On Codes and Learning With Errors Over Function Fields

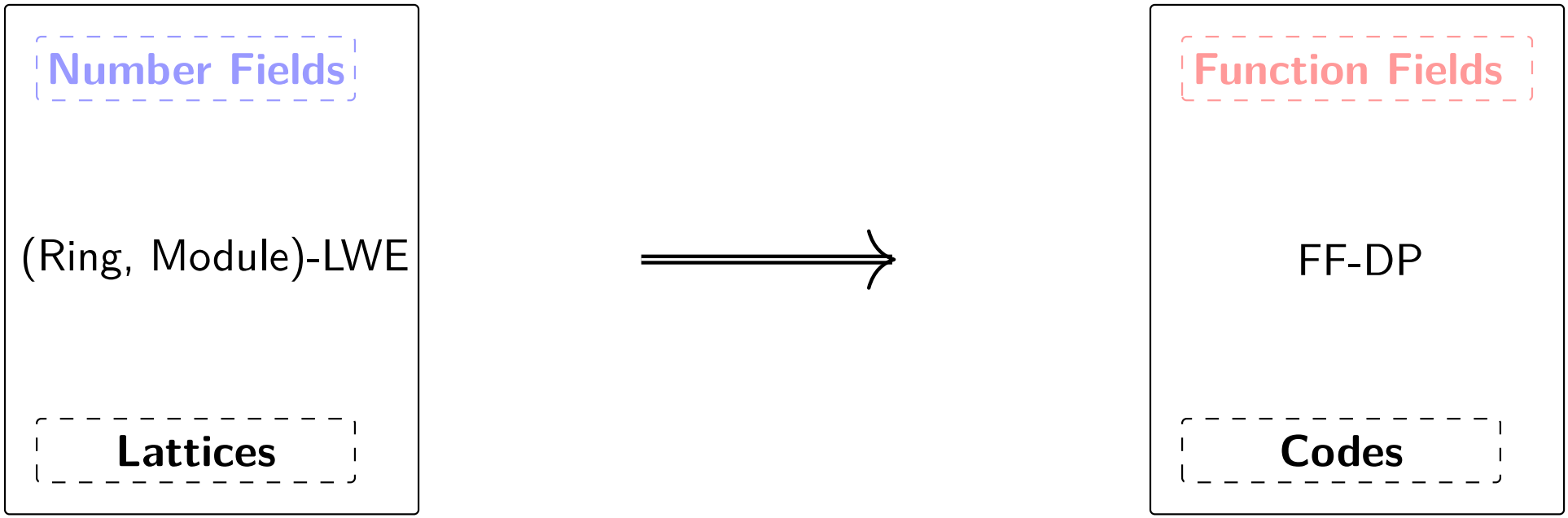
Maxime Bombar, Alain Couvreur, Thomas Debris-Alazard

LIX, École polytechnique & Inria

Crypto 2022
Santa Barbara, CA, USA

August, 2022

This Work



- First Search-to-Decision reductions for QC-Decoding Problems,
- Proves pseudorandomness assumptions in MPC.

