Structured Codes for Cryptography: from Source of Hardness to Applications

PhD Defense

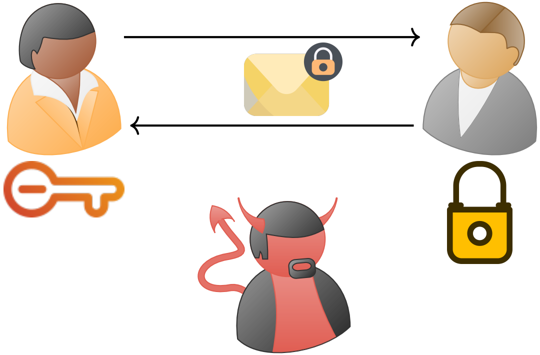
Maxime Bombar

Under the supervision of Alain Couvreur and Thomas Debris-Alazard

December 15, 2023

Outline

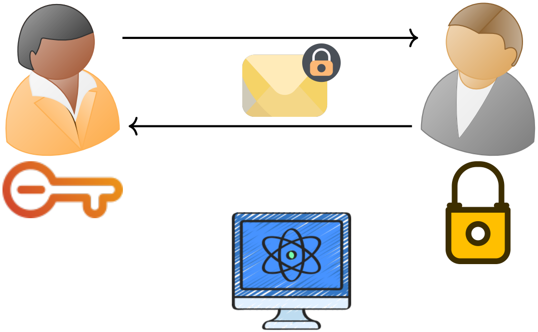
Public Key Cryptography



Hard Computational Problems

- Integer Factorisation
- (Elliptic Curve) Discrete Logarithm
- Euclidean Lattices
- Coding Theory
- ...

Public Key Cryptography



Quantum Menace (Shor, 1994)

Hard Computational Problems

- ~~Integer Factorisation~~
- ~~(Elliptic Curve) Discrete Logarithm~~
- Euclidean Lattices
- Coding Theory
- ...

Error-Based

Considered for standardisation

Input: $\left(\mathbf{A} \in \mathbb{F}_q^{k \times n},\ \mathbf{s}\mathbf{A} + \mathbf{e} \right)$

Target: $\mathbf{s} \in \mathbb{F}_q^n$

How to choose $\mathbf{e} \in \mathbb{F}_q^n$ to make this problem hard?

Error-based Cryptography

Input: $\left(\mathbf{A} \in \mathbb{F}_q^{k \times n}, \; \mathbf{s}\mathbf{A} + \mathbf{e} \right)$

Target: $\mathbf{s} \in \mathbb{F}_q^n$

How to choose $\mathbf{e} \in \mathbb{F}_q^n$ to make this problem hard?

- "Small" coefficients: Lattice-based cryptography
- Few non-zero coefficients: (Hamming) **Code-based cryptography**
- Small "rank": Rank-based cryptography

The Decoding Problem (Hamming)

Input: $\left(\mathbf{A}, \ \mathbf{s}\mathbf{A} + \mathbf{e} \right)$

Target: $\mathbf{s}$

- Studied for over 60 years (Prange, 1962);
- Hardness depends on the Hamming weight of $\mathbf{e}$;
- Very hard in some regimes.

Two approaches for Code-Based Encryption

McEliece (1978)

- Oldest cryptosystem currently not (quantumly) broken;
- Does not only relies on the Decoding Problem;
- Many instantiations have been broken (original one still secure).

Two approaches for Code-Based Encryption

McEliece (1978)

- Oldest cryptosystem currently not (quantumly) broken;
- Does not only relies on the Decoding Problem;
- Many instantiations have been broken (original one still secure).

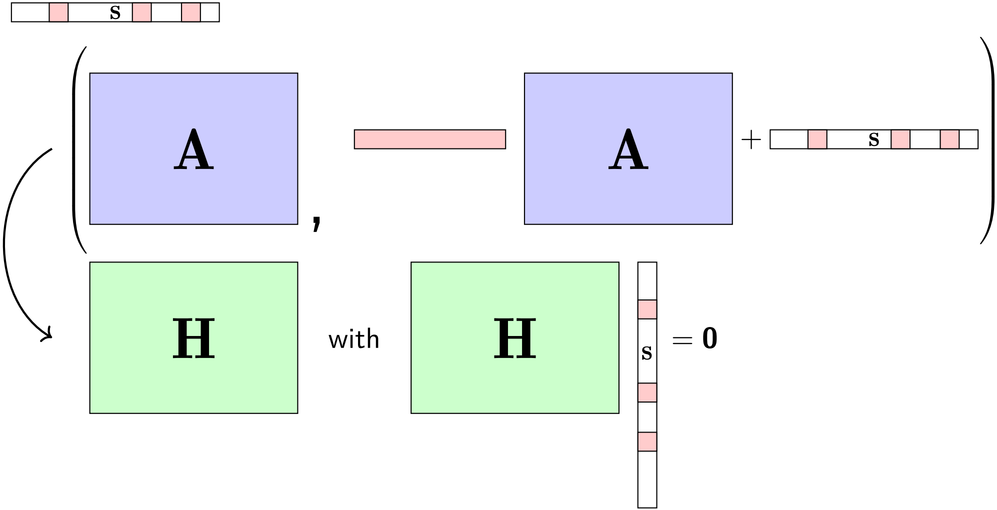
Alekhnovich (2003)

Truly relies on the Problem of Decoding random linear codes.

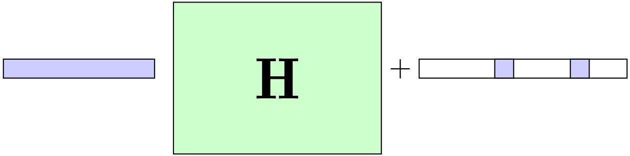
Alekhnovich cryptosystem (2003)

Secret key:

Public key:

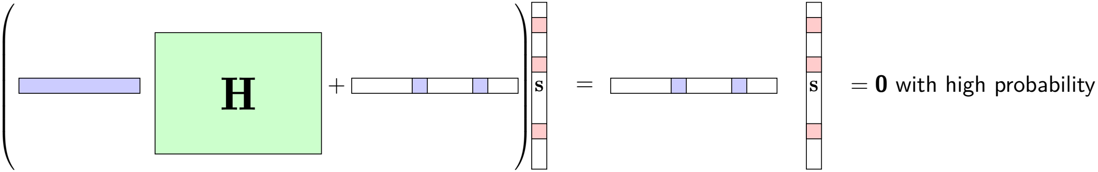


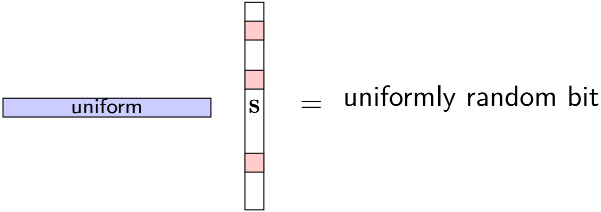
To encrypt 0, send



To encrypt 1, send

To decrypt a received $\mathbf{y} \in \mathbb{F}_2^n$ compute $\langle \mathbf{y}, \mathbf{s} \rangle$: **Distinguisher**.





The Decisional Decoding Problem

Distinguish $\left(\mathbf{A},\ \mathbf{s}\mathbf{A} + \mathbf{e}\right)$

From $\left(\mathbf{A},\ \mathbf{y}\right)$ uniform

How hard can it be?

