On Codes and Learning With Errors Over Function Fields

Maxime Bombar, Alain Couvreur, Thomas Debris-Alazard

LIX, École Polytechnique & Inria

GT Grace

March, 22 2022

Outline

A hard computational problem

Error correcting code

- $\mathscr{C} = \{\boldsymbol{mG} \mid \boldsymbol{m} \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^n$;
- Hamming weight: $|\boldsymbol{x}| \stackrel{\text{def}}{=} \#\{i \mid x_i \neq 0\}$.
- Hamming distance: $d_H(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} |\boldsymbol{x} - \boldsymbol{y}|$.

Decoding Problem - DP

Data. $(\boldsymbol{G}, \mathbf{y} = \boldsymbol{mG} + \boldsymbol{e})$ with $\boldsymbol{G} \stackrel{\$}{\leftarrow} \mathbb{F}_q^{k \times n}$, $\boldsymbol{m} \stackrel{\$}{\leftarrow} \mathbb{F}_q^k$ and $\boldsymbol{e} \leftarrow \mathbb{F}_q^n$ such that $|\boldsymbol{e}| = t$.

Goal. Find $\boldsymbol{m}$.

Code-based cryptography

Decoding Problem in cryptography

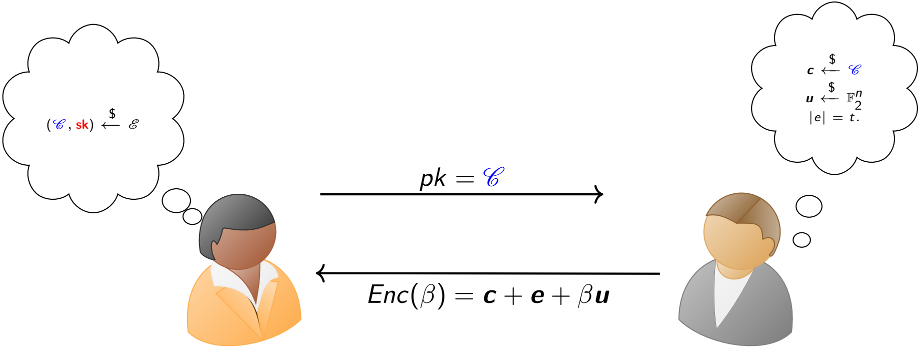
- McEliece (1978)
- **Alekhnovich** (2003)

Alekhnovich cryptosystem (2003)

$t \ll n$

$\mathscr{E} = \{(\mathscr{C}, \mathbf{sk}) \mid \mathscr{C} \text{ is a code with } \mathbf{sk} \in \mathscr{C}^{\perp} \text{ of weight } t\}$

Encrypt one bit $\beta \in \{0, 1\}$.



Alekhnovich cryptosystem (2003)

Encrypt one bit $\beta \in \{0, 1\}$.

$$Enc(\beta) = \begin{cases} \boldsymbol{c} + \boldsymbol{e} & \text{if } \beta = 0 \\ \text{random} & \text{if } \beta = 1 \end{cases}$$

Decryption

- $\langle \mathbf{sk}, Enc(0) \rangle = \langle \mathbf{sk}, \boldsymbol{c} + \boldsymbol{e} \rangle = \langle \mathbf{sk}, \boldsymbol{e} \rangle = 0$ w.h.p.
- $\langle \mathbf{sk}, Enc(1) \rangle = \langle \mathbf{sk}, random \rangle = 0$ with proba $\frac{1}{2}$.

Message Security

Hard to distinguish $\boldsymbol{c} + \boldsymbol{e}$ from random.

Decision Decoding Problem

- $(\boldsymbol{G}, \boldsymbol{y}) \leftarrow \mathcal{D}_0$ if $\boldsymbol{G} \xleftarrow{\$} \mathbb{F}_q^{k \times n}$ and $\boldsymbol{y} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ where $\boldsymbol{m} \xleftarrow{\$} \mathbb{F}_q^k$ and $|\boldsymbol{e}| = t$.
- $(\boldsymbol{G}, \boldsymbol{y}) \leftarrow \mathcal{D}_1$ if $\boldsymbol{G} \xleftarrow{\$} \mathbb{F}_q^{k \times n}$ and $\boldsymbol{y} \xleftarrow{\$} \mathbb{F}_q^n$.

