On Codes and Learning With Errors Over Function Fields

Maxime Bombar, Alain Couvreur, Thomas Debris-Alazard

LIX, École polytechnique & Inria

Caramba seminar

May 03, 2022

Outline

Code-based encryption schemes

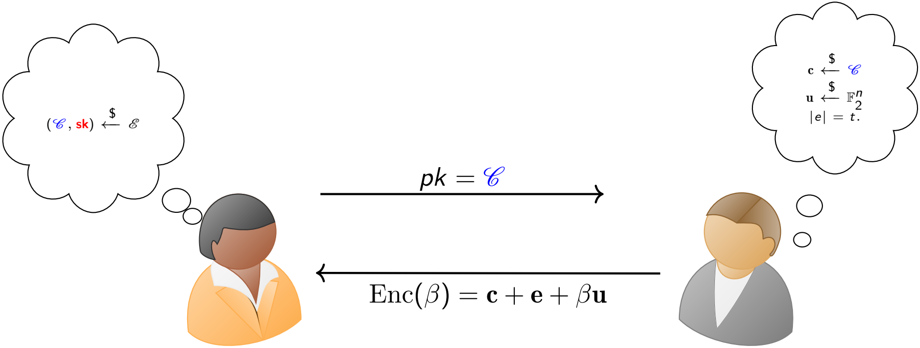
Decoding Problem in cryptography

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

Alekhnovich cryptosystem (2003)

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

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



Alekhnovich cryptosystem (2003)

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

$$\mathrm{Enc}(\beta) = \begin{cases} \mathbf{c}+\mathbf{e} \quad (\text{where } \textbf{sk} \perp \mathbf{c}) & \text{if } \beta = 0 \\ \text{random} & \text{if } \beta = 1 \end{cases}$$

Decryption

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

Message Security

Hard to **distinguish** $\mathbf{c}+\mathbf{e}$ from random $\approx$ Code-based analogue of DDH.

Decoding Problems

Search/Computational Decoding Problem

Data. Random matrix $\mathbf{G}$ and noisy codeword $\mathbf{mG} + \mathbf{e}$ with $|\mathbf{e}| = t$.

Goal. Recover $\mathbf{m}$.

Decisional Decoding Problem

Data. $(\mathbf{G}, \mathbf{b})$ where $\mathbf{b}$ is either random, or noisy codeword $\mathbf{mG} + \mathbf{e}$ with $|\mathbf{e}| = t$.

Goal. Distinguish between these two cases.

Fisher, Stern (1996)

Decisional Decoding Problem is as hard as Search Decoding Problem.

Efficiency Alekhnovich ?

Public-key = random $\mathscr{C}$ represented by $\mathbf{G} \in \mathbb{F}_q^{k \times n}$

Huge public-key: $\Theta(n^2)$

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

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

$\Rightarrow$ 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.

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

$$\mathbf{m} \begin{pmatrix} \mathbf{a}^{(1)} & \mathbf{a}^{(2)} \\ \circlearrowright & \circlearrowright \end{pmatrix} + \begin{pmatrix} \mathbf{e}^{(1)} & \mathbf{e}^{(2)} \end{pmatrix} \xrightarrow{\sim} \begin{cases} \mathbf{m}(X)\mathbf{a}^{(1)}(X) + \mathbf{e}^{(1)}(X) \in \mathcal{R} \\ \mathbf{m}(X)\mathbf{a}^{(2)}(X) + \mathbf{e}^{(2)}(X) \in \mathcal{R} \end{cases}$$

Structured versions of Decoding Problems

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

Search version

Data. Samples $(\mathbf{a}^{(i)}, \mathbf{b}^{(i)} = \mathbf{m}\mathbf{a}^{(i)} + \mathbf{e}^{(i)})$ with same $\mathbf{m} \xleftarrow{\$} \mathcal{R}$, where $\mathbf{a}^{(i)} \xleftarrow{\$} \mathcal{R}$, and $\mathbf{e}^{(i)} \leftarrow \mathcal{R}$ such that $|\mathbf{e}^{(i)}| = t$.

Goal. Find $\mathbf{m} \in \mathcal{R}$.

Decisional version

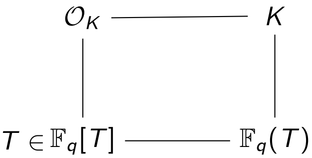
Data. Samples $(\mathbf{a}^{(i)}, \mathbf{b}^{(i)})$ where either all $\mathbf{b}^{(i)}$ are uniformly random, or are of the form $\mathbf{m}\mathbf{a}^{(\mathbf{i})} + \mathbf{e}^{(\mathbf{i})}$.

Goal. Distinguish between these two cases.

NO known reduction...