Distinguish $\left(\mathbf{A}, \quad \mathbf{s}\mathbf{A} + \mathbf{e} \right)$

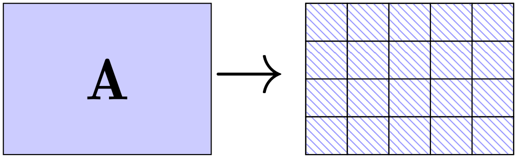
From $\left(\mathbf{A}, \quad \mathbf{y} \right)$ uniform

As hard as Decoding Problem (Search-to-Decision Reduction): (Fischer, Stern, 1996)

Adding Structure for Efficiency

$$\begin{pmatrix} a_0 & a_1 & \dots & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & \dots & a_{n-2} \\ \vdots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ a_1 & a_2 & \dots & a_{n-1} & a_0 \end{pmatrix}$$

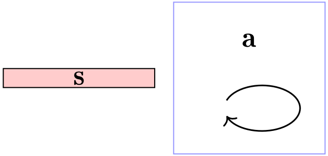
Circulant matrix



A Polynomial Representation

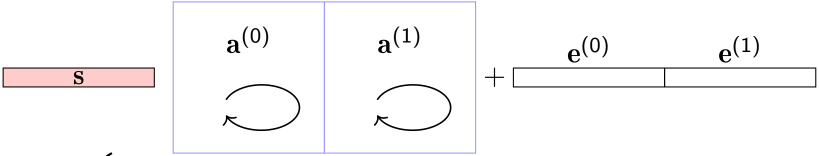
Bonus: Supports fast operations.

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



$$\longleftrightarrow \mathrm{s}(X) \cdot \mathbf{a}(X) \mod (X^n - 1)$$

A Polynomial Representation (Cont'd)



$$\begin{cases} \mathbf{s}(X)\mathbf{a}^{(0)}(X) + \mathbf{e}^{(0)}(X) \in \mathbb{F}_q[X] / (X^n - 1) \\ \\ \mathbf{s}(X)\mathbf{a}^{(1)}(X) + \mathbf{e}^{(1)}(X) \in \mathbb{F}_q[X] / (X^n - 1) \end{cases}$$

Structured Variants of the Decoding Problem

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

Search Version

Input. N samples of the form $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + \mathbf{e})$ where $\mathbf{a} \leftarrow \mathcal{R}$, and $|\mathbf{e}| = t$.

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

Decision Version

Goal. Distinguish between $(\mathbf{a}, \mathbf{y}^{\mathsf{unif}})$ and $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + \mathbf{e})$, given N samples.

Remark. BIKE and HQC (NIST 4th round).

Hardness of Structured Variants

Still believed to be hard in general

Decoding algorithms don't perform much better with Quasi-Cyclic codes.

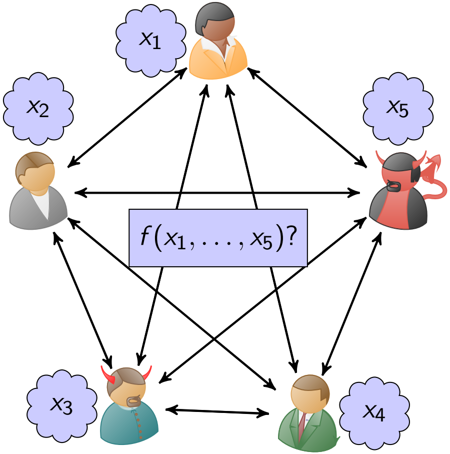
At the beginning of this thesis

No search-to-decision reduction.

Natural questions

- Which choices of $\mathcal{R}$ yield secure instances?
- Are there other applications than traditional encryption?

Secure Multi-Party Computation (MPC)



Main Bottleneck: Communication

MPC in the Correlated Randomness Model

A key observation by Beaver (1991)

- It is possible to push the secure computation **before** the inputs are known using **correlated random sequences**. ✓
- This preprocessing remains very slow. ✗

Pseudorandom Correlation Generators (Boyle, Couteau, Gilboa, Ishai 2018, + Kohl, Scholl 2019, 2020)

- Generating correlated randomness with **minimal interaction**. ✓
- Relies on variants of (Decisional) Decoding Problems.
- Structured variants for more powerful correlations, extension to N parties.

Underlying ring: $\mathbb{F}_q[X]/(F(X)) \simeq \mathbb{F}_q \times \cdots \times \mathbb{F}_q \to \deg(F) \leqslant q$ copies of $\mathbb{F}_q$.

Question: Can we reduce q?

Outline

State of Affairs

Structured codes are very appealing:

- Enable efficient cryptography;
- Even advanced primitives.

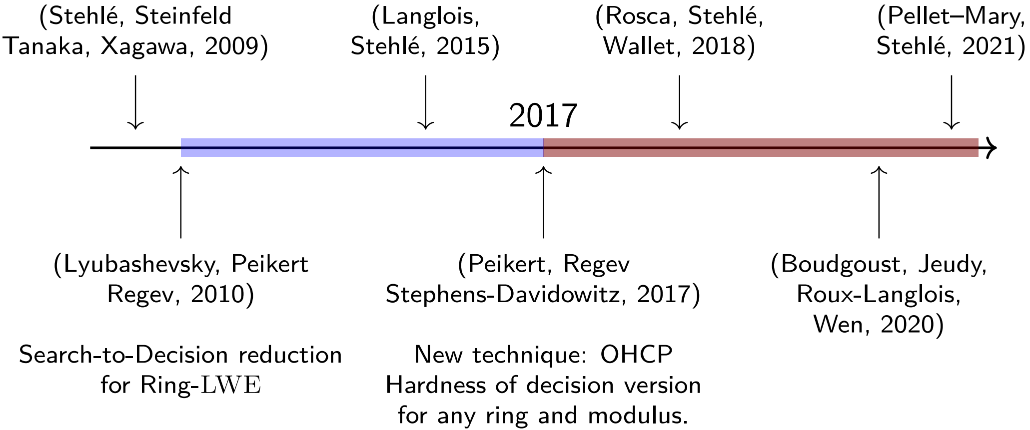
But lack of strong foundations:

- No search-to-decision reduction;
- “Exotic” structures less studied.

Lattice-based cryptography has been faced with similar issues:

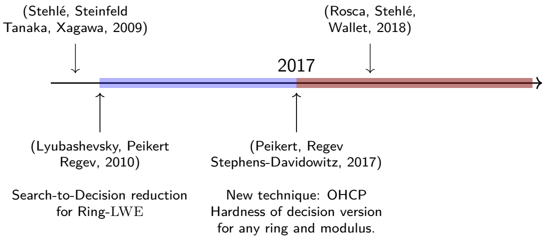
- Solved with framework from algebraic number theory;
- This is what improved faith in Euclidean lattices compared to codes.

Structured Lattices: a History of Reductions[1]

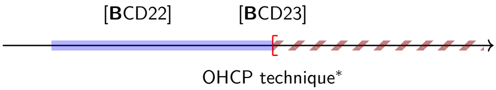


[1]Not exhaustive

Codes are Catching-Up



Lattice-Based

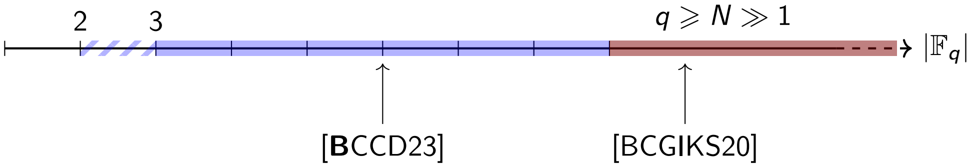


Code-Based

B., Couvreur, Debris-Alazard

- 2022: *On Codes and Learning with Errors over Function Fields*
- 2023: *Pseudorandomness of Decoding, Revisited: Adapting OHCP to Code-Based Cryptography*

$\rightarrow$ *Caveat when considering the case of structured codes.



- **B.**, Couteau, Couvreur, Ducros, 2023: *Correlated Pseudorandomness from the Hardness of Quasi-Abelian Decoding*.

