).

Remark 9. In the situation above with $k = n$, it might be worth noting that while $\mathcal{K}_2$ is Galois (being the compositum of two cyclic extensions of coprime degrees), $\mathcal{K}_1$ is not Galois over $\mathbb{Q}$ in general. However, if we let $\mathcal{M}(\theta) = \mathbb{Q}[x]/\mu$, then $\mathcal{L}_1$ is a cyclic extension of $\mathcal{M}$, with defining polynomial $g_0 - \theta g_1$. Furthermore, $\mathcal{M}$ and $\mathcal{H}$ are linearly disjoint because p is inert in $\mathcal{H}$ while it splits in $\mathcal{M}$. Therefore,

κ	g_0	g_1	$\sigma(\alpha) =$
2	x^2+1	x	$1/\alpha$
	x^2-1	x	$-1/\alpha$
	x^2	1	$-\alpha$
3	x^3-3x-1	x^2+x	$-(\alpha+1)/\alpha$
4	x^4-6x^2+1	x^3-x	$(1+\alpha)/(1-\alpha)$
6	$x^6+6x^5-20x^3-15x^2+1$	$2x^5+5x^4-5x^2-2x$	$(1+2\alpha)/(1-\alpha)$

Table 4: Table from [3]. Automorphisms come from the Conjugation method (§2.1). The automorphism leaves g_0/g_1 invariant. Its expression and order are identical for both number fields.

η	h	minimal polynomial of	$\sigma_h(\iota) =$
2	$\Psi_3 = x^2+x+1$	$e^{2i\pi/3}$	$-1-\iota$
3	x^3-x^2-2x+1	$e^{2i\pi/7}+e^{-2i\pi/7}$	$\frac{-1}{1+\iota}$
4	$\Psi_{10} = x^4-x^3+x^2-x+1$	$e^{i\pi/5}$	ι^2

Table 5: Examples of polynomials h with explicit automorphisms that can be constructed from cyclotomic fields and their subfields.

$\mathcal{MH}$ is cyclic over $\mathcal{M}$ and $\mathcal{K}_1$ is a Galois extension of $\mathcal{M}$. For $\mathcal{K}_1$ to be Galois over $\mathbb{Q}$, we would need the automorphism of $\mathcal{M}$ to extend to a $\mathbb{Q}$-automorphism of $\mathcal{K}_1$, which may or may not be the case. E.g., it does occur with the first row of Table 4 if $\mu = x^2 + D$, since $(g_0/g_1)(-\alpha_1) = -(g_0/g_1)(\alpha_1) = -\mu = \overline{\mu}$. But that is not a general fact.

4 Speed-up with TNFS automorphisms

Notations. Throughout this section, let $\mathcal{K}$ be one of the middle fields in Figure 3. We keep the notations and assumptions of §2.2 and §3. Let σ be a TNFS automorphism of order k on $\mathcal{K}$ (in particular, $k \mid n$). Let ζ be a power of p such that $\overline{\sigma}(x) = x^\zeta$. We observe that ζ is a k-th primitive root of unity modulo ℓ. The notations $\mathcal{K}^{\sigma^s}$ and $\mathbb{F}_{p^n}^{\overline{\sigma}^s}$ refer to the subfield fixed point-wise by σ^s and $\overline{\sigma}^s$, respectively, with s an integer.

A TNFS automorphism of order k helps accelerate the relation collection step by a factor of approximately k. This is due to the fact that the factor basis is stable under the automorphism's action since the conjugate of a prime ideal is a prime ideal of equal norm. Consequently, conjugating an equation on both sides provides "for free" a new equation, and iterating with powers of the automorphisms yields the claimed speed-up. Even when we take into

account the complications explained in [11, §3.4], the qualitative observation that automorphisms yield a speed-up that is commensurate with k still holds.

As for the linear algebra step, one hopes that the virtual logarithms of k conjugate ideals can be recovered from the virtual logarithm of one of these ideals. Since for all $x \in \mathbb{F}_{p^n}^\times$, we have the connection $\log\left(x^{\overline{\sigma}}\right) \equiv \zeta \log(x) \pmod{\ell}$, we would like the following similar condition to hold.

Condition 10. *For each* $\mathfrak{p} \in \mathcal{F}$, $\operatorname{vlog}(\mathfrak{p}^\sigma) \equiv \zeta \operatorname{vlog} \mathfrak{p} \pmod{\ell}$.

If Condition 10 holds, we can reduce the matrix size by a factor of k and hence accelerate the linear algebra step by a factor of approximately k^2 since sparse linear algebra's complexity is nearly quadratic. Unfortunately, this is not true in general. The reason for failure lies in complications related to Schirokauer maps and the units, as we examine now.

4.1 Obstacles to speeding up the linear algebra step

A virtual logarithm vanishes on the elements fixed by a TNFS automorphism.

Lemma 11. *Let* $\phi \in \Gamma$ *be such that* $\sigma(\phi) = \phi$, *then* $\operatorname{vlog} \phi = 0$.

Proof. There exists a generator ξ of $\mathbb{F}_{p^n}^\times$ such that $\operatorname{vlog} \phi = \log_\xi(\overline{\phi}) \bmod \ell$, where $\overline{\phi}$ is the projection of ϕ to $\mathbb{F}_{p^n}$. From Definition 8 we have $\overline{\sigma}(\overline{\phi}) = \overline{\sigma(\phi)} = \overline{\phi}$, hence, $\overline{\phi} \in \mathbb{F}_{p^n}^{\overline{\sigma}}$. By [17, Lemma 2], the logarithm of a proper subfield element vanishes modulo ℓ. This yields $\log_\xi(\overline{\phi}) \equiv 0 \pmod{\ell}$.

Corollary 12. *Let* $\phi \in \Gamma$ *be such that there exists* s *a proper divisor of* k *with* $\sigma^s(\phi) = \phi$. *Then* $\operatorname{vlog} \phi = 0$.

We deduce the following result on virtual logarithms over orbits.

Proposition 13. *Let* $c = \#\operatorname{Cl}(\mathcal{O}_\mathcal{K})$, *and let* $\mathfrak{p}$ *be a prime ideal. There exists* $a \in \mathcal{K}^\sigma$ *such that*

$$\sum_{i=0}^{k-1} \operatorname{vlog}\left(\mathfrak{p}^{\sigma^i}\right) = -c^{-1}\ \Lambda(a) \cdot \operatorname{vlog} \mathbf{\Lambda}.$$

Proof. By the class group theorem, there exists $\gamma \in \mathcal{K}$ such that $(\gamma) = \mathfrak{p}^c$. Therefore, for $i \in [\![0, k-1]\!]$, $(\gamma^{\sigma^i}) = (\mathfrak{p}^{\sigma^i})^c$, and so $\operatorname{val}_{\mathfrak{p}^{\sigma^i}}(\gamma^{\sigma^i}) = c$ is the only non-zero valuation. Applying the vlog map, we get for all $0 \le i \le k-1$, $\operatorname{vlog}\left(\gamma^{\sigma^i}\right) = \Lambda\left(\gamma^{\sigma^i}\right) \cdot \operatorname{vlog} \mathbf{\Lambda} + c\ \operatorname{vlog}\left(\mathfrak{p}^{\sigma^i}\right)$. Summing the k equations, we get

$$\operatorname{vlog}\left(\prod_{i=0}^{k-1} \gamma^{\sigma^i}\right) = \Lambda\left(\prod_{i=0}^{k-1} \gamma^{\sigma^i}\right) \cdot \operatorname{vlog} \mathbf{\Lambda} + c \sum_{i=0}^{k-1} \operatorname{vlog}\left(\mathfrak{p}^{\sigma^i}\right).$$

The left hand side is zero by Lemma 11 and the result follows with $a = \prod_{i=0}^{k-1} \gamma^{\sigma^i}$.

Since $\sum_{i=0}^{k-1} \zeta^i = 0$, Condition 10 forces the sum in Proposition 13 to be zero, so the right-hand side of the equality vanishes as well. Since computing $\#\operatorname{Cl}(\mathcal{O}_\mathcal{K})$, a, or $\mathbf{\Lambda}$ is hard, we need careful virtual logarithm constructions to ensure this vanishing without the need to compute these quantities.

4.2 Literature on speeding up the linear algebra step

In this section, we examine constructions from the literature in which Condition 10 is satisfied. All these constructions work only with order-2 TNFS automorphisms, in which case Condition 10 is just $\operatorname{vlog}\mathfrak{p}^\sigma = -\operatorname{vlog}\mathfrak{p}$.

Vanishing virtual logarithm on units for order two automorphisms. A *complex multiplication field* (CM field) is a number field that is totally imaginary and that has a totally real subfield of index 2. Assume that $\mathcal{K}$ is CM. We say that $(\mathcal{K}, \sigma)$ is CM+TNFS if the subfield of index 2 of $\mathcal{K}$ is $\tilde{\mathcal{K}} := \mathcal{K}^{\sigma^{k/2}}$.