Taking height

$$\underbrace{\mathbb{F}_q[X]/(X^n-1)}_{\text{World of Computations}} = \mathbb{F}_q[T][X]/(T, X^n + T - 1) = \underbrace{\mathcal{O}_K/T\mathcal{O}_K}_{\text{World of Proofs}}$$



Idea:

- Get inspired by Euclidean lattices
- Number field - Function field analogy

Learning With Errors (2005)

$$\left(\overset{a^{(1)} \,\cdots\cdots\, a^{(r)}}{\boxed{}}\right), \left(\overset{a^{(1)} \,\cdots\cdots\, a^{(r)}}{\boxed{}}\right)\left(\boxed{s}\right) + \left(\;\right)\begin{matrix} e^{(1)} \\ \vdots \\ e^{(r)} \end{matrix} \in (\mathbb{Z}/q\mathbb{Z})^r$$

Search LWE

Data. Samples $(\mathbf{a}^{(i)}, b^{(i)} = \langle \mathbf{a}^{(i)}, \mathbf{s} \rangle + e^{(i)} \in \mathbb{Z}/q\mathbb{Z})$ with same $\mathbf{s}$, where $\mathbf{a}^{(i)} \xleftarrow{\$} \mathbb{Z}/q\mathbb{Z}$ and $e^{(i)}$ is distributed according to some discrete Gaussian.

Goal. Recover $\mathbf{s}$.

Decision LWE

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

Goal. Distinguish between these two cases.

Learning With Errors (2005)

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

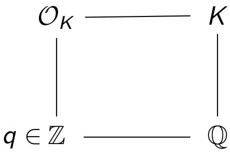
Same issues as Alekhnovich

- Large key size
- Not very efficient

$\Rightarrow$ Structured versions

Ring-LWE [LPR10]

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



Search-RLWE

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

Goal. Find $\mathbf{s}$.

Decision-RLWE

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

Goal. Distinguish between these two cases.

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.

Outline

Number field - Function field analogy

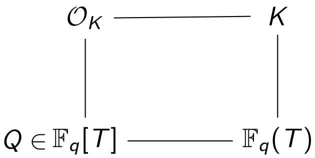
An old analogy

(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 $\mathcal{O}_K/Q\mathcal{O}_K$.



Search FF-DP

Data. Samples $(\mathbf{a}^{(\mathbf{i})}, \mathbf{b}^{(\mathbf{i})} = \mathbf{m}\mathbf{a}^{(\mathbf{i})} + \mathbf{e}^{(i)})$ with $\mathbf{a}^{(\mathbf{i})} \stackrel{\$}{\leftarrow} \mathcal{O}_K/Q\mathcal{O}_K$, $\mathbf{e}^{(i)} \leftarrow \psi$.

Goal. Find $\mathbf{m} \in \mathcal{O}_K/Q\mathcal{O}_K$.

Decision FF-DP

Data. Samples $(\mathbf{a}^{(\mathbf{i})}, \mathbf{b}^{(i)})$ with $\mathbf{a}^{(\mathbf{i})} \stackrel{\$}{\leftarrow} \mathcal{O}_K/Q\mathcal{O}_K$ and $\mathbf{b}^{(i)}$ either all random or $\mathbf{m}\mathbf{a}^{(\mathbf{i})} + \mathbf{e}^{(\mathbf{i})}$.

Goal. Distinguish between these two cases.

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) $\Leftrightarrow \mathfrak{P} = \mathfrak{P}_1 \ldots \mathfrak{P}_r$ 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,

$$\mathcal{H}_i = \left\{(r_1, \ldots, r_i, (as + e \mod \mathfrak{P}_{i+1}), \ldots, (as + e \mod \mathfrak{P}_r)) \mid r_\ell \xleftarrow{\$} \mathcal{O}_K/\mathfrak{P}_\ell\right\}$$

$\mathcal{H}_0 =$ Distribution of $as + e$
$\mathcal{H}_r =$ Uniform distribution

(Step 1) Hybrid Argument

If $\mathscr{A}$ distinguishes $\mathcal{H}_0$ from $\mathcal{H}_r$ then $\mathscr{A}$ distinguishes $\mathcal{H}_{i_0}$ from $\mathcal{H}_{i_0-1}$ for some i_0.

Search to decision reduction

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

$$\mathcal{H}_i = \left\{(r_1, \ldots, r_i, (as + e \mod \mathfrak{P}_{i+1}), \ldots, (as + e \mod \mathfrak{P}_r)) \mid r_\ell \xleftarrow{\$} \mathcal{O}_K/\mathfrak{P}_\ell\right\}$$