Decision Decoding Problem

Data. $(\boldsymbol{G}, \boldsymbol{y}) \leftarrow \mathcal{D}_b$ where $b \xleftarrow{\$} \{0, 1\}$.

Question. Is $b = 0$ or $b = 1$?

Goal. Good answer with proba $\frac{1}{2} + \varepsilon$.

Fisher, Stern (1996), Alekhnovich (2003)

Decision Decoding Problem is harder than Search Decoding Problem.

Efficiency ?

Public-key = Random code = Random matrix
$\Rightarrow$ Huge public key: $\Theta(n^2)$
$\Theta(\lambda^4)$ for security of 2^λ

Reducing the size of the key ?

Quasi-Cyclic codes

Idea: Use codes with many automorphisms, *e.g. Quasi-Cyclic*.

Codes having a generator (or parity-check) matrix formed by multiple circulant blocks

$$G = \begin{pmatrix} \boldsymbol{a}^{(1)} & \cdots & \boldsymbol{a}^{(r)} \\ \circlearrowright & \cdots & \circlearrowright \end{pmatrix}$$

$\Rightarrow$ Public key is now only one row.

Polynomial representation

$$\mathcal{R} = \mathbb{F}_q[X]/(X^n - 1)$$

Isomorphism between circulant matrices and polynomial ring.

$$\begin{pmatrix} a_0 & a_1 & \dots & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & \dots & a_{n-2} \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{pmatrix} \xrightarrow{\simeq} \boldsymbol{a}(X) = \sum_{i=0}^{n-1} a_i X^i \in \mathcal{R}$$

$$\boldsymbol{m} \begin{pmatrix} \boldsymbol{a}^{(1)} & \boldsymbol{a}^{(2)} \\ \circlearrowleft & \circlearrowleft \end{pmatrix} + \begin{pmatrix} \boldsymbol{e}^{(1)} & \boldsymbol{e}^{(2)} \end{pmatrix} \xrightarrow{\simeq} \begin{cases} \boldsymbol{m}(x)\boldsymbol{a}^{(1)}(X) + \boldsymbol{e}^{(1)}(X) \in \mathcal{R} \\ \\ \boldsymbol{m}(x)\boldsymbol{a}^{(2)}(X) + \boldsymbol{e}^{(2)}(X) \in \mathcal{R} \end{cases}$$

Structured versions of Decoding Problems

$$\mathcal{R} \text{ Ring, } e.g.\ \mathbb{F}_q[X]/(X^n - 1)$$

Search version

Data. r samples $(\boldsymbol{a}, \mathbf{b} = \boldsymbol{m}\boldsymbol{a} + \boldsymbol{e})$ with <u>same</u> $\boldsymbol{m} \xleftarrow{\$} \mathcal{R}$, where $\boldsymbol{a} \xleftarrow{\$} \mathcal{R}$, and $\boldsymbol{e} \leftarrow \mathcal{R}$ such that $|\boldsymbol{e}| = t$.

Goal. Find $\boldsymbol{m}$.

Decision version

Data. r samples $(\boldsymbol{a}, \boldsymbol{b})$ where either all $\boldsymbol{b}$ are uniformly random, or are of the form $\boldsymbol{m}\boldsymbol{a} + \boldsymbol{e}$.

Goal. Distinguish between these two cases.

Structured versions of Decoding Problems

- Security of several code-based cryptosystems rely on the QC versions.
- No known search to decision reduction.
- "*During the third round, NIST encourages further research into the relationship between the decision and search versions of the QCSD with parity problems*" $\sim$ Nist Second Round report.
- Ring-LPN is a special case when rate goes to zero, and error is Bernouilli.