Proposition 14. *Let $(\mathcal{K}, \sigma)$ be* CM+TNFS *as above. Then, the index $v = [\mathcal{O}_{\mathcal{K}}^\times : \mathcal{O}_{\tilde{\mathcal{K}}}^\times]$ is finite and $\operatorname{vlog} u = 0$ for all $u \in \mathcal{O}_{\mathcal{K}}^\times/(\mathcal{O}_{\mathcal{K}}^\times)^\ell$.*

Proof. The fact that v is finite follows from Dirichlet's unit theorem. Furthermore, v is coprime to ℓ by Assumption 1. A consequence is that an $\mathbb{F}_\ell$-basis of the vector space $\mathcal{O}_{\tilde{\mathcal{K}}}^\times/(\mathcal{O}_{\tilde{\mathcal{K}}}^\times)^\ell$ is also a basis of $\mathcal{O}_{\mathcal{K}}^\times/(\mathcal{O}_{\mathcal{K}}^\times)^\ell$. Therefore, any element of $\mathcal{O}_{\mathcal{K}}^\times/(\mathcal{O}_{\mathcal{K}}^\times)^\ell$ has a representative $u \in \tilde{\mathcal{K}}$, which implies $\sigma^{k/2}(u) = u$. Applying Corollary 12 we get $\operatorname{vlog} u = 0$.

The above proposition implies $\operatorname{vlog}\mathbf{\Lambda} = 0$ and thus by Proposition 13, Condition 10 holds. In fact, if both $(\mathcal{K}_1, \sigma_1)$ and $(\mathcal{K}_2, \sigma_2)$ are CM+TNFS, then the virtual logarithm vanishes on all the units and no Schirokauer map is needed. In [3], Barbulescu et al. construct TNFS diagrams with double-sided CM fields for extension degrees 4 and 6, but only with TNFS automorphisms of order 2. Zhu et al. [38] generalize this to arbitrary finite fields of even extension degree. To our knowledge, there are no known constructions for double-sided CM fields with an automorphism of order larger than 2.

Partial vanishing over the units. In [5], Barbulescu proposes alternative constructions where the virtual logarithm map vanishes on only a subset of the units. The examples use number fields $\mathcal{K}$ with automorphisms σ of orders 2, 3, 4, and 6, where $\mathcal{K}^\sigma$ forces some units to have zero virtual logarithm. Our work is an extension of this idea. We explore the full Galois subfield lattice $\{\mathcal{K}^{\sigma^i}\}$ and introduce an adequate *Galois Schirokauer map*.

Vanishing Schirokauer map for order two automorphisms. By Proposition 13, the other alternative to ensure Condition 10 is to construct a Schirokauer map that vanishes on the field elements fixed by the automorphism. In the 521-bit record [12] on $\mathbb{F}_{p^6}$, De Micheli et al. construct such a Schirokauer map with an order-2 TNFS-automorphism σ. We now examine their construction.

Let $m = [\mathcal{K} : \mathbb{Q}]$. Since $\mathcal{K}^\sigma$ has index 2, let $\omega \in \mathcal{K}$ be such that $\mathcal{K} = \mathcal{K}^\sigma(\omega)$. For $\gamma \in \Gamma/\Gamma^\ell$, compute $\mathbf{A}(\gamma)$ from Equation (1) and decompose it as $\mathbf{A}(\gamma) \bmod \ell\mathcal{O} = \gamma_0 + \gamma_1\omega \bmod \ell\mathcal{O}$ where γ_0 and γ_1 are polynomials of degree at most $m/2 - 1$. A Schirokauer map Λ on γ is defined by taking r independent integer linear combinations of the coefficients of γ_1, which is possible if and only if $r \leq m/2$.

This Schirokauer map vanishes on the elements fixed by σ. Indeed, if γ belongs to $\mathcal{K}^\sigma$, then so does any lift of $\mathbf{A}(\gamma)$, and hence γ_1 is zero and so is $\Lambda(\gamma)$. The authors provide two such constructions on two finite field instances of degrees 6 and 12. However, the construction is specific to order-2 automorphisms. Generalizing the construction to order-k automorphisms requires $r \leq m/k$, which is too restrictive. Specifically, since $r \geq m/2 - 1$ by Dirichlet's theorem, the above requirement fails whenever $k > 4$ or ($k = 4$ and $m > 4$) or ($k = 3$ and $m > 6$).

5 New Galois Schirokauer map for virtual logarithms

Why do we need a new Schirokauer map? For an order-k TNFS automorphism σ, one would like to identify the virtual logarithms of all prime ideals in a σ-orbit from a single representative, via the relation $\log(x^{\overline{\sigma}}) \equiv \zeta \log(x)$ in $\mathbb{F}_\ell$, and its analogue that is Condition 10. For $k > 2$, this typically fails with standard Schirokauer maps: the unit contribution $\Lambda(\gamma) \cdot \mathrm{vlog}\, \mathbf{\Lambda}$ in relations is not compatible with σ, and fixed subfield elements introduce additional constraints (cf. Proposition 13) that cannot be enforced without controlling units. Our goal is therefore to construct a computable linear map Λ such that

(i) it *vanishes* on elements coming from proper fixed subfields $\mathcal{K}^{\sigma^s}$ (so that the corresponding unit contributions disappear),
(ii) it has a simple *compatible* rule under σ, namely $\Lambda(\gamma^\sigma) = \zeta\, \mathbf{C}\, \Lambda(\gamma)$ for a fixed matrix $\mathbf{C}$.

5.1 Vanishing on some powers of the automorphism

Our construction of a new Schirokauer map comes at the cost of reducing the rank of the Schirokauer map. The following definition extends the one from [12].

Definition 15 (Galois Schirokauer map (GSM)). *A Galois Schirokauer map (GSM) on $(\mathcal{K}, \sigma)$ is a linear map $\Lambda : \Gamma/\Gamma^\ell \longrightarrow (\mathbb{Z}/\ell\mathbb{Z})^w$ for some integer w, which is trivial on proper subfields of $\mathcal{K}$ fixed by powers of σ. The integer w is referred to as the rank of Λ.*

The rank w of a GSM can be smaller than the unit rank r of the field, which departs from Definition 3. Nevertheless, we will prove that the vanishing property on $\{\mathcal{K}^{\sigma^s}\}_{s|k, s\neq k}$ compensates in many cases, and that Assumption 4 can be adjusted accordingly.

Definition 16 (Construction of a GSM). *Let $m = [\mathcal{K} : \mathbb{Q}]$, and let σ be an order-k TNFS automorphism on $\mathcal{K}$. Let d be a divisor of k. Recall that $\zeta \in \mathbb{F}_\ell$ is such that $\overline{\sigma}(x) = x^\zeta$ and $\zeta^k \equiv 1 \pmod{\ell}$. Let $a_0, \ldots, a_{m/k-1} \in \mathcal{K}^\sigma$ and $y \in \mathcal{K}$ be such that $\{a_i y^{\sigma^j}\}_{0\leq i\leq m/k-1,\ 0\leq j\leq k-1}$ is a $\mathbb{Q}$-basis of $\mathcal{K}$ (which exists by the normal basis theorem). We define a GSM of rank $w = d \cdot m/k$, denoted $\Lambda^{(\mathcal{K},\sigma,d)} : \Gamma/\Gamma^\ell \to (\mathbb{Z}/\ell\mathbb{Z})^{d\cdot m/k}$, as follows:*

– *Compute $\mathbf{A}(\gamma) \bmod \ell\mathcal{O}$ as defined by Equation (1).*

– *Decompose* $\mathbf{A}(\gamma)$ *in the above basis as*

$$\mathbf{A}(\gamma) \equiv \sum_{i=0}^{m/k-1} \sum_{j=0}^{k-1} \gamma_{i,j} \cdot a_i y^{\sigma^j} \mod \ell\mathcal{O},$$

– *Define* $\Lambda^{(\mathcal{K},\sigma,d)}$ *in matrix form as follows, where indices* j *run over* $\mathbb{Z}/k\mathbb{Z}$*:*

$$\Lambda^{(\mathcal{K},\sigma,d)} : \begin{cases} \Gamma/\Gamma^\ell \longrightarrow & (\mathbb{Z}/\ell\mathbb{Z})^{d\cdot m/k} \\ \gamma \longmapsto & \begin{pmatrix} \sum_{j\equiv 0[d]} \gamma_{0,j}\zeta^j & \cdots & \sum_{j\equiv 0[d]} \gamma_{m/k-1,j}\zeta^j \\ \vdots & & \vdots \\ \sum_{j\equiv d-1[d]} \gamma_{0,j}\zeta^j & \cdots & \sum_{j\equiv d-1[d]} \gamma_{m/k-1,j}\zeta^j \end{pmatrix} \end{cases}$$

The map $\Lambda^{(\mathcal{K},\sigma,d)}$ is a linear map. However, not every divisor d makes it a GSM, as we must ensure that this map vanishes on subfields. The following lemma and proposition address this.