(Step 2) Guess and search

- $\mathbf{g} \in \mathcal{O}_K/\mathfrak{P}_{i_0}$ guess for $s \mod \mathfrak{P}_{i_0}$.
- $\mathbf{v} \xleftarrow{\$} \mathcal{O}_K/\mathfrak{P}_{i_0}$; $\mathbf{h} = \mathrm{CRT}^{-1}(\mathbf{r_1}, \ldots, \mathbf{r_{i_0-1}}, 0, \ldots, 0)$
- $(\mathbf{a}, \mathbf{b} = \mathbf{as} + \mathbf{e}) \mapsto (\mathbf{a}', \mathbf{b}') = (\mathbf{a} + \mathbf{v}, \mathbf{b} + \mathbf{vg} + \mathbf{h})$
- $\mathbf{a}' =$ random
- $\mathbf{b}' = \mathbf{a}'\mathbf{s} + (\mathbf{g} - \mathbf{s})\mathbf{v} + \mathbf{e} + \mathbf{h}$
- $$\mathbf{b}' = \begin{cases} \mathbf{a}'\mathbf{s} + \mathbf{e} \mod \mathfrak{P}_{i_0} & \text{If guess } \mathbf{g} \text{ is good} \\ \text{random} \mod \mathfrak{P}_{i_0} & \text{If guess } \mathbf{g} \text{ is wrong} \end{cases}$$

Search to decision reduction

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

$$\mathcal{H}_i = \left\{ (r_1, \ldots, r_i, (as + e \mod \mathfrak{P}_{i+1}), \ldots, (as + e \mod \mathfrak{P}_r)) \mid r_\ell \overset{\$}{\leftarrow} \mathcal{O}_K/\mathfrak{P}_\ell \right\}$$

(Step 2 cont'd) Guess and search

- $\mathbf{a}' =$ random
- $$\mathbf{b}' \leftarrow \begin{cases} \mathcal{H}_{i_0 - 1} & \text{If guess is good} \\ \mathcal{H}_{i_0} & \text{If guess is wrong} \end{cases}$$
- $\Rightarrow \mathscr{A}$ can tell whether we guessed correctly !

We can recover $\mathbf{s} \mod \mathfrak{P}_{i_0}$ with an exhaustive search in $\mathcal{O}_K/\mathfrak{P}_{i_0} = \mathbb{F}_{q^\ell}$.

Search to decision reduction

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

We can recover $\mathrm{s} \mod \mathfrak{P}_{i_0}$.

Fact. For any j there exists $\sigma \in \mathrm{Gal}(K/\mathbb{F}_q(T))$ such that $\sigma(\mathfrak{P}_j) = \mathfrak{P}_{i_0}$.

(Step 3) Permute the factors

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

- $\sigma(\mathbf{a}) \xleftarrow{\$} \mathcal{O}_K/\mathfrak{P}$;
- $\sigma(\mathbf{b}) = \sigma(\mathbf{a})\sigma(\mathrm{s}) + \sigma(\mathbf{e})$;
- If $\sigma(\mathrm{s}) \equiv s_{i_0} \mod \mathfrak{P}_{i_0}$ then $\mathrm{s} \equiv \sigma^{-1}(s_{i_0}) \mod \mathfrak{P}_j$;
- ⚠ σ needs to keep distribution of $\mathbf{e}$.

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

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

$\mathbb{Q}$	$\mathbb{F}_q(T)$
$\mathbb{Z}$	$\mathbb{F}_q[T]$
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)
$K = \mathbb{Q}[\zeta]$	$K = \mathbb{F}_q(T)[\lambda]$
$\mathcal{O}_K = \mathbb{Z}[\zeta]$	$\mathcal{O}_K = \mathbb{F}_q[T][\lambda]$
$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/(n))^{\times}$	$\mathrm{Gal}(K/\mathbb{F}_q(T)) \simeq (\mathbb{F}_q[T]/(M))^{\times}$
Cyclotomic	Carlitz

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

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

$\rightarrow$ It proves an asumption made in MPC.

Ring-LPN [LAPIN, HKLPK12]

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

- Samples $(\mathbf{a}^{(i)}, \mathbf{a}^{(i)}\mathbf{s} + \mathbf{e}^{(i)})$.
- What is the error distribution ?

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

Ring-LPN [LAPIN, HKLPK12]

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

- Samples $(\mathbf{a}^{(i)}, \mathbf{a}^{(i)}\mathbf{s} + \mathbf{e}^{(i)})$.
- What is the error distribution ?

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

Not Galois invariant ...

Ring-LPN [LAPIN, HKLPK12]

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

- Samples $(\mathbf{a}^{(i)}, \mathbf{a}^{(i)}\mathbf{s} + \mathbf{e}^{(i)})$.
- What is the error distribution ?

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

Not Galois invariant ...

Idea: Change the basis

Ring-LPN [LAPIN, HKLPK12]

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

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

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

Ring-LPN [LAPIN, HKLPK12]

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

- Samples $(\mathbf{a}, \mathbf{as} + \mathbf{e})$ where $\mathbf{e} = e_0\beta_0 + \cdots + e_{r-1}\beta_{r-1}$ 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 <u>any</u> function field would apply to codes like in $\mathrm{BIKE}/\mathrm{HQC}$ (NIST).

Conclusion and perspectives

FF-DP

- Other meaningful examples ?
- Other metrics ?
- Develop a "Switching-Modulus" technique
- Extensions to more general function fields

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 in $\mathcal{O}_K$ or $\mathcal{O}_K / T\mathcal{O}_K$.

Thank you for your attention.