ON CODES AND LEARNING WITH ERRORS OVER FUNCTION FIELDS

MAXIME BOMBAR [1,2], ALAIN COUVREUR [2,1], AND THOMAS DEBRIS–ALAZARD [2,1]

Abstract. It is a long standing open problem to find search to decision reductions for structured versions of the decoding problem of linear codes. Such results in the lattice-based setting have been carried out using number fields: Polynomial–LWE, Ring–LWE, Module–LWE and so on. We propose a function field version of the LWE problem. This new framework leads to another point of view on structured codes, *e.g.* quasi-cyclic codes, strengthening the connection between lattice-based and code-based cryptography. In particular, we obtain the first search to decision reduction for structured codes. Following the historical constructions in lattice–based cryptography, we instantiate our construction with function fields analogues of cyclotomic fields, namely *Carlitz* extensions, leading to search to decision reductions on various versions of Ring-LPN, which have applications to secure multi party computation and to an authentication protocol.

Key words: Code-based cryptography · Search to decision reductions · LWE · Function fields · Carlitz modules

1. Introduction

Code-based cryptography. Error correcting codes are well known to provide quantum resistant cryptographic primitives such as authentication protocols [Ste93; Hey+12], signatures [CFS01; DST19] or encryption schemes such as McEliece [McE78]. These code-based cryptosystems were built to rely on the following hard problem: finding a close (or far away) codeword to a given word, a task called *decoding*. In the case of random linear codes of length n, which is the standard case, this problem can be expressed as follows. First, we are given a vector space $\mathcal{C}$ (*i.e.* the code) of $\mathbb{F}_q^n$ generated by the rows of some random matrix $\mathbf{G} \in \mathbb{F}_q^{k\times n}$, namely:

$$\mathcal{C} \stackrel{\text{def}}{=} \{\mathbf{mG} \mid \mathbf{m} \in \mathbb{F}_q^k\}. \tag{1}$$

[1] Laboratoire LIX, École Polytechnique, Institut Polytechnique de Paris, 1 rue Honoré d'Estienne d'Orves, 91120 Palaiseau Cedex

[2] Inria

E-mail addresses: maxime.bombar@inria.fr, alain.couvreur@inria.fr, thomas.debris@inria.fr.

This work was funded by the French Agence Nationale de la Recherche through ANR JCJC COLA (ANR-21-CE39-0011), ANR BARRACUDA (ANR-21-CE39-0009-BARRACUDA) and *Plan France 2030* (ANR-22-PETQ-0008).

The decoding problem corresponds, given $\mathbf{G}$ (in other words $\mathcal{C}$) and some noisy codeword $\mathbf{mG}+\mathbf{e}$ where the number of non-zero coordinates of $\mathbf{e}$ is equal to t (its Hamming weight is $|\mathbf{e}| = t$), to find the error $\mathbf{e}$ or what amounts to the same, the original codeword $\mathbf{mG}$.

Usually this decoding problem is considered in the regime where the code rate $R \stackrel{\text{def}}{=} \frac{k}{n}$ is fixed, but there are also other interesting parameters for cryptographic applications. For instance, the Learning Parity with Noise problem (LPN) corresponds to the decoding problem where n is the number of samples, k the length of the secret while the error is sampled according to a Bernoulli distribution of fixed rate t/n. As the number of samples in LPN is unlimited, this problem actually corresponds to decoding a random code of rate arbitrarily close to 0.

While the security of many code-based cryptosystems relies on the hardness of the decoding problem, it can also be based on finding a "short" codeword for the Hamming metric (as in [Mis+12] or in [App+17; Bra+19; Yu+19] to build collision resistant hash functions). It turns out that decoding and finding short codewords are closely related. It has been shown in [DRT21] (following the original quantum reduction of Regev in the lattice/LWE case [Reg05]) that decoding some code $\mathcal{C}$ is quantumly-harder than finding a short codeword in its dual $\mathcal{C}^\perp$ (for the standard inner product in $\mathbb{F}_q^n$). A reduction from decoding to the problem of finding short codewords is also known but in an LPN context [App+17; Bra+19; Yu+19].

Despite the promising approach of McEliece, there are two drawbacks if one follows it to design a cryptosystem. First, the public data in McEliece is a representation of a code which has to look like random. Assuming this pseudo-randomness property, the security relies on the hardness of the decoding problem. In that case one needs to publish $\Omega(n^2)$ bits but at the same time, best generic decoding algorithms have a complexity exponential in the number t of errors to correct. Therefore, to reach a security level of 2^λ, the public data are of order $\Theta(\lambda^2)$ if $t = \Theta(n)$ or even worse of the order $\Theta(\lambda^4)$ if $t = \Theta(\sqrt{n})$. On the other hand, in McEliece-like cryptosystems, the owner of the secret key has to know an efficient decoding algorithm for the public code. It turns out that codes for which we know an efficient decoding algorithm are obtained via polynomial evaluations (*e.g.* Goppa codes) or short vectors (*e.g.* MDPC codes). Thus, the owner of the secret key has to hide the peculiar description of the code he publishes. It leads to the fact that in McEliece-like cryptosystems, the security also relies on the difficulty to distinguish the code that is made public from a random one. This is a second assumption to make in addition to the hardness of the decoding problem.

Alekhnovich cryptosystem. In 2003, Alekhnovich [Ale03] introduced a new approach to design an encryption scheme based on error correcting codes. Unlike McEliece cryptosystem, Alekhnovich truly relies on the hardness of decoding random codes. It starts from a random code $\mathcal{C}$ and proceeds as follows:

- *Key Generation.* Let $\mathbf{e}_{\mathsf{sk}} \in \mathbb{F}_2^n$ of small Hamming weight. The public key is $(\mathcal{C}, \mathbf{c} + \mathbf{e}_{\mathsf{sk}})$ where $\mathbf{c} \in \mathcal{C}$ and the secret key is $\mathbf{e}_{\mathsf{sk}}$.

- *Encryption.* To encrypt one bit $\beta \in \{0,1\}$ set:
  - $\mathsf{Enc}(1) \stackrel{\text{def}}{=} \mathbf{u}$ where $\mathbf{u} \in \mathbb{F}_2^n$ is a uniformly random vector.
  - $\mathsf{Enc}(0) \stackrel{\text{def}}{=} \mathbf{c}^* + \mathbf{e}$ where $\mathbf{e}$ is of small Hamming weight and $\mathbf{c}^*$ lies in the dual of the code $\mathcal{C}_{\mathsf{pub}}$ spanned by $\mathcal{C}$ and $\mathbf{c} + \mathbf{e}_{\mathsf{sk}}$.

- *Decryption.* The decryption of $\mathsf{Enc}(\beta)$ is $\langle \mathsf{Enc}(\beta), \mathbf{e}_{\mathsf{sk}} \rangle$, where $\langle \cdot, \cdot \rangle$ is the usual inner product on $\mathbb{F}_2^n$.

The correction of this procedure relies on the fact that

$$\langle \mathsf{Enc}(0), \mathbf{e}_{\mathsf{sk}} \rangle = \langle \mathbf{c}^* + \mathbf{e}, \mathbf{e}_{\mathsf{sk}} \rangle = \langle \mathbf{e}, \mathbf{e}_{\mathsf{sk}} \rangle,$$

where we used that $\mathbf{e}_{\mathsf{sk}} \in \mathcal{C}_{\mathsf{pub}}$ while $\mathbf{c}^*$ lies in its dual. Now, this inner product is equal to 0 with overwhelming probability as $\mathbf{e}_{\mathsf{sk}}$ and $\mathbf{e}$ are of small Hamming weight. On the other hand, $\langle \mathsf{Enc}(1), \mathbf{e}_{\mathsf{sk}} \rangle$ is a uniformly random bit.

Therefore, contrary to McEliece cryptosystem, the security of Alekhnovich scheme does not depend on hiding the description of a code:

- *Key security.* Recovering the private key from public data amounts to decoding the random code $\mathcal{C}$, or finding a short vector in the code spanned by $\mathcal{C}$ and $\mathbf{c} + \mathbf{e}_{\mathsf{sk}}$.
- *Message security.* Recovering the plaintext from the ciphertext is tantamount to *distinguishing* a noisy codeword from a uniformly random vector.

The message security relies on the *decision* version of the decoding problem. Search and decision versions of the decoding problem are known to be computationally equivalent using Goldreich-Levin theorem [FS96]. However, Alekhnovich cryptosystem suffers from major drawbacks:

(1) Encrypting one bit amounts to sending n bits;
(2) The public key size is quadratic in the length of ciphertexts.

While the first issue can easily be addressed, the second flaw needs more work, and as is, Alekhnovich cryptosystem is not practical. However, the approach itself was a major breakthrough in code-based cryptography. It was inspired by the work of Ajtai and Dwork [AD97] whose cryptosystem is based on solving hard lattice problems. The latter reference from Ajtai and Dwork is also the inspiration of Regev famous Learning With Errors (LWE) problem [Reg05], which is at the origin of an impressive line of work. As Alekhnovich cryptosystem, the original LWE cryptosystem was not practical either and, to address this issue, structured versions were proposed, for instance Polynomial-LWE [Ste+09], Ring–LWE [LPR10], Module–LWE [LS15].

Structured decoding problem. In the same fashion, for code–based public key encryptions, it has been proposed to restrict to codes that can be represented more compactly to reduce the key sizes. In McEliece setting, the story begins in 2005 with the results of [Gab05] that suggest to use ℓ–quasi-cyclic codes, *i.e.* codes that are generated by a matrix $\mathbf{G}$ formed out of ℓ blocks:

$$\mathbf{G} = \begin{pmatrix} \mathbf{rot}\left(\mathbf{a}^{(1)}\right) & \cdots & \mathbf{rot}\left(\mathbf{a}^{(\ell)}\right) \end{pmatrix}, \tag{2}$$

each block being a circulant matrix, *i.e.* of the form

$$\mathbf{rot}(\mathbf{a}) \stackrel{\text{def}}{=} \begin{pmatrix} a_0 & a_1 & \dots & \dots & a_{k-1} \\ a_{k-1} & a_0 & \dots & \dots & a_{k-2} \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_{k-1} & a_0 \end{pmatrix} \text{ with } \mathbf{a} \in \mathbb{F}_q^k.$$

The key point is that such codes have a large automorphism group G, and instead of publishing a whole basis, one can only publish a generating set for the $\mathbb{F}_q[G]$–module structure of the code. That is to say, a family of vectors whose orbit under the action of G spans the code. For instance, in the case of quasi-cyclic codes (2), one can publish only the first row of the ℓ-circulant generator matrix. It can be argued that the quasi–cyclicity could be used to improve the speed-up of generic decoding, but the best known approach in the generic case uses DOOM [Sen11] which allows to divide the complexity of decoding by at most $\sqrt{\#G}$, the latter complexity remaining exponential with the same exponent. Hence, one can keep the same security parameter, while the size of the public key can be divided by a factor $O(\#G)$.

This idea leads to very efficient encryption schemes such as BIKE [Agu+21a], in the McEliece fashion, or HQC [Agu+21b] which is closer to Ring–LWE. Both proposals use 2-quasi-cyclic codes and have been selected to the third round of NIST competition as alternate candidates. Other structured variants of the decoding problem (referred to as Ring–LPN) were also proposed with applications to authentication [Hey+12] or secure MPC [Boy+20]. Note that the idea to use codes equipped with a non trivial ring action has also been used in rank metric [Ara+19; Agu+19].

In other words, the security of those cryptosystems now rely on some structured variant of the decoding problem.

A Polynomial representation. It turns out that a convenient way of seeing ℓ-quasi-cyclic codes, is to represent blocks of their generator matrix as elements of the quotient ring $\mathbb{F}_q[X]/(X^n-1)$, via the $\mathbb{F}_q$–isomorphism:

$$\begin{cases} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[X]/(X^n-1) \\ \mathbf{a} \stackrel{\text{def}}{=} (a_0, \ldots, a_{n-1}) & \longmapsto & \mathbf{a}(X) \stackrel{\text{def}}{=} \sum_{i=0}^{n-1} a_i X^i. \end{cases}$$

A simple computation shows that the product of two elements of $\mathbb{F}_q[X]/(X^n-1)$ can be represented with the operator $\mathbf{rot}(\cdot)$:

$$\mathbf{u}(X)\mathbf{v}(X) \mod (X^n-1) = \mathbf{u} \cdot \mathbf{rot}(\mathbf{v}) = \mathbf{v} \cdot \mathbf{rot}(\mathbf{u}) = \mathbf{v}(X)\mathbf{u}(X) \mod (X^n-1).$$

From now on, $\mathbf{u}$ can denote either a vector of $\mathbb{F}_q^n$ or a polynomial in $\mathbb{F}_q[X]/(X^n-1)$, and the product of two elements $\mathbf{uv}$ is defined as above.

Consider an ℓ-quasi-cyclic code with a generator matrix $\mathbf{G}$ in ℓ-circulant form. Let $\mathbf{s} \in \mathbb{F}_q^n$ be a secret word of the ambient space and let $\mathbf{e} \in \mathbb{F}_q^{\ell n}$ be an error vector. Under the above map, the noisy codeword $\mathbf{sG}+\mathbf{e}$ is represented by ℓ samples of the form $\mathbf{sa}^{(j)}+\mathbf{e}^{(j)} \in \mathbb{F}_q[X]/(X^n-1)$ and the decoding problem of ℓ-circulant codes corresponds to recovering the secret $\mathbf{s}$ given ℓ samples. This can be seen as a code analogue of the Ring–LWE problem, with access to a fixed number of samples ℓ. The rate of the code is $\frac{1}{\ell}$, so increasing the number of samples corresponds to decode a code whose rate goes to 0.

A natural generalization would be to consider multiple rows of circulant blocks. In this situation, the generator matrix $\mathbf{G}$ is of the form

$$\mathbf{G} = \begin{pmatrix} \mathbf{rot}(\mathbf{a}^{(1,1)}) & \cdots & \mathbf{rot}(\mathbf{a}^{(1,\ell)}) \\ \vdots & & \vdots \\ \mathbf{rot}(\mathbf{a}^{(m,1)}) & \cdots & \mathbf{rot}(\mathbf{a}^{(m,\ell)}) \end{pmatrix}$$

and a noisy codeword $\mathbf{sG}+\mathbf{e}$ is now represented by ℓ samples of the form

$$\sum_{i=1}^{m} \mathbf{s}_i \mathbf{a}^{(i,j)} + \mathbf{e}_j \in \mathbb{F}_q[X]/(X^n-1)$$

where $\mathbf{s}$ can be considered as a collection of m secrets $\mathbf{s}_1, \ldots, \mathbf{s}_m$. This would be the code analogue of Module–LWE, with a rank m module and ℓ samples, introduced in [LS15].

Contrary to structured lattice cryptosystems, up to now, no reduction from the search to the decision version of the structured decoding problem was known. This was pointed out by NIST [Ala+20], and was a reason for those code-based cryptosystems to be only considered as alternate candidates for the third round. Actually even before NIST standardization process, this lack of search to decision reduction was already pointed out by the authors of the Ring–LPN based authentication scheme Lapin [Hey+12].

Our contribution. To handle this lack of search to decision reduction in the code setting, we propose in this article a new generic problem called FF–DP, for *Function Field Decoding Problem*, in the Ring–LWE fashion. One of the key ideas consists in using function fields instead of number fields, the latter being used in the lattice case. This framework enables us to adapt directly the search to decision reduction of [LPR10] in the case of codes. Frequently in the literature on Ring–LWE, the search to decision reduction is instantiated with cyclotomic number fields. In the same spirit we present an instantiation with function fields analogues of cyclotomic fields, namely the so-called *Carlitz extensions*. As we show, this framework is for instance enough to provide a search to decision reduction useful in the context of Lapin [Hey+12] or for a q–ary analogue of Ring–LPN used for secure multiparty computation [Boy+20]. If our reduction does not work for every schemes based on structured codes such as HQC, we believe that our work paves the way towards a full reduction.

Remark 1.1. Note that the use of function fields in coding theory is far from being new. Since the early 80's and the seminal work of Goppa [Gop81], it is well–known that codes called *Algebraic Geometry* (AG) codes can be constructed from algebraic curves or equivalently from function fields and that some of these codes have better asymptotic parameters than random ones [TVZ82]. However, the way they are used in the present work is completely different. Indeed, AG codes are a natural generalization of Reed–Solomon and, in particular, are codes benefiting from efficient decoding algorithms (see for instance surveys [HP95; BH08; CR21]). In the present article, the approach is somehow orthogonal to the AG codes setting since we use function fields in order to introduce generic problems related to structured codes for which the decoding problem is supposed to be hard.