Lemma 17. $\Lambda^{(\mathcal{K},\sigma,d)}(\gamma^\sigma) = \zeta \mathbf{C}_d \Lambda^{(\mathcal{K},\sigma,d)}(\gamma)$*, where* $\mathbf{C}_d$ *is the* $d \times d$ *matrix*

$$\mathbf{C}_d = \begin{pmatrix} 0 & & & 1 \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}.$$

Proof. Since σ fixes $\ell\mathcal{O}$, we have $\mathbf{A}(\gamma^\sigma) \equiv \mathbf{A}(\gamma)^\sigma \pmod{\ell\mathcal{O}}$. The latter decomposes as follows, still with indices j running over $\mathbb{Z}/k\mathbb{Z}$:

$$\mathbf{A}(\gamma)^\sigma \equiv \sum_{i=0}^{m/k-1} \sum_j \gamma_{i,j}\ y^{\sigma^{j+1}} \equiv \sum_{i=0}^{m/k-1} \sum_j \gamma_{i,j-1}\ y^{\sigma^j} \mod \ell\mathcal{O}.$$

Finally, we have

$$\begin{aligned} \Lambda^{(\mathcal{K},\sigma,d)}(\gamma^\sigma) &= \zeta \begin{pmatrix} \sum_{j\equiv 0[d]} \gamma_{0,j-1}\ \zeta^{j-1} & \cdots & \sum_{j\equiv 0[d]} \gamma_{m/k-1,j-1}\ \zeta^{j-1} \\ \vdots & & \vdots \\ \sum_{j\equiv d-1[d]} \gamma_{0,j-1}\ \zeta^{j-1} & \cdots & \sum_{j\equiv d-1[d]} \gamma_{m/k-1,j-1}\ \zeta^{j-1} \end{pmatrix} \\ &= \zeta \mathbf{C}_d \Lambda^{(\mathcal{K},\sigma,d)}(\gamma). \end{aligned}$$

Proposition 18. *If* $d \mid \prod_{p,\mathrm{val}_k(p)>0} p^{\mathrm{val}_p(k)-1}$*, then* $\Lambda^{(\mathcal{K},\sigma,d)}$ *is a GSM. In particular, if* k *is square-free, only* $d = 1$ *works.*

Proof. Let $\Lambda = \Lambda^{(\mathcal{K},\sigma,d)}$. For e a proper divisor of k and $\gamma \in \mathcal{K}^{\sigma^e}$ we have by Lemma 17 $\Lambda(\gamma) = \Lambda\left(\gamma^{\sigma^e}\right) = \zeta^e \mathbf{C}_d^e \Lambda(\gamma)$. Thus, $(\zeta^e \mathbf{C}_d^e - \mathbf{I}_d)\,\Lambda(\gamma) = 0$. If the matrices $\{\zeta^e \mathbf{C}_d^e - \mathbf{I}_d\}_{e|k,e\neq k}$ are all invertible, we have $\Lambda(\gamma) = 0$ as desired. Given such an e, the matrix determinant is $(-1)^d \zeta^{ed} \chi_{\mathbf{C}_d^e}(\zeta^{-e})$, where $\chi_{\mathbf{C}_d^e}$ is the

characteristic polynomial of $\mathbf{C}_d^e$. Since the eigenvalues of $\mathbf{C}_d^e$ are $\{\zeta^{i\cdot e\cdot k/d}\}_{i=0}^{d-1}$, we have

$$\begin{aligned}\chi_{\mathbf{C}_d^e}(X) &= \prod_{i=0}^{d-1}\left(X-\zeta^{i\cdot e\cdot k/d}\right)\\ &= \left(\prod_{i=0}^{\frac{d}{\gcd(e,d)}-1}\left(X-\zeta^{i\cdot e\cdot k/d}\right)\right)^{\gcd(e,d)}\\ &= \left(X^{\frac{d}{\gcd(e,d)}}-1\right)^{\gcd(e,d)},\end{aligned}$$

where the second equality comes from $\min\{i\in\mathbb{N}\mid \zeta^{i\cdot e\cdot k/d}=1\} = \min\{i\in\mathbb{N}\mid ie/d\in\mathbb{N}\} = d/\gcd(e,d)$. Consequently, $\zeta^e\mathbf{C}_d^e-\mathbf{I}_d$ is invertible if and only if $\zeta^{-ed/\gcd(e,d)}\neq 1$, which is equivalent to $k\nmid \operatorname{lcm}(e,d)$. We easily verify that this holds for all e only if d meets the announced condition.

Example 19. Consider a TNFS diagram as in Figure 3, constructed with the conjugation method for $\mathbb{F}_{p^6}$ (i.e., $n=6$). Let $m_1=[\mathcal{K}_1:\mathbb{Q}]=12$ and $m_2=[\mathcal{K}_2:\mathbb{Q}]=6$, and let (σ_1,σ_2) be a TNFS automorphism of order $k=6$, so that $d=1$. We now examine the GSM construction given by $\Lambda_1=\Lambda^{(\mathcal{K}_1,\sigma_1,d)}$ and $\Lambda_2=\Lambda^{(\mathcal{K}_2,\sigma_2,d)}$.

- **GSM on side $\mathcal{K}_2$.** The rank of Λ_2 is $d\cdot m_2/k=1$. Let $\{y, y^{\sigma_2},\ldots,y^{\sigma_2^5}\}$ be a $\mathbb{Q}$-basis of $\mathcal{K}_2$ with $y\in\mathcal{K}_2$. We compute $\Lambda_2(\gamma)$ as follows. We have $\mathbf{A}(\gamma)\equiv\sum_{j=0}^5\gamma_j y^{\sigma_2^j} \pmod{\ell\mathcal{O}}$, and $\Lambda_2(\gamma)=\sum_{j=0}^5\gamma_j\,\zeta^j\in\mathbb{Z}/\ell\mathbb{Z}$. Moreover, we can check that $\Lambda_2(\gamma^{\sigma_2})=\zeta\Lambda_2(\gamma)$.
- **GSM on side $\mathcal{K}_1$.** The rank of Λ_1 is $d\cdot m_1/k=2$. Let $\{a_i y^{\sigma^j}\}_{0\le i\le 1,\ 0\le j\le 5}$ be a $\mathbb{Q}$-basis of $\mathcal{K}_1$ with $y\in\mathcal{K}_1$ and $a\in\mathcal{K}_1^{\sigma_1}$. We compute $\Lambda_1(\gamma)$ as follows. We have $\mathbf{A}(\gamma)\equiv a_0\sum_{j=0}^5\gamma_{0,j}y^{\sigma_1^j}+a_1\sum_{j=0}^5\gamma_{1,j}y^{\sigma_1^j} \pmod{\ell\mathcal{O}}$. Then

$$\Lambda_1(\gamma)=\left(\sum_{j=0}^5\gamma_{0,j}\,\zeta^j,\ \sum_{j=0}^5\gamma_{1,j}\,\zeta^j\right)\ \in(\mathbb{Z}/\ell\mathbb{Z})^2.$$

  Moreover, we can check that $\Lambda_1(\gamma^{\sigma_1})=\zeta\Lambda_1(\gamma)$.

Remark 20. We can generalize the above example. Consider the case of $\mathbb{F}_{p^n}$ with a TNFS automorphism of even order $k\mid n$, where $k=2^sq$, $s\ge 1$ and q odd. Then $d=2^{s-1}$ works, so that the rank of $\Lambda_i=\Lambda^{(\mathcal{K}_i,\sigma_i,d)}$ is $2^{s-1}\cdot[\mathcal{K}_i:\mathbb{Q}]/k$. In other words, for $n=k=6$ the ranks of (Λ_1,Λ_2) are $(2,1)$ as above, and for $n=k=12$ their ranks are $(4,2)$.

5.2 Computing virtual logarithms with Galois Schirokauer maps

Let U be the subgroup of $\mathcal{O}^\times$ generated by $\bigcup_{s\mid k,s\neq k}(\mathcal{O}^\times\cap\mathcal{K}^{\sigma^s})$. Let V be the abelian group $\mathcal{O}^\times/(U\cdot(\mathcal{O}^\times)^\ell)$, which we view as a $\mathbb{F}_\ell$-vector space. By Assumption 1, we have $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell = V\oplus(U/U^\ell)$.

Consider $\Lambda^{(\mathcal{K},\sigma,d)}$ as in Definition 16, with d as large as Proposition 18 allows, so that $\Lambda^{(\mathcal{K},\sigma,d)}$ is a GSM. We need the following adjustment of Assumption 4.

Assumption 21. *The restriction of $\Lambda^{(\mathcal{K},\sigma,d)}$ to V has full rank $v := \dim V$.*

Assumption 21 requires that $\Lambda^{(\mathcal{K},\sigma,d)}$ have enough coordinates. More precisely, given $w = d \cdot m/k$ the rank of $\Lambda^{(\mathcal{K},\sigma,d)}$, it implies

$$w \geq v = \dim V. \tag{6}$$

Note that Inequality (6) is equivalent to the existence of a system of fundamental units of $\mathcal{K}$ in which at most w units do not belong to U. In the usual Schirokauer map case, one guarantees that $r = \dim(\mathcal{O}^\times/(\mathcal{O}^\times)^\ell)$ coordinates can be chosen from $\overline{\mathbf{A}}$ in Equation (1), and then assumes that they are free, i.e., they form a basis of the dual $(\mathcal{O}^\times/(\mathcal{O}^\times)^\ell)^\dagger$ (Assumption 4). The GSM context is similar: Inequality (6) holds and we assume that v coordinates of the GSM are free, meaning they form a basis of the dual $V^\dagger$ (Assumption 21).

Proposition 22. *Assume that Assumption 21 holds. Let $((\Lambda^{(\mathcal{K},\sigma,d)})_j)_{j=1}^v$ be a basis of $(\mathcal{O}^\times/(U \cdot (\mathcal{O}^\times)^\ell)^\dagger$. Then, $((\Lambda^{(\mathcal{K},\sigma,d)})_j)_{j=1}^v \sqcup \mathcal{F}$ can be extended to a basis of $(\Gamma/\Gamma^\ell)^\dagger$ (so that in particular, Assumption 4 holds), but the added linear forms do not contribute to a* vlog *map that is written along this basis.*

Proof. Let $\Lambda = ((\Lambda^{(\mathcal{K},\sigma,d)})_j)_{j=1}^v$ for brevity. Let $\boldsymbol{\Lambda} = (\lambda_j)_{j=1}^v$ be the dual basis of Λ within V. Extend it to a basis $(\boldsymbol{\Lambda} = (\lambda_j)_{j=1}^v, \boldsymbol{\Lambda'} = (\lambda'_j)_{j=1}^{r-v})$ of $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell$, in such a way that all λ'_j belong to U/U^ℓ. Since $\Lambda(\lambda'_j) = 0$, the dual basis of $(\boldsymbol{\Lambda}, \boldsymbol{\Lambda'})$ is of the form (Λ, Λ') for some $(r-v)$-dimensional linear map Λ'. Now following the discussion in §2.2, a vlog map writes as

$$\operatorname{vlog}\phi = \Lambda(\phi) \cdot \operatorname{vlog}\boldsymbol{\Lambda} + \Lambda'(\phi) \cdot \operatorname{vlog}\boldsymbol{\Lambda'} + (\operatorname{val}_\mathfrak{p}\phi)_{\mathfrak{p}\in\mathcal{F}} \cdot \operatorname{vlog}\boldsymbol{\mathcal{F}}.$$

By Corollary 12, $\operatorname{vlog}\boldsymbol{\Lambda'} = 0$, so the computation of Λ' is not needed.