Outline

1. Motivations
2. Function Field Decoding Problem
3. Carlitz module
4. Instantiations & applications

Learning With Errors (2005)

$$\begin{array}{c} a_1 \cdots\cdots\cdots a_r \\ \begin{pmatrix} \quad & \quad & \quad \\ \quad & \quad & \quad \\ \quad & \quad & \quad \end{pmatrix} \end{array}, \begin{array}{c} a_1 \cdots\cdots\cdots a_r \\ \begin{pmatrix} \quad & \quad & \quad \\ \quad & \quad & \quad \\ \quad & \quad & \quad \end{pmatrix} \end{array} \begin{pmatrix} \\ s \\ \\ \end{pmatrix} + \begin{pmatrix} \quad \\ \quad \\ \quad \end{pmatrix} \begin{array}{c} e_1 \\ \vdots \\ e_r \end{array} \in (\mathbb{Z}/q\mathbb{Z})^n$$

Search LWE

Data. Independent $(\boldsymbol{a}, b = \langle \boldsymbol{a}, \boldsymbol{s} \rangle + e \in \mathbb{Z}/q\mathbb{Z})$ with secret $\boldsymbol{s}$, where $\boldsymbol{a}$ random and e distributed according to some discrete Gaussian.

Goal. Recover $\boldsymbol{s}$.

Decision LWE

Data. Independent $(\boldsymbol{a}, b)$ where either all b are uniformly random, or are of the form $\langle \boldsymbol{a}, \boldsymbol{s} \rangle + e \mod q$.

Goal. Distinguish between these two cases.

Learning With Errors (2005)

Hard Problems in Euclidean Lattices $\underset{\text{(Quantum)}}{<}$ Search LWE $=$ Decision LWE $<$ Crypto

Same issues as Alekhnovich

- Large key size
- Not very efficient

$\Rightarrow$ Structured versions

Ring-LWE (2010)

- $K = \mathbb{Q}[X]/(X^n + 1),\ n = 2^\ell$
  cyclotomic number field
- $\mathcal{O}_K = \mathbb{Z}[X]/(X^n + 1)$,
  ring of integers
- $q \in \mathbb{Z}$ prime.

$$\begin{tikzcd} \mathcal{O}_K \arrow[r, dash] \arrow[d, dash] & K \arrow[d, dash] \\ q \in \mathbb{Z} \arrow[r, dash] & \mathbb{Q} \end{tikzcd}$$

Search-RLWE

Data. Independent $(\mathbf{a}, \mathbf{b} = \mathbf{as} + \mathbf{e})$ with $\mathbf{a} \xleftarrow{\$} \mathcal{O}_K/q\mathcal{O}_K$, $\mathbf{e} \leftarrow$ Gaussian.

Goal. Find $\mathbf{s}$.

Decision-RLWE

Data. Independent $(\mathbf{a}, \mathbf{b})$ with $\mathbf{a} \xleftarrow{\$} \mathcal{O}_K/q\mathcal{O}_K$ and $\mathbf{b}$ either random or $\mathbf{as} + \mathbf{e}$.

Goal. Distinguish between these two cases.

Taking height

Idea:

- RLWE uses *Number fields* and *ring of integers* for proofs (*Krull* dimension 1).
- Can we lift $\mathbb{F}_q[X]/(X^n - 1)$ to dimension 1 ?

This Work

This work

- A new generic problem: Function Field Decoding Problem FF-DP,
- A new framework to make proofs,
- A search to decision reduction for QC-codes based on $\mathbb{F}_q[X]/(X^{q-1}-1)$,
- Search to decision reductions for structured versions of LPN,
- Applications to MPC.

Wishful thinking

Number field - Function field analogy

(Informal) Finite extensions of $\mathbb{Q}$ and finite extensions of $\mathbb{F}_q(T)$ share many properties.