A function field approach. Lattice-based cryptography has a long standing history of using number fields and their rings of integers to add some structure and reduce the key sizes. Recall that number fields are algebraic extensions of $\mathbb{Q}$ of the form

$$K \stackrel{\text{def}}{=} \mathbb{Q}[X]/(f(X)),$$

where f is an irreducible polynomial, and the ring of integers $\mathscr{O}_K$ is the integral closure of $\mathbb{Z}$ in K, *i.e.* it is the subring of K composed of elements which are roots of monic polynomials with coefficients in $\mathbb{Z}$. For instance, cyclotomic extensions are of the form $K = \mathbb{Q}(\zeta_m) = \mathbb{Q}[X]/(\Phi_m(X))$ where ζ_m is a primitive m-th root of unity and Φ_m is the m-th cyclotomic polynomial. The ring of cyclotomic integers has a very specific form, namely $\mathscr{O}_K = \mathbb{Z}[\zeta_m]$. One of the most used case is when m is a power of 2. In this case, setting $m = 2n$, we have $\Phi_m = \Phi_{2n} = X^n + 1$ and $\mathscr{O}_K = \mathbb{Z}[X]/(X^n + 1)$. Such rings have been widely used since they benefit from a very fast arithmetic thanks to the fast Fourier transform. In the Ring–LWE setting, one reduces all the samples modulo a large prime element $q \in \mathbb{Z}$ called the *modulus* and hence considers the ring $(\mathbb{Z}/q\mathbb{Z})[X]/(X^n + 1)$. Due to inherent considerations of the Euclidean metric, errors are drawn according to a *continuous* distribution (e.g a Gaussian distribution) χ over the Euclidean space $K \otimes_{\mathbb{Q}} \mathbb{R} = \mathbb{R}[X]/(X^n + 1)$ and one has to introduce a technical tool called *smoothing parameter* to handle the *discrete* error distributions used in practice. It should be noted that an equivalent of the smoothing parameter will not be necessary in our case because our error model will remain discrete.

When moving from structured lattices to structured codes, it would be tantalizing to consider the ring $\mathbb{F}_q[X]/(X^n - 1)$ as the analogue of $\mathbb{Z}[X]/(X^n + 1)$. However, if the two rings have a similar expression they have a fundamental difference. Note for instance that the former is finite while the latter is infinite. From a more algebraic point of view, $\mathbb{F}_q[X]/(X^n - 1)$ is said to have *Krull dimension* 0 while $\mathbb{Z}[X]/(X^n + 1)$ has *Krull dimension* 1. In particular, the former has only a finite number of ideals while the latter has infinitely many prime ideals. The main idea of the present article is to lift the decoding problem and to see $\mathbb{F}_q[X]/(X^n - 1)$ as a quotient R/I of some ring R of Krull dimension 1. The ideal I will be the analogue of the *modulus*. This setting can be achieved using so-called *function fields*. It could be argued that the results of this article could have been obtained without introducing function fields. However, we claim that function fields are crucial for at least three reasons:

(1) Introducing function fields permits to establish a strong connection between cryptography based on structured lattices involving number fields on the one hand and cryptography based on structured codes on the other hand.
(2) Number theory has a rich history with almost one hundred years of development of the theory of function fields. We expect that, as number fields did for structured lattices, function fields will yield a remarkable toolbox to study structured codes and cryptographic questions related to them.
(3) A third and more technical evidence is that a crucial part of the search to decision reduction involves some Galois action. We claim that, even if for a specific instantiation, this group action could have been described in a pedestrian way on the finite ring $\mathbb{F}_q[X]/(X^n - 1)$, without knowing the context of function fields, such a group action would really look like "a rabbit pulled out of a hat". In short, this group action, which is crucial to conclude the

search to decision reduction, cannot appear to be something natural without considering function fields.

It is well–known for a long time that there is a noticeable analogy between the theory of number fields and that of function fields. Starting from the ground, the rings $\mathbb{Z}$ and $\mathbb{F}_q[T]$ share a lot of common features. For instance, they both have an Euclidean division. Now if one considers their respective fraction fields $\mathbb{Q}$ and $\mathbb{F}_q(T)$, finite extensions of $\mathbb{Q}$ yield the number fields while finite separable extensions of $\mathbb{F}_q(T)$ are called *function fields* because they are also the fields of rational functions on curves over finite fields. Now, a similar arithmetic theory can be developed for both with rings of integers, orders, places and so on. Both rings of integers are *Dedekind domains*. In particular, every ideal factorizes uniquely into a product of prime ideals, and the quotient by any non-zero ideal is always finite. A dictionary summarizing this analogy between number fields and function fields is represented in Table 1. Note that actually, many properties that are known for function fields are only conjectures for number fields. The best example is probably the Riemann hypothesis which has been proved by Weil in the early 1940s in the function field case.

Number fields	Function fields
$\mathbb{Q}$	$\mathbb{F}_q(T)$
$\mathbb{Z}$	$\mathbb{F}_q[T]$
Prime numbers $q \in \mathbb{Z}$	Irreducible polynomials $Q \in \mathbb{F}_q[T]$
$K = \mathbb{Q}[X]/(f(X))$	$K = \mathbb{F}_q(T)[X]/(f(T,X))$
$\mathscr{O}_K$ = Integral closure of $\mathbb{Z}$ *Dedekind* domain	$\mathscr{O}_K$ = Integral closure of $\mathbb{F}_q[T]$ *Dedekind* domain
characteristic 0	**characteristic > 0**

TABLE 1. The Number Field-Function Field Analogy

With this analogy in hand, the idea is to find a nice function field K with ring of integers $\mathscr{O}_K$ and an irreducible polynomial $Q \in \mathbb{F}_q[T]$, called the *modulus*, such that $\mathscr{O}_K/Q\mathscr{O}_K = \mathbb{F}_q[X]/(X^n - 1)$. Following the path of [LPR10], we are able to provide a search to decision reduction for our generic problem FF–DP when three conditions hold:

(1) The function field K is Galois.
(2) The modulus Q does not ramify in $\mathscr{O}_K$, meaning that the ideal $Q\mathscr{O}_K$ factorizes in product of distinct prime ideals.
(3) The distribution of errors is invariant under the action of the Galois group.

This framework is enough to provide a search to decision reduction useful in the context of LAPIN [Hey+12] or for a q–ary analogue of Ring–LPN used for secure MPC [Boy+20]. It should be emphasized that, in the case of LAPIN, the search to decision reduction requires to adapt the definition of the noise which will remain built by applying independent Bernouilli variables but with a peculiar choice of $\mathbb{F}_2$–basis of the underlying ring $\mathbb{F}_2[X]/(f(X))$. The chosen basis is a *normal* basis, *i.e.* is globally invariant with respect to the Galois action. This change of basis is very similar to the one performed in lattice based-cryptography when, instead of considering the monomial basis $1, X, \ldots, X^{n-1}$ in an order $\mathbb{Z}[X]/(f(X))$, one considers the canonical basis after applying the Minkowski embedding. Indeed, the latter is Galois invariant. We emphasize that, here again, the function field point of view brings in a Galois action which cannot appear when only considering a ring such as $\mathbb{F}_2[X]/(f(X))$. This is another evidence of the need for introducing function fields.

Outline of the article. The present article is organised as follows. Section 2 recalls the necessary background about function fields (definitions and important properties). In Section 3 we present

the FF–DP problem (search and decision versions) as well as our main theorem (Theorem 3.10) which states the search to decision reduction in the function field setting. A proof of this theorem is given in Section 4. A reader only interested about the framework of functions fields and our instantiations can safely skip this section. In Section 5 we give a self contain presentation of Carlitz extensions. They will be used to instantiate our search to decision reduction in Section 6, which provides our applications.

2. Prerequisites on function fields

In this section, we list the minimal basic notions on the arithmetic of function fields that are needed in the sequel. A dictionary drawing the analogies has been given in Table 1. For further references on the arithmetic of function fields, we refer the reader to [Sti09; Ros02].

Starting from a finite field $\mathbb{F}_q$, *a function field* is a finite extension K of $\mathbb{F}_q(T)$ of degree $n > 0$ of the form

$$K = \mathbb{F}_q(T)[X]/(P(T, X))$$

where $P(T, X) \in \mathbb{F}_q(T)[X]$ is irreducible of degree n. The field $K \cap \overline{\mathbb{F}}_q$ is referred to as *the field of constants* or *constant field* of K, where $\overline{\mathbb{F}}_q$ is the algebraic closure of $\mathbb{F}_q$. In the sequel, we will assume that $\mathbb{F}_q$ is the full field of constants of K, which is equivalent for $P(T, X)$ to be irreducible even regarded as a an element of $\overline{\mathbb{F}}_q(T)[X]$ ([Sti09, Cor. 3.6.8]).

Similarly to the number field case, one can define the ring of integers $\mathscr{O}_K$ as the the ring of elements of K which are the roots of a monic polynomial in $\mathbb{F}_q[T][X]$. This ring is a *Dedekind domain*. In particular, any ideal $\mathfrak{P}$ has a unique decomposition $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ where the $\mathfrak{P}_i$'s are prime ideals.

In the sequel, we frequently focus on the following setting represented in the diagram below: starting from a prime ideal $\mathfrak{p}$ of $\mathbb{F}_q[T]$ (which is nothing but the ideal generated by an irreducible polynomial $Q(T)$ of $\mathbb{F}_q[T]$), we consider the ideal $\mathfrak{P} \stackrel{\text{def}}{=} \mathfrak{p}\mathscr{O}_K$ and its decomposition:

$$\mathfrak{P} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}.$$

$$\begin{array}{ccc} \mathfrak{P} \subset \mathscr{O}_K & \longrightarrow & K \\ \big| & & \big| \\ \mathfrak{p} \subset \mathbb{F}_q[T] & \longrightarrow & \mathbb{F}_q(T) \end{array}$$

The prime ideals $\mathfrak{P}_i$'s are said to *lie above* $\mathfrak{p}$. The exponents e_i's are referred to as the *ramification indexes*, and the extension is said to be *unramified* at $\mathfrak{P}$ when all the e_i's are equal to 1. Another important constant related to a $\mathfrak{P}_i$ is its *inertia degree*, which is defined as the extension degree $f_i \stackrel{\text{def}}{=} [\mathscr{O}_K/\mathfrak{P}_i : \mathbb{F}_q[T]/\mathfrak{p}]$ (one can prove that $\mathscr{O}_K/\mathfrak{P}_i$ and $\mathbb{F}_q[T]/\mathfrak{p}$ are both finite fields). The Chinese Remainder Theorem (CRT) induces a ring isomorphism between $\mathscr{O}_K/\mathfrak{P}$ and $\prod_{i=1}^r \mathscr{O}_K/\mathfrak{P}_i^{e_i}$. In particular, when the extension is unramified at $\mathfrak{P}$, the quotient $\mathscr{O}_K/\mathfrak{P}$ is a product of finite fields. Finally, a well-known result asserts that

$$n = [K : \mathbb{F}_q(T)] = \sum_{i=1}^{r} e_i f_i. \tag{3}$$

Finite Galois extensions. Recall that a finite algebraic field extension L/K is said to be a *Galois extension* when the automorphism group

$$\mathrm{Aut}(L/K) \stackrel{\text{def}}{=} \{\sigma \colon L \to L \mid \sigma \text{ is an isomorphism with } \sigma(a) = a \text{ for all } a \in K\}$$

has cardinality $[L : K]$. In that case, we refer to $\mathrm{Aut}(L/K)$ as the *Galois group* of L/K and write $\mathrm{Gal}(L/K) \stackrel{\text{def}}{=} \mathrm{Aut}(L/K)$. Galois extensions whose Galois group is abelian are called *abelian extensions*. Galois extensions have many properties that do not hold in general field extensions.

When L/K is a Galois extension, and if H is a subgroup of $G \stackrel{\text{def}}{=} \mathrm{Gal}(L/K)$, then the set

$$L^H \stackrel{\text{def}}{=} \{a \in L \mid \sigma(a) = a \text{ for all } \sigma \in H\}$$

is a field called the *fixed field* of H. By definition $L^G = K$. Furthermore, the extension L/L^H is Galois with Galois group H. On the other hand, the extension L^H/K may not be Galois in general, but it is the case when H is a normal subgroup of G, and $\mathrm{Gal}(L^H/L) = G/H$. This is particularly true when L is an abelian extension. Consider $K/\mathbb{F}_q(T)$ a Galois function field (*i.e.* a function field K which is a Galois extension of $\mathbb{F}_q(T)$), with Galois group $G \stackrel{\text{def}}{=} \mathrm{Gal}(K/\mathbb{F}_q(T))$. Then, G keeps $\mathscr{O}_K$ globally invariant. Furthermore, given $\mathfrak{p}$ a prime ideal of $\mathbb{F}_q[T]$, the group G acts transitively on the set $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$ of prime ideals of $\mathscr{O}_K$ lying above $\mathfrak{p}$: for any $i \neq j$ there exists $\sigma \in \mathrm{Gal}(K/\mathbb{F}_q(T))$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. In particular, all the ramification indexes e_i (*resp.* the inertia degrees f_i) are equal and denoted by e (*resp.* f): $\mathfrak{P} \stackrel{\text{def}}{=} \mathfrak{p}\mathscr{O}_K = (\mathfrak{P}_1 \ldots \mathfrak{P}_r)^e$ and (3) becomes $n = efr$. Another consequence which will be crucial for the applications, is that the action of G on $\mathscr{O}_K$ is well–defined on $\mathscr{O}_K/\mathfrak{P}$ and simply permutes factors $\mathscr{O}_K/\mathfrak{P}_i^e$. The *decomposition group* of $\mathfrak{P}_i$ over $\mathfrak{p}$ is

$$D_{\mathfrak{P}_i/\mathfrak{p}} \stackrel{\text{def}}{=} \{\sigma \in G \mid \sigma(\mathfrak{P}_i) = \mathfrak{P}_i\}.$$

It has cardinality $e \times f$. In particular, when K is unramified at $\mathfrak{P}$, the field $\mathscr{O}_K/\mathfrak{P}_i$ is $\mathbb{F}_{q^{f \deg(\mathfrak{p})}}$ and the action of $D_{\mathfrak{P}_i/\mathfrak{p}}$ on it is the Frobenius automorphism: the reduction modulo $\mathfrak{P}_i$ yields an isomorphism

$$D_{\mathfrak{P}_i/\mathfrak{p}} \simeq \mathrm{Gal}(\mathbb{F}_{q^{f \deg(\mathfrak{p})}}/\mathbb{F}_{q^{\deg(\mathfrak{p})}}). \tag{4}$$

Finally, all the decomposition groups of primes above $\mathfrak{p}$ are conjugate: for any $i \neq j$ there exists $\sigma \in G$ such that $D_{\mathfrak{P}_i/\mathfrak{p}} = \sigma D_{\mathfrak{P}_j/\mathfrak{p}} \sigma^{-1}$.

3. A function field approach for search to decision reduction

Search and decision problems. In this section, we introduce a new generic problem that we call FF–DP, which is the analogue of Ring–LWE in the context of function fields. Then, we give our main theorem which states the search-to-decision reduction of FF–DP. Since function fields and number fields share many properties, the present search to decision reduction, that is proven in Section 4, will work similarly as in [LPR10].

Consider a function field $K/\mathbb{F}_q(T)$ with constant field $\mathbb{F}_q$ and ring of integers $\mathscr{O}_K$ and let $Q(T) \in \mathbb{F}_q[T]$. Let $\mathfrak{P} \stackrel{\text{def}}{=} Q\mathscr{O}_K$ be the ideal of $\mathscr{O}_K$ generated by Q. Recall that $\mathscr{O}_K/\mathfrak{P}$ is a finite set. FF–DP is parameterized by an element $\mathbf{s} \in \mathscr{O}_K/\mathfrak{P}$ called the *secret* and ψ be a probability distribution over $\mathscr{O}_K/\mathfrak{P}$ called the *error distribution*.

Definition 3.1 (FF–DP Distribution)**.** *A sample $(\mathbf{a}, \mathbf{b}) \in \mathscr{O}_K/\mathfrak{P} \times \mathscr{O}_K/\mathfrak{P}$ is distributed according to the* FF–DP *distribution modulo $\mathfrak{P}$ with secret $\mathbf{s}$ and error distribution ψ if*

- *$\mathbf{a}$ is uniformly distributed over $\mathscr{O}_K/\mathfrak{P}$,*
- *$\mathbf{b} = \mathbf{as} + \mathbf{e} \in \mathscr{O}_K/\mathfrak{P}$ where $\mathbf{e}$ is distributed according to ψ.*

A sample drawn according to this distribution will be denoted by $(\mathbf{a}, \mathbf{b}) \leftarrow \mathscr{F}_{\mathbf{s},\psi}$.

The aim of the search version of the FF–DP problem is to recover the secret $\mathbf{s}$ given samples drawn from $\mathscr{F}_{\mathbf{s},\psi}$. This is formalized in the following problem.