The following proposition formalizes the conditions needed to use the new GSM to define a virtual logarithm map in a discrete logarithm computation.

Proposition 23 (Conditions to define a vlog **with a GSM).** *Let $(\mathcal{K}_1, \mathcal{K}_2)$ be as in Figure 3, of degree over $\mathbb{Q}$ equal to $(2n, n)$. Let (σ_1, σ_2) be a TNFS automorphism of order k. Let $d = \prod_{p,\operatorname{val}_k(p)>0} p^{\operatorname{val}_p(k)-1}$ so that for $i \in \{1,2\}$, $\Lambda_i = \Lambda^{(\mathcal{K}_i,\sigma_i,d)}$, given by Definition 16, is a GSM of rank $w_i = d \cdot [\mathcal{K}_i : \mathbb{Q}]/k$.*

Suppose Inequality (6) holds, i.e., that for $i \in \{1,2\}$ there exists a system of fundamental units in $\mathcal{K}_i$ in which at most w_i units do not belong to $\bigcup_{s|k,s\neq k} \mathcal{K}_i^{\sigma_i^s}$. Then if Assumption 21 holds, (Λ_1, Λ_2) can be used as a replacement for a standard Schirokauer map in discrete logarithm computations.

5.3 Compatibility with the automorphisms

Proposition 22 shows that our GSM can be extended to a good enough Schirokauer map for TNFS, in the sense that Assumption 4 would hold for that extension. Therefore, if TNFS succeeds (which implies that we have sufficiently

many relations), then the virtual logarithm map that is defined via that extension is, by construction, correct in the sense that it factors through the finite field via a non-trivial discrete logarithm map. We will now use this to prove that Condition 10 is met.

Consider σ a TNFS automorphism of order k on side $\mathcal{K}$ and recall that $\zeta \in \mathbb{F}_\ell$ is a k-th primitive root of unity (and also a power of p) such that $\overline{\sigma} : x \mapsto x^\zeta$. We need two intermediate lemmas.

Lemma 24. *Let* vlog *be a virtual logarithm map on side $\mathcal{K}$. Then for all $\gamma \in \Gamma/\Gamma^\ell$,* $\mathrm{vlog}(\gamma^\sigma) = \zeta\,\mathrm{vlog}(\gamma)$.

Proof. Denote by Ψ the projection to the finite field as in Figure 3. A virtual logarithm map vlog as in Definition 5 is proportional to a logarithm of the finite field. That is, there exists a generator $\xi \in \mathbb{F}_{p^n}^\times$ such that for all $\gamma \in \Gamma/\Gamma^\ell$, $\mathrm{vlog}(\gamma) = \log_\xi(\Psi(\gamma))$. Therefore,

$$\begin{aligned}\mathrm{vlog}(\gamma^\sigma) &= \log_\xi\left(\Psi(\gamma^\sigma)\right)\\ &= \log_\xi\left(\Psi(\gamma)^{\overline{\sigma}}\right) \text{ by Definition 8}\\ &= \log_\xi(\Psi(\gamma)^\zeta) = \zeta\log_\xi(\Psi(\gamma)) = \zeta\,\mathrm{vlog}(\gamma)\end{aligned}$$

Lemma 25. *Consider $\Lambda^{(\mathcal{K},\sigma,d)}$ from Definition 16 and assume that Assumption 21 holds. Then* $\mathbf{C}_d^T\,\mathrm{vlog}\,\mathbf{\Lambda} = \mathrm{vlog}\,\mathbf{\Lambda}$

Proof. For ease of presentation denote $\Lambda = \Lambda^{(\mathcal{K},\sigma,d)}$. Consider $u \in V$. On the one hand, from Lemma 24, we have $\mathrm{vlog}(u^\sigma) = \zeta\,\mathrm{vlog}(u) = \zeta\Lambda(u)\cdot\mathrm{vlog}\,\mathbf{\Lambda}$, where the last equality comes from the fact that u has zero valuation on prime ideals. On the other hand,

$$\begin{aligned}\mathrm{vlog}(u^\sigma) &= \Lambda(u^\sigma)\cdot\mathrm{vlog}\,\mathbf{\Lambda}\\ &= \zeta\mathbf{C}_d\Lambda(u)\cdot\mathrm{vlog}\,\mathbf{\Lambda}\\ &= \zeta\Lambda(u)\cdot\mathbf{C}_d^T\,\mathrm{vlog}\,\mathbf{\Lambda}.\end{aligned}$$

In conclusion, we have for all $u \in V$, $\Lambda(u)\cdot\left(\mathbf{C}_d^T\,\mathrm{vlog}\,\mathbf{\Lambda} - \mathrm{vlog}\,\mathbf{\Lambda}\right) = 0$. By Assumption 21, Λ has full rank on V, which implies $\mathbf{C}_d^T\,\mathrm{vlog}\,\mathbf{\Lambda} - \mathrm{vlog}\,\mathbf{\Lambda} = 0$.

Remark 26. Lemma 25 is trivial when $d = 1$ since $\mathbf{C}_1 = 1$.

The following theorem states that a virtual logarithm defined with our GSM satisfies Condition 10, as claimed.

Theorem 27. *Let $(\mathcal{K}_1, \mathcal{K}_2)$ be as in Figure 3 with a TNFS automorphism (σ_1, σ_2) of order k. Let $d = \prod_{p,\mathrm{val}_k(p)>0} p^{\mathrm{val}_p(k)-1}$. Following Definition 16, define two GSMs by $\Lambda_i = \Lambda^{(\mathcal{K}_i,\sigma_i,d)}$ for $i = 1, 2$. Assume that Inequality* (6) *and Assumption 21 hold. Let* $\mathrm{vlog} = (\mathrm{vlog}_1, \mathrm{vlog}_2)$ *be a virtual logarithm map defined with (Λ_1, Λ_2). Then Condition 10 holds. That is, for all $i = 1, 2$, $\forall\mathfrak{p} \in \mathcal{F}_i$,* $\mathrm{vlog}_i(\mathfrak{p}^{\sigma_i}) = \zeta\,\mathrm{vlog}_i(\mathfrak{p})$.

Proof. By Proposition 23, (Λ_1, Λ_2) can be used to define a virtual logarithm map. We drop the subscript i and consider one of the two sides. Consider $\mathfrak{p} \in \mathcal{F}$. Let $c = \#\operatorname{Cl}(\mathcal{O}_\mathcal{K})$. There exists $\gamma \in \Gamma$ such that $(\gamma) = \mathfrak{p}^c$, and $(\gamma^\sigma) = (\mathfrak{p}^\sigma)^c$. Then $\operatorname{vlog}(\gamma^\sigma) = c\ \operatorname{vlog}(\mathfrak{p}^\sigma) + \Lambda(\gamma^\sigma) \cdot \operatorname{vlog} \boldsymbol{\Lambda}$. That is

$$\begin{aligned}
\operatorname{vlog}(\mathfrak{p}^\sigma) &= c^{-1} \left(\operatorname{vlog}(\gamma^\sigma) - \Lambda(\gamma^\sigma) \cdot \operatorname{vlog} \boldsymbol{\Lambda}\right) \\
&= c^{-1} \left(\zeta \operatorname{vlog}(\gamma) - \zeta \mathbf{C}_d \Lambda(\gamma) \cdot \operatorname{vlog} \boldsymbol{\Lambda}\right) \text{ by Lemmas 24 and 17} \\
&= c^{-1} \left(\zeta \operatorname{vlog}(\gamma) - \zeta \Lambda(\gamma) \cdot \mathbf{C}_d^T \operatorname{vlog} \boldsymbol{\Lambda}\right) \\
&= c^{-1} \left(\zeta \operatorname{vlog}(\gamma) - \zeta \Lambda(\gamma) \cdot \operatorname{vlog} \boldsymbol{\Lambda}\right) \text{ by Lemma 25} \\
&= \zeta \operatorname{vlog}(\mathfrak{p}) \text{ by Equation (5).}
\end{aligned}$$

5.4 Shrinking the linear system

We have proved that under Assumption 21, our GSM is sufficient to obtain a successful TNFS computation. Let us now show that using Theorem 27 and Proposition 22, the linear system can be shrunk significantly.