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

Function Field Decoding Problem - FF-DP

- $K = \mathbb{F}_q(T)[X]/(f(T,X))$
- $\mathcal{O}_K$ ring of integers
- $Q \in \mathbb{F}_q[T]$ irreducible.
- ψ some probability distribution over $\mathcal{O}_K/Q\mathcal{O}_K$.

$$\begin{tikzcd} \mathcal{O}_K \arrow[r, dash] \arrow[d, dash] & K \arrow[d, dash] \\ Q \in \mathbb{F}_q[T] \arrow[r, dash] & \mathbb{F}_q(T) \end{tikzcd}$$

Search FF-DP

Data. Samples $(\mathbf{a}, \mathbf{b} = \mathbf{a}\boldsymbol{s} + \boldsymbol{e})$ with $\mathbf{a} \xleftarrow{\$} \mathcal{O}_K/Q\mathcal{O}_K$, $\boldsymbol{e} \leftarrow \psi$.

Goal. Find $\boldsymbol{s} \in \mathcal{O}_K/Q\mathcal{O}_K$.

Decision FF-DP

Data. Samples $(\mathbf{a}, \boldsymbol{b})$ with $\mathbf{a} \xleftarrow{\$} \mathcal{O}_K/Q\mathcal{O}_K$ and $\boldsymbol{b}$ either all random or $\mathbf{a}\mathbf{s} + \mathbf{e}$.

Goal. Distinguish between these two cases.

An example

- $K = \mathbb{F}_q(T)[X]/(X^n + T - 1)$
- $\mathcal{O}_K = \mathbb{F}_q[T][X]/(X^n + T - 1)$
- $\mathcal{O}_K / T\mathcal{O}_K = \mathbb{F}_q[X]/(X^n - 1)$
- ψ uniform over Hamming weight t

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, dash] \arrow[d, dash] & K \arrow[d, dash] \\
T \in \mathbb{F}_q[T] \arrow[r, dash] & \mathbb{F}_q(T)
\end{tikzcd}$$

- Search FF-DP = Quasi-Cyclic DP
- Decision FF-DP = Decision QC-DP

Goal: Search to decision reduction for FF-DP.

Main theorem

Let K be a function field with constant field $\mathbb{F}_q$, $Q \in \mathbb{F}_q[T]$ irreducible.

Assume that

(1) K is a Galois extension of $\mathbb{F}_q(T)$ of not too large degree.

(2) Ideal $\mathfrak{P} = Q\mathcal{O}_K$ does not ramify and has not too large inertia.

(3) For all $\sigma \in \mathrm{Gal}(K/\mathbb{F}_q(T))$, if $x \leftarrow \psi$ then $\sigma(x) \leftarrow \psi$.

Then solving decision FF-DP is as hard as solving search FF-DP.

(2) $\Leftrightarrow \mathfrak{P} = \mathfrak{P}_1 \dots \mathfrak{P}_r$ with $\mathfrak{P}_i$ prime ideals and $\mathcal{O}_K/\mathfrak{P}_i = \mathbb{F}_{q^\ell}$ with ℓ *small*.

Search to decision reduction

$$as + e \in \mathcal{O}_K/\mathfrak{P} \simeq \mathcal{O}_K/\mathfrak{P}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{P}_r$$

With CRT notations,

$$\mathcal{H}_i = \{(r_1, \ldots, r_i, as + e, \ldots, as + e) \mid r_i \xleftarrow{\$} \mathcal{O}_K/\mathfrak{P}_i\}$$

$$\begin{aligned} \mathcal{H}_0 = &\quad \text{Distribution of } as + e \\ \mathcal{H}_r = &\quad \text{Uniform distribution} \end{aligned}$$

(Step 1) Hybrid Argument

If $\mathscr{A}$ distinguishes $\mathcal{H}_0$ from $\mathcal{H}_r$ then $\mathscr{A}$ distinguishes $\mathcal{H}_i$ from $\mathcal{H}_{i-1}$ for some i.