Problem 3.2 (FF–DP, Search version)**.** *Let $\mathbf{s} \in \mathscr{O}_K/\mathfrak{P}$, and let ψ be a probability distribution over $\mathscr{O}_K/\mathfrak{P}$. An instance of* FF–DP *problem consists in an oracle giving access to independent samples $(\mathbf{a}, \mathbf{b}) \leftarrow \mathscr{F}_{\mathbf{s},\psi}$. The goal is to recover $\mathbf{s}$.*

Remark 3.3. This problem should be related to structured versions of the decoding problem. Indeed, recall from the discussion in the introduction that, using the polynomial representation, the decoding problem of random quasi-cyclic codes corresponds to recovering a secret polynomial $\mathbf{s}(X) \in \mathbb{F}_q[X]/(X^n - 1)$ given access to samples of the form $\mathbf{as} + \mathbf{e} \in \mathbb{F}_q[X]/(X^n - 1)$ where $\mathbf{a}$ is uniformly distributed in $\mathbb{F}_q[X]/(X^n - 1)$. This can be rephrased within the FF–DP framework as follows. Consider the polynomial $f(T, X) \stackrel{\text{def}}{=} X^n + T - 1 \in \mathbb{F}_q(T)[X]$. When n is not divisible by the

characteristic of $\mathbb{F}_q$, f is a separable polynomial. Moreover, by Eisenstein criterion f is irreducible. Define the function field K generated by f, namely the extension $K \stackrel{\text{def}}{=} \mathbb{F}_q(T)[X]/(f(T,X))$. One can prove that $\mathscr{O}_K$ is exactly $\mathbb{F}_q[T][X]/(f(T,X))$. Now, let $\mathfrak{p}$ be the ideal of $\mathbb{F}_q[T]$ defined by the irreducible polynomial T, and let $\mathfrak{P} \stackrel{\text{def}}{=} \mathfrak{p}\mathscr{O}_K = T\mathscr{O}_K$ be the corresponding ideal of $\mathscr{O}_K$. Then the following isomorphisms hold

$$\mathscr{O}_K/\mathfrak{P} \simeq \mathbb{F}_q[T,X]/(T, X^n + T - 1) \simeq \mathbb{F}_q[X]/(X^n - 1).$$

With this particular instantiation, $\mathscr{O}_K/\mathfrak{P}$ is exactly the ambient space from which the samples are defined in the structured versions of the decoding problem. As a consequence, FF–DP is a generalization of structured versions of the decoding problem, when considering arbitrary function fields and ideals.

For cryptographic applications, we are also interested in the *decision* version of this problem. The goal is now to distinguish between the FF–DP distribution and the uniform distribution over $\mathscr{O}_K/\mathfrak{P} \times \mathscr{O}_K/\mathfrak{P}$.

Problem 3.4 (FF–DP, Decision version)**.** *Let* $\mathbf{s}$ *be drawn uniformly at random in* $\mathscr{O}_K/\mathfrak{P}$ *and let* ψ *be a probability distribution over* $\mathscr{O}_K/\mathfrak{P}$*. Define* $\mathcal{D}_0$ *to be the uniform distribution over* $\mathscr{O}_K/\mathfrak{P} \times \mathscr{O}_K/\mathfrak{P}$*, and* $\mathcal{D}_1$ *to be the* FF–DP *distribution with secret* $\mathbf{s}$ *and error distribution* ψ*. Furthermore, let* b *be a uniform element of* $\{0,1\}$*. Given access to an oracle* $\mathcal{O}_b$ *providing samples from distribution* $\mathcal{D}_b$*, the goal of the decision* FF–DP *is to recover* b*.*

Remark 3.5. For some applications, for instance to MPC, it is more convenient to have the secret $\mathbf{s}$ drawn from the error distribution ψ instead of the uniform distribution over $\mathscr{O}_K/\mathfrak{P}$. In the lattice-based setting, this version is sometimes called LWE with *short secret* or LWE in *Hermite normal form*. However, both decision problems are easily proved to be computationally equivalent, see [Lyu11, Lemma 3]. The proof applies directly to FF–DP.

A *distinguisher* between two distributions $\mathcal{D}_0$ and $\mathcal{D}_1$ is a probabilistic polynomial time (PPT) algorithm $\mathcal{A}$ that takes as input an oracle $\mathcal{O}_b$ corresponding to a distribution $\mathcal{D}_b$ with $b \in \{0,1\}$ and outputs an element $\mathcal{A}(\mathcal{O}_b) \in \{0,1\}$. Consider the following approach for solving a decision problem between two distributions $\mathcal{D}_0$ and $\mathcal{D}_1$, pick $b \leftarrow \{0,1\}$ and answer b regardless of the input. This algorithm solves this problem with probability $1/2$ which is not interesting. The efficiency of an algorithm $\mathcal{A}$ solving a decision problem is measured by the difference between its probability of success and $1/2$. The relevant quantity to consider is the *advantage* defined as:

$$\mathrm{Adv}_{\mathcal{A}}(\mathcal{D}_0, \mathcal{D}_1) \stackrel{\text{def}}{=} \frac{1}{2}\left(\mathbb{P}(\mathcal{A}(\mathcal{O}_b) = 1 \mid b = 1) - \mathbb{P}(\mathcal{A}(\mathcal{O}_b) = 1 \mid b = 0)\right)$$

where the probabilities are computed over the internal randomness of $\mathcal{A}$, a uniform $b \in \{0,1\}$ and inputs according to a distribution $\mathcal{D}_b$. The advantage of a distinguisher $\mathcal{A}$ measures how good it is to solve a distinguishing problem. Indeed, it is classical fact that:

$$\mathbb{P}(\mathcal{A}(\mathcal{O}_b) = b) = \frac{1}{2} + \mathrm{Adv}_{\mathcal{A}}(\mathcal{D}_0, \mathcal{D}_1).$$

Remark 3.6. Even if it means answering $1 - \mathcal{A}(\mathcal{O}_b)$ instead of $\mathcal{A}(\mathcal{O}_b)$, the advantage can always be assumed to be a positive quantity.

A module version. Instead of considering one secret $\mathbf{s} \in \mathscr{O}_K/\mathfrak{P}$, we could use multiple secrets $(\mathbf{s}_1, \ldots, \mathbf{s}_d) \in (\mathscr{O}_K/\mathfrak{P})^d$. This generalization has been considered in lattice-based cryptography under the terminology Module-LWE [LS15], where the secret can be thought as an element of $\mathscr{O}_K^d$ which is a free $\mathscr{O}_K$-module of rank d, before a reduction modulo $\mathfrak{P}$ on each component. This would yield the following definition.

Definition 3.7 (MFF–DP Distribution)**.** *Let* $d \geqslant 1$ *be an integer. A sample* $(\mathbf{a}, \mathbf{b}) \in (\mathscr{O}_K/\mathfrak{P})^d \times \mathscr{O}_K/\mathfrak{P}$ *is distributed according to the* MFF–DP *distribution modulo* $\mathfrak{P}$ *with secret* $\mathbf{s} \stackrel{def}{=} (\mathbf{s}_1, \ldots, \mathbf{s}_d) \in (\mathscr{O}_K/\mathfrak{P})^d$ *and error distribution* ψ *over* $\mathscr{O}_K/\mathfrak{P}$ *if*

- $\mathbf{a}$ *is uniformly distributed over* $(\mathscr{O}_K/\mathfrak{P})^d$*,*

- $\mathbf{b} = \sum_{i=1}^{d} \mathbf{a}_i \mathbf{s}_i + \mathbf{e} \in \mathscr{O}_K/\mathfrak{P}$ *where* $\mathbf{e}$ *is distributed according to* ψ.

The search and decision problems associated to MFF–DP can be defined as a natural generalization of Problems 3.2 and 3.4.

Problem 3.8 (MFF–DP, Search version)**.** *Let* $\mathbf{s} \in (\mathscr{O}_K/\mathfrak{P})^d$ *be a collection of elements of* $\mathscr{O}_K/\mathfrak{P}$ *called the secrets, and let* ψ *be a probability distribution over* $\mathscr{O}_K/\mathfrak{P}$*. An instance of the* MFF–DP *problem consists in an oracle giving access to independent samples* $(\mathbf{a}, \mathbf{b})$ *from the* MFF–DP *distribution with secrets* $\mathbf{s}$ *and error distribution* ψ*. The goal is to recover* $\mathbf{s}$*.*

Problem 3.9 (MFF–DP, Decision version)**.** *Let* $\mathbf{s}$ *be drawn uniformly at random in* $(\mathscr{O}_K/\mathfrak{P})^d$ *and let* ψ *be a probability distribution over* $\mathscr{O}_K/\mathfrak{P}$*. Define* $\mathcal{D}_0$ *to be the uniform distribution over* $(\mathscr{O}_K/\mathfrak{P})^d \times \mathscr{O}_K/\mathfrak{P}$*, and* $\mathcal{D}_1$ *to be the* MFF–DP *distribution with secrets* $\mathbf{s}$ *and error distribution* ψ*. Furthermore, let* b *be a uniform element of* $\{0, 1\}$*. Given access to an oracle* $\mathcal{O}_b$ *providing samples from distribution* $\mathcal{D}_b$*, the goal of the decision* MFF–DP *is to recover* b*.*

Search to decision reduction. There is an obvious reduction from the decision to the search version of FF–DP. Indeed, if there exists an algorithm $\mathcal{A}$ that given access to the $\mathscr{F}_{\mathbf{s},\psi}$ distribution is able to recover the secret $\mathbf{s}$, then it yields to a distinguisher between $\mathscr{F}_{\mathbf{s},\psi}$ and the uniform distribution. The converse reduction needs more work. However, due to the strong analogy between function and number fields, our proof is in fact essentially the same as in [LPR10; Lyu11]. More precisely, we have the following theorem.

Theorem 3.10 (Search to decision reduction for FF–DP)**.** *Let* $K/\mathbb{F}_q(T)$ *be a Galois function field of degree* n *with field of constants* $\mathbb{F}_q$*, and denote by* $\mathscr{O}_K$ *its ring of integers. Let* $Q(T) \in \mathbb{F}_q[T]$ *be an irreducible polynomial. Consider the ideal* $\mathfrak{P} \stackrel{def}{=} Q\mathscr{O}_K$*. Assume that* $\mathfrak{P}$ *does not ramify in* $\mathscr{O}_K$*, and denote by* f *its inertia degree. Let* ψ *be a probability distribution over* $\mathscr{O}_K/\mathfrak{P}$*, closed under the action of* $\mathrm{Gal}(K/\mathbb{F}_q(T))$*, meaning that if* $\mathbf{e} \leftarrow \psi$*, then for any* $\sigma \in \mathrm{Gal}(K/\mathbb{F}_q(T))$*, we have* $\sigma(\mathbf{e}) \leftarrow \psi$*. Let* $\mathbf{s} \in \mathscr{O}_K/\mathfrak{P}$*.*

Suppose that we have an access to $\mathscr{F}_{\mathbf{s},\psi}$ *and there exists a distinguisher between the uniform distribution over* $\mathscr{O}_K/\mathfrak{P}$ *and the* FF–DP *distribution with uniform secret and error distribution* ψ*, running in time* t *and having an advantage* ε*. Then there exists an algorithm that recovers* $\mathbf{s} \in \mathscr{O}_K/\mathfrak{P}$ *(with an overwhelming probability in* n*) in time*

$$O\left(\frac{n^4}{f^3} \times \frac{1}{\varepsilon^2} \times q^{f \deg(Q)} \times t\right).$$

Remark 3.11. We have assumed implicitly in the statement of the theorem that we have an efficient access to the Galois group of $K/\mathbb{F}_q(T)$ and its action can be computed in polynomial time.

Remark 3.12. There are many degrees of freedom in the previous statement: choice of the function field K (and on the degree n), choice of the polynomial Q (and on f and $\deg(Q)$). For our instantiations, we will often choose the "modulus" Q to be a linear polynomial ($\deg(Q) = 1$) and K will be a (subfield of) a cyclotomic function field.

Remark 3.13. Due to the continuity of error distributions used in lattice-based cryptography, a technical tool called the *smoothing parameter* was introduced by Micciancio and Regev in [MR04]. It characterizes how a Gaussian distribution is close to uniform, both modulo the lattice, and is ubiquitously used in reductions. However, in the function field setting, we do not need to introduce such a tool because the error distribution is discrete and already defined on the quotient $\mathscr{O}_K/\mathfrak{P}$.

Remark 3.14. In [LS15], Langlois and Stehlé proved a search to decision reduction for the module version of LWE. The idea is to use the distinguisher in order to retrieve the secrets one by one. Their proof applies *mutatis mutandis* to MFF–DP, resulting in a time overhead of d, where d denotes the rank of the underlying module, *i.e.* the number of secrets. The main change is in the *guess and search* step (Step 3 in the proof presented in Section 4) where the randomization is applied on only one component of $\mathbf{a}$ to recover one secret, and repeating the process d times (one for each secret). More precisely, for MFF–DP, the running time claimed in Theorem 3.10 should

be replaced with

$$O\left(d \times \frac{n^4}{f^3} \times \frac{1}{\varepsilon^2} \times q^{f \deg(Q)} \times t\right).$$

4. Search to Decision Reductions: Proof of Theorem 3.10

In this section, we give a proof of Theorem 3.10. It is very similar to the one for Ring-LWE and lattices. It uses four steps that we describe. Combining them provides the aforementioned result. The main line of proof is as follows. We use an hybrid argument to reduce the search domain, and then proceed to an exhaustive search using the distinguisher to recover $\mathbf{s}$ modulo all the factors of $\mathfrak{P}$. Finally, using the Chinese Remainder Theorem (CRT) one can recover $\mathbf{s}$ completely. The key point here is the action of the Galois group on the primes and that the error distribution is Galois invariant.

Let $\mathfrak{P} = \mathfrak{P}_1 \dots \mathfrak{P}_r$ be the decomposition of $\mathfrak{P}$, we have

$$r = n/f$$

where we used the assumptions over $\mathfrak{P}$ and $K/\mathbb{F}_q(T)$ made in Theorem 3.10, namely that $K/\mathbb{F}_q(T)$ is a Galois extension of degree n and unramified at $\mathfrak{P}$ with inertia degree f.

Step 1: Worst to Average Case. Recall that in the definition of Problem 3.4 the secret $\mathbf{s}$ is supposed to be *uniformly* distributed over $\mathscr{O}_K/\mathfrak{P}$, while in the search version the secret is *fixed*. In other words, the decision problem is somehow an *average* case problem, while the search version should work in *any* case. Fortunately, this can easily be addressed by randomizing the secret. Indeed, for any sample $(\mathbf{a}, \mathbf{b}) \leftarrow \mathscr{F}_{\mathbf{s},\psi}$ with fixed secret $\mathbf{s}$, if $\mathbf{s}' \leftarrow \mathscr{O}_K/\mathfrak{P}$, then $(\mathbf{a}, \mathbf{b} + \mathbf{a}\mathbf{s}')$ is now a sample from $\mathscr{F}_{\mathbf{s}+\mathbf{s}',\psi}$ with secret $\mathbf{s} + \mathbf{s}'$ uniformly distributed over $\mathscr{O}_K/\mathfrak{P}$.

Step 2: Hybrid argument. Let $\mathcal{A}$ be the distinguisher between the uniform distribution over $\mathscr{O}_K/\mathfrak{P}$ and the FF–DP distribution with uniform secret and error distribution ψ, running in time t and having an advantage ε. We use a simple hybrid argument to prove that $\mathcal{A}$ can also distinguish in time t between two consecutive *hybrid* distributions with advantage at least ε/r.

The factorization of $\mathfrak{P}$ is $\mathfrak{P}_1 \dots \mathfrak{P}_r$. A sample $(\mathbf{a}, \mathbf{b})$ is said to be distributed according to the hybrid distribution $\mathcal{H}_i$ if it is of the form $(\mathbf{a}', \mathbf{b}' + \mathbf{h})$ where $(\mathbf{a}', \mathbf{b}') \leftarrow \mathscr{F}_{\mathbf{s},\psi}$ and $\mathbf{h} \in \mathscr{O}_K/\mathfrak{P}$ is uniformly distributed modulo $\mathfrak{P}_j$ for $j \leqslant i$ and $\mathbf{0}$ modulo the other factors. Such an $\mathbf{h}$ can easily be constructed using the Chinese Remainder Theorem. In particular, for $i = 0$, $\mathbf{h}$ is $\mathbf{0}$ modulo all the factors of $\mathfrak{P}$, therefore $\mathbf{h} = \mathbf{0}$ and $\mathcal{H}_0 = \mathscr{F}_{\mathbf{s},\psi}$. On the other hand, when $i = r$, the element $\mathbf{h}$ is uniformly distributed over $\mathscr{O}_K/\mathfrak{P}$, therefore $\mathcal{H}_r$ is *exactly* the uniform distribution over $\mathscr{O}_K/\mathfrak{P}$.

Lemma 4.1 (Hybrid argument)**.** *There exists* i_0 *such that* $\mathrm{Adv}_{\mathcal{A}}(\mathcal{H}_{i_0}, \mathcal{H}_{i_0+1}) \geqslant \frac{\varepsilon}{r}$.