Code-based encryption schemes

Decoding Problem in cryptography

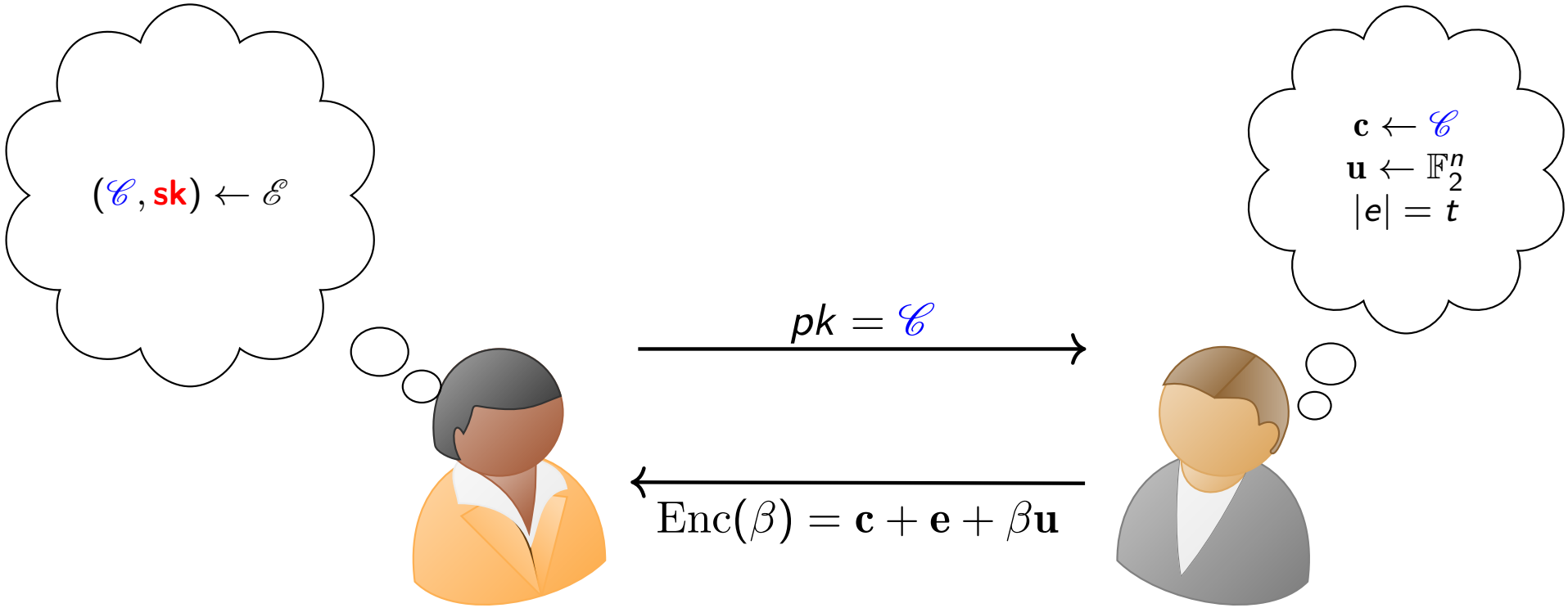
- McEliece (1978)
- **Alekhnovich** (2003)

Alekhnovich cryptosystem (2003)

$t \ll n$

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

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



Alekhnovich cryptosystem (2003)

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

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

Decryption

- $\langle \mathbf{sk}, \mathrm{Enc}(0) \rangle = \langle \mathbf{sk}, \mathbf{c}+\mathbf{e} \rangle = \langle \mathbf{sk}, \mathbf{e} \rangle = 0$ w.h.p. ($\mathbf{sk} \perp \mathbf{c}$ and $\mathbf{sk}, \mathbf{e}$ small)
- $\langle \mathbf{sk}, \mathrm{Enc}(1) \rangle = \langle \mathbf{sk}, \mathrm{random} \rangle = 0$ 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.

Fischer, 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: $\Theta(n^2)$

Slow encryption.

$\Rightarrow$ Add some structure.

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

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

$\Rightarrow$ 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.

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

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

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 $\mathbf{m} \leftarrow \mathcal{R}$, where $\mathbf{a}^{(i)} \leftarrow \mathcal{R}$, 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...

Proof ?

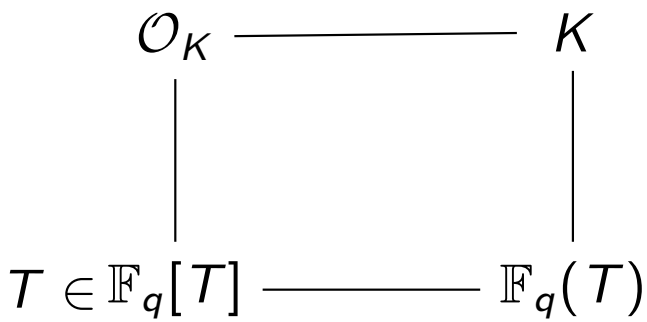
How can we prove such a search to decision reduction ?

Taking height

Idea:

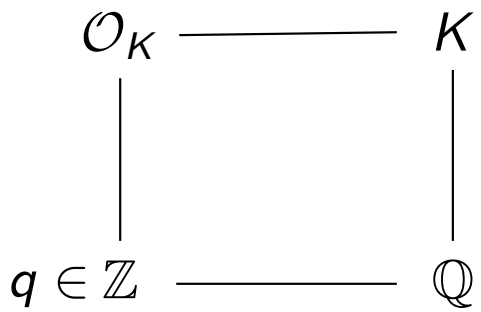
- Get inspired by Euclidean lattices
- Number field - Function field analogy

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



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 $\mathbf{a}^{(i)} \leftarrow \mathcal{O}_K/q\mathcal{O}_K$, $\mathbf{e}^{(i)} \leftarrow$ Gaussian.

Goal. Find $\mathbf{s}$.