The linear system is represented in matrix form: rows correspond to equations, and columns correspond to unknowns, which are either coordinates of $\operatorname{vlog} \boldsymbol{\Lambda}$ (a few columns) or of $\operatorname{vlog} \boldsymbol{\mathcal{F}}$ (all others). We first consider "special ideals". If $\mathfrak{p} \in \mathcal{F}$ is fixed by σ^s for some s a proper divisor of k, then $\mathfrak{p}^c$ is generated by an element $\gamma_\mathfrak{p}$ that is also fixed by σ^s. We have $\operatorname{vlog} \gamma_\mathfrak{p} = \Lambda(\gamma_\mathfrak{p}) \cdot \operatorname{vlog} \boldsymbol{\Lambda} + c \operatorname{vlog} \mathfrak{p}$. Since Λ is a GSM, we have $\Lambda(\gamma_\mathfrak{p}) = 0$, and Lemma 11 concludes that $\operatorname{vlog} \mathfrak{p} = 0$. The columns corresponding to such ideals are removed from the matrix, which shrinks its size (albeit insignificantly).

Now consider the most common situation where $\mathfrak{p}$ from the factor basis is not fixed by σ^s for any proper divisor $s \mid k$. Since $\operatorname{vlog}(\mathfrak{p}^\sigma) = \zeta \operatorname{vlog}(\mathfrak{p})$, we can express the k unknowns $(\operatorname{vlog}(\mathfrak{p}), \ldots, \operatorname{vlog}(\mathfrak{p}^{\sigma^{k-1}}))$ in only $\operatorname{vlog}(\mathfrak{p})$. This is done as follows. Denote $C_0, \ldots, C_{k-1}$ the columns corresponding to $\mathfrak{p}, \ldots, \mathfrak{p}^{\sigma^{k-1}}$. These k columns are replaced by one column equal to $C = \sum_{i=0}^{k-1} \zeta^i C_i$. Since this case is the most common, the linear system size is reduced by a factor of roughly k. The number of required relations is reduced by the same factor.

To estimate the performance gain in the linear algebra, it is crucial to examine the coefficient sizes of the new matrix and not only its dimension. Indeed, since the original matrix is sparse with coefficients mostly equal to -1, 0, or 1, the Block-Wiedemann algorithm [10] accomplishes the linear algebra step in approximately λN^2 arithmetic operations (mostly additions), where λ designates the average number of non-zero coefficients per row and N the matrix dimension. The aforementioned operation reduces the matrix dimension to $\approx N/k$, while maintaining the average number of non-zero coefficients per row roughly λ. In fact, in most relations, at most one ideal appears per orbit. Further, the non-zero coefficients in the matrix become polynomials in ζ, most often $\pm\zeta^i$ for $0 \le i \le k-1$. The trick is to decompose the matrix M in the basis ζ. Write $M = M_0 + M_1\zeta + \cdots + M_{k-1}\zeta^{k-1}$, where each matrix M_i, of dimension approximately N/k, has coefficients in $\{-1, 0, 1\}$, and an average density around

λ/k non-zero coefficients per row. Each matrix-vector multiplication Mv in the Wiedemann algorithm can instead be accomplished by k matrix-vector multiplications with the matrices M_i, and $k \cdot N/k$ multiplications by powers of ζ:

$$Mv = \sum_{i=0}^{k-1} \zeta^i \left(M_i v\right).$$

The number of arithmetic operations for a matrix-vector product is thus $k \cdot \lambda/k \cdot (N/k) = \lambda \cdot N/k$ additions in $\mathbb{Z}/\ell\mathbb{Z}$ and $k \cdot N/k$ multiplications with k-th roots of unity in $\mathbb{Z}/\ell\mathbb{Z}$. Counted in number of arithmetic operations, the cost of a matrix-vector multiplication drops to approximately $(\lambda + k) \cdot N/k$. Overall, we get the cost of the linear algebra using order-k TNFS automorphisms, that is $(\lambda + k)(N/k)^2$ operations.[5] This needs to be compared with the cost of the linear algebra if the automorphisms are not used, which is λN^2. In conclusion, we expect that linear algebra is faster by a factor

$$\frac{\lambda}{\lambda + k} \cdot k^2. \tag{7}$$

Since the order k (e.g., $k = 6, 12$) is small compared to λ ($\lambda \approx 200$ in record-size computations such as [9]), we approximate the acceleration factor to k^2.

6 Application: acceleration of the linear algebra step with TNFS automorphisms of order 6 and 12

We show in this section how to construct a TNFS diagram over $\mathbb{F}_{p^6}$ (resp. $\mathbb{F}_{p^{12}}$) using the *Conjugation* polynomial selection method while satisfying two key properties. First, the resulting diagram enjoys a TNFS automorphism of order 6 (resp. 12). Second, the GSM from Definition 16 satisfies Inequality (6). The TNFS automorphism accelerates the relation collection step by a factor of approximately 6 (resp. 12). Furthermore, as a consequence of Theorem 27, it speeds up the linear algebra step by a factor of approximately 36 (resp. 144).

6.1 Construction of TNFS automorphisms of order 6 and 12

The extension degree n is 6 or 12. It decomposes as $n = \eta\kappa$ with η and κ coprime and non-trivial (hence two possible setups for $n = 6$, and two setups for $n = 12$). In all these setups, we have the following result.

Proposition 28. *Let $(p, n, \eta, \kappa, h, \mu, \rho, g_0, g_1, f_1, f_2)$ be as in the Conjugation method, with η and κ coprime, and let an automorphism of the rational fraction g_0/g_1 be given as in Table 4. Then the induced automorphisms $\sigma_1 \in \mathrm{Aut}(\mathcal{K}_1)$ and $\sigma_2 \in \mathrm{Aut}(\mathcal{K}_2)$ both fix a prime ideal of degree n above p, that is, (σ_1, σ_2) is a TNFS automorphism as defined in Definition 8.*

[5] The distinction between additions and multiplications is barely relevant here. For most sparse operations (additions), memory access penalties easily dwarf the difference in cost, while in contrast multiplications are done on dense vectors.

Proof. By construction, the ideal $\mathfrak{p}_i = \langle p, g_0(\alpha_i) - \rho g_1(\alpha_i)\rangle$ is a prime ideal of degree n above p in $\mathcal{O}_{\mathcal{K}_i}$ for $i \in \{1, 2\}$. Since the automorphism of Table 4 leaves g_0/g_1 invariant and fixes $\rho \in \mathbb{F}_p$ as well, it follows that $\sigma_i(\mathfrak{p}_i) \subset \mathfrak{p}_i$.

6.2 Large enough rank for the Galois Schirokauer map

To satisfy Inequality (6), we need to bound the number of units not belonging to subfields. The following result plays a key role.

Theorem 29. *Let K be a cyclic Galois extension of a number field N, with a generating N-automorphism τ of even order $2q$ with q odd. Let $R = K^{\tau^2}$ and let $\mathrm{nr}(R)$ (resp. $\mathrm{nr}(N)$) denote the number of real embeddings of R (resp. N). Let $L = K^{\tau^q}$ so that we have the diagram of Figure 6. Then the rank of $\mathcal{O}_K^\times$ modulo the subgroup generated by $\mathcal{O}_K^\times \cap (L \cup R)$ is*

$$\frac{q-1}{2}\left(\frac{[K:\mathbb{Q}]}{2q} + \mathrm{nr}(R) - \mathrm{nr}(N)\right).$$

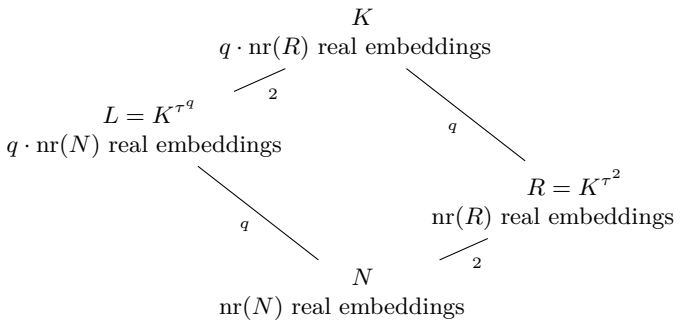


Fig. 6: Lattice of subfields in Theorem 29.

Proof. The number field L is a Galois extension of odd degree q of N. Let β be a generating element of L, and let $P \in N[x]$ be its minimal polynomial. The Galois group $\langle \tau^2 \rangle$ acts transitively on its roots. Since τ^2 is a field automorphism, it takes β to a polynomial in β with coefficients in N. Assume there exists $\psi : L \mapsto \mathbb{C}$ a complex embedding such that $\psi(N) \subset \mathbb{R}$. Then P^ψ is an odd-degree real polynomial, and one of its roots is real. By transitivity, all conjugates of that real root by powers of τ^2 are also real, which shows that $\psi(L) \subset \mathbb{R}$, and ψ is among a class of q conjugate Galois embeddings that extend the same $\psi(N) \hookrightarrow \mathbb{R}$. Of course, any real embedding of L embeds the subfield N into $\mathbb{R}$ as well, so that we proved $\mathrm{nr}(L) = q\,\mathrm{nr}(N)$. The same argument implies $\mathrm{nr}(K) = q\,\mathrm{nr}(R)$. As a

consequence, the unit ranks of N, L, R, and K are as follows, using the formula $r_K = \frac{1}{2}([K:\mathbb{Q}] + \mathrm{nr}(K)) - 1$:

$$\begin{aligned} r_N &= \frac{1}{2}\left(\frac{[K:\mathbb{Q}]}{2q} + \mathrm{nr}(N)\right) - 1 \\ r_L &= \frac{1}{2}\left(\frac{[K:\mathbb{Q}]}{2} + q\,\mathrm{nr}(N)\right) - 1 \\ r_R &= \frac{1}{2}\left(\frac{[K:\mathbb{Q}]}{q} + \mathrm{nr}(R)\right) - 1 \\ r_K &= \frac{1}{2}\left([K:\mathbb{Q}] + q\,\mathrm{nr}(R)\right) - 1. \end{aligned}$$

The unit excess is $r_K - r_L - r_R + r_N$, and the claimed expression follows easily.