Proof. By definition, $\mathrm{Adv}_{\mathcal{A}}(\mathcal{H}_0, \mathcal{H}_r) = \varepsilon$. Furthermore, the following equality holds:

$$\mathrm{Adv}_{\mathcal{A}}(\mathcal{H}_0, \mathcal{H}_r) = \sum_{i=0}^{r-1} \mathrm{Adv}_{\mathcal{A}}(\mathcal{H}_i, \mathcal{H}_{i+1}).$$

Therefore, it exists $i_0 \in [\![0, r-1]\!]$ such that $\mathrm{Adv}_{\mathcal{A}}(\mathcal{H}_{i_0}, \mathcal{H}_{i_0+1}) \geqslant \frac{\mathrm{Adv}_{\mathcal{A}}(\mathcal{H}_0, \mathcal{H}_r)}{r} = \frac{\varepsilon}{r}$. □

This hybrid argument has shown the existence of an i_0 such that $\mathcal{A}$ has an advantage ε/r for distinguishing distributions $\mathcal{H}_{i_0}$ and $\mathcal{H}_{i_0+1}$. In what follows, everything is analysed as if we knew this index i_0. In practice we can run $\mathcal{A}$ concurrently with all the r instances $(\mathcal{H}_i, \mathcal{H}_{i+1})$'s. Computations on the right index i_0 will output the secret $\mathbf{s}$ (which can be verified) as it will be explained afterward. Therefore, our reduction will output $\mathbf{s}$ with a "resource overhead" given by at most a factor r.

Step 3: Guess and search. Given i_0 such as in Lemma 4.1. The idea is to perform an exhaustive search in $\mathscr{O}_K/\mathfrak{P}_{i_0+1}$ and to use $\mathcal{A}$ to recover $\mathbf{s} \mod \mathfrak{P}_{i_0+1}$.

Lemma 4.2. *Let $\mathcal{A}$ be a distinguisher with advantage δ between hybrid distributions $\mathcal{H}_{i_0}$ and $\mathcal{H}_{i_0+1}$, with secret $\mathbf{s}$, running in time t. Then there exists an algorithm $\mathcal{B}$ that recovers $\mathbf{s} \mod \mathfrak{P}_{i_0+1}$ with overwhelming probability in n in time $O\left(q^{f\deg(Q)} \times \frac{n}{\delta^2} \times t\right)$.*

Proof. Our algorithm will proceed with a *guess and search* technique using the distinguisher $\mathcal{A}$ in hand. The idea is to *guess* the value of $\mathbf{s} \mod \mathfrak{P}_{i_0+1}$ and transform any sample $(\mathbf{a}, \mathbf{b}) \leftarrow \mathscr{F}_{\mathbf{s},\psi}$ into a sample of $\mathcal{H}_{i_0}$ if the guess is correct, and into a sample of $\mathcal{H}_{i_0+1}$ if the guess is incorrect.

Transformation: Let $\mathbf{g}_{i_0+1} \in \mathscr{O}_K/\mathfrak{P}_{i_0+1}$. It will be our guess for $\widehat{\mathbf{s}} \stackrel{\text{def}}{=} \mathbf{s} \mod \mathfrak{P}_{i_0+1}$. Let us consider now the following operations

- Take $\mathbf{g} \in \mathscr{O}_K/\mathfrak{P}$ such that $\mathbf{g} \equiv \mathbf{g}_{i_0+1} \mod \mathfrak{P}_{i_0+1}$ and $\mathbf{g} \equiv \mathbf{0} \mod \mathfrak{P}_j$ for $j \neq i_0+1$.
- Sample $\mathbf{h}_j \leftarrow \mathscr{O}_K/\mathfrak{P}_j$ for $1 \leqslant j \leqslant i_0$ and take $\mathbf{h} \in \mathscr{O}_K/\mathfrak{P}$ such that $\mathbf{h} \equiv \mathbf{h}_j \mod \mathfrak{P}_j$ for $1 \leqslant j \leqslant i_0$ and $\mathbf{h} \equiv \mathbf{0} \mod \mathfrak{P}_j$ for $j \geqslant i_0+1$.
- Sample $\mathbf{v}_{i_0+1} \leftarrow \mathscr{O}_K/\mathfrak{P}_{i_0+1}$ and take $\mathbf{v} \in \mathscr{O}_K/\mathfrak{P}$ such that $\mathbf{v} \equiv \mathbf{v}_{i_0+1} \mod \mathfrak{P}_{i_0+1}$ and $\mathbf{v} \equiv \mathbf{0} \mod \mathfrak{P}_j$ for $j \neq i_0+1$.

All those operations can be done via the CRT. Now, for each sample $(\mathbf{a}, \mathbf{b} \stackrel{\text{def}}{=} \mathbf{as} + \mathbf{e}) \leftarrow \mathscr{F}_{\mathbf{s},\psi}$, define $(\mathbf{a}', \mathbf{b}')$ with

$$\mathbf{a}' \stackrel{\text{def}}{=} \mathbf{a} + \mathbf{v} \quad \text{and} \quad \mathbf{b}' \stackrel{\text{def}}{=} \mathbf{b} + \mathbf{h} + \mathbf{vg}.$$

Note that for each sample $(\mathbf{a}, \mathbf{b})$, the corresponding $\mathbf{a}'$ is still uniformly distributed over $\mathscr{O}_K/\mathfrak{P}$ and $\mathbf{b}' = \mathbf{a}'\mathbf{s} + \mathbf{e} + \mathbf{h}'$ with $\mathbf{h}' \stackrel{\text{def}}{=} \mathbf{h} + (\mathbf{g} - \mathbf{s})\mathbf{v}$. Furthermore, $\mathbf{h}$ verifies:

$$\begin{cases} \mathbf{h}' \equiv \mathbf{h}_j & \mod \mathfrak{P}_j \text{ for } j \leqslant i_0 \\ \mathbf{h}' \equiv (\mathbf{g}_{i_0+1} - \widehat{\mathbf{s}})\mathbf{v}_{i_0+1} & \mod \mathfrak{P}_{i_0+1} \\ \mathbf{h}' \equiv \mathbf{0} & \mod \mathfrak{P}_j \text{ for } j > i_0+1. \end{cases}$$

In particular, $\mathbf{h}'$ is uniformly distributed modulo $\mathfrak{P}_j$ for $j \leqslant i_0$ and $\mathbf{0}$ modulo $\mathfrak{P}_j$ for $j > i_0+1$.

Now, if the guess is correct, meaning $\mathbf{g}_{i_0+1} = \widehat{\mathbf{s}}$, then $\mathbf{h}' \equiv 0 \mod \mathfrak{P}_{i_0+1}$, hence $(\mathbf{a}', \mathbf{b}')$ is distributed according to $\mathcal{H}_{i_0}$. On the other hand, if the guess is incorrect, $(\mathbf{g}_{i_0+1} - \widehat{\mathbf{s}}) \neq \mathbf{0}$ in $\mathscr{O}_K/\mathfrak{P}_{i_0+1}$. But $\mathscr{O}_K$ is a Dedekind domain and $\mathfrak{P}_{i_0+1}$ is a prime ideal, therefore it is also maximal and $\mathscr{O}_K/\mathfrak{P}_{i_0+1}$ is in fact a *field*. Since $\mathbf{v}_{i_0+1}$ is uniformly distributed in $\mathscr{O}_K/\mathfrak{P}_{i_0+1}$, so is $(\mathbf{g}_{i_0+1} - \widehat{\mathbf{s}})\mathbf{v}_{i_0+1}$. In particular, $\mathbf{h}'$ is also uniformly distributed modulo $\mathfrak{P}_{i_0+1}$. Hence, $(\mathbf{a}', \mathbf{b}')$ is distributed according to $\mathcal{H}_{i_0+1}$.

The algorithm $\mathcal{B}$ proceeds as follows: for each $(\mathbf{a}, \mathbf{b}) \leftarrow \mathscr{F}_{\mathbf{s},\psi}$, it applies the previous transformation to get a sample $(\mathbf{a}', \mathbf{b}')$, and then uses the distinguisher $\mathcal{A}$. Repeating the procedure m times (for each guess $\mathbf{g}_{i_0+1}$), for m large enough, and doing a majority voting allows to recover $\widehat{\mathbf{s}}$ with overwhelming probability. More precisely, it relies on the use of the Chernoff bound.

Proposition 4.3 (Chernoff bound)**.** *Let $(X_j)_{1 \leqslant j \leqslant m}$ be m independent Bernouilli random variables with parameter $1/2 + \delta$. Let $X \stackrel{def}{=} \sum_{j=1}^{m} X_j$. Then*

$$\mathbb{P}\left(X \leqslant \frac{m}{2}\right) \leqslant e^{-2m\delta^2}.$$

Consider m trials of the guess and search procedure, and let X_j denote the indicator random variable that the j-th run returns the correct value. Since $\mathcal{A}$ has distinguishing advantage δ, X_j is a Bernouilli with parameter $\frac{1}{2} + \delta$.

After m trials, the procedure fails if and only if more than $m/2$ runs are wrong. By Chernoff bound, the probability that it happens is less than $e^{-2m\delta^2}$. Therefore, by choosing $m \geqslant \ln(\frac{1}{\mu})\frac{1}{2\delta^2}$, the above procedure returns the correct guess with probability at least $1 - \mu$. Therefore if one sets $\mu = 2^{-\Theta(n)}$ (to get an overwhelming probability of success), it is enough to choose m as $\Theta\left(\frac{n}{\delta^2}\right)$. It enables to check if our guess $\widehat{\mathbf{s}} = \mathbf{s} \mod \mathfrak{P}_{i_0+1}$ is correct or not with overwhelming probability. To recover $\mathbf{s} \mod \mathfrak{P}_{i_0+1}$ it remains to try all the possible guesses $\widehat{\mathbf{s}} \in \mathscr{O}_K/\mathfrak{P}_{i_0+1}$. But the size of $\mathscr{O}_K/\mathfrak{P}_{i_0+1}$ is given by $q^{f\deg(Q)}$, which yields the claimed time complexity. □

Step 4: Action of the Galois group. Until Step 3, we are able to recover the secret $\mathbf{s}$ modulo one of the factors. In order to recover the full secret, we use the Galois group $G \stackrel{\text{def}}{=} \mathrm{Gal}(K/\mathbb{F}_q(T))$.

This last part is *crucial* for the reduction to work. Recall that G acts transitively on the set of prime ideals above $\mathfrak{p}$, *i.e.* for every $i \neq j$, there exists $\sigma \in G$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$.

Lemma 4.4. *Fix $\mathbf{s} \in \mathscr{O}_K/\mathfrak{P}$. Let $1 \leqslant i \leqslant r$ and let $\mathcal{A}$ be an algorithm running in time t, and recovering $\mathbf{s} \mod \mathfrak{P}_i$ by making queries to an oracle for $\mathscr{F}_{\mathbf{s},\psi}$. Then there exists an algorithm $\mathcal{B}$ running in time $O(t \times r)$ that recovers the full secret $\mathbf{s}$.*

Proof. We build $\mathcal{B}$ as follows: for every factor $\mathfrak{P}_j$ of $\mathfrak{P}$, it chooses $\sigma \in \mathrm{Gal}(K/\mathbb{F}_q(T))$ such that $\sigma(\mathfrak{P}_j) = \mathfrak{P}_i$. Then, for each sample $(\mathbf{a}, \mathbf{b}) \leftarrow \mathscr{F}_{\mathbf{s},\psi}$, it runs $\mathcal{A}$ on the input $(\sigma(\mathbf{a}), \sigma(\mathbf{b}))$ to recover an element $\mathbf{s}_j$ and stores $\sigma^{-1}(\mathbf{s}_j)$.

Note that $\mathrm{Gal}(K/\mathbb{F}_q(T))$ keeps the uniform distribution over $\mathscr{O}_K/\mathfrak{P}$. In particular, for every sample $(\mathbf{a}, \mathbf{b}) \leftarrow \mathscr{F}_{\mathbf{s},\psi}$, the corresponding $\sigma(\mathbf{a})$ is also uniformly distributed over $\mathscr{O}_K/\mathfrak{P}$. Furthermore, $\mathbf{b} = \mathbf{as} + \mathbf{e}$ with $\mathbf{e} \leftarrow \psi$. Therefore, $\sigma(\mathbf{b}) = \sigma(\mathbf{a})\sigma(\mathbf{s}) + \sigma(\mathbf{e})$. But ψ is Galois invariant by assumption, and hence $\sigma(\mathbf{e})$ is also distributed according to ψ. In particular, $(\sigma(\mathbf{a}), \sigma(\mathbf{b}))$ is a valid sample of $\mathscr{F}_{\sigma(\mathbf{s}),\psi}$.

Now, our algorithm $\mathcal{A}$ is able to recover $\mathbf{s}_j \overset{\text{def}}{=} \sigma(\mathbf{s}) \mod \mathfrak{P}_i$ in time t, and

$$\sigma^{-1}(\mathbf{s}_j) = \sigma^{-1}(\sigma(\mathbf{s}) \mod \mathfrak{P}_i) = \mathbf{s} \mod \sigma^{-1}(\mathfrak{P}_i) = \mathbf{s} \mod \mathfrak{P}_j.$$

Therefore, we are able to recover $\mathbf{s} \mod \mathfrak{P}_j$ for any $1 \leqslant j \leqslant r$. To compute the full secret $\mathbf{s}$ it remains to use the Chinese Remainder Theorem. The running time of this full procedure is given by a $O(t \times r)$ which concludes the proof. □

5. Cyclotomic Function Fields and the Carlitz Module

In Section 3, we introduced the generic problem FF–DP and noticed that our search to decision reduction given in Section 4 needed Galois function fields. In [LPR10], it was proposed to use cyclotomic number fields to instantiate the Ring–LWE problem. Here, we propose to instantiate FF–DP with the function field analogue, namely *Carlitz* extensions. We give a self contained presentation of the theory of Carlitz extensions. The interested reader can refer to [Ros02, ch. 12], [Nie01] and the excellent survey [Con] for further reference.

Carlitz extensions are function fields analogues of the cyclotomic extensions of $\mathbb{Q}$. A dictionary summarizing the similarities is given in Table 2. These extensions were discovered by Carlitz in the late 1930s but the analogy was not well known until the work of his student Hayes who studied them in [Hay74] to give an explicit construction of the abelian extensions of the rational function field $\mathbb{F}_q(T)$ and prove an analogue of the usual Kronecker-Webber theorem which states that any abelian extension of $\mathbb{Q}$ are subfields of cyclotomic number fields. This result was generalized in the following years with the work of Drinfeld and Goss to yield a complete solution to Hilbert twelfth problem in the function field setting. In the number field setting, such an explicit construction is only known for abelian extensions of $\mathbb{Q}$ (cyclotomic extensions), imaginary quadratic number fields (via the theory of elliptic curves with complex multiplication).

The first idea that comes to mind when one wants to build cyclotomic function fields is to adjoin roots of unity to the field $\mathbb{F}_q(T)$. However, roots of unity are already *algebraic* over $\mathbb{F}_q$. In other words, adding them only yields so–called *extensions of constants.*

Example 5.1. *Let ζ_n be an n–th root of unity in $\mathbb{F}_q(T)$. Note that it belongs to some* finite *extension of $\mathbb{F}_q$. Let $\mathbb{F}_{q^m}$ be the extension of $\mathbb{F}_q$ of minimal degree such that $\zeta_n \in \mathbb{F}_{q^m}$ (it can be $\mathbb{F}_q$ itself). Then*

$$\mathbb{F}_q(T)[\zeta_n] = \mathbb{F}_{q^m}(T),$$

and the field of constants of $\mathbb{F}_q(T)[\zeta_n]$ is $\mathbb{F}_{q^m}$.

However, in our reduction setting, such extensions will only increase the size of the search space in Step 3. More precisely, if K is an algebraic extension of $\mathbb{F}_q(T)$, the constant field of K is always a subfield of $\mathscr{O}_K/\mathfrak{P}$ for any prime ideal $\mathfrak{P}$ of $\mathscr{O}_K$. But recall that in our search to decision reduction, we need to do an exhaustive search in this quotient $\mathscr{O}_K/\mathfrak{P}$, so we need it to be as small as possible. Henceforth, we cannot afford constant field extensions. For Carlitz extensions, this will be ensured by Theorem 5.16.

Example 5.2. *As a matter of example, consider the polynomial* T^2+T+1 *over* $\mathbb{F}_2$*. It is irreducible. Let* $\zeta_3 \in \mathbb{F}_4$ *be one of its roots. It is a cube root of* 1*. Now, consider the field extension* $K \overset{def}{=} \mathbb{F}_2(T)(\zeta_3) = \mathbb{F}_4(T)$ *and let* $\mathscr{O}_K$ *be the integral closure of* $\mathbb{F}_2[T]$ *in* K*. The prime ideal* $\mathfrak{p} \overset{def}{=} (T^2+T+1)$ *of* $\mathbb{F}_2[T]$ *splits into two prime ideals* $\mathfrak{P}_1$ *and* $\mathfrak{P}_2$ *in* $\mathscr{O}_K$*. But* $\mathscr{O}_K/\mathfrak{P}_1 = \mathscr{O}_K/\mathfrak{P}_2 = \mathbb{F}_4 = \mathbb{F}_2[T]/\mathfrak{p}$ *and we do not win anything by considering the extension* $K/\mathbb{F}_2(T)$*.*

5.1. **Roots of unity and torsion.** As mentioned in the beginning of this section, it is not sufficient to add roots of unity. One has to go deeper into the algebraic structure that is adjoined to $\mathbb{Q}$. Indeed, the set of all m–th roots of unity, denoted by $\mu_m \subset \mathbb{C}$, turns out to be an abelian group under multiplication. Moreover, μ_m is in fact *cyclic*, generated by any *primitive* root of unity.