- Variant of the Decoding Problem based on **Group Algebras** (Generalise Quasi-Cyclic).
- "Impossibility" result for $q = 2$.

Not a timeline

Cryptanalysis in the Rank-Metric

$\mathbb{F}_{q^m}$-linear codes endowed with the **rank-metric**: Yet another form of structured codes.

- **B.**, Couvreur, 2021: *Decoding Supercodes of Gabidulin Codes and Application to Cryptanalysis*
- **B.**, Couvreur, 2022: *Right-Hand Side Decoding of Gabidulin Codes and Applications*

Outline

A number theoretic framework

Structured lattice problems

Defined using **Number Fields** and their **Rings of Integers**.

e.g. $\mathcal{R} = {}^{\mathcal{O}_K}\!/_{q\mathcal{O}_K}$ where

- $\mathcal{O}_K = {}^{\mathbb{Z}[X]}\!/_{(X^n+1)}$, with $n = 2^\ell$.
- $q \in \mathbb{Z}$.

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

Wishful Thinking

$$\mathbb{F}_q[X]/(X^n - 1) \text{ looks similar to } \mathbb{Z}[X]/(X^n + 1).$$

Can we build analogous cryptographic constructions with both rings?

Wishful Thinking

$$\mathbb{F}_q[X]/(X^n-1) \text{ looks similar to } \mathbb{Z}[X]/(X^n+1).$$

Can we build analogous cryptographic constructions with both rings?

- $\mathbb{F}_q[X]/(X^n-1)$ has *Krull dimension* 0;
- $\mathbb{Z}[X]/(X^n+1)$ has *Krull dimension* 1.

$\rightarrow$ Analogue of $\mathcal{O}_K/q\mathcal{O}_K$ instead?

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

$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, no head] \arrow[d, no head] & K \arrow[d, no head] \\
T \in \mathbb{F}_q[T] \arrow[r, no head] & \mathbb{F}_q(T)
\end{tikzcd}$$

Idea: Number field - Function field analogy

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 error 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

Input. N samples of the form $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + \mathbf{e})$ where $\mathbf{a} \leftarrow \mathcal{O}_K/Q\mathcal{O}_K$, and $\mathbf{e} \leftarrow \psi$.

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

Decision FF-DP

Goal. Distinguish between $(\mathbf{a}, \mathbf{y}^{\text{unif}})$ and $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + \mathbf{e})$, given N samples.

Main theorem of [**B**CD22]

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** degree.

(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.

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

Proof similar to Ring-LWE from (Lyubashevsky, Peikert, Regev, 2010).

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.

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 $\mathbb{F}_{q^m}(T)$.

Cyclotomic function field (Good idea)

(Carlitz, 1938; Hayes, 1974)

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:

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

$$\Lambda_M \stackrel{\text{def}}{=} \left\{\lambda \in \overline{\mathbb{F}_q(T)} \mid M \cdot \lambda = 0\right\}.$$

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**.

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

$\mathbb{Q}$

$\mathbb{Z}$

Prime numbers $q \in \mathbb{Z}$

$$\mathbb{U}_n = \langle \zeta \rangle \simeq {}^{\mathbb{Z}}/_{(n)} \text{ (groups)}$$

$$d \mid n \iff \mathbb{U}_d \subset \mathbb{U}_n \text{ (subgroups)}$$

$$K = \mathbb{Q}[\zeta]$$
$$\mathcal{O}_K = \mathbb{Z}[\zeta]$$

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \left({}^{\mathbb{Z}}/_{(n)}\right)^{\times}$$

Cyclotomic

$\mathbb{F}_q(T)$

$\mathbb{F}_q[T]$

Irreducible polynomials $Q \in \mathbb{F}_q[T]$

$$\Lambda_M = \langle \lambda \rangle \simeq {}^{\mathbb{F}_q[T]}/_{(M)} \text{ (modules)}$$

$$D \mid M \iff \Lambda_D \subset \Lambda_M \text{ (submodules)}$$

$$K = \mathbb{F}_q(T)[\lambda]$$
$$\mathcal{O}_K = \mathbb{F}_q[T][\lambda]$$

$$\mathrm{Gal}(K/\mathbb{F}_q(T)) \simeq \left({}^{\mathbb{F}_q[T]}/_{(M)}\right)^{\times}$$

Carlitz

Important example

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

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

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

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

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

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

Totally Split QC–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

$$\zeta \cdot P(X) = P(\zeta X) \Rightarrow \text{ Support is } \textbf{Galois invariant}!$$

Search to decision reduction

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

$$\mathbb{F}_q[X] / (X^{q-1}-1) \simeq \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{q-1 \text{ copies}} \rightarrow \text{Ring used for MPC applications!}$$

Outline

Action of a Cyclic Group

Observation. ${}^{\mathbb{F}_q[X]}\big/_{(X^{q-1}-1)}$ is endowed with the action of $\mathrm{Gal}(K/\mathbb{F}_q(T)) \stackrel{\text{def}}{=} \mathbb{F}_q^\times$.

More generally. ${}^{\mathbb{Z}}\big/_{n\mathbb{Z}}$ acts linearly upon ${}^{\mathbb{F}_q[X]}\big/_{(X^n-1)}$.

They are examples of **Group Algebras**.

Group algebras

Finite (abelian) group G, $\quad \mathbb{F}_q[G] = \left\{ \sum_{g\in G} a_g g \mid a_g \in \mathbb{F}_q \right\} \simeq \mathbb{F}_q^{|G|}$

$$\left(\sum_{g\in G} a_g g \right) \left(\sum_{g\in G} b_g g \right) \stackrel{\text{def}}{=} \sum_{g\in G} \left(\sum_{h\in G} a_h b_{h^{-1}g} \right) g.$$

$G = \{1\}$	$\mathbb{F}_q[G] = \mathbb{F}_q,$
$G = \mathbb{Z}/N\mathbb{Z}$	$\mathbb{F}_q[G] = \mathbb{F}_q[X]/(X^N - 1),$
$G = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$	$\mathbb{F}_q[G] = \mathbb{F}_q[X, Y]/(X^N - 1, Y^M - 1).$

Hamming weight is well-defined given an ordering of G!

Quasi-abelian codes

A quasi-abelian code is an $\mathbb{F}_q[G]$-submodule of $\mathbb{F}_q[G]^\ell$

$$n \stackrel{\text{def}}{=} |G|.$$

$$\mathbf{\Gamma} = \begin{pmatrix} \gamma_{1,1} & \cdots & \gamma_{1,\ell} \\ \vdots & \ddots & \vdots \\ \gamma_{k,1} & \cdots & \gamma_{k,\ell} \end{pmatrix} \in \mathbb{F}_q[G]^{k\times\ell}$$

$$\mathcal{C} \stackrel{\text{def}}{=} \{\mathbf{m}\mathbf{\Gamma} \mid \mathbf{m} \in \mathbb{F}_q[G]^k\}.$$

$$n \updownarrow \underbrace{\begin{pmatrix} M_{\gamma_{1,1}} & M_{\gamma_{1,2}} & \cdots\cdots & M_{\gamma_{1,\ell}} \\ M_{\gamma_{2,1}} & M_{\gamma_{2,2}} & \cdots\cdots & M_{\gamma_{2,\ell}} \\ \vdots & \vdots & & \vdots \\ M_{\gamma_{k,1}} & M_{\gamma_{k,2}} & \cdots\cdots & M_{\gamma_{k,\ell}} \end{pmatrix}}_{\ell n} \in \mathbb{F}_q^{kn\times\ell n}$$

Quasi-Abelian Decoding Problem

$\mathcal{R} \stackrel{\text{def}}{=} \mathbb{F}_q[G]$ abelian group algebra, ψ (sparse) error distribution over $\mathcal{R}$.