We can apply Theorem 29 to the TNFS case. Since this section applies to even k in general, let us write it as $k = 2^s q$. Let us use the same notations as in Remark 20 and Proposition 23. The rank of Λ_i is $2^{s-1} \cdot [\mathcal{K}_i : \mathbb{Q}]/k = [\mathcal{K}_i : \mathbb{Q}]/(2q)$. Both $\mathcal{K}_1$ and $\mathcal{K}_2$ meet the conditions of Theorem 29, relative to the base field $\mathcal{K}_i^{\sigma_i^{k/(2q)}}$. If we let $\tau_i = \sigma_i^{k/(2q)}$, the fields we are really interested in are the topmost part of the subfield lattices below $\mathcal{K}_1$ and $\mathcal{K}_2$. In order to reconnect this with the TNFS situation (e.g., Figure 3) we need to distinguish based on which of η or κ is even. Corresponding diagrams, in the $n = k$ case, are given in Figure 7 as an illustration. Notice that as far as units are concerned, the field $\mathcal{H}$ does not appear in the lattices of Figure 7 when η is even. In that case, $\mathcal{H}$ is just one of the subfields of $\mathcal{K}_i^{\sigma_i^{\eta}}$, which may or may not be the field $\mathcal{K}_i^{\sigma_i^{\eta}/2}$.

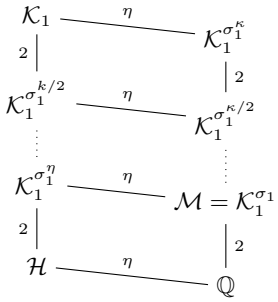
As argued in §5.2, the unit excess of $\mathcal{K}$ relative to *all* fixed subfields is $\dim V$ and therefore the quantity computed by Theorem 29 is an upper bound on $\dim V$. This bound is to be compared with $[\mathcal{K} : \mathbb{Q}]/(2q)$. This leads to the following statement, whose proof is straightforward. Note that the sub-case 30a below applies to $n = 6$ and $n = 12$.

Theorem 30. *Let notations be as above. Inequality* (6) *is satisfied if and only if on each side, the fields N and R of Theorem 29 are such that*

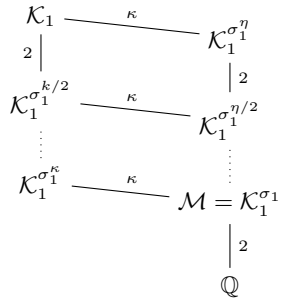
$$\mathrm{nr}(N) \geq \mathrm{nr}(R) + \frac{q-3}{q-1} \cdot \frac{[\mathcal{K}:\mathbb{Q}]}{2q}.$$

In particular, the following conditions are sufficient to obtain a linear algebra speedup by a factor of approximately k^2, provided that Assumption 21 holds:

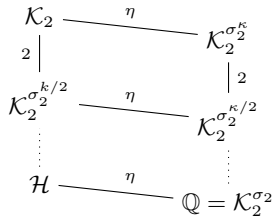
(a) $q = 3$ *and the subfields* $R = \mathcal{K}_i^{\sigma_i^{k/q}}$ *have no real embeddings;*
(b) $q = 5$*, the subfields* $R = \mathcal{K}_i^{\sigma_i^{k/q}}$ *have no real embeddings, and at least half of the embeddings of the subfields* $N = \mathcal{K}_i^{\sigma_i^{k/(2q)}}$ *are real;*
(c) more generally if on each side, R is a CM field and N is a totally real field.



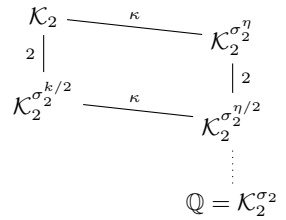
(a) $\mathcal{K}_1$ with $n = k = \eta\kappa$ and κ even.



(b) $\mathcal{K}_1$ with $n = k = \eta\kappa$ and η even.



(c) $\mathcal{K}_2$ with $n = k = \eta\kappa$ and κ even.



(d) $\mathcal{K}_2$ with $n = k = \eta\kappa$ and η even.

Fig. 7: Subfield lattices of $\mathcal{K}_1$ and $\mathcal{K}_2$ in the TNFS context, in the $n = k$ case.

As a conclusion, let us narrow down the scope to $n = 6$ or $n = 12$. Sufficient conditions for a working TNFS automorphism setup with the Conjugation method, following Theorem 30a, can be laid out as follows. When η is even, i.e., with $(n, \eta, \kappa) \in \{(6, 2, 3), (12, 4, 3)\}$, the polynomial h must be chosen with no real roots. On the contrary, when κ is even, i.e., with $(n, \eta, \kappa) \in \{(6, 3, 2), (12, 3, 4)\}$, the polynomials f_1 and f_2 must both be chosen without real roots. These conditions ensure that Theorem 30a holds.

6.3 Application to other automorphism orders?

The natural continuation of this work is to extend the use of Galois Schirokauer maps to composite orders beyond 6 and 12. The question is twofold. First, we need to find polynomial constructions that adapt to more general degrees, and provide convenient automorphisms. This is not always straightforward. Cyclotomic polynomials and the defining polynomials of their subfields are a good source (as in Table 5), but coefficient sizes can become an obstacle. More generally, the observation of [19] is that this problem is not easy. In addition, when n is a prime power, κ and η cannot be taken coprime and the construction must be amended, which escapes the setting of the present paper.

The second aspect is whether we can find constructions where Inequality (6) holds. The dimensions of the GSM are provided by Proposition 18 and their values are listed in Table 8 for various values of n, assuming we seek a TNFS

automorphism of optimal order $k = n$. Theorem 30a relies crucially on $q = 3$, and shows that $k = 24$ would work. The constraints of Theorem 30 become more strict as q grows. We leave such constructions to future work. Another potential future direction consists in counting units in more subfields than the subfields of indices 2 and q in Theorem 29: in fact, all prime factors of k can be considered, which leads to a subtle counting challenge if the number of prime factors of k is three or more.

n	4	6	8	9	10	12	14	15
Ranks	$(4,2)$	$(2,1)$	$(8,4)$	$(6,3)$	$(2,1)$	$(4,2)$	$(2,1)$	$(2,1)$
n	16	18	20	21	22	24	25	26
Ranks	$(16,8)$	$(6,3)$	$(4,2)$	$(2,1)$	$(2,1)$	$(8,4)$	$(10,5)$	$(2,1)$

Table 8: Ranks of the GSM of Definition 16 on $(\mathcal{K}_1, \mathcal{K}_2)$ of absolute degrees $(2n, n)$, and constructed with TNFS automorphisms of order $k = n$.

7 Experimental validation: acceleration of the linear algebra step

To validate our findings, we provide a SageMath implementation of the Tower Number Field Sieve in which the user can choose to use the usual Schirokauer map, or our construction of a Galois Schirokauer map together with TNFS automorphisms. We demonstrate our results by applying TNFS to degree-6 and degree-12 finite fields. Our SageMath implementation is available at

`https://github.com/hal-aswad/tnfs-galois-automorphisms`

together with the complete data of our experiments (polynomials, TNFS parameters…). All computations are carried out using SageMath version 10.8. We emphasize that our implementation is not optimized. In fact, all presented examples in this section can be solved with elementary algorithms. The goal of our implementation is twofold. First, it shows that our theoretical findings work and allow us to compute discrete logarithms. Second, it demonstrates the 6-fold and 12-fold reductions in the size of the matrix in TNFS brought by our work. These results are presented in Table 9. Regardless of whether automorphisms are used, no example works with the setup ($n = 12$, $\eta = 3$, $\kappa = 4$). Our explanation is that the sieve dimension, which is $2\eta = 6$, is too small given that the characteristic size is small. To make such examples work, it is necessary to consider sieve elements with degree larger than 1 over $\mathcal{H}$, which is not supported by our code, or to increase the characteristic size, thus reaching values that are beyond what SageMath can handle in a reasonable amount of time.

$\mathbb{F}_{p^n}$	bitsize of p^n	Setup: (η, κ)	(Matrix dimension), rank	
			Without automorphism	**Our work**
$\mathbb{F}_{29^6}$	30	$(2, 3)$	$(34686 \times 24006), 23334$	$(5849 \times 4001),\ 3878$
$\mathbb{F}_{37^6}$	32	$(3, 2)$	$(1177 \times 510), 502$	$(202 \times 85),\ 81$
$\mathbb{F}_{53^6}$	35	$(2, 3)$	*	$(15580 \times 9874),\ 9666$
$\mathbb{F}_{17^{12}}$	50	$(4, 3)$	$(86934 \times 23196), 22647$	$(7311 \times 1936),\ 1874$
$\mathbb{F}_{53^{12}}$	69	$(4, 3)$	*	$(22674 \times 15469),\ 15291$

Table 9: Experimental results. Comparison of the matrix size depending on whether TNFS automorphisms (of orders 6 and 12) are used. A * indicates that SageMath killed the computation because of the large matrix size. The complete data of these computations are provided in the git repository.