In commutative algebra, abelian groups are $\mathbb{Z}$-*modules*. Here the action of $\mathbb{Z}$ is given by exponentiation: $n \in \mathbb{Z}$ acts on $\zeta \in \mu_m$ by $n \cdot \zeta \overset{\text{def}}{=} \zeta^n$. This action of $\mathbb{Z}$ can in fact be extended to all $\overline{\mathbb{Q}}^\times$. When working with modules over a ring, it is very natural to consider the *torsion elements*, *i.e.* elements of the module that are annihilated by an element of the ring. The torsion elements in the $\mathbb{Z}$–module $\overline{\mathbb{Q}}^\times$ are the $\zeta \in \overline{\mathbb{Q}}^\times$ such that $\zeta^m = 1$ for some $m > 0$; these are precisely the roots of unity. In other words, the cyclotomic number fields are obtained by adjoining to $\mathbb{Q}$ torsions elements of the $\mathbb{Z}$–module $\overline{\mathbb{Q}}^\times$.

Under the analogy summed up in Table 1, replacing $\mathbb{Z}$ by $\mathbb{F}_q[T]$ and $\mathbb{Q}$ by $\mathbb{F}_q(T)$, we would like to consider some $\mathbb{F}_q[T]$–module and adjoin to $\mathbb{F}_q(T)$ the torsion elements. Note that $\mathbb{F}_q[T]$–modules are in particular $\mathbb{F}_q$–vector spaces. The natural candidate could be $\overline{\mathbb{F}_q(T)}$ with $\mathbb{F}_q[T]$ acting by multiplication. However, the torsion elements are not very interesting. Indeed if there is some $f \in \overline{\mathbb{F}_q(T)}$ and some $a \in \mathbb{F}_q[T] \setminus \{0\}$ such that $af = 0$ then, $f = 0$. Therefore, for the usual action by multiplication, only 0 is a torsion element. Thus, we need to define *another* $\mathbb{F}_q[T]$–module structure, in the same way that we did not consider the natural action of $\mathbb{Z}$ by multiplication. This new module structure can be defined using so called *Carlitz polynomials*: for each polynomial $M \in \mathbb{F}_q[T]$, we define its Carlitz polynomial $[M](X)$ as a polynomial in X with coefficients in $\mathbb{F}_q[T]$, and $M \in \mathbb{F}_q[T]$ will act on $\alpha \in \overline{\mathbb{F}_q(T)}$ by $M \cdot \alpha \overset{\text{def}}{=} [M](\alpha)$. In the literature, the notation α^M can also be found to emphasize the analogy with the action of $\mathbb{Z}$ by exponentiation, but it can be confusing. In the same way that the action of $\mathbb{Z}$ was multiplicative: $(\alpha\beta)^n = \alpha^n\beta^n$, the action of $\mathbb{F}_q[T]$ will be *additive*: $[M](\alpha+\beta) = [M](\alpha) + [M](\beta)$. In other words, $[M](X)$ should be an *additive polynomial*. In positive characteristic this can easily be achieved by considering q–polynomials, *i.e.* polynomials whose monomials are only q–th powers of X, namely of the form

$$P(X) = p_0X + p_1X^q + \cdots + p_rX^{q^r}.$$

Remark 5.3. q–polynomials with coefficients in some finite field $\mathbb{F}_{q^m}$ are also used in coding theory to build so called *rank metric codes*. However, here we consider q–polynomials with coefficients in $\mathbb{F}_q[T]$.

5.2. **Carlitz polynomials.** The definition of Carlitz polynomial will proceed by induction and linearity. Define $[1](X) \overset{\text{def}}{=} X$ and $[T](X) \overset{\text{def}}{=} X^q + TX$. For $n \geqslant 2$, define

$$[T^n](X) \overset{\text{def}}{=} [T]([T^{n-1}](X)) = [T^{n-1}](X)^q + T[T^{n-1}](X).$$

Then, for a polynomial $M = \sum_{i=0}^n a_iT^i \in \mathbb{F}_q[T]$, define $[M](X)$ by forcing $\mathbb{F}_q$–linearity:

$$[M](X) \overset{\text{def}}{=} \sum_{i=0}^n a_i[T^i](X).$$

Example 5.4. *We have,*

- $[T^2](X) = [T](X^q + TX) = X^{q^2} + (T^q + T)X^q + T^2X$
- $[T^2+T+1](X) = [T^2](X) + [T](X) + [1](X) = X^{q^2} + (T^q+T+1)X^q + (T^2+T+1)X$

By construction, Carlitz polynomials are additive polynomials, and $\mathbb{F}_q$–linear. Furthermore, for two polynomials $M, N \in \mathbb{F}_q[T]$, $[MN](X) = [M]([N](X)) = [N]([M](X))$. In particular, Carlitz polynomials commute with each other under composition law, which is not the case in general for q–polynomials.

5.3. **Carlitz module.** Endowed with this $\mathbb{F}_q[T]$–module structure, $\overline{\mathbb{F}_q(T)}$ is called the *Carlitz module*.

Definition 5.5. *For $M \in \mathbb{F}_q[T]$, $M \neq 0$, let $\Lambda_M \overset{def}{=} \{\lambda \in \overline{\mathbb{F}_q(T)} \mid [M](\lambda) = 0\}$. This is the module of M–torsion of the Carlitz module.*

Example 5.6. $\Lambda_T = \{\lambda \in \overline{\mathbb{F}_q(T)} \mid \lambda^q + T\lambda = 0\} = \{0\} \cup \{\lambda \mid \lambda^{q-1} = -T\}$.

In the same way that μ_m is an abelian group (*i.e.* a $\mathbb{Z}$–module), note that Λ_M is also a submodule of the Carlitz module: for $\lambda \in \Lambda_M$ and $A \in \mathbb{F}_q[T]$, $[A](\lambda) \in \Lambda_M$. In particular, Λ_M is an $\mathbb{F}_q$–vector space.

Example 5.7. *The module Λ_T defined in Example 5.6 is an $\mathbb{F}_q$–vector space of dimension 1. In particular, for $\lambda \in \Lambda_T$, and $A \in \mathbb{F}_q[T]$, $[A](\lambda)$ must be a multiple of λ. In fact the Carlitz action of A on λ is through the constant term of A: writing $A = TB + A(0)$ we have*

$$[A](\lambda) = [TB + A(0)](\lambda) = [B](\underbrace{[T](\lambda)}_{=0}) + A(0)[1](\lambda) = A(0)\lambda.$$

More generally, even if in general Λ_M is not of dimension 1 over $\mathbb{F}_q$, it is always a *cyclic* $\mathbb{F}_q[T]$–module: as an $\mathbb{F}_q[T]$–module it can be generated by only one element. This is specified in the following theorem.

Theorem 5.8 ([Nie01, Lemma 3.2.2])**.** *There exists $\lambda_0 \in \Lambda_M$ such that $\Lambda_M = \{[A](\lambda_0) \mid A \in \mathbb{F}_q[T]/(M)\}$ and the generators of Λ_M are the $[A](\lambda_0)$ for all A prime to M. The choice of a generator yields a non canonical isomorphism $\Lambda_M \simeq \mathbb{F}_q[T]/(M)$ as $\mathbb{F}_q[T]$–modules.*

Remark 5.9. The previous theorem needs to be related to the cyclotomic case: given the choice of a primitive m–th root of unity, there is a group isomorphism between μ_m and $\mathbb{Z}/m\mathbb{Z}$. Moreover all the m–th roots of unity are of the form ζ^k for $k \in [\![0, m-1]\!]$ and the generators of μ_m are the ζ^k for k prime to m.

5.4. **Carlitz extensions.** Recall that the cyclotomic number fields are obtained as extensions of $\mathbb{Q}$ generated by the elements of μ_m. In the similar fashion, for a polynomial $M \in \mathbb{F}_q[T]$, let

$$K_M \overset{\text{def}}{=} \mathbb{F}_q(T)(\Lambda_M) = \mathbb{F}_q(T)(\lambda_M),$$

where λ_M is a generator of Λ_M. One of the most important fact about the cyclotomic number field $\mathbb{Q}(\zeta_m)$ is that it is a finite Galois extension of $\mathbb{Q}$, with Galois group isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$. There is an analogue statement for the Carlitz extensions.

Theorem 5.10 ([Nie01, Th. 3.2.6])**.** *Let $M \in \mathbb{F}_q[T]$, $M \neq 0$. Then K_M is a finite Galois extension of $\mathbb{F}_q(T)$, with Galois group isomorphic to $(\mathbb{F}_q[T]/(M))^\times$. The isomorphism is given by*

$$\begin{cases} (\mathbb{F}_q[T]/(M))^\times & \longrightarrow & \mathrm{Gal}(K_M/\mathbb{F}_q(T)) \\ A & \longmapsto & \sigma_A, \end{cases}$$

where σ_A is completely determined by $\sigma_A(\lambda_M) = [A](\lambda_M)$.

Remark 5.11. In particular, Carlitz extensions are *abelian*.

Another important fact about cyclotomic extensions is the simple description of their ring of integers. Namely, for $K = \mathbb{Q}(\zeta_m)$, we have $\mathscr{O}_K = \mathbb{Z}[\zeta_m] = \mathbb{Z}[X]/(\Phi_m(X))$ where Φ_m denotes the m–th cyclotomic polynomial. This property also holds for Carlitz extensions.

Theorem 5.12 ([Ros02, Th. 2.9])**.** *Let $\mathscr{O}_M$ be the integral closure of $\mathbb{F}_q[T]$ in K_M. Then $\mathscr{O}_M = \mathbb{F}_q[T][\lambda_M]$. In particular, let $P(T, X) \in \mathbb{F}_q[T][X]$ be the minimal polynomial of λ_M. Then,*

$$K_M = \mathbb{F}_q(T)[X]/(P(T, X)) \quad \textit{and} \quad \mathscr{O}_M = \mathbb{F}_q[T][X]/(P(T, X)).$$

Example 5.13. *Reconsider Example 5.6 and the module* $\Lambda_T = \{0\} \cup \{\lambda \mid \lambda^{q-1} = -T\}$. *The polynomial* $X^{q-1} + T$ *is Eisenstein in* (T) *and therefore is irreducible. Hence,*

$$K_T = \mathbb{F}_q(T)[X]/(X^{q-1} + T).$$

Moreover it is Galois, with Galois group $(\mathbb{F}_q[T]/(T))^\times \simeq \mathbb{F}_q^\times$. *A non-zero element* $a \in \mathbb{F}_q^\times$ *will act on* $f(T, X) \in K_T$ *by*

$$a \cdot f(T, X) \stackrel{def}{=} f(T, [a](X)) = f(T, aX).$$

The integral closure of $\mathbb{F}_q[T]$ *in* K_T *is*

$$\mathscr{O}_T \stackrel{def}{=} \mathbb{F}_q[T][X]/(X^{q-1} + T)$$

and

$$\mathscr{O}_T/((T+1)\mathscr{O}_T) = \mathbb{F}_q[T][X]/(T+1, X^{q-1} + T) = \mathbb{F}_q[X]/(X^{q-1} - 1). \tag{5}$$

Finally, the following theorem characterizes the splitting behaviour of primes in Carlitz extensions. A very similar result holds for cyclotomic extensions.

Theorem 5.14 ([Ros02, Th. 12.10])**.** *Let* $M \in \mathbb{F}_q[T]$, $M \neq 0$, *and let* $Q \in \mathbb{F}_q[T]$ *be a monic, irreducible polynomial. Consider the Carlitz extension* K_M *and let* $\mathscr{O}_M$ *denote its ring of integers. Then,*

- *If* Q *divides* M, *then* $Q\mathscr{O}_M$ *is totally ramified.*
- *Otherwise, let* f *be the smallest integer* f *such that* $Q^f \equiv 1 \mod M$. *Then* $Q\mathscr{O}_M$ *is unramified and has inertia degree* f. *In particular,* Q *splits completely if and only if* $Q \equiv 1 \mod M$.

Note that in Ring–LWE, the prime modulus q is often chosen such that $q \equiv 1 \mod m$ so that it splits completely in the cyclotomic extension $\mathbb{Q}(\zeta_m)$.

Example 5.15. *In the previous example,* $T+1 \equiv 1 \mod T$ *and therefore* $(T+1)$ *splits completely in* $\mathscr{O}_T$. *Indeed,*

$$\mathscr{O}_T/((T+1)\mathscr{O}_T) = \mathbb{F}_q[X]/(X^{q-1} - 1) = \prod_{\alpha \in \mathbb{F}_q^\times} \mathbb{F}_q[X]/(X - \alpha)$$

is a product of $q - 1$ *copies of* $\mathbb{F}_q$.

It is crucial for the applications that the constant field of K be not too big because, in the search–to–decision reduction, it determines the search space in Step 3 of the proof of Theorem 3.10. The following non-trivial theorem gives the field of constants of Carlitz extensions.

Theorem 5.16 ([Ros02, Cor. of Th. 12.14])**.** *Let* $M \in \mathbb{F}_q[T]$, $M \neq 0$. *Then* $\mathbb{F}_q$ *is the full* constant field *of* K_M.

The similarities between Carlitz function fields and cyclotomic number fields are summarized in Table 2.

6. Applications

In the current section, we present two applications of our proof techniques. It provides search to decision reductions to generic problems whose hardness assumption has been used to assess the security of some cryptographic designs. The first application concerns Oblivious Linear Evaluation (OLE) which is a crucial primitive for secure multi-party computation. The second one is an authentication protocol called Lapin. Both designs rely on the hardness of variants of the so-called Learning Parity with Noise (LPN) problem.

$\mathbb{Q}$	$\mathbb{F}_q(T)$
$\mathbb{Z}$	$\mathbb{F}_q[T]$
Prime numbers $q \in \mathbb{Z}$	Irreducible polynomials $Q \in \mathbb{F}_q[T]$
$\mu_m = \langle \zeta \rangle \simeq \mathbb{Z}/m\mathbb{Z}$ (groups)	$\Lambda_M = \langle \lambda \rangle \simeq \mathbb{F}_q[T]/(M)$ (modules)
$d \mid m \Leftrightarrow \mu_d \subset \mu_m$ (subgroups)	$D \mid M \Leftrightarrow \Lambda_D \subset \Lambda_M$ (submodules)
$a \equiv b \mod m \Rightarrow \zeta^a = \zeta^b$	$A \equiv B \mod M \Rightarrow [A](\lambda) = [B](\lambda)$
$K = \mathbb{Q}[\zeta]$ $\mathscr{O}_K = \mathbb{Z}[\zeta]$	$K = \mathbb{F}_q(T)[\lambda]$ $\mathscr{O}_K = \mathbb{F}_q[T][\lambda]$
$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$	$\mathrm{Gal}(K/\mathbb{F}_q(T)) \simeq (\mathbb{F}_q[T]/(M))^\times$
Cyclotomic	**Carlitz**

TABLE 2. Analogies between cyclotomic and Carlitz

6.1. **LPN and its structured variants.** Let us start this subsection by the definitions of the distribution that is involved in the LPN problem.

Definition 6.1 (Learning Parity with Noise (LPN) distribution)**.** *Let k be a positive integer, $\mathbf{s} \in \mathbb{F}_q^k$ be a uniformly distributed vector and $p \in [0, \frac{1}{2})$. A sample $(\mathbf{a}, b) \in \mathbb{F}_q^k \times \mathbb{F}_q$ is distributed according to the* LPN *distribution with secret $\mathbf{s}$ if*

- $\mathbf{a}$ *is uniformly distributed over $\mathbb{F}_q^k$;*
- $b \stackrel{def}{=} \langle \mathbf{a}, \mathbf{s} \rangle + e$ *where $\langle \cdot, \cdot \rangle$ denotes the canonical inner product over $\mathbb{F}_q^k$ and e is a q–ary Bernouilli random variable with parameter p, namely $\mathbb{P}(e = 0) = 1 - p$ and $\mathbb{P}(e = a) = \frac{p}{q-1}$ for $a \in \mathbb{F}_q^\times$.*

A sample drawn according to this distribution will be denoted $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \leftarrow \mathcal{D}_{\mathbf{s},p}^{\mathsf{LPN}}$.

Remark 6.2. This definition is a generalization of the usual LPN distribution defined over $\mathbb{F}_2$. In this situation, the error distribution is a usual Bernouilli: $\mathbb{P}(e = 0) = 1 - p$ and $\mathbb{P}(e = 1) = p$.

Remark 6.3. Sometimes in the literature, the distribution is directly defined for n samples, leading to $(\mathbf{G}, \mathbf{s} \cdot \mathbf{G} + \mathbf{e})$ where $\mathbf{G}$ is drawn uniformly at random over the space $\mathbb{F}_q^{k \times n}$ of $k \times n$ matrices whose coefficients lie in $\mathbb{F}_q$ and $\mathbf{e} \stackrel{\text{def}}{=} (e_1, \ldots, e_n)$ where the e_i's are independent Bernouilli random variables with parameter p.