Decision-RLWE

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

Goal. Distinguish between these two cases.

A function field version

Number field - Function field analogy

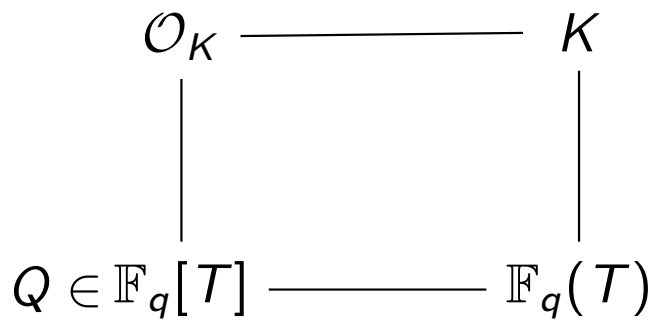
An old analogy

(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 $Q \in \mathbb{F}_q[T]$
$K = \mathbb{Q}[X]/(f(X))$	$K = \mathbb{F}_q(T)[X]/(f(T,X))$
$\mathcal{O}_K$	$\mathcal{O}_K$
= Integral closure of $\mathbb{Z}$	= Integral closure of $\mathbb{F}_q[T]$
Dedekind domain	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 $(\mathbf{a^{(i)}}, \mathbf{b^{(i)}} = \mathbf{m}\mathbf{a^{(i)}} + \mathbf{e}^{(i)})$ with $\mathbf{a^{(i)}} \leftarrow \mathcal{O}_K/Q\mathcal{O}_K$, $\mathbf{e}^{(i)} \leftarrow \psi$.

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

Decision FF-DP

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

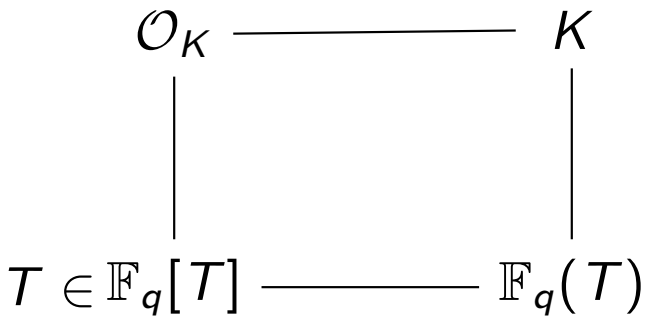
Goal. Distinguish between these two cases.

What about hardness ?

What matters is **instantiations**.

Recall previous example

- $K = \mathbb{F}_q(T)[X]/(X^n + T - 1)$
- $\mathcal{O}_K = \mathbb{F}_q[T][X]/(X^n + T - 1)$ ring of integers
- $Q(T) = T \in \mathbb{F}_q[T]$ irreducible.



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

Search FF-DP = QC-DP $\Rightarrow$ Hard !

$$(\mathbf{a}^{(i)}, \mathbf{b}^{(i)} = \mathbf{m}\mathbf{a}^{(i)} + \mathbf{e}^{(i)} \mod T\mathcal{O}_K) \approx \mathbf{m} \begin{pmatrix} \mathbf{a}^{(1)} & & \mathbf{a}^{(N)} \\ \circlearrowleft & \cdots & \circlearrowleft \end{pmatrix} + \begin{pmatrix} \mathbf{e}^{(1)} & \cdots & \mathbf{e}^{(N)} \end{pmatrix}$$

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*.

Proof follows [LPR10].

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.

Cyclotomic function field

Intuition:

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

- $\Lambda_M := \{z \in \overline{\mathbb{F}_q(T)} \mid [M](z) = 0\}$ 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)
$K = \mathbb{Q}[\zeta]$ $\mathcal{O}_K = \mathbb{Z}[\zeta]$	$K = \mathbb{F}_q(T)[\lambda]$ $\mathcal{O}_K = \mathbb{F}_q[T][\lambda]$
$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/(n))^x$	$\mathrm{Gal}(K/\mathbb{F}_q(T)) \simeq (\mathbb{F}_q[T]/(M))^x$
Cyclotomic	Carlitz

Important example

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

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

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

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

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

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

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.

$\rightarrow$ Proves an asumption made in MPC,

$\rightarrow$ Can generalize to other (quasi-)group codes,

$\rightarrow$ Other instantiations apply to several variants of Module/Ring-LPN.

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 some Ring-LPN.

Extension to any function field would apply to codes like in $\mathrm{BIKE}/\mathrm{HQC}$ (NIST).

Thank you for your attention.