$\mathbb{F}_{p^n}$	h	μ	g_0	g_1	f_2
$\mathbb{F}_{29^6}$	Φ_3	x^2+1	x^3-3x-1	x^2+x	$12g_0-g_1$
$\mathbb{F}_{37^6}$	x^3-x^2-2x+1	x^2+1	x^2+1	x	$6g_0-g_1$
$\mathbb{F}_{53^6}$	Φ_3	x^2+1	x^3-3x-1	x^2+x	$9g_0-5g_1$
$\mathbb{F}_{17^{12}}$	Φ_{10}	x^2+4	x^3-3x-1	x^2+x	$2g_0-g_1$
$\mathbb{F}_{53^{12}}$	Φ_{10}	x^2+1	x^3-3x-1	x^2+x	$9g_0-5g_1$

Table 10: Additional data for Table 9 (f_1 is always $\mathrm{Res}(\mu(y), g_0 - yg_1)$).

Polynomial selection. For $n = 6, 12$, to compute discrete logarithms in $\mathbb{F}_{p^n}$, the polynomials must be selected with the Conjugation method presented in §2.1 and Table 4. This ensures the presence of an order-n TNFS automorphism as proved by Proposition 28. Moreover, the polynomials must be chosen with the constraints on the number of real roots of Theorem 30a. The choice of the polynomials is done by the method `polyselect` in `tnfs.py`. The user must set adequate polynomials $(h, f_1, \mu \dots)$ in the method `set_from_family`. Our choices are reproduced in Table 10.

Relation collection. We use the special-q technique to collect relations [31]. Only one special-q ideal is considered per orbit. Thereafter, if the automorphisms are not used in the code, we simulate their "non-use" by expanding each relation into n conjugate relations, which is done with the method `expand_list_phi`. If the automorphisms are used, we do not expand the relations and proceed to the next step. This is carried out by the method `relation_collection` in `tnfs.py`.

Linear algebra. We construct the GSM as in Definition 16 and Remark 20. Then, via matrix multiplication in our code, we replace each set of n conjugate columns by one column, and remove the columns corresponding to prime ideals fixed by a power of the automorphism, as explained in §5.4. Consequently, the number of columns is reduced by a factor slightly larger than n and the

number of rows by a factor of n. We have not implemented the Wiedemann algorithm in SageMath. Instead, we use SageMath functions to solve the linear system and check that we obtain a virtual logarithm map as expected. Therefore, we only compare the sizes of the matrices depending on whether the order-n TNFS automorphism is exploited or not. Table 9 presents the matrix sizes on several finite fields of degree 6 and 12. In the `tnfs.py` file, the method `relation_matrices` constructs the matrix of relations, and the methods `linear_algebra` and `modified_linear_algebra` find a kernel element of the matrix. The first applies when the automorphisms are not used, and the second when they are used. Integrating the GSM constructions in the CADO-NFS software [1] and modifying the linear algebra to deal with the matrix decomposition in the basis ζ explained in §5.4 is left for future work.

Final step: verification. While we do not implement the *individual logarithm* step—as our work does not improve it—we ensure the consistency of the virtual logarithm map computed by our linear algebra step. This is achieved by considering numerous sieve elements ϕ in one of the two middle number fields that correspond to relations from previous steps. Subsequently, we confirm that their virtual logarithms correspond to the logarithms, in some basis ξ, of their projection to the finite field. This is done as follows.

We choose ξ as a generator of the subgroup of order ℓ of the finite field's multiplicative group. For each considered ϕ, we compute on the one hand its virtual logarithm $\mathrm{vlog}\,\phi$ using the output of our algorithm, and on the other hand its logarithm $\log_\xi(\phi)$ in the basis ξ using the logarithm function implemented in SageMath. We then verify that the quotient $(\mathrm{vlog}\,\phi)/\log_\xi(\phi) \bmod \ell$ is consistent for several dozen choices of ϕ. The function `log_consistency_check` within `tnfs.py` does this verification.

Furthermore, to illustrate a complete computation, we implement the individual logarithm step and compute the discrete logarithms of ten randomly selected elements in each of the fields $\mathbb{F}_{37^6}$ and $\mathbb{F}_{17^{12}}$ with respect to ξ. The resulting values are verified by raising ξ to the computed logarithms.

7.1 Running a discrete logarithm computation

In the following, B, q_0, and q_1 denote respectively the smoothness bound, the smallest special-q prime, and the largest special-q prime used. In each special-q lattice, the search for relations is carried out in a ball of dimension $2 \times \eta$ and radius `rad`. The radius is set according to the input E so that the total size of the search space is approximately the size of the hypercube $[-E, E]^{2\cdot\eta}$. See `tnfs.py` for the exact expression of `rad`. Moreover, in some of the computations, a *line-sieve* is used to factor all elements ϕ with coefficient sizes bounded by the parameter E_l. This allows one to find relations that do not involve any prime ideal within the special-q range.

The user can run a computation with the `play_tnfs.sage` script. The variable `attempt` selects the parameters of the example that is run. The boolean `use_auto` determines whether TNFS automorphism are used, and the integer d

must be set according to Proposition 18 (i.e., $d = 1$ when $n = 6$, and $d = 2$ when $n = 12$).

8 Proof of Proposition 2

Let $j : \Gamma \to \mathcal{I}$ be the map that takes an element to the principal ideal it generates. Let c be the class number of $\mathcal{K}$, which is coprime to ℓ by Assumption 1. The Dirichlet-Chevalley-Hasse unit theorem [21, Theorem 8.2] states that $\Gamma \simeq \mu_{\mathcal{K}} \times \mathcal{O}^\times \times j(\Gamma)$ and that $j(\Gamma) \subset \mathcal{I}$ is a free abelian group. Therefore, Γ/Γ^ℓ, as well as $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell$ and $\mathcal{I}/\mathcal{I}^\ell$, are all finite-dimensional $\mathbb{F}_\ell$-vector spaces.

We prove that we have the following exact sequence and that it splits:

$$1 \longrightarrow \mathcal{O}^\times/(\mathcal{O}^\times)^\ell \xrightarrow{i} \Gamma/\Gamma^\ell \xrightarrow{j} \mathcal{I}/\mathcal{I}^\ell \longrightarrow 1.$$

In the following, an element x is written $\overline{x}$ when considered modulo ℓ-th powers.

The morphism i is injective. Consider $x \in \mathcal{O}^\times$ such that $i(\overline{x}) = \overline{1}$. That is, there exists $\gamma \in \Gamma$ such that $x\gamma^\ell = 1$. We deduce $\gamma^\ell = x^{-1}$, which is an algebraic integer. Let $P(X)$ be a monic polynomial with integer coefficients such that $P(\gamma^\ell) = 0$. Then $P(X^\ell)$ is a monic polynomial with integer coefficients vanishing on γ, so $\gamma \in \mathcal{O}$. Furthermore, γ belongs to $\mathcal{O}^\times$ since $\gamma(x\gamma^{\ell-1}) = 1$. In conclusion, we have $x \equiv 1 \pmod{(\mathcal{O}^\times)^\ell}$.

The morphism j is surjective. The morphism j maps $\gamma \bmod \Gamma^\ell$ to $(\gamma) \bmod \mathcal{I}^\ell$. It is clearly well defined; let us prove its surjectivity. Let $a, b \in \mathbb{Z}$ be such that $ac + b\ell = 1$. Consider $I \in \mathcal{I}$. We have

$$I = I^{ac+b\ell} = (I^a)^c (I^b)^\ell,$$

which implies $I \equiv (I^a)^c \pmod{\mathcal{I}^\ell}$. By definition of the class number, there exists $\gamma \in \Gamma$ such that $(I^a)^c = (\gamma)$, and therefore, $j(\overline{\gamma}) \equiv I \pmod{\mathcal{I}^\ell}$.

The sequence is exact. It remains to prove that $\mathrm{Im}(i) = \mathrm{Ker}(j)$. We clearly have the direct inclusion. For the other inclusion, let $\overline{\gamma} \in \mathrm{Ker}(j)$, and let $\gamma \in \Gamma$ be any representative of $\overline{\gamma}$. There exists $I \in \mathcal{I}$ such that $(\gamma) = I^\ell$, which means that I^ℓ is the identity element in the class group. Since ℓ is coprime to the class number, then I is the identity element in the class group as well, and so is I^{-1}. Therefore, there exists $\gamma' \in \Gamma$ such that $I^{-1} = (\gamma')$. Consequently, $(\gamma\gamma'^\ell) = I^\ell I^{-\ell} = \mathcal{O}$, which implies that $\gamma\gamma'^\ell \in \mathcal{O}^\times$. Since $\gamma\gamma'^\ell = (\gamma\gamma'^{\ell-1})\gamma'$, γ' is also a unit and so $\overline{\gamma}$ belongs to $\mathcal{O}^\times/(\mathcal{O}^\times)^\ell = \mathrm{Im}(i)$.

The sequence splits. For each ideal $I \in \mathcal{F}$, let $\gamma_I \in \Gamma$ be a generator of I^c. Since $\mathcal{F}$ generates $\mathcal{I}$, we can extend γ homomorphically to $\mathcal{I}$. Recall Bézout's identity $ac + b\ell = 1$ with $a, b \in \mathbb{Z}$ and define the section $s : \mathcal{I}/\mathcal{I}^\ell \to \Gamma/\Gamma^\ell$ as $s(\overline{I}) = \overline{\gamma_I^a}$. The morphism s is clearly well defined. Further, for all $\overline{I} \in \mathcal{I}/\mathcal{I}^\ell$, we have $j(s(\overline{I})) = j(\overline{\gamma_I^a}) = \overline{(\gamma_I^a)} = \overline{I^{ac}} = \overline{I}$. Therefore, $j \circ s = \mathrm{Id}$, and the sequence splits.