The security of many cryptosystems in the literature rests on the LPN assumption which informally asserts that it is hard to distinguish a sample $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e) \leftarrow \mathcal{D}_{\mathbf{s},p}^{\mathsf{LPN}}$ from a sample $(\mathbf{a}, t)$ where both $\mathbf{a}$ and t are drawn uniformly at random.

Remark 6.4. Note that, according to Remark 6.3, when considering a fixed number n of samples, the LPN assumption is nothing but the decision version of the decoding problem, namely distinguishing noisy codewords of a random code from uniformly random vectors.

Similarly to the LWE problem, structured versions of LPN have been defined ([Hey+12; DP12; Boy+20]).

Definition 6.5 (Ring–LPN distribution)**.** *Fix a positive integer r, a public polynomial $f(X) \in \mathbb{F}_q[X]$ of degree r and $\mathbf{s} \in \mathbb{F}_q[X]/(f(X))$ be a uniformly distributed polynomial. A sample $(\mathbf{a}, \mathbf{b})$ is distributed according to the* RLPN *distribution with secret $\mathbf{s}$ if*

- $\mathbf{a}$ *is drawn uniformly at random over $\mathbb{F}_q[X]/(f(X))$;*

- $\mathbf{b} \stackrel{def}{=} \mathbf{as} + \mathbf{e}$ *where* $\mathbf{e} \stackrel{def}{=} e_0 + e_1 X + \cdots + e_{r-1} X^{r-1} \in \mathbb{F}_q[X]/(f(X))$ *has coefficients* e_i*'s which are independent* q*–ary Bernouilli random variables with parameter* p*.*

A sample drawn according to this distribution will be denoted $(\mathbf{a}, \mathbf{as} + \mathbf{e}) \leftarrow \mathcal{D}^{\mathsf{RLPN}}_{\mathbf{s},p}$*.*

Note that the map

$$\begin{cases} \mathbb{F}_q[X]/(f(X)) & \longrightarrow & \mathbb{F}_q[X]/(f(X)) \\ \mathbf{m}(X) & \longmapsto & \mathbf{a}(X)\mathbf{m}(X) \mod f(X) \end{cases}$$

can be represented in the canonical basis by an $r \times r$ matrix $\mathbf{A}$. Using this point of view, one sample of RLPN can be regarded as r specific samples of LPN.

Definition 6.6 (Module–LPN distribution)**.** *Fix positive integers* r *and* d*, a public polynomial* $f(X) \in \mathbb{F}_q[X]$ *of degree* r *and* $\mathbf{s}$ *be uniformly distributed over* $(\mathbb{F}_q[X]/(f(X)))^d$*. A sample* $(\mathbf{a}, \mathbf{b})$ *is distributed according to the* MLPN *distribution with secrets* $\mathbf{s}$ *if*

- $\mathbf{a}$ *is drawn uniformly at random over* $(\mathbb{F}_q[X]/(f(X)))^d$*;*
- $\mathbf{b} \stackrel{def}{=} \langle \mathbf{a}, \mathbf{s} \rangle + \mathbf{e} = \sum_{i=1}^{d} \mathbf{a}_i \mathbf{s}_i + \mathbf{e}$*, where* $\mathbf{e} \stackrel{def}{=} e_0 + e_1 X + \cdots + e_{r-1} X^{r-1} \in \mathbb{F}_q[X]/(f(X))$ *has coefficients* e_i*'s which are independent Bernouilli random variables with parameter* p*.*

A sample drawn according to this distribution will be denoted $(\mathbf{a}, \mathbf{b}) \leftarrow \mathcal{D}^{\mathsf{MLPN}}_{\mathbf{s},p}$

In the above definitions, the noise distribution is chosen independently on each coefficient of $\mathbf{e}(X) \in \mathbb{F}_q[X]/(f(X))$. One can also consider the situation where the coefficients of $\mathbf{e}(X)$ are chosen to form a vector of $\mathbb{F}_q^r$ of fixed Hamming weight t. This point of view is closer to the usual decoding problem, and is the one adopted in [Boy+20].

To conclude, note that the choice of the noise in the Ring– and Module–LPN distribution is made relatively to the canonical basis $(X^i)_{0 \leqslant i \leqslant r-1}$ since it seems to be the most natural one. However, one could have made another choice. This will be discussed in the sequel.

6.2. **Relation with decoding problems.** According to Remark 6.4, distinguishing n samples of an LPN distribution $\mathcal{D}^{\mathsf{LPN}}_{\mathbf{s},p}$ from the uniform distribution is equivalent to distinguishing noisy codewords of a known random code from uniformly random words. It can be regarded as the decision version of the decoding problem for a code of fixed dimension (here the length of the secret $\mathbf{s}$) and whose length n goes to infinity and hence whose rate goes to zero. Similarly, distinguishing samples from a distribution $\mathcal{D}^{\mathsf{RLPN}}_{\mathbf{s},p}$ and a uniform one is equivalent to the decision version of the decoding problem of structured codes whose basis is block-wise defined as

$$\begin{pmatrix} \mathbf{A}_1 & \cdots & \mathbf{A}_m \end{pmatrix}$$

where, for any $i \in [\![1, n]\!]$, $\mathbf{A}_i$ is the matrix representation in the canonical basis of $\mathbb{F}_q[X]/(f(X))$ of the multiplication by some random element $\mathbf{a}_i \in \mathbb{F}_q[X]/(f(X))$. In particular, considering the case $f(X) = X^\ell - 1$, we recover, the decoding problem for ℓ–quasi–cyclic codes.

Remark 6.7 (A version with "short-secret")*.* Sometimes, the RLPN distribution is considered such that the secret $\mathbf{s}$ is distributed according to the error distribution. In other words, we are given a sample of the form $(\mathbf{a}, \mathbf{as} + \mathbf{e})$ where $\mathbf{a}$ is uniformly distributed in $\mathbb{F}_q[X]/(X^\ell - 1)$ and $\mathbf{s}, \mathbf{e}$ are both of small Hamming weight t. This is nothing else than a "syndrome" version of the quasi-cyclic decoding problem. Indeed, let $\mathbf{A}$ denote the matrix representation of the multiplication by $\mathbf{a}$ (in the canonical basis), and let $\mathbf{H} \stackrel{\text{def}}{=} \begin{pmatrix} I_\ell & \mathbf{A} \end{pmatrix}$. Then $\mathbf{H}$ is the parity-check matrix of a random double-circulant quasi-cyclic code, written in systematic form, and $\mathbf{as} + \mathbf{e}$ is nothing but the polynomial representation of the syndrome $\mathbf{Hv}^\top$, with $\mathbf{v} = \begin{pmatrix} \mathbf{s} & \mathbf{e} \end{pmatrix} \in \mathbb{F}_q^{2\ell}$ is a (regular) error of weight $2t$, where we identified a polynomial with the vector of its coefficients.

In particular, the version with "short-secret" (corresponding to a decoding problem written in terms of syndromes), is equivalent to the original version (corresponding to a decoding problem written in terms of noisy codewords).

Search to decision. Here we present search to decision reductions in two different settings corresponding to two choices of the modulus $f(X)$ in the Ring–LPN problem. Both have been used

in the literature for specific applications that are quickly recalled.

A q–ary version of Ring–LPN with a totally split modulus f. In [Boy+20], the authors introduce Ring–LPN over the finite field $\mathbb{F}_q$ and with a modulus f which is totally split, *i.e.* has distinct roots, all living in the ground field $\mathbb{F}_q$.

Motivation: Oblivious Linear Evaluations for secure Multi Party Computation (MPC). The goal of secure multiparty computation (MPC) is to allow a group of people to perform together the computation of a function f on their own secret data. For many applications, the function f to be computed will be modelled by an arithmetic circuit over a finite field $\mathbb{F}_q$. It is well known that many secure multiparty computation protocols can benefit from using correlated randomness distributed to all the parties prior to engaging in the actual protocol. Inded, suppose that two users Alice and Bob share parts of some elements of $\mathbb{F}_q$ using secret sharing. Basically, for any element $\alpha \in \mathbb{F}_q$ they wish to share, Alice receives $\alpha - r_\alpha$ where r_α is uniformly random over $\mathbb{F}_q$ and Bob receives r_α, which reveals nothing on the actual element α. Such a distribution is called *additive shares of* α. Now, if Alice and Bob share additive parts of α and β, they can locally compute additive shares of the sum $\alpha+\beta$: Alice can compute $\alpha+\beta-(r_\alpha+r_\beta)$ and Bob can compute $r_\alpha + r_\beta$. Usually in MPC, an additive share of an element $\alpha \in \mathbb{F}_q$ is denoted by $[\![\alpha]\!]$. We will use this notation from now on. With this notation, we just showed that $[\![\alpha+\beta]\!] = [\![\alpha]\!] + [\![\beta]\!]$. The hard part in the multiparty computation of an arithmetic circuit is therefore to perform multiplications in $\mathbb{F}_q$ on additive shares. The crucial observation due to Beaver [Bea91] is the following. Suppose that Alice and Bob receive an additive sharing of uniformly random elements $\mathbf{u} \in \mathbb{F}_q$ and $\mathbf{v} \in \mathbb{F}_q$, as well as their product $\mathbf{w} = \mathbf{uv}$. Then, Alice and Bob can locally compute shares $[\![\alpha + \mathbf{u}]\!]$ and $[\![\beta + \mathbf{v}]\!]$. The idea is that they can *reveal* their shares to make $\gamma \stackrel{\text{def}}{=} \alpha + \mathbf{u}$ and $\delta \stackrel{\text{def}}{=} \beta + \mathbf{v}$ completely public. Note that since $\mathbf{u}$ and $\mathbf{v}$ are supposed to be uniformly random in $\mathbb{F}_q$, this reveals nothing on α and β. On the other hand,

$$\begin{aligned}\alpha\beta &= (\alpha + \mathbf{u} - \mathbf{u})(\beta + \mathbf{v} - \mathbf{v}) \\ &= (\alpha + \mathbf{u})(\beta + \mathbf{v}) - \mathbf{v}(\alpha + \mathbf{u}) - \mathbf{u}(\beta + \mathbf{v}) + \mathbf{uv} \\ &= \gamma\delta - \mathbf{v}\gamma - \mathbf{u}\delta + \mathbf{w}\end{aligned}$$

where the boldfont elements are additively shared between the parties by hypothesis, and the other are completely known to everybody. In other words, the product $\alpha\beta$ is now an affine[1] combination of public data and random elements of which each party has an additive share. More precisely, an additive sharing of the product $\alpha\beta$ can be locally computed by each party as

$$[\![\alpha\beta]\!] = [\![\gamma\delta]\!] - [\![\mathbf{v}]\!]\gamma - [\![\mathbf{u}]\!]\delta + [\![\mathbf{w}]\!].$$

Nevertheless, since the multiplication triple $(\mathbf{u}, \mathbf{v}, \mathbf{w})$ essentially acts as a one-time pad, it cannot be reused to compute a different multiplication. In other words, the main goal is now to generate a large number of such random triples, one for each multiplication gates in the arithmetic circuit.

A close notion, and actually easier to generate, is the so-called OLE-correlation (*Oblivious Linear Evaluation*): a quadruple (u, v, x, y) is said to have the OLE-correlation if u, v, x are uniformly distributed in some finite ring $\mathscr{R}$ and such that $uv = x + y$. Two parties Alice and Bob are said to *share* an OLE (u, v, r, s) if Alice receives (u, r) and Bob receives (v, s). In other words, Alice and Bob each receive one factor, as well as a random additive part, of some random product uv. Now, assume that Alice and Bob share *two* independent OLE$'s(u_1, v_1, r_1, s_1)$ and (u_2, v_2, r_2, s_2) over the finite field $\mathbb{F}_q$. Then, Alice can locally compute

$$C_A \stackrel{\text{def}}{=} r_1 + u_1u_2 + r_2$$

and similarly Bob can compute

$$C_B \stackrel{\text{def}}{=} s_1 + v_1v_2 + s_2.$$

[1] Since the affine part is actually public, it suffices that one party adds it to its share while the other does not.

Note that

$$\begin{aligned} C_A + C_B &= (r_1 + s_1) + (u_1u_2 + v_1v_2) + (r_2 + s_2) \\ &= (u_1v_1) + (u_1u_2 + v_1v_2) + (u_2v_2) \\ &= (u_1 + v_1)(u_2 + v_2). \end{aligned}$$

In other words, Alice owns (u_1, u_2, C_A) and Bob owns (v_1, v_2, C_B) which are additive shares of the random multiplication triple $(u_1 + v_1, u_2 + v_2, (u_1 + v_1)(u_2 + v_2))$, *i.e.* it suffices to distribute *two* $\mathsf{OLE}'s$ in order to generate *one* multiplication triple, which can then be consumed during the online phase for each multiplication gate of the arithmetic circuit.

Therefore, a crucial objective in MPC is now to be able to generate a large number of pseudo-random correlated pairs $((u_i, r_i), (v_i, s_i))_i$ such that for any i, we have $r_i + s_i = u_iv_i$.

In [Boy+20], the authors propose to generate such sequences of elements as follows. We work in the ring $\mathscr{R} \stackrel{\text{def}}{=} \mathbb{F}_q[X]/(f(X))$ where f has only simple roots, all lying in $\mathbb{F}_q$. Alice receives two sparse polynomials $\mathbf{e}_0^A, \mathbf{e}_1^A \in \mathscr{R}$ and Bob receives two sparse polynomials $\mathbf{e}_0^B, \mathbf{e}_1^B \in \mathscr{R}$. Because of the sparseness, one can efficiently distribute to Alice and Bob additive shares of $\mathbf{e}_i^A\mathbf{e}_j^B$ for $(i, j) \in \{0, 1\}^2$ using *Function Secret Sharing* for distributed point functions [GI14; BGI16]. That is, for any such (i, j) Alice receives $\mathbf{e}_i^A\mathbf{e}_j^B + \mathbf{r}_{ij}$ and Bob receives $\mathbf{r}_{ij}$ where $\mathbf{r}_{ij}$ is uniformly random over $\mathscr{R}$. Next, a uniformly random element $\mathbf{a} \in \mathscr{R}$ is made public, Alice computes $\mathbf{u} = \mathbf{a}\mathbf{e}_0^A + \mathbf{e}_1^A$ and Bob computes $\mathbf{v} = \mathbf{a}\mathbf{e}_0^B + \mathbf{e}_1^B$. Then, shares of $\mathbf{uv}$ are obtained as follows: Alice computes

$$\mathbf{r} \stackrel{\text{def}}{=} \mathbf{a}^2(\mathbf{e}_0^A\mathbf{e}_0^B + \mathbf{r}_{00}) + \mathbf{a}(\mathbf{e}_0^A\mathbf{e}_1^B + \mathbf{e}_1^A\mathbf{e}_0^B + \mathbf{r}_{01} + \mathbf{r}_{10}) + (\mathbf{e}_1^A\mathbf{e}_1^B + \mathbf{r}_{11})$$

and Bob computes

$$\mathbf{s} = \mathbf{a}^2(\mathbf{r}_{00}) + \mathbf{a}(\mathbf{r}_{01} + \mathbf{r}_{10}) + \mathbf{r}_{11},$$

which are additive shares of $\mathbf{uv}$. Finally, given a pseudorandom correlated pairs $(\mathbf{u}, \mathbf{r}), (\mathbf{v}, \mathbf{s})$ where $\mathbf{u}, \mathbf{v}, \mathbf{r}, \mathbf{s} \in \mathscr{R} \simeq \mathbb{F}_q[X]/(f(X))$ and f is supposed to be split, by the Chinese Remainder Theorem, we generate $\deg f$ pseudorandom correlated pairs $(u_i, r_i), (v_i, s_i)$, with $u_i, v_i, r_i, s_i \in \mathbb{F}_q$. The pseudorandomness of the u_i's and the v_i's, or equivalently the pseudorandomness of $\mathbf{u}, \mathbf{v}$ rests on the RLPN or equivalently the FF–DP assumption, together with Remark 6.7.

Search to decision reduction in the [Boy+20]-case. Consider the case of Ring–LPN over $\mathscr{R} = \mathbb{F}_q[X]/(f(X))$, where

$$f(X) \stackrel{\text{def}}{=} \prod_{a \in \mathbb{F}_q^\times} (X - a) = X^{q-1} - 1.$$

Let us re-introduce the Carlitz function field of Examples 5.6 and 5.13, namely

$$K_T = \mathbb{F}_q(T)[X]/(X^{q-1} + T).$$

According to Equation (5) in Example 5.13, we have

$$\mathscr{O}_T/(T + 1)\mathscr{O}_T \simeq \mathbb{F}_q[X]/(X^{q-1} - 1),$$

which is precisely the ring we consider for the Ring LPN version of [Boy+20]. Therefore, instantiating our FF–DP problem with this function field, modulus $T + 1$, ideal $\mathfrak{P} \stackrel{\text{def}}{=} (T + 1)\mathscr{O}_K$ and applying Theorem 3.10, we directly obtain the following search to decision reduction.