Search Version

Input. N samples of the form $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + \mathbf{e})$ where $\mathbf{a} \leftarrow \mathcal{R}^\ell$, and $\mathbf{e} \leftarrow \psi$.

Goal. Find $\mathbf{s} \in \mathcal{R}^\ell$.

Decision Version

Goal. Distinguish between $(\mathbf{a}, \mathbf{y}^{\mathsf{unif}})$ and $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + \mathbf{e})$, given N samples.

Generalise both plain ($G = \{1\}$) and quasi-cyclic ($G = \mathbb{Z}/n\mathbb{Z}$) decoding problems.

A multivariate setting for MPC applications

Goal. Find G such that $\mathbb{F}_q[G] \simeq \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{N \text{ copies}}$ with $N \gg 1$.

A multivariate setting for MPC applications

Goal. Find G such that $\mathbb{F}_q[G] \simeq \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{N \text{ copies}}$ with $N \gg 1$.

Idea. Take $G = (\mathbb{Z}/(q-1)\mathbb{Z})^t$ for some $t \geqslant 1$.

$$
\begin{aligned}
\mathbb{F}_q[G] = \; & \mathbb{F}_q[X_1, \ldots, X_t]/(X_1^{q-1} - 1, \ldots, X_t^{q-1} - 1) \\
\simeq \; & \prod_{(\zeta_1,\ldots,\zeta_t) \in (\mathbb{F}_q^\times)^t} \mathbb{F}_q[X_1, \ldots, X_t]/(X_1 - \zeta_1, \ldots, X_t - \zeta_t) \\
\simeq \; & \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{(q-1)^t \text{ copies}}
\end{aligned}
$$

- As many copies as wished as long as $q \geqslant 3$! ✓
- Problem when $q = 2$. ✗

Hardness of the Quasi-Abelian Decoding Problem?

- No efficient decoding algorithm, even 50 years after their introduction [*W*77].
- Previous Search-to-Decision reduction extends to this instantiation!

Outline

Conclusion and Perspectives

Conclusion.

- A new algebraic framework to unify structured variants of the decoding problem.
- Bring insight on structured variants.
- The group action is the key to the reduction:

  $\rightarrow$ Naturally appears with the function field framework;
  $\rightarrow$ Otherwise, seems completely pulled out of a hat.
- More general rings endowed with a group action seems to yield secure variants.

Perspectives and Future Work

Foundations.

- Improve the analysis of [**B**CD23] to handle structured codes.
  $\rightarrow$ **Rényi Divergence?**
- Extend this OHCP technique to get reduction for other metrics
  (*e.g.* rank metric, Lee metric, ...)?
- Developping new tools to specifically target structured codes.
  $\rightarrow$ **Representation theory?**

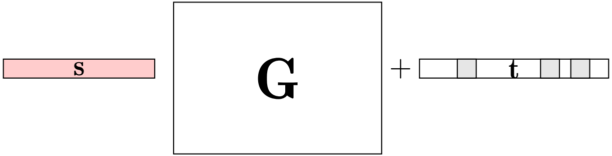
Applications.

- Circumvent the impossiblity result to make the PCG construction work over $\mathbb{F}_2$?
  $\rightarrow$ **(Reverse) Multiplication Friendly Embedding?**
- Improving efficiency of the construction
  $\rightarrow$ **Fast computation in (modular) group algebra?**
- Implementations.

Backup Slides

Outline

From Decoding to LPN [BLVW19, YZ21]

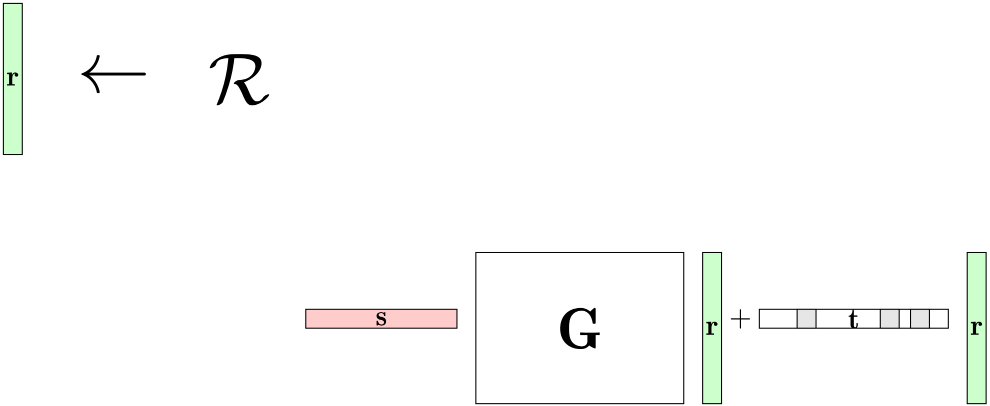


From Decoding to LPN [BLVW19, YZ21]

$$\mathbf{r} \leftarrow \mathcal{R}$$

$$\left(\mathbf{s} \, \mathbf{G} + \mathbf{t} \right) \mathbf{r}$$

From Decoding to LPN [BLVW19, YZ21]

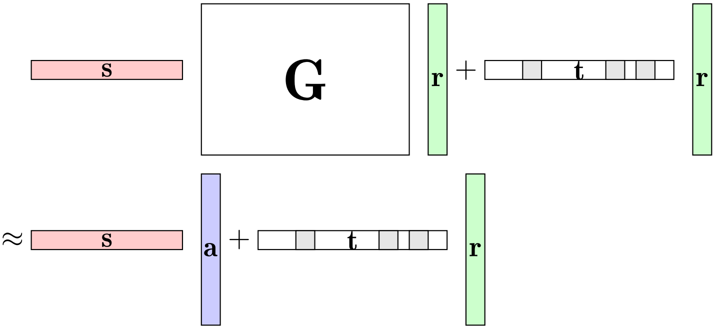


Building LPN-like Oracle

$$\mathbf{s}\,\mathbf{G}\,\mathbf{r} + \mathbf{t}\,\mathbf{r}$$

$$\approx \mathbf{s}\,\mathbf{a} + \mathbf{t}\,\mathbf{r}$$

- $\mathbf{G}\mathbf{r} \approx^{?}$ uniform
- $(\mathbf{G}\mathbf{r}, \mathbf{t} \cdot \mathbf{r})$ are correlated ...



Statistically close

- → **Average-case:** Leftover hash lemma
- → **Worst-case:** Notion of smoothing distribution ([BLVW19, YZ21, DDRT23, DR23])

Bernoulli Smoothing

(Non Standard) Notation

$$r_i \leftarrow \mathrm{Ber}(\omega) \text{ if } r_i \text{ Bernoulli with } \mathbb{P}(r_i = 1) = \frac{1}{2}\left(1 - 2^{-\omega}\right).$$

Remark: $\mathrm{Ber}(\omega_1) + \mathrm{Ber}(\omega_2) = \mathrm{Ber}(\omega_1 + \omega_2)$.

$$\mathbf{s}\,\mathbf{G}\,\mathbf{r} + \mathbf{t}\,\mathbf{r} \approx \mathbf{s}\,\mathbf{a} + \mathrm{Ber}(\omega|\mathbf{t}|)$$

Smoothing bounds from [DR23]

A continuous hybrid argument

- $(\mathbf{G}, \mathbf{y} \stackrel{\text{def}}{=} \mathbf{sG} + \mathbf{t})$
- Distinguisher $\mathscr{A}$ between LPN(ω_0) and LPN(∞).
- $\mathscr{A}$ makes N queries to the oracle and has advantage ε.

We build LPN($\omega|\mathbf{t}|$) oracle.