It remains to prove the basis statement. Since ℓ is coprime to $|\mu_{\mathcal{K}}|$, the quotient $\mu_{\mathcal{K}}/\mu_{\mathcal{K}}^\ell$ is trivial. Furthermore, we have the following vector space isomorphism

$$\mathcal{O}^\times/(\mathcal{O}^\times)^\ell \simeq (\mathbb{Z}/\ell\mathbb{Z})^r,$$

thus proving the unique representation of units modulo $(\mathcal{O}^\times)^\ell$ in a system of fundamental units. The unique representation of ideals within $\mathcal{I}/\mathcal{I}^\ell$ in the set $\mathcal{F}/\mathcal{F}^\ell$ directly results from the unique factorization of ideals.

Acknowledgements This work was supported by the PEPR project ANR-PECY-22-0010 "Cryptanalyse".

References

1. The CADO-NFS Development Team. CADO-NFS, An Implementation of the Number Field Sieve Algorithm, `https://cado-nfs.inria.fr/`, development version of January 2026
2. Al Aswad, H., Pierrot, C.: Individual discrete logarithm with sublattice reduction. Des. Codes Cryptogr. pp. 1–33 (2023). `https://doi.org/10.1007/s10623-023-01282-w`
3. Barbulescu, R., Gaudry, P., Guillevic, A., Morain, F.: Improving NFS for the discrete logarithm problem in non-prime finite fields. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part I. LNCS, vol. 9056, pp. 129–155. Springer, Berlin, Heidelberg (Apr 2015). `https://doi.org/10.1007/978-3-662-46800-5_6`
4. Barbulescu, R., Gaudry, P., Joux, A., Thomé, E.: A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 1–16. Springer, Berlin, Heidelberg (May 2014). `https://doi.org/10.1007/978-3-642-55220-5_1`
5. Barbulescu, R.: How to get rid of units (2015), `https://www.lix.polytechnique.fr/~guillevic/catrel-workshop/Razvan_Barbulescu_CATRELworkshop.pdf`, workshop slides
6. Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: Security in Communication Networks. vol. 2576, pp. 257–267. Springer (2002). `https://doi.org/10.1007/3-540-36413-7_19`
7. Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. SIAM J. Comput. **32**(3), 586–615 (2003). `https://doi.org/10.1137/S0097539701398521`
8. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Berlin, Heidelberg (Dec 2001). `https://doi.org/10.1007/3-540-45682-1_30`
9. Boudot, F., Gaudry, P., Guillevic, A., Heninger, N., Thomé, E., Zimmermann, P.: Comparing the difficulty of factorization and discrete logarithm: A 240-digit experiment. In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020, Part II. LNCS, vol. 12171, pp. 62–91. Springer, Cham (Aug 2020). `https://doi.org/10.1007/978-3-030-56880-1_3`
10. Coppersmith, D.: Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm. Math. Comp. **62**(205), 333–350 (1994). `https://doi.org/10.1090/S0025-5718-1994-1192970-7`
11. De Micheli, G., Gaudry, P., Pierrot, C.: Lattice enumeration for tower NFS: A 521-bit discrete logarithm computation. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part I. LNCS, vol. 13090, pp. 67–96. Springer, Cham (Dec 2021). `https://doi.org/10.1007/978-3-030-92062-3_3`
12. De Micheli, G., Gaudry, P., Pierrot, C.: Lattice enumeration and automorphisms for tower NFS: A 521-bit discrete logarithm computation. Journal of Cryptology **37**(1), 6 (Jan 2024). `https://doi.org/10.1007/s00145-023-09487-x`

13. Gaudry, P., Guillevic, A., Morain, F.: Discrete logarithm record in GF(p^3) of 592 bits (180 decimal digits) (2016), https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;ae418648.1608
14. Gordon, D.M.: Discrete logarithms in GF(p) using the number field sieve. SIAM J. Discret. Math. **6**(1), 124–138 (1993). https://doi.org/10.1137/0406010
15. Granger, R., Kleinjung, T., Zumbrägel, J.: On the discrete logarithm problem in finite fields of fixed characteristic. Transactions of the American Mathematical Society **370**(5), 3129–3145 (2018). https://doi.org/10.1090/tran/7027
16. Grémy, L., Guillevic, A., Morain, F., Thomé, E.: Computing discrete logarithms in $\mathbb{F}_{p^6}$. In: Adams, C., Camenisch, J. (eds.) SAC 2017. LNCS, vol. 10719, pp. 85–105. Springer, Cham (Aug 2017). https://doi.org/10.1007/978-3-319-72565-9_5
17. Guillevic, A.: Computing individual discrete logarithms faster in GF(p^n) with the NFS-DL algorithm. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part I. LNCS, vol. 9452, pp. 149–173. Springer, Berlin, Heidelberg (Nov / Dec 2015). https://doi.org/10.1007/978-3-662-48797-6_7
18. Guillevic, A.: Faster individual discrete logarithms in finite fields of composite extension degree. Math. Comp. **88**(317), 1273–1301 (2019). https://doi.org/10.1090/mcom/3376
19. Guillevic, A.: Selection de polynômes pour TNFS (Oct 2025), https://people.rennes.inria.fr/Aurore.Guillevic//talks/25-10-09-Versailles.pdf, seminar slides
20. Hayasaka, K., Aoki, K., Kobayashi, T., Takagi, T.: An experiment of number field sieve for discrete logarithm problem over GF(p^n). JSIAM Letters **6**, 53–56 (2014). https://doi.org/10.14495/jsiaml.6.53
21. Janusz, G.J.: Algebraic number fields, Grad. Stud. Math., vol. 7. Amer. Math. Soc., 2nd edn. (1996)
22. Joux, A.: A one round protocol for tripartite Diffie–Hellman. Journal of Cryptology **17**(4), 263–276 (Sep 2004). https://doi.org/10.1007/s00145-004-0312-y
23. Joux, A., Lercier, R., Smart, N., Vercauteren, F.: The number field sieve in the medium prime case. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 326–344. Springer, Berlin, Heidelberg (Aug 2006). https://doi.org/10.1007/11818175_19
24. Kim, T., Barbulescu, R.: Extended tower number field sieve: A new complexity for the medium prime case. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 543–571. Springer, Berlin, Heidelberg (Aug 2016). https://doi.org/10.1007/978-3-662-53018-4_20
25. Kim, T., Jeong, J.: Extended tower number field sieve with application to finite fields of arbitrary composite extension degree. In: Fehr, S. (ed.) PKC 2017, Part I. LNCS, vol. 10174, pp. 388–408. Springer, Berlin, Heidelberg (Mar 2017). https://doi.org/10.1007/978-3-662-54365-8_16
26. Kleinjung, T., Wesolowski, B.: Discrete logarithms in quasi-polynomial time in finite fields of fixed characteristic. Journal of the American Mathematical Society **35**, 581–624 (2022). https://doi.org/10.1090/jams/985
27. McGuire, G., Robinson, O.: Lattice Sieving in Three Dimensions for Discrete Log in Medium Characteristic. Journal of Mathematical Cryptology **15**(1), 223 – 236 (2021). https://doi.org/10.1515/jmc-2020-0008
28. Menezes, A., Okamoto, T., Vanstone, S.A.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory **39**(5), 1639–1646 (1993). https://doi.org/10.1109/18.259647

29. Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **84**, 1234–1243 (2001). https://doi.org/10119/4432
30. Pierrot, C.: The multiple number field sieve with conjugation and generalized Joux-Lercier methods. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part I. LNCS, vol. 9056, pp. 156–170. Springer, Berlin, Heidelberg (Apr 2015). https://doi.org/10.1007/978-3-662-46800-5_7
31. Pollard, J.M.: The lattice sieve. In: Lenstra, A.K., Lenstra, Jr., H.W. (eds.) The development of the number field sieve. Lecture Notes in Math., vol. 1554, pp. 43–49. Springer–Verlag (1993). https://doi.org/doi.org/10.1007/BFb0091538
32. Robinson, O.: An implementation of the extended tower number field sieve using 4d sieving in a box and a record computation in $\mathbb{F}_{p^4}$. arXiv preprint 2212.04999 (2022). https://doi.org/10.48550/arXiv.2212.04999
33. Sarkar, P., Singh, S.: New complexity trade-offs for the (multiple) number field sieve algorithm in non-prime fields. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 429–458. Springer, Berlin, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49890-3_17
34. Sarkar, P., Singh, S.: A unified polynomial selection method for the (tower) number field sieve algorithm. Adv. Math. Commun. **13**(3), 435–455 (2019). https://doi.org/10.3934/amc.2019028
35. Schirokauer, O.: Discrete logarithms and local units. Philosophical Transactions of the Royal Society of London. Series A: Physical and Engineering Sciences **345**(1676), 409–423 (1993). https://doi.org/10.1098/rsta.1993.0139
36. Thomé, E.: Théorie algorithmique des nombres et applications à la cryptanalyse de primitives cryptographiques. Habilitation thesis, Université de Lorraine (Dec 2012), https://theses.hal.science/tel-00765982
37. Wiedemann, D.: Solving sparse linear equations over finite fields. IEEE Trans. Inform. Theory **32**(1), 54–62 (1986). https://doi.org/10.1109/TIT.1986.1057137
38. Zhu, Y., Liu, J.: Constructing CM fields for NFS to accelerate DL computation in non-prime finite fields. IEEE Trans. Inform. Theory **69**(6), 4045–4055 (2023). https://doi.org/10.1109/TIT.2023.3244631