Theorem 6.8 (Search to decision reduction for totally-split Ring–LPN)**.** *Let K_T be the Carlitz extension of T–torsion over $\mathbb{F}_q$, and denote by $\mathscr{O}_T$ its ring of integers. Consider the ideal $\mathfrak{P} \stackrel{def}{=} (T + 1)\mathscr{O}_{K_T}$. Then $\mathfrak{P}$ splits completely in $q - 1$ factors $\mathfrak{P}_1 \dots \mathfrak{P}_{q-1}$ and*

$$\mathscr{O}_K/\mathfrak{P} \simeq \prod_{i=1}^{q-1} \mathscr{O}_K/\mathfrak{P}_i \simeq \mathbb{F}_q \times \cdots \times \mathbb{F}_q.$$

Let ψ denote the uniform distribution over polynomials in $\mathbb{F}_q[X]/(X^{q-1} - 1)$ of fixed Hamming weight, or the q–ary Bernouilli distribution. Let $\mathbf{s} \in \mathbb{F}_q[X]/(X^{q-1} - 1)$. Suppose that we have access

to $\mathscr{F}_{\mathbf{s},\psi}$ and that there exists a distinguisher between the uniform distribution over $\mathbb{F}_q[X]/(X^{q-1}-1)$ and $\mathscr{F}_{\mathbf{s},\psi}$ with uniform secret and error distribution ψ, running in time t and having advantage ε.

Then there exists an algorithm that recovers $\mathbf{s}$ with overwhelming probability (in q) in time

$$O\left(q^5 \times \frac{1}{\varepsilon^2} \times t\right).$$

Proof. The only thing that remains to be proved is that the error distribution is Galois invariant. According to Theorem 5.10 and Example 5.13, the Galois group of $K_T/\mathbb{F}_q(T)$ is isomorphic to $(\mathbb{F}_q[T]/(T))^\times \simeq \mathbb{F}_q^\times$. Furthermore, we proved that an element $b \in \mathbb{F}_q^\times$ acts on $f(T,X) \in K_T$ by

$$b \cdot f(T,X) = f(T,[b](X)) = f(T,bX).$$

For this example it can actually be understood directly using *Kummer theory* (see [Sti09, Proposition 3.7.3]). Indeed, $\mathbb{F}_q$, and hence $\mathbb{F}_q(T)$, contains the $(q-1)$–th roots of unity. Moreover, K_T is nothing but the extension of $\mathbb{F}_q(T)$ spanned by a primitive $(q-1)$–th root of $-T$. Therefore, it is a *Kummer extension* and the action of the Galois group is characterized by $X \mapsto \zeta \cdot X$ for every $(q-1)$–th root of unity ζ. But here, the set of $(q-1)$–th roots of unity is *precisely* $\mathbb{F}_q^\times$. The Galois action on K_T and $\mathscr{O}_T$ induces an action of $\mathbb{F}_q^\times$ on

$$\mathscr{O}_T/(T+1)\mathscr{O}_T \simeq \mathbb{F}_q[X]/(X^{q-1}-1)$$

by $b \cdot m(X) \stackrel{\text{def}}{=} m(bX)$. Note that, this operation has no incidence on the Hamming weight of m: it actually *does not change its Hamming support*. Therefore, we easily see here that Galois action keeps the noise distribution invariant. □

Remark 6.9. Note that our search to decision reduction could have been performed here without introducing the function field and only considering the ring $\mathbb{F}_q[X]/(X^{q-1}-1)$. Recall that the first ingredient of the reduction is to decompose this ring by the Chinese Remainder Theorem. Here it would give the product $\prod_{a\in\mathbb{F}_q^\times} \mathbb{F}_q[X]/(X-a)$. The final step of the reduction requires the introduction of a group action which induces a permutation of the factors in $\prod_{a\in\mathbb{F}_q^\times} \mathbb{F}_q[X]/(X-a)$. It is precisely what the group action $b \cdot m(X) = m(bX)$ does: it sends the factor $\mathbb{F}_q[X]/(X-a)$ onto $\mathbb{F}_q[X]/(X-b^{-1}a)$. However, introducing this action on the level of $\mathbb{F}_q[X]/(X^{q-1}-1)$ does not look very natural. It turns out that the introduction of function fields permits to interpret this action in terms of a Galois one.

Case H is a strict subgroup of $\mathbb{F}_q^\times$. Now assume the polynomial f has the form

$$f(X) = \prod_{a\in H} (X-a)$$

with H being a strict subgroup of $\mathbb{F}_q^\times$. To instantiate our search to decision reduction we need to find a group action that keeps the noise distribution invariant.

Lemma 6.10. *There exists a Galois function field K with its ring of integers $\mathscr{O}_K$ such that $H = \mathrm{Gal}(K/\mathbb{F}_q(T))$ and $\mathscr{O}_K/(T+1)\mathscr{O}_K = \mathbb{F}_q[X]/(f(X))$. Moreover, the action of H keeps the Hamming support invariant.*

Proof. Consider again the Carlitz extension K_T. It has a *cyclic* Galois group $G \simeq \mathbb{F}_q^\times$ of cardinality $q-1$. Let $h \stackrel{\text{def}}{=} \#H$. It divides $q-1$. Since G is cyclic, it has a *unique* subgroup N of cardinality $\frac{q-1}{h}$. Let $L \stackrel{\text{def}}{=} K_T^N$ be the fixed field of N. Since $(T+1)$ splits completely in $\mathscr{O}_T$, it also splits completely in any intermediate field. In particular, it splits completely in $\mathscr{O}_L \stackrel{\text{def}}{=} \mathscr{O}_T^H$ the ring of integers of L, we have

$$\mathscr{O}_L/(T+1)\mathscr{O}_L \simeq \mathbb{F}_q[X]/(f(X)).$$

Now, since G is *abelian*, N is *normal* in G. In particular, $L/\mathbb{F}_q(T)$ is a Galois extension, with Galois group $G/N \simeq H$. By the same argument as in the previous paragraph, the action of H on $\mathbb{F}_q[X]/(f(X))$ only permutes the factors, but keeps the *supports* invariant. In particular, the noise distribution is not moved under the action of H. □

This lemma immediately implies a search to decision reduction analogue to theorem (6.8).

Remark 6.11. When the roots of $f(X)$ do not form a subgroup of G, but a *coset* bH instead, *i.e.* $f(X) = \prod_{\alpha \in bH}(X - \alpha)$, then it suffices to perform a translation by b prior: $X \mapsto bX$ also keeps all the distributions invariant (including the uniform), and $\mathbb{F}_q[X]/(f(X))$ is mapped onto $\mathbb{F}_q[X]/(g(X))$ where $g(X) \stackrel{\text{def}}{=} \prod_{\alpha \in H}(X - \alpha)$, which yields the result by seeing the action of H as arising from a Galois action.

Ring–LPN with a modulus f splitting in irreducible polynomials of the same degree. Another cryptographic design whose security rests on the Ring–LPN assumption is an authentication protocol named Lapin [Hey+12]. In the conclusion of their article, the authors mention that

> "*it would be particularly interesting to find out whether there exists an equivalence between the decision and the search versions of the problem similar to the reductions that exist for* LPN *and Ring–*LWE".

For this protocol, the problem is instantiated with the binary field $\mathbb{F}_2$ and with a modulus polynomial f which splits as a product of m distinct irreducible polynomials

$$f(X) = f_1(X) \cdots f_m(X).$$

In this setting and using our techniques, we can provide a search to decision reduction when the f_i's have all the same degree d. Furthermore, for the reduction to run in polynomial time, we need to have $d = O(\log(\deg f))$. In this setting, the Chinese Reminder Theorem entails that

$$\mathbb{F}_2[X]/(f(X)) \simeq \prod_{i=1}^{m} \mathbb{F}_2[X]/(f_i(X)),$$

and the right–hand side is a product of m copies of $\mathbb{F}_{2^d}$. Such a product can be realised as follows. Consider a function field K which is a Galois extension of $\mathbb{F}_2(T)$ with Galois group G and denote by $\mathscr{O}_K$ the integral closure of $\mathbb{F}_2[T]$ in K. Suppose that the ideal (T) of $\mathbb{F}_2[T]$ is unramified in $\mathscr{O}_K$ with inertia degree d. Then $T\mathscr{O}_K$ splits into a product of prime ideals:

$$T\mathscr{O}_K = \mathfrak{P}_1 \cdots \mathfrak{P}_m \qquad \text{and} \qquad \mathscr{O}_K/T\mathscr{O}_K \simeq \prod_{i=1}^{m} \mathscr{O}_K/\mathfrak{P}_i,$$

where, here again, the right–hand side is a product of m copies of $\mathbb{F}_{2^d}$.

Next, the idea is now to apply Theorem 3.10 in this setting. However, there is here a difficulty since for our search to decision reduction to hold, the noise should arise from a Galois invariant distribution. Thus, if we want the noise distribution to be Galois invariant we need to have a Galois invariant $\mathbb{F}_2$–basis of the algebra $\mathscr{O}_K/T\mathscr{O}_K$. The first question should be whether such a basis exists. The existence of such a basis can be deduced from deep results of number theory due to Noether [Noe32; Cha96] and asserting the existence of local normal integral bases at non ramified places. Here we give a pedestrian proof resting only on basic facts of number theory. Since this result also holds for larger finite fields, from now on, the underlying field is not supposed to be $\mathbb{F}_2$ anymore.

Proposition 6.12. *Let $K/\mathbb{F}_q(T)$ be a finite Galois extension of Galois group G and $\mathscr{O}_K$ be the integral closure of $\mathbb{F}_q[T]$ in K. Let $Q \in \mathbb{F}_q[T]$ be an irreducible polynomial of degree 1 such that the corresponding prime ideal is unramified and has inertia degree d. Denote by $\mathfrak{P}_1 \cdots \mathfrak{P}_m$ the decomposition of the ideal $Q\mathscr{O}_K$. Then, G acts on the finite dimensional algebra $\mathscr{O}_K/Q\mathscr{O}_K$ and there exists $\mathbf{x} \in \mathscr{O}_K/Q\mathscr{O}_K$ such that $(\sigma(\mathbf{x}))_{\sigma \in G}$ is an $\mathbb{F}_q$–basis of $\mathscr{O}_K/Q\mathscr{O}_K$.*

Proof. Consider the decomposition group $D_{\mathfrak{P}_1/Q}$. As explained Section 2 and in particular in Equation (4), since $Q\mathscr{O}_K$ is unramified, this decomposition group is isomorphic to $\mathrm{Gal}(\mathscr{O}_K/Q\mathscr{O}_K, \mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_{q^d}, \mathbb{F}_q)$. This entails in particular that $\#D_P = d$.

According to the Chinese Remainder Theorem,

$$\mathscr{O}_K/Q\mathscr{O}_K \simeq \mathscr{O}_K/\mathfrak{P}_1 \times \cdots \times \mathscr{O}_K/\mathfrak{P}_m.$$

Next, from the Normal basis Theorem (see for instance [LN97, Thm. 2.35]), there exists $\mathbf{a} \in \mathscr{O}_K/\mathfrak{P}_1$ such that $(\sigma(\mathbf{a}))_{\sigma \in D_{\mathfrak{P}_1/Q}}$ is an $\mathbb{F}_q$–basis of $\mathscr{O}_K/\mathfrak{P}_1$. Now, let

$$\mathbf{b} \stackrel{\text{def}}{=} (\mathbf{a}, 0, \ldots, 0) \in \prod_{i=1}^{m} \mathscr{O}_K/\mathfrak{P}_\mathrm{i} \simeq \mathscr{O}_K/Q\mathscr{O}_K.$$

We claim that $(\sigma(\mathbf{b}))_{\sigma \in G}$ is an $\mathbb{F}_q$–basis of $\mathscr{O}_K/Q\mathscr{O}_K$. Indeed, denote by V the $\mathbb{F}_q$–span of $\{\sigma(\mathbf{b}) \mid \sigma \in G\}$ and suppose that V is a proper subspace of $\mathscr{O}_K/Q\mathscr{O}_K$. Then, there exists $i \in [\![1, m]\!]$ such that

$$V \cap \mathscr{O}_K/\mathfrak{P}_i \subsetneq \mathscr{O}_K/\mathfrak{P}_i,$$

where we denote by $\mathscr{O}_K/\mathfrak{P}_i$ the subspace $\{0\} \times \cdots \times \{0\} \times \mathscr{O}_K/\mathfrak{P}_i \times \{0\} \times \cdots \times \{0\}$ of $\prod_i \mathscr{O}_K/\mathfrak{P}_i$.

Since G acts transitively on the $\mathfrak{P}_i$'s, there exists $\sigma_0 \in G$ such that $\sigma_0(\mathfrak{P}_1) = \mathfrak{P}_i$. Then, $\sigma_0(\mathbf{b}) \in V \cap \mathscr{O}_K/\mathfrak{P}_i$ and so does $\sigma\sigma_0(\mathbf{b})$ for any $\sigma \in D_{\mathfrak{P}_i/P}$. Since $V \cap \mathscr{O}_K/\mathfrak{P}_i \subsetneq \mathscr{O}_K/\mathfrak{P}_i$, then $\dim_{\mathbb{F}_q} V < d$ while $\#D_{\mathfrak{P}_i/P} = d$. Hence, there exist nonzero elements $(\lambda_\sigma)_{\sigma \in D_{\mathfrak{P}_i/P}} \in \mathbb{F}_q^d$ such that

$$\sum_{\sigma \in D_{\mathfrak{P}_i/P}} \lambda_\sigma \sigma\sigma_0(\mathbf{b}) = 0. \tag{6}$$

Applying σ_0^{-1} to (6), we get

$$\sum_{\sigma \in D_{\mathfrak{P}_i/P}} \lambda_\sigma \sigma_0^{-1}\sigma\sigma_0(\mathbf{b}) = 0.$$

As mentioned in Section 2, we have $\sigma_0^{-1} D_{\mathfrak{P}_i/Q} \sigma_0 = D_{\mathfrak{P}_1/Q}$ and we deduce that the above sum is in $\mathscr{O}_K/\mathfrak{P}_1$ and, since $\mathbf{a}$ is a generator of a normal basis of $\mathbb{F}_q$, we deduce that the λ_σ's are all zero. A contradiction. □

The previous proposition asserts the existence of a *normal* $\mathbb{F}_q$–basis of the space $\mathscr{O}_K/Q\mathscr{O}_K$, *i.e.* a Galois invariant basis. For any such basis, $(\mathbf{b}_\sigma)_{\sigma \in G}$ one can define a Galois noise distribution by sampling linear combinations of elements of this basis whose coefficients are independent Bernouilli random variables. Our Ring–LPN distribution is hence defined as pairs $(\mathbf{a}, \mathbf{b}) \in \mathscr{O}_K/Q\mathscr{O}_K \times \mathscr{O}_K/Q\mathscr{O}_K$ such that $\mathbf{a}$ is drawn uniformly at random and $\mathbf{b} = \mathbf{as} + \mathbf{e}$ where $\mathbf{e}$ is a noise term drawn from the previously described distribution.

Definition 6.13 (Galois modulus)**.** *Let r and d be positive integers. A polynomial $f(X) \in \mathbb{F}_q[X]$ of degree r is called a Galois modulus of inertia d if there exists a Galois function field $K/\mathbb{F}_q(T)$ and a polynomial $Q(T) \in \mathbb{F}_q[T]$ of degree one such that $\mathbb{F}_q[X]/(f(X)) \simeq \mathscr{O}_K/Q\mathscr{O}_K$ and the ideal $Q\mathscr{O}_K$ has inertia degree d and does not ramify.*

This definition entails that for a polynomial $f(X) \in \mathbb{F}_q[X]$ to be a Galois modulus, it needs to factorize in $\mathbb{F}_q[X]$ as a product of distinct irreducible polynomials of same degree d.

Carlitz extensions permit to easily exhibit many Galois moduli of given inertia d. Indeed, let $M(T) \in \mathbb{F}_q[T]$ be any divisor of $T^d - 1$ which vanishes at least at one primitive d–th root of unity. Set

$$r \stackrel{\text{def}}{=} \frac{\#\left(\mathbb{F}_q[X]/(M(X))\right)^\times}{d}.$$

Then, any polynomial $f(X) \in \mathbb{F}_q[X]$ which is a product of r distinct irreducible polynomials of degree d is a Galois modulus. Indeed, $\mathbb{F}_q[X]/(f(X))$ is isomorphic to a product of r copies of $\mathbb{F}_{2^d}$ and, since the multiplicative order of T modulo $M(T)$ is d, from Theorem 5.14 so does $\mathscr{O}_M/T\mathscr{O}_M$.

