On Codes and Learning With Errors Over Function Fields (Part 2)

Maxime Bombar, Alain Couvreur, Thomas Debris-Alazard

LIX, École Polytechnique & Inria

GT Grace

March, 22 + April, 19 2022

Outline

Code-based encryption schemes

Decoding Problem in cryptography

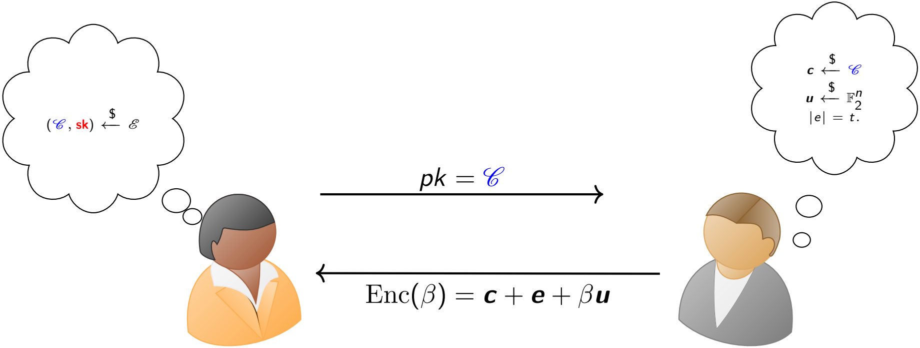
- McEliece (1978)
- **Alekhnovich** (2003)

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 $\beta \in \{0, 1\}$.

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

Decryption

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

Message Security

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

Decoding Problems

Search/Computational Decoding Problem

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

Goal. Recover $\boldsymbol{m}$.

Decisional Decoding Problem

Data. $(\boldsymbol{G}, \boldsymbol{b})$ where $\boldsymbol{b}$ is either random, <u>or</u> noisy codeword $\boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$ with $|\boldsymbol{e}| = t$.

Goal. Distinguish between these two cases.

Fisher, Stern (1996)

Decisional Decoding Problem is <u>as hard as</u> Search Decoding Problem.

Efficiency Alekhnovich ?

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

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

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

$\Rightarrow$ 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.

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

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

Structured versions of Decoding Problems

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

Search version

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

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

Decisional version

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

Goal. Distinguish between these two cases.

<u>NO</u> known reduction...

Taking height

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

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

Idea:

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

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

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

Decision FF-DP

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

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 n.

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

(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.

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 n.

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

(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.

$\varepsilon =$ decisional advantage, $t =$ running time of distinguisher.

We can recover the secret in $\mathcal{O}_K/\mathfrak{P}$ in time

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

How to instantiate FF-DP ?

What do we need ?

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

Ring-LWE instantiation with <u>cyclotomic</u> 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 $n \cdot z \overset{\text{def}}{=} z^n$.
- $\mathbb{U}_n = \{z \in \overline{\mathbb{Q}} \mid z^n = 1\} =$ 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

$\mathbb{Q}$	$\mathbb{F}_q(T)$
$\mathbb{Z}$	$\mathbb{F}_q[T]$
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)
$a \equiv b \mod n \Rightarrow \zeta^a = \zeta^b$	$A \equiv B \mod M \Rightarrow [A](\lambda) = [B](\lambda)$
$K = \mathbb{Q}[\zeta]$	$K = \mathbb{F}_q(T)[\lambda]$
$\mathcal{O}_K = \mathbb{Z}[\zeta]$	$\mathcal{O}_K = \mathbb{F}_q[T][\lambda]$
$\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/(n))^\times$	$\mathrm{Gal}(K/\mathbb{F}_q(T)) \simeq (\mathbb{F}_q[T]/(M))^\times$
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

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

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 <u>same</u> degree d, then $\mathcal{R} \simeq \mathcal{O}_K / T\mathcal{O}_K$ where K is some <u>explicit</u> 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 BIKE or HQC.

Conclusion and perspectives

Perspectives.

- Extensions to more general function fields
- Develop a "Switching-Modulus" technique

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.