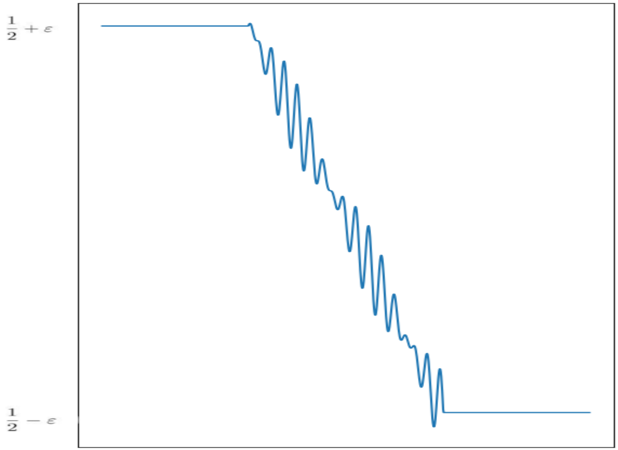
- $\mathscr{A}$ can be given any LPN(ω)-like oracle.
- Will accept with some probability $p(\omega)$.

- $p(\omega_0) = \frac{1}{2} + \varepsilon$
- $p(\omega) \to \frac{1}{2} - \varepsilon$ as $\omega \to \infty$

- $p(\omega)$ unknown for $\omega \in (\omega_0, \infty)$
- But can be estimated via statistical methods.

Acceptance behaviour of $\mathscr{A}^{\text{LPN}(\omega)}$ **must** change as $\omega \to \infty$.

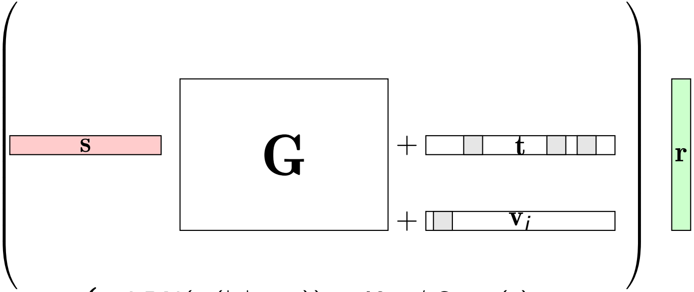
Estimating $p(\omega)$



Wishful thinking: Testing Support Membership

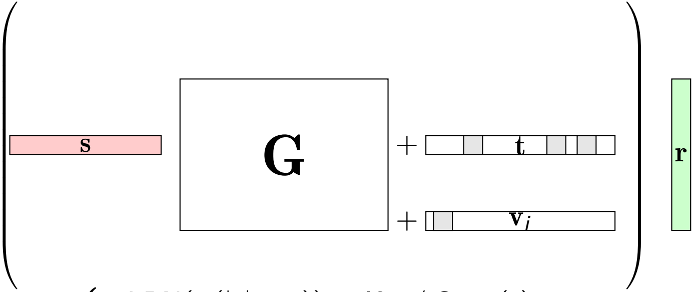
$$\left(\mathbf{s} \quad \mathbf{G} + \mathbf{t} \right) \quad \mathbf{r}$$

Wishful thinking: Testing Support Membership



$$\approx \begin{cases} \mathsf{LPN}(\omega(|\mathbf{t}|+1)) & \text{If } i \notin \mathsf{Supp}(\mathbf{t}) \\ \mathsf{LPN}(\omega(|\mathbf{t}|-1)) \\ \text{or } \mathsf{LPN}(\omega|\mathbf{t}|) & \text{Else} \end{cases}$$

Wishful thinking: Testing Support Membership



$$\approx \begin{cases} \mathsf{LPN}(\omega(|\mathbf{t}|+1)) & \text{If } i \notin \mathsf{Supp}(\mathbf{t}) \\ \mathsf{LPN}(\omega(|\mathbf{t}|-1)) \\ \text{ or } \mathsf{LPN}(\omega|\mathbf{t}|) & \text{Else} \end{cases}$$

Not so easy to distinguish those two situations...

Shift your oracles

Idea: *Zoom in* and sample $\mathbf{r} \leftarrow \mathsf{Ber}^{\otimes n}(2^x \omega_0)$.

$$\mathcal{O}_0(x) \approx \mathsf{LPN}(2^x \omega_0 |\mathbf{t}|) \quad \text{and} \quad \mathcal{O}_{\mathbf{v}_i}(x) \approx \mathsf{LPN}(2^x \omega_0 |\mathbf{t} + \mathbf{v}_i|).$$

Define $p(x) \overset{\text{def}}{=} \mathbb{P}(\mathcal{A}^{\mathcal{O}_0(x)} \text{ accepts})$.

$$\mathbb{P}(\mathcal{A}^{\mathcal{O}_{\mathbf{v}_i}(x)} \text{accepts}) = p\left(x + \log \frac{|\mathbf{t} + \mathbf{v}_i|}{|\mathbf{t}|}\right)$$

where

$$\log \frac{|\mathbf{t} + \mathbf{v}_i|}{|\mathbf{t}|} = \begin{cases} \log(1 + \frac{1}{t}) > 0 & \text{if } i \notin \mathrm{Supp}(\mathbf{t}) \\ \leqslant 0 & \text{if } i \in \mathrm{Supp}(\mathbf{t}). \end{cases}$$

Shift your oracles (Cont'd)

Change of behaviour in $\mathbb{P}(\mathcal{A}^{\mathcal{O}_0(x)}$ accepts) should happen at some point x_0.

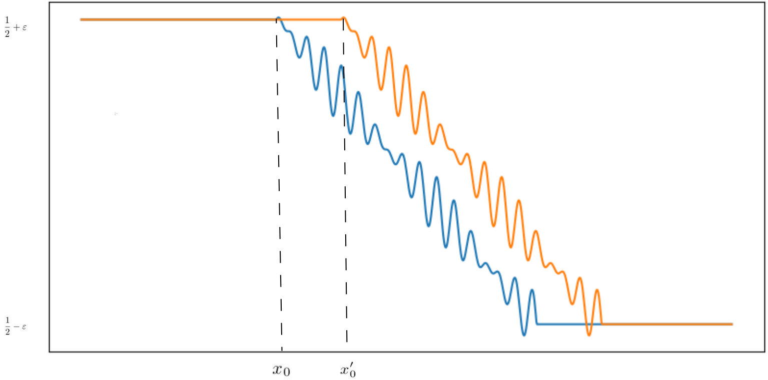
If $i \notin \mathrm{Supp}(\mathbf{t})$, behaviour of $\mathbb{P}(\mathcal{A}^{\mathcal{O}_{\mathbf{v}_i}(x)}$accepts) changes at some x_0' such that

$$x_0' = x_0 + \log\left(1 + \frac{1}{t}\right) \approx x_0 + \frac{1}{t}.$$

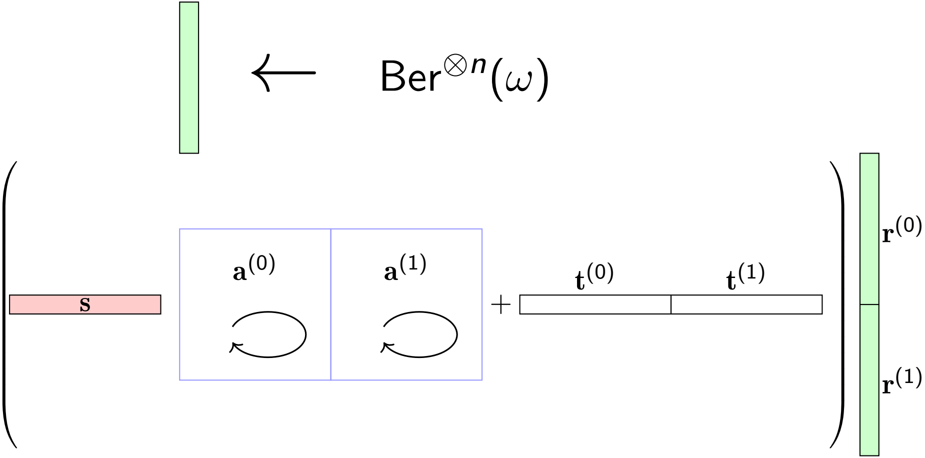
Oracle Comparison Problem from [PRS17]

p is very constrained (Lipschitz etc...) $\Rightarrow$ This can actually be detected in **polynomial time**!