Example 6.14. *The polynomial $f(X) \stackrel{def}{=} X^{63} + X^7 + 1 \in \mathbb{F}_2[X]$ is a* Galois *modulus of inertia* 9*. Indeed, let $M(T) \stackrel{def}{=} T^6 + T^3 + 1$ and consider K_M the Carlitz extension of M–torsion. Denote by $\mathscr{O}_M$ the integral closure of $\mathbb{F}_2[T]$ in $\mathscr{O}_M$. Then $T^9 \equiv 1 \mod M$ and 9 is the smallest integer that has this property. By Theorem 5.14, the ideal $T\mathscr{O}_M$ splits into 7 ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_7$ and has inertia 9. Hence, $\mathscr{O}_M/(T\mathscr{O}_M) \simeq \mathbb{F}_q[X]/(f(X))$.*

Remark 6.15. The polynomial $f(X)$ of Example 6.14 is also *lightness-preserving* in the sense of [DP12, Def 2.22] which can be used to instantiate Ring-LPN.

We are now ready to define a new noise distribution which is Galois invariant for Ring–LPN. We propose to consider it in Lapin as it enables to apply our search to decision reduction. In the following definition, $\mathcal{B}$ denotes a normal basis whose existence is ensured by Proposition 6.12. Note that $\mathcal{B}$ need not be exactly the normal basis constructed in the proof of Proposition 6.12. This is discussed further, after the statement of Theorem 6.17.

Definition 6.16 (Normal Ring–LPN distribution)**.** *Let r, d be positive integers, $p \in [0, \frac{1}{2})$ and let $f(X) \in \mathbb{F}_q[X]$ be a* Galois *modulus of degree r with inertia d. Denote by $\mathcal{B} \stackrel{def}{=} (\sigma(\mathbf{c})(X))_{\sigma \in G_f}$ the normal basis of $\mathbb{F}_q[X]/(f(X))$ where G_f is the Galois group of the related function field.*

A sample $(\mathbf{a}, \mathbf{b})$ is distributed according to the Normal RLPN *distribution relatively to basis $\mathcal{B}$, with secret $\mathbf{s}$ if*

- $\mathbf{a}$ *is drawn uniformly at random over $\mathbb{F}_q[X]/(f(X))$;*
- $\mathbf{b} \stackrel{def}{=} \mathbf{as} + \mathbf{e}$*, where $\mathbf{e}(X) \stackrel{def}{=} \sum_{\sigma \in G_f} e_\sigma \sigma(\mathbf{c})(X) \in \mathbb{F}_q[X]/(f(X))$ has coefficients e_i's which are independent q–ary Bernouilli random variables with parameter p.*

Theorem 6.17. *The decision Ring–LPN is equivalent to its search version for the normal Ring–LPN distribution.*

Let us discuss further the choice of the noise distribution and hence that of a Galois-invariant basis. In [Hey+12], the authors discuss the case of Ring–LPN when the modulus f splits and mention that in this situation, the Ring–LPN problem reduces to a smaller one by projecting the samples onto a factor $\mathbb{F}_q[X]/(f_i(X))$ of the algebra $\mathbb{F}_q[X]/(f(X))$. The projection onto such a factor, reduces the size of the inputs but increases the rate of the noise.

It should be emphasized that the Galois invariant basis constructed in the proof of Proposition 6.12 yields a noise which is partially cancelled when applying the projection $\mathscr{O}_K/Q\mathscr{O}_K \to \mathscr{O}_K/\mathfrak{P}_i$, hence, this choice of normal basis might be inaccurate. On the other hand, Proposition 6.12 is only an existence result and it turns out actually that a random element of $\mathscr{O}_K/Q\mathscr{O}_K$ generates a normal basis with a high probability. Indeed, the existence of such a normal basis can be reformulated as $\mathscr{O}_K/Q\mathscr{O}_K$ is a free $\mathbb{F}_q[G]$–module of rank 1 and a generator $\mathbf{a} \in \mathscr{O}_K/Q\mathscr{O}_K$ is an $\mathbb{F}_q[G]$–basis of $\mathscr{O}_K/Q\mathscr{O}_K$. Now, any other element of $\mathbb{F}_q[G]^\times \mathbf{a}$ is also a generator of a normal basis. Consequently, the probability that a uniformly random element of $\mathscr{O}_K/Q\mathscr{O}_K$ is a generator of a normal basis is

$$\frac{\#\mathbb{F}_q[G]^\times}{\#\mathbb{F}_q[G]}.$$

If for instance, G is cyclic of order N prime to q. Then $X^N - 1$ splits into a product of distinct irreducible factors $u_1 \cdots u_r$ and $\mathbb{F}_q[G] \simeq \mathbb{F}_q[X]/(X^N - 1) \simeq \prod_i \mathbb{F}_q[X]/(u_i(X))$. In this context, the probability that a uniformly random element of $\mathscr{O}_K/Q\mathscr{O}_K$ generates a normal basis is

$$\frac{\prod_{i=1}^r (q^{\deg u_i} - 1)}{q^N}.$$

Conclusion

We introduced a new formalism to study generic problems useful in cryptography based on structured codes. This formalism rests on the introduction of function fields as counterparts of the number fields appearing in cryptography based on structured lattices. Thanks to this new point of view, we succeeded in producing the first search to decision reduction in the spirit of Lyubashevsky, Peikert and Regev's one for Ring-LWE. We emphasize that such reductions were completely absent in cryptography based on structured codes and we expect them to be a first step towards further search to decision reductions.

If one puts into perspective our current assessment with lattice-based cryptography, [LPR10] focuses on cyclotomic number fields, and defined the error distribution to be a Gaussian over $\mathbb{R}^n$ through the Minkowski embedding. Furthermore, the modulus q was chosen to split completely.

Then, following this result, [LS15] uses a "switching modulus" technique in order to relax the arithmetic assumption on the prime modulus, so that it can be arbitrarily chosen. Finally, the search to decision reduction has been proved in [RSW18] to hold even when the extension is not Galois, using the Oracle with Hidden Center Problem (OHCP) technique from [PRS17]. Note that this powerful technique has been used recently to provide a search to decision reduction in the context of NTRU [PS21]. Even though our work does not reflect these recent progresses, we believe, as it was shown by our instantiations, that the introduction of the function field framework paves the way for using these techniques in the code setting in order to get a full reduction applying to cryptosystems such as HQC or BIKE.

REFERENCES

[Agu+21a] Carlos Aguilar Melchor, Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Shay Gueron, Tim Güneysu, et al. *BIKE*. Round 3 Submission to the NIST Post-Quantum Cryptography Call, v. 4.2. Version 4.2. Sept. 2021. URL: https://bikesuite.org.

[Agu+21b] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Edoardo Persichetti, Gilles Zémor, and Jurjen Bos. *HQC*. Round 3 Submission to the NIST Post-Quantum Cryptography Call. https://pqc-hqc.org/doc/hqc-specification_2021-06-06.pdf. June 2021.

[Agu+19] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Gilles Zémor, Alain Couvreur, and Adrien Hauteville. *Rank Quasi Cyclic (RQC)*. Second round submission to the NIST post-quantum cryptography call. Apr. 2019. URL: https://pqc-rqc.org.

[AD97] Miklós Ajtai and Cynthia Dwork. "A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence". In: *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, El Paso, Texas, USA, May 4-6, 1997*. 1997, pp. 284–293. URL: http://doi.acm.org/10.1145/258533.258604.

[Ala+20] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, et al. *Status report on the second round of the NIST post-quantum cryptography standardization process*. 2020.

[Ale03] Alekhnovich, Michael. "More on Average Case vs Approximation Complexity". In: *44th Symposium on Foundations of Computer Science (FOCS 2003), 11-14 October 2003, Cambridge, MA, USA, Proceedings*. IEEE Computer Society, 2003, pp. 298–307. URL: https://doi.org/10.1109/SFCS.2003.1238204.

[App+17] Benny Applebaum, Naama Haramaty, Yuval Ishai, Eyal Kushilevitz, and Vinod Vaikuntanathan. "Low-Complexity Cryptographic Hash Functions". In: *ITCS*. Vol. 67. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017, 7:1–7:31.

[Ara+19] Nicolas Aragon, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Adrien Hauteville, Olivier Ruatta, Jean-Pierre Tillich, Gilles Zémor, Carlos Aguilar Melchor, Slim Bettaieb, et al. *ROLLO (merger of Rank-Ouroboros, LAKE and LOCKER)*. Second round submission to the NIST post-quantum cryptography call. NIST Round 2 submission for Post-Quantum Cryptography. Mar. 2019. URL: https://pqc-rollo.org.

[Bea91] Donald Beaver. "Efficient Multiparty Protocols Using Circuit Randomization". In: *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*. Ed. by Joan Feigenbaum. Vol. 576. Lecture Notes in Computer Science. Springer, 1991, pp. 420–432.

[BH08] Peter Beelen and Tom Høholdt. "The decoding of algebraic geometry codes". In: *Advances in algebraic geometry codes*. Vol. 5. Ser. Coding Theory Cryptol. World Sci. Publ., Hackensack, NJ, 2008, pp. 49–98.

[Boy+20] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. "Efficient Pseudorandom Correlation Generators from Ring-LPN". In: *Advances in Cryptology - CRYPTO*. Ed. by Daniele Micciancio and Thomas Ristenpart. Cham: Springer International Publishing, 2020, pp. 387–416.

[BGI16] Elette Boyle, Niv Gilboa, and Yuval Ishai. "Function Secret Sharing: Improvements and Extensions". In: *ACM CCS 2016: 23rd Conference on Computer and Communications Security*. Ed. by Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi. Vienna, Austria: ACM Press, Oct. 2016, pp. 1292–1303.

[Bra+19] Zvika Brakerski, Vadim Lyubashevsky, Vinod Vaikuntanathan, and Daniel Wichs. "Worst-Case Hardness for LPN and Cryptographic Hashing via Code Smoothing". In: *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11478. LNCS. Springer, 2019, pp. 619–635. URL: https://doi.org/10.1007/978-3-030-17659-4%5C_21.

[Cha96] Robin J. Chapman. "A simple proof of Noether's Theorem". In: *Glasgow Math. J.* 38 (1996), pp. 49–51.

[Con] Keith Conrad. *Carlitz extensions*. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/carlitz.pdf.

[CFS01] Nicolas Courtois, Matthieu Finiasz, and Nicolas Sendrier. "How to Achieve a McEliece-based Digital Signature Scheme". In: *Advances in Cryptology - ASIACRYPT 2001*. Vol. 2248. LNCS. Gold Coast, Australia: Springer, 2001, pp. 157–174.

[CR21] Alain Couvreur and Hugues Randriambololona. "Algebraic geometry codes and some applications". In: *A concise encyclopedia of coding theory*. CRC press, 2021. Chap. 15, pp. 307–361.

[DP12] Ivan Damgård and Sunoo Park. "Is Public-Key Encryption Based on LPN Practical?" In: *IACR Cryptol. ePrint Arch.* (2012), p. 699. URL: http://eprint.iacr.org/2012/699.

[DRT21] Thomas Debris-Alazard, Maxime Remaud, and Jean-Pierre Tillich. *Quantum Reduction of Finding Short Code Vectors to the Decoding Problem*. preprint. arXiv:2106.02747. Nov. 2021. URL: https://arxiv.org/abs/2106.02747.

[DST19] Thomas Debris-Alazard, Nicolas Sendrier, and Jean-Pierre Tillich. "Wave: A New Family of Trapdoor One-Way Preimage Sampleable Functions Based on Codes". In: *Advances in Cryptology - ASIACRYPT 2019, Part I*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11921. LNCS. Kobe, Japan: Springer, Dec. 2019, pp. 21–51. URL: https://doi.org/10.1007/978-3-030-34578-5%5C_2.

[FS96] Jean-Bernard Fischer and Jacques Stern. "An efficient pseudo-random generator provably as secure as syndrome decoding". In: *Advances in Cryptology - EUROCRYPT'96*. Ed. by Ueli Maurer. Vol. 1070. LNCS. Springer, 1996, pp. 245–255. ISBN: ISBN 978-3-540-61186-8.

[Gab05] Philippe Gaborit. "Shorter keys for code based cryptography". In: *Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)*. Bergen, Norway, Mar. 2005, pp. 81–91.

[GI14] Niv Gilboa and Yuval Ishai. "Distributed Point Functions and Their Applications". In: *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*. Ed. by Phong Q. Nguyen and Elisabeth Oswald. Vol. 8441. Lecture Notes in Computer Science. Springer, 2014, pp. 640–658.

[Gop81] Valerii D. Goppa. "Codes on algebraic curves". In: *Dokl. Akad. Nauk SSSR* 259.6 (1981). In Russian, pp. 1289–1290.

[Hay74] David R Hayes. "Explicit class field theory for rational function fields". In: *Transactions of the American Mathematical Society* 189 (1974), pp. 77–91.

[Hey+12] Stephan Heyse, Eike Kiltz, Vadim Lyubashevsky, Christof Paar, and Krzysztof Pietrzak. "Lapin: An efficient authentication protocol based on Ring-LPN". In: *Fast Software Encryption - 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012*. Ed. by Anne Canteaut. Vol. 7549. LNCS. Washington DC, United States: Springer, 2012, pp. 346–365.

[HP95] Tom Høholdt and Ruud Pellikaan. "On the decoding of algebraic–geometric codes". In: *IEEE Trans. Inform. Theory* 41.6 (Nov. 1995), pp. 1589–1614.

[LS15] Adeline Langlois and Damien Stehlé. "Worst-case to average-case reductions for module lattices". In: *Des. Codes Cryptogr.* 75 (2015), pp. 565–599. URL: https://hal.archives-ouvertes.fr/hal-01240452.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*. Second. Vol. 20. Encyclopedia of Mathematics and its Applications. With a foreword by P. M. Cohn. Cambridge University Press, Cambridge, 1997, pp. xiv+755. ISBN: 0-521-39231-4.

[Lyu11] Vadim Lyubashevsky. "Search to decision reduction for the learning with errors over rings problem". In: *ITW*. IEEE, 2011, pp. 410–414.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *Advances in Cryptology - EUROCRYPT2010*. Vol. 6110. LNCS. Springer, 2010, pp. 1–23. URL: http://dx.doi.org/10.1007/978-3-642-13190-5_1.

[McE78] Robert J. McEliece. "A Public-Key System Based on Algebraic Coding Theory". In: DSN Progress Report 44. Jet Propulsion Lab, 1978, pp. 114–116.

[MR04] D. Micciancio and O. Regev. "Worst-case to average-case reductions based on Gaussian measures". In: *45th Annual IEEE Symposium on Foundations of Computer Science*. 2004, pp. 372–381.

[Mis+12] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. *MDPC-McEliece: New McEliece Variants from Moderate Density Parity-Check Codes*. 2012. URL: http://eprint.iacr.org/2012/409.

[Nie01] Niederreiter, Harald and Xing, Chaoping. *Rational points on curves over finite fields: theory and applications*. Vol. 288. Cambridge University Press, 2001.

[Noe32] Emmy Noether. "Normalbasis bei Körpern ohne Höhere Verzweigung". In: *J. Reine Angew. Math.* 167 (1932), pp. 147–152.

[PRS17] Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. "Pseudorandomness of ring-LWE for any ring and modulus". In: *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*. 2017, pp. 461–473.

[PS21] Alice Pellet-Mary and Damien Stehlé. "On the hardness of the NTRU problem". In: *Asiacrypt 2021 - 27th Annual International Conference on the Theory and Applications of Cryptology and Information Security*. Advances in Cryptology – ASIACRYPT 2021. Lecture Notes in Computer Science, vol 13090. Singapore, Singapore, Dec. 2021. URL: https://hal.archives-ouvertes.fr/hal-03348022.

[Reg05] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*. 2005, pp. 84–93. URL: http://doi.acm.org/10.1145/1060590.1060603.

[RSW18] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. "On the ring-LWE and polynomial-LWE problems". In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2018, pp. 146–173.

[Ros02] Michael Rosen. *Number Theory in Function Fields*. Graduate Texts in Mathematics. Springer, 2002. ISBN: 978-1-4757-6046-0.

[Sen11] Nicolas Sendrier. "Decoding One Out of Many". In: *Post-Quantum Cryptography 2011*. Vol. 7071. LNCS. 2011, pp. 51–67.

[Ste+09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. "Efficient Public Key Encryption Based on Ideal Lattices". In: *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*. Ed. by

Mitsuru Matsui. Vol. 5912. LNCS. Springer, 2009, pp. 617–635. URL: https://doi.org/10.1007/978-3-642-10366-7%5C_36.

[Ste93] Jacques Stern. "A New Identification Scheme Based on Syndrome Decoding". In: *Advances in Cryptology - CRYPTO'93*. Ed. by D.R. Stinson. Vol. 773. LNCS. Springer, 1993, pp. 13–21.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*. Second. Vol. 254. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 2009, pp. xiv+355. ISBN: 978-3-540-76877-7.

[TVZ82] Michael A. Tsfasman, Sergei G. Vlăduţ, and T. Zink. "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound". In: *Math. Nach.* 109.1 (1982), pp. 21–28.

[Yu+19] Yu Yu, Jiang Zhang, Jian Weng, Chun Guo, and Xiangxue Li. "Collision Resistant Hashing from Sub-exponential Learning Parity with Noise". In: *ASIACRYPT (2)*. Vol. 11922. Lecture Notes in Computer Science. Springer, 2019, pp. 3–24.