Search to decision reduction

$$as + e \in \mathcal{O}_K/\mathfrak{P} \simeq \mathcal{O}_K/\mathfrak{P}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{P}_r$$

$$\mathcal{H}_i = \{(r_1, \ldots, r_i, as + e, \ldots, as + e) \mid r_i \xleftarrow{\$} \mathcal{O}_K/\mathfrak{P}_i\}$$

(Step 2) Guess and search

- $\boldsymbol{g} \in \mathcal{O}_K/\mathfrak{P}_i$ guess for $s \mod \mathfrak{P}_i$.
- $\boldsymbol{v} \xleftarrow{\$} \mathcal{O}_K/\mathfrak{P}_i \quad ; \quad \boldsymbol{h} = \mathrm{CRT}^{-1}(\mathbf{r_1}, \ldots, \mathbf{r_{i-1}}, 0, \ldots, 0)$
- $(\mathbf{a}, \mathbf{b} = \mathbf{a}\boldsymbol{s} + \boldsymbol{e}) \mapsto (\boldsymbol{a}', \boldsymbol{b}') = (\mathbf{a} + \boldsymbol{v}, \mathbf{b} + \boldsymbol{v}\boldsymbol{g} + \boldsymbol{h})$
- $\mathbf{a}' =$ random
- $\boldsymbol{b}' = \mathbf{a}'\boldsymbol{s} + (\boldsymbol{g} - \boldsymbol{s})\boldsymbol{v} + \boldsymbol{e} + \boldsymbol{h}$
- $$\boldsymbol{b}' = \begin{cases} \mathbf{a}'\boldsymbol{s} + \boldsymbol{e} \mod \mathfrak{P}_i & \text{If guess is good} \\ \text{random} \mod \mathfrak{P}_i & \text{If guess is wrong} \end{cases}$$

Search to decision reduction

$$as + e \in \mathcal{O}_K/\mathfrak{P} \simeq \mathcal{O}_K/\mathfrak{P}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{P}_r$$

$$\mathcal{H}_i = \{(r_1, \ldots, r_i, as + e, \ldots, as + e) \mid r_i \xleftarrow{\$} \mathcal{O}_K/\mathfrak{P}_i\}$$

(Step 2 cont'd) Guess and search

- $\mathbf{a}' =$ random
- $$\boldsymbol{b}' \leftarrow \begin{cases} \mathcal{H}_{i-1} & \text{If guess is good} \\ \mathcal{H}_i & \text{If guess is wrong} \end{cases}$$
- $\Rightarrow \mathscr{A}$ can tell whether we guessed correctly !

We can recover $\boldsymbol{s} \mod \mathfrak{P}_i$ with an exhaustive search in $\mathcal{O}_K/\mathfrak{P}_i = \mathbb{F}_{q^\ell}$.

Search to decision reduction

$$as + e \in \mathcal{O}_K/\mathfrak{P} \simeq \mathcal{O}_K/\mathfrak{P}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{P}_r$$

We can recover $\boldsymbol{s} \mod \mathfrak{P}_i$.

Fact. For any j there exists $\sigma \in \mathrm{Gal}(K/\mathbb{F}_q(T))$ such that $\sigma(\mathfrak{P}_j) = \mathfrak{P}_i$.

(Step 3) Permute the factors

$(\mathbf{a}, \mathbf{b}) \mapsto (\sigma(\mathbf{a}), \sigma(\mathbf{b}))$

- $\sigma(\mathbf{a}) \xleftarrow{\$} \mathcal{O}_K/\mathfrak{P}$;
- $\sigma(\mathbf{b}) = \sigma(\mathbf{a})\sigma(\boldsymbol{s}) + \sigma(\boldsymbol{e})$;
- If $\sigma(\boldsymbol{s}) \equiv s_i \mod \mathfrak{P}_i$ then $\boldsymbol{s} \equiv \sigma^{-1}(s_i) \mod \mathfrak{P}_j$;
- ⚠ σ needs to keep distribution of $\boldsymbol{e}$.

How to instantiate FF-DP ?

What do we need ?