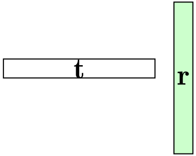
Shifted hybrid argument



What about Structured Variants?

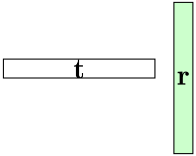


What about Structured Variants?



$$\longleftrightarrow \sum_k \underbrace{\left(\sum_{i+j \equiv k \mod n} t_i r_j \right)}_{\sim \mathrm{Ber}(\omega |\mathbf{t}|)} X^k$$

What about Structured Variants?



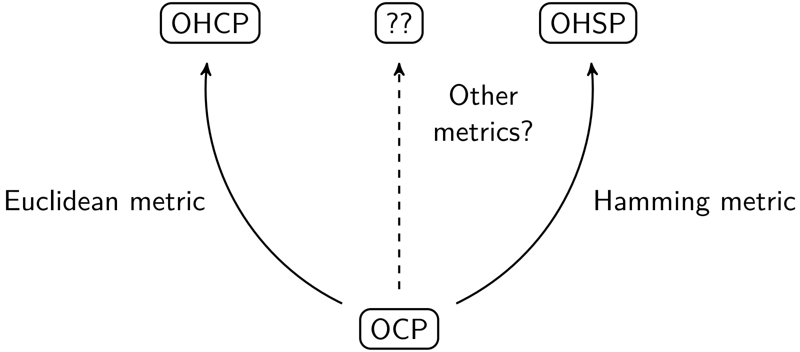
$$\longleftrightarrow \sum_k \underbrace{\left(\sum_{i+j \equiv k \mod n} t_i r_j \right)}_{\sim \mathrm{Ber}(\omega|\mathbf{t}|)} X^k$$

NOT independent ...

Open questions

→ How to make the reduction work in the structured case?

→ Find better smoothing bounds to improve the reduction?



Outline

Considering inertia: the case of LAPIN

(Heyse, Kiltz, Lyubashevsky, Paar, Pietrzak, 2012)

$$\mathcal{R} = {}^{\mathbb{F}_q[X]}\!\big/_{(F(X))} \text{ with } F(X) = F_1(X) \cdots F_{r/d}(X), \quad \deg F_i = d.$$

- Samples $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + \mathbf{e})$
- $\mathbf{e}(X) = e_0 + e_1 X + \cdots + e_{r-1} X^{r-1} \leftarrow \mathsf{Ber}_q(\omega)[X]_{\leqslant r-1}$

Considering inertia: the case of LAPIN

(Heyse, Kiltz, Lyubashevsky, Paar, Pietrzak, 2012)

$$\mathcal{R} = {}^{\mathbb{F}_q[X]}\!\big/_{(F(X))} \text{ with } F(X) = F_1(X)\cdots F_{r/d}(X), \quad \deg F_i = d.$$

- Samples $(\mathbf{a}, \mathbf{a}\cdot\mathbf{s} + \mathbf{e})$
- $\mathbf{e}(X) = e_0 + e_1 X + \cdots + e_{r-1}X^{r-1} \leftarrow \mathsf{Ber}_q(\omega)[X]_{\leqslant r-1}$

Not Galois invariant ...

Considering inertia: the case of LAPIN

(Heyse, Kiltz, Lyubashevsky, Paar, Pietrzak, 2012)

$$\mathcal{R} = {}^{\mathbb{F}_q[X]}\diagup_{(F(X))} \text{ with } F(X) = F_1(X) \cdots F_{r/d}(X), \quad \deg F_i = d.$$

- Samples $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + \mathbf{e})$
- $\mathbf{e}(X) = e_0 + e_1 X + \cdots + e_{r-1} X^{r-1} \leftarrow \mathrm{Ber}_q(\omega)[X]_{\leqslant r-1}$

Not Galois invariant ...

Idea: Change the basis!

Considering inertia: the case of LAPIN

(Heyse, Kiltz, Lyubashevsky, Paar, Pietrzak, 2012)

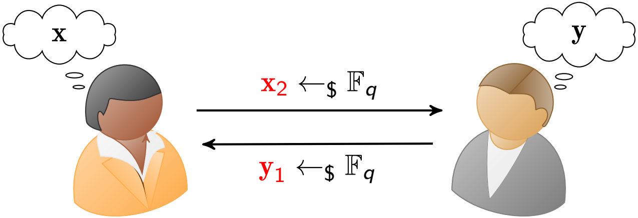
$$\mathcal{R} = {}^{\mathbb{F}_q[X]}\!\big/\!_{(F(X))} \text{ with } F(X) = F_1(X) \cdots F_{r/d}(X), \quad \deg F_i = d.$$

- Samples $(\mathbf{a}, \mathbf{a} \cdot \mathbf{s} + \mathbf{e})$
- $\mathbf{e}(X) = e_0\beta_0 + e_1\beta_1 + \cdots + e_{r-1}\beta_{r-1}; \quad \beta_i \leftarrow \mathrm{Ber}_q(\omega)$

Normal Distribution

- $\mathcal{R} \simeq {}^{\mathcal{O}_K}\!\big/\!_{T\mathcal{O}_K}$ with **explicit** Carlitz extension K.
- ${}^{\mathcal{O}_K}\!\big/\!_{T\mathcal{O}_K}$ admits **many** Galois invariant $\mathbb{F}_q$-basis.
- **Decision** Ring-LPN with respect to such a basis is as hard as **Search**.

Outline



$\mathbf{x}_1 \stackrel{\text{def}}{=} \mathbf{x} - \mathbf{x}_2 \approx \$$

$\mathbf{y}_1$

$\mathbf{x}_2$

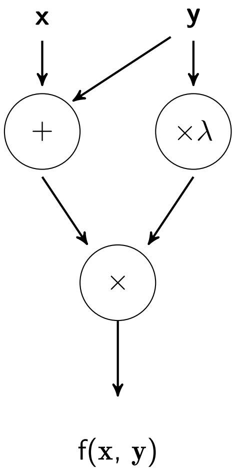
$\mathbf{y}_2 \stackrel{\text{def}}{=} \mathbf{y} - \mathbf{y}_1 \approx \$$

Additive reconstruction

$$\mathbf{x}_1 + \mathbf{x}_2 = \mathbf{x}$$
$$\mathbf{y}_1 + \mathbf{y}_2 = \mathbf{y}$$

Secure Multiparty Computation over $\mathbb{F}_q$

- $\textsc{Shares}(\mathbf{x}+\mathbf{y}) = \textsc{Shares}(\mathbf{x}) + \textsc{Shares}(\mathbf{y}) \Rightarrow$ free ✓
- $\textsc{Shares}(\lambda\mathbf{x}) = \lambda\textsc{Shares}(\mathbf{x}) \Rightarrow$ free ✓
- Multiplications $\Rightarrow$ Require communication $\Rightarrow$ Costly ✗.

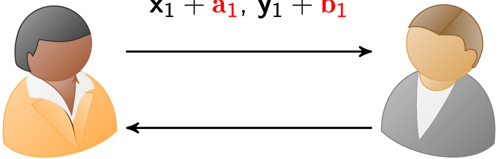


Beaver's idea [Bea91][2]: Correlated Randomness

Assume each party has additive shares of a *random* multiplication $(\mathbf{a}, \mathbf{b}, \mathbf{c} = \mathbf{a} \cdot \mathbf{b})$.

$\mathbf{x}_1 + \mathbf{a}_1,\ \mathbf{y}_1 + \mathbf{b}_1$

$\mathbf{x}_1, \mathbf{y}_1$
$\mathbf{a}_1, \mathbf{b}_1, \mathbf{c}_1$



$\mathbf{x}_2, \mathbf{y}_2$
$\mathbf{a}_2, \mathbf{b}_2, \mathbf{c}_2$

$\mathbf{x}_2 + \mathbf{a}_2,\ \mathbf{y}_2 + \mathbf{b}_2$

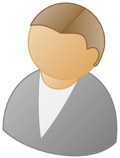
[1] *Efficient multiparty protocols using circuit randomization*, Beaver - CRYPTO '91

Beaver's idea [Bea91][2]: Correlated Randomness

Assume each party has additive shares of a *random* multiplication $(\mathbf{a}, \mathbf{b}, \mathbf{c} = \mathbf{a} \cdot \mathbf{b})$.

$\mathbf{x}_1, \mathbf{y}_1$
$\mathbf{a}_1, \mathbf{b}_1, \mathbf{c}_1$

$\alpha = \mathbf{x} + \mathbf{a}$
$\beta = \mathbf{y} + \mathbf{b}$



$\mathbf{x}_2, \mathbf{y}_2$
$\mathbf{a}_2, \mathbf{b}_2, \mathbf{c}_2$

α and β totally hide $\mathbf{x}$ and $\mathbf{y}$.

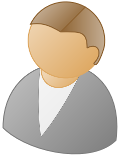
[1] *Efficient multiparty protocols using circuit randomization*, Beaver - CRYPTO '91

Beaver's idea [Bea91][2]: Correlated Randomness

Assume each party has additive shares of a *random* multiplication $(\mathbf{a}, \mathbf{b}, \mathbf{c} = \mathbf{a} \cdot \mathbf{b})$.

$\mathbf{x}_1, \mathbf{y}_1$
$\mathbf{a}_1, \mathbf{b}_1, \mathbf{c}_1$

$\alpha = \mathbf{x} + \mathbf{a}$
$\beta = \mathbf{y} + \mathbf{b}$



$\mathbf{x}_2, \mathbf{y}_2$
$\mathbf{a}_2, \mathbf{b}_2, \mathbf{c}_2$

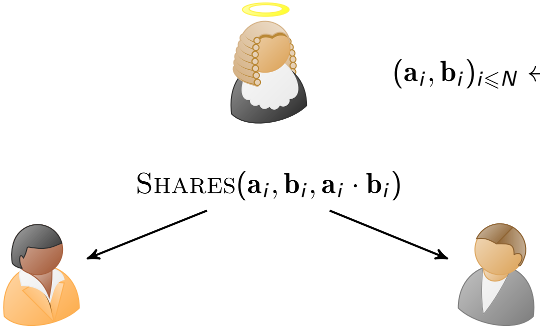
$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= (\mathbf{x} + \mathbf{a} - \mathbf{a}) \cdot (\mathbf{y} + \mathbf{b} - \mathbf{b}) \\ &= (\alpha - \mathbf{a}) \cdot (\beta - \mathbf{b}) \\ &= \alpha \cdot \beta - \alpha \cdot \mathbf{b} - \beta \cdot \mathbf{a} + \mathbf{c} \end{aligned}$$

[1] *Efficient multiparty protocols using circuit randomization*, Beaver - CRYPTO '91

The Correlated Randomness Model

Preprocessing

$$(\mathbf{a}_i, \mathbf{b}_i)_{i \leqslant N} \leftarrow (\mathbb{F}_q \times \mathbb{F}_q)^N$$



$$\textsc{Shares}(\mathbf{a}_i, \mathbf{b}_i, \mathbf{a}_i \cdot \mathbf{b}_i)$$

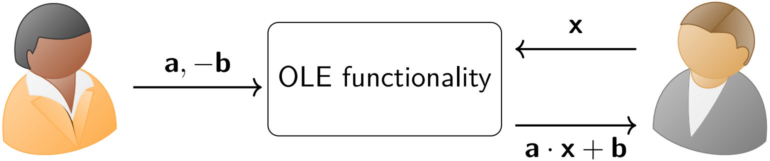
Fast online protocol using one triple per multiplication

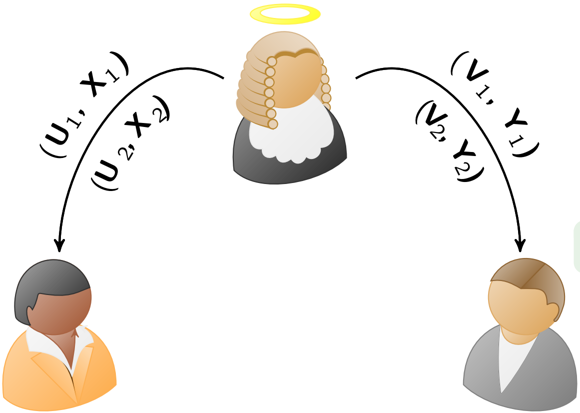
How to efficiently distribute many ($N \approx 2^{20}, 2^{30}$) random multiplication triple?

Another Correlation: Oblivious Linear Evaluations

OLE correlation

$(\mathbf{U}, \mathbf{X}, \mathbf{V}, \mathbf{Y})$ such that $\mathbf{U} \cdot \mathbf{V} = \mathbf{X} + \mathbf{Y}$.





$$\mathbf{Z}_A + \mathbf{Z}_B = (\mathbf{U}_1 + \mathbf{V}_2) \cdot (\mathbf{U}_2 + \mathbf{V}_1)$$

$$\mathbf{Z}_A \stackrel{\text{def}}{=} \mathbf{X}_1 + \mathbf{U}_1 \cdot \mathbf{U}_2 + \mathbf{X}_2 \qquad \mathbf{Z}_B \stackrel{\text{def}}{=} \mathbf{Y}_1 + \mathbf{V}_1 \cdot \mathbf{V}_2 + \mathbf{Y}_2$$

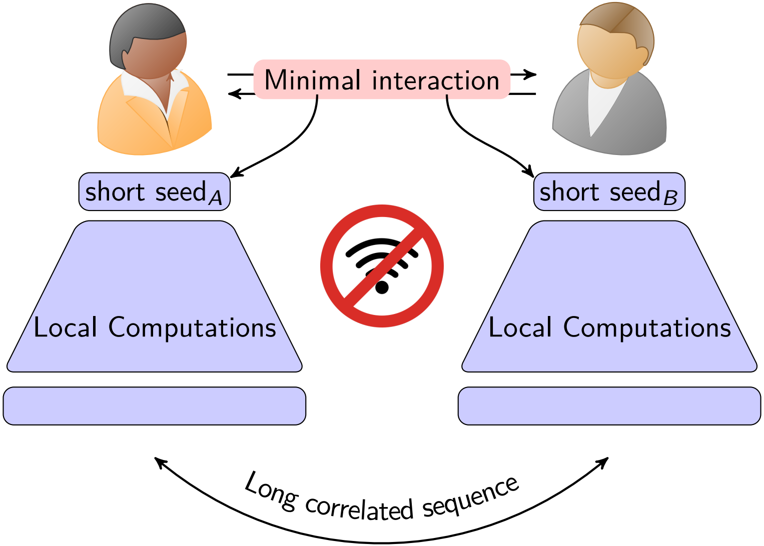
Goal: Distribute **a lot** of random OLE's over $\mathbb{F}_q$.