- Galois function field $K/\mathbb{F}_q(T)$ with small field of constants;
- Nice behaviour of places;
- Galois invariant distribution.

Ring-LWE instantiation with cyclotomic number fields.

Outline

Cyclotomic function field (Bad idea)

We want an analogue of cyclotomic number field.

$\mathbb{Q}[\zeta_n]$ is built by adding the n-th roots of 1.
What about $\mathbb{F}_q(T)$?

A false good idea

Adding roots of 1 to $\mathbb{F}_q(T)$ yields <u>extension of constants</u>
$\Rightarrow$ We get $\mathbb{F}_{q^m}(T)$.

Reduction needs an exhaustive search ...

Cyclotomic function field (Good idea)

Intuition:

- $\overline{\mathbb{Q}}^{\times}$ is endowed with a $\mathbb{Z}$-module structure by $n \cdot z \stackrel{\text{def}}{=} z^n$.
- $\mathbb{U}_n = \{z \in \overline{\mathbb{Q}} \mid z^n = 1\} = n$-torsion elements.

Idea:

- $\mathbb{Z} \leftrightarrow \mathbb{F}_q[T] \Rightarrow$ Consider a new $\mathbb{F}_q[T]$-module structure on $\overline{\mathbb{F}_q(T)}$.
- Add torsion elements to $\mathbb{F}_q(T)$.

Carlitz Polynomials

For $M \in \mathbb{F}_q[T]$ define $[M] \in \mathbb{F}_q(T)[X]$ by:

- $[1](X) = X$
- $[T](X) = X^q + TX$
- $\mathbb{F}_q$-Linearity + $[M_1 M_2](X) = [M_1]([M_2](X))$

Fact. $[M]$ is a q-polynomial in X with coefficients in $\mathbb{F}_q[T]$.

Examples:

- For $c \in \mathbb{F}_q$, $[c](X) = cX$
- $[T^2](X) = (X^q + TX)^q + T(X^q + TX) = X^{q^2} + (T^q + T)X^q + T^2 X$

Carlitz Module

Fact. $\mathbb{F}_q[T]$ acts on $\overline{\mathbb{F}_q(T)}$ by $M \cdot z = [M](z)$.
$\overline{\mathbb{F}_q(T)}$ endowed with this action is called the $\mathbb{F}_q$-Carlitz module.

- $\Lambda_M \stackrel{\text{def}}{=} \{z \in \overline{\mathbb{F}_q(T)} \mid [M](z) = 0\}$ M-torsion elements $\simeq \mathbb{U}_n$.
- $\mathbb{F}_q(T)[\Lambda_M] =$ cyclotomic function field.
- $\mathrm{Gal}(K/\mathbb{F}_q(T)) \simeq (\mathbb{F}_q[T]/(M))^\times$ (Efficiently computable).

Cyclotomic VS Carlitz

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

Important example

$$[T](X) = X^q + TX$$

$$\Lambda_T = \{z \mid z^q + Tz = 0\} = \{0\} \cup \{z \mid z^{q-1} = -T\};$$

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

$$\mathcal{O}_K = \mathbb{F}_q[T][X]/(X^{q-1} + T);$$

$$\mathrm{Gal}(K/\mathbb{F}_q(T)) = (\mathbb{F}_q[T]/T)^\times = \mathbb{F}_q^\times;$$

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

Outline

Quasi–Cyclic Decoding

- $K = \mathbb{F}_q(T)[\Lambda_T]$, $\qquad \mathcal{O}_K/(T+1)\mathcal{O}_K = \mathbb{F}_q[X]/(X^{q-1}-1)$.
- $\mathrm{Gal}(K/\mathbb{F}_q(T)) = \mathbb{F}_q^\times$ acts on $\mathbb{F}_q[X]/(X^{q-1}-1)$ via
  $\zeta \cdot P(X) = P(\zeta X) \Rightarrow$ Support is Galois invariant !

Search to decision reduction

Decision $QC-$decoding in $\mathbb{F}_q[X]/(X^{q-1}-1)$ is as hard as Search.

This assumption has also been used for MPC.

Ring-LPN

$p \in [0, 1/2)$, ring $\mathcal{R} = \mathbb{F}_q[X]/(f(X))$ with $f(X) = f_1(X) \cdots f_r(X)$.

- Samples $(\boldsymbol{a}, \boldsymbol{as} + \boldsymbol{e})$.
- What is the error distribution ?

Ring-LPN

$p \in [0, 1/2)$, ring $\mathcal{R} = \mathbb{F}_q[X]/(f(X))$ with $f(X) = f_1(X) \cdots f_r(X)$.

- Samples $(\boldsymbol{a}, \boldsymbol{as} + \boldsymbol{e})$.
- What is the error distribution ?

$\boldsymbol{e}(X) = e_0 + e_1 X + \cdots + e_{r-1} X^{r-1}$ with independent $e_i \leftarrow \mathcal{B}_q(p)$.

Ring-LPN

$p \in [0, 1/2)$, ring $\mathcal{R} = \mathbb{F}_q[X]/(f(X))$ with $f(X) = f_1(X) \cdots f_r(X)$.

- Samples $(\boldsymbol{a}, \boldsymbol{as} + \boldsymbol{e})$.
- What is the error distribution ?

$\boldsymbol{e}(X) = e_0 + e_1 X + \cdots + e_{r-1} X^{r-1}$ with independent $e_i \leftarrow \mathcal{B}_q(p)$.

Not Galois invariant ...

Ring-LPN

$p \in [0, 1/2)$, ring $\mathcal{R} = \mathbb{F}_q[X]/(f(X))$ with $f(X) = f_1(X) \cdots f_r(X)$.

- Samples $(\boldsymbol{a}, \boldsymbol{as} + \boldsymbol{e})$.
- What is the error distribution ?

$\boldsymbol{e}(X) = e_0 + e_1 X + \cdots + e_{r-1} X^{r-1}$ with independent $e_i \leftarrow \mathcal{B}_q(p)$.

Not Galois invariant ...

Idea: Change the basis

Ring-LPN

$p \in [0, 1/2)$, ring $\mathcal{R} = \mathbb{F}_q[X]/(f(X))$ with $f(X) = f_1(X) \cdots f_r(X)$.

- Samples $(\boldsymbol{a}, \boldsymbol{as} + \boldsymbol{e})$ where $\boldsymbol{e} = e_0\beta_0 + \cdots + e_{r-1}\beta_{r-1}$ and $e_i \leftarrow \mathcal{B}_q(p)$.

e.g. Canonical basis $(1, X, \ldots, X^{r-1})$.

Normal Distribution Ring-LPN

- If $f_i(X)$ have the same degree d, then $\mathcal{R} \simeq \mathcal{O}_K / T\mathcal{O}_K$ where K is some explicit Carlitz extension in which T has inertia d and does not ramify.
- $\mathcal{O}_K / T\mathcal{O}_K$ admits many $\mathbb{F}_q$–Galois invariant basis.
- Decision Ring-LPN with respect to such a basis is as hard as Search.

Conclusion

	Ring-LWE	FF-DP	
2010:	Cyclotomic number fields Special modulus	Galois function fields Special modulus	✓
2014:	Any modulus	?	✗
2017-2018:	Any number field Completely different technique: OHCP	?	✗

Already useful for special QC codes used in MPC, or for particular Ring-LPN.

Extension to any function field would apply to codes like in BIKE or HQC.

Conclusion and perspectives

Perspectives.

- Extensions to more general function fields, and modulus.
- Study this problem on its own
- Inspect what happens at infinity ?

For MPC we would like K such that

- $\mathcal{O}_K/T\mathcal{O}_K \simeq \mathbb{F}_2^N$ with $N \simeq 2^{20}$ or 2^{30}
- Efficient representation of *sparse* elements of $\mathcal{O}_K$ or $\mathcal{O}_K/T\mathcal{O}_K$
- Efficient multiplication.

Thank you for your attention.