Wishful thinking. ([BCGIKS20][3]) Take a ring $\mathcal{R} \simeq \mathbb{F}_q \times \cdots \times \mathbb{F}_q$

$$\begin{array}{ccc} \boxed{\textbf{ONE}\text{ OLE over }\mathcal{R}} & \qquad & \mathbf{U} \cdot \mathbf{V} = \mathbf{X} + \mathbf{Y} \\ \downarrow & & \\ \boxed{\textbf{Many}\text{ OLE over }\mathbb{F}_q} & & \mathbf{u}_i \cdot \mathbf{v}_i = \mathbf{x}_i + \mathbf{y}_i \end{array}$$

[3] *Efficient Pseudorandom Correlation Generators from Ring-LPN*, Boyle, Couteau, Gilboa, Ishai, Kohl, Sholl - CRYPTO '20

Pseudorandom Correlation Generator (PCG)



PCG for OLE [BCGIKS20]

There exists a protocol to efficiently distribute additive shares of **sparse** vectors.[4]

Idea: Take $\mathcal{R} = \mathbb{F}_q[X]/(F(X))$ where $F(X)$ splits completely.

- Sample randomly $\mathbf{a} \leftarrow \mathcal{R}$.
- Set $\mathbf{U} \stackrel{\text{def}}{=} \mathbf{a} \cdot \mathbf{e}_1 + \mathbf{f}_1 \approx^? \$$
- Set $\mathbf{V} \stackrel{\text{def}}{=} \mathbf{a} \cdot \mathbf{e}_2 + \mathbf{f}_2 \approx^? \$$

Where $\mathbf{e}_i, \mathbf{f}_i$ are random **sparse** polynomials.

$$\mathbf{U} \cdot \mathbf{V} = \mathbf{a}^2(\mathbf{e}_1\mathbf{e}_2) + \mathbf{a}(\mathbf{e}_1\mathbf{f}_2 + \mathbf{e}_2\mathbf{f}_1) + \mathbf{f}_1\mathbf{f}_2$$

[4] *Function secret sharing*, Boyle, Gilboa, Ishai - EUROCRYPT '15

PCG for OLE [BCGIKS20]

There exists a protocol to efficiently distribute additive shares of **sparse** vectors.[4]

Idea: Take $\mathcal{R} = \mathbb{F}_q[X]/(F(X))$ where $F(X)$ splits completely.

- Sample randomly $\mathbf{a} \leftarrow \mathcal{R}$.
- Set $\mathbf{U} \stackrel{\text{def}}{=} \mathbf{a} \cdot \mathbf{e}_1 + \mathbf{f}_1 \approx^? \$$
- Set $\mathbf{V} \stackrel{\text{def}}{=} \mathbf{a} \cdot \mathbf{e}_2 + \mathbf{f}_2 \approx^? \$$

Where $\mathbf{e}_i, \mathbf{f}_i$ are random **sparse** polynomials.

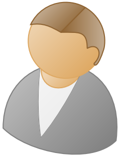
$$\begin{aligned}\mathbf{U} \cdot \mathbf{V} &= \mathbf{a}^2(\boxed{\mathbf{e}_1\mathbf{e}_2}) + \mathbf{a}(\boxed{\mathbf{e}_1\mathbf{f}_2} + \boxed{\mathbf{e}_2\mathbf{f}_1}) + \boxed{\mathbf{f}_1\mathbf{f}_2} \\ &= \text{Linear combination of } \textit{somewhat} \text{ sparse polynomials.}\end{aligned}$$

[4] *Function secret sharing*, Boyle, Gilboa, Ishai - EUROCRYPT '15

PCG for OLE [BCGIKS20]

$$\mathcal{R} = \mathbb{F}_q[X]/(F(X)) \simeq \mathbb{F}_q \times \cdots \times \mathbb{F}_q$$

$$\mathbf{U} = \mathbf{a} \cdot \mathbf{e}_1 + \mathbf{f}_1 \approx^? \$$$
$$\mathbf{V} = \mathbf{a} \cdot \mathbf{e}_2 + \mathbf{f}_2 \approx^? \$$$



$\textsc{Seed}_A = (\mathbf{a}, \mathbf{e}_1, \mathbf{f}_1, \textsc{Shares}(\mathbf{e}_i\mathbf{f}_j))$

$\downarrow$

Locally compute $\mathbf{U}, \textsc{Share}(\mathbf{UV})$
$\Rightarrow$ OLE's over $\mathbb{F}_q$ via CRT

$\textsc{Seed}_B = (\mathbf{a}, \mathbf{e}_2, \mathbf{f}_2, \textsc{Shares}(\mathbf{e}_i\mathbf{f}_j))$

$\downarrow$

Locally Compute $\mathbf{V}, \textsc{Share}(\mathbf{UV})$
$\Rightarrow$ OLE's over $\mathbb{F}_q$ via CRT

PCG for OLE [BCGIKS20]

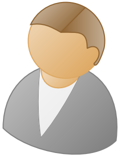
$\mathcal{R} = \mathbb{F}_q[X]/(F(X)) \simeq \mathbb{F}_q \times \cdots \times \mathbb{F}_q$ $\Rightarrow$ Only works for large q

$$\mathbf{U} = \mathbf{a} \cdot \mathbf{e}_1 + \mathbf{f}_1 \approx^? \$$$
$$\mathbf{V} = \mathbf{a} \cdot \mathbf{e}_2 + \mathbf{f}_2 \approx^? \$$$

$\textsc{Seed}_A = (\mathbf{a}, \mathbf{e}_1, \mathbf{f}_1, \textsc{Shares}(\mathbf{e}_i \mathbf{f}_j))$

$\downarrow$

Locally compute $\mathbf{U}, \textsc{Share}(\mathbf{UV})$
$\Rightarrow$ OLE's over $\mathbb{F}_q$ via CRT



$\textsc{Seed}_B = (\mathbf{a}, \mathbf{e}_2, \mathbf{f}_2, \textsc{Shares}(\mathbf{e}_i \mathbf{f}_j))$

$\downarrow$

Locally Compute $\mathbf{V}, \textsc{Share}(\mathbf{UV})$
$\Rightarrow$ OLE's over $\mathbb{F}_q$ via CRT

PCG for OLE [BCGIKS20]

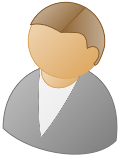
$\mathcal{R} = \mathbb{F}_q[X]/(F(X)) \simeq \mathbb{F}_q \times \cdots \times \mathbb{F}_q$ $\Rightarrow$ Only works for large q

$$\mathbf{U} = \mathbf{a} \cdot \mathbf{e}_1 + \mathbf{f}_1 \boxed{\approx^? \$}$$
$$\mathbf{V} = \mathbf{a} \cdot \mathbf{e}_2 + \mathbf{f}_2 \boxed{\approx^? \$}$$

$\textsc{Seed}_A = (\mathbf{a}, \mathbf{e}_1, \mathbf{f}_1, \textsc{Shares}(\mathbf{e}_i\mathbf{f}_j))$

$\downarrow$

Locally compute $\mathbf{U}, \textsc{Share}(\mathbf{UV})$
$\Rightarrow$ OLE's over $\mathbb{F}_q$ via CRT



$\textsc{Seed}_B = (\mathbf{a}, \mathbf{e}_2, \mathbf{f}_2, \textsc{Shares}(\mathbf{e}_i\mathbf{f}_j))$

$\downarrow$

Locally Compute $\mathbf{V}, \textsc{Share}(\mathbf{UV})$
$\Rightarrow$ OLE's over $\mathbb{F}_q$ via CRT

Quasi-Abelian (Syndrome) Decoding

Search version

Data. Random $\mathbf{H} \leftarrow \mathbb{F}_q[G]^{(\ell-k)\times\ell}$, a target weight $t \leqslant n$ and $\mathbf{s} \in \mathbb{F}_q[G]^{\ell-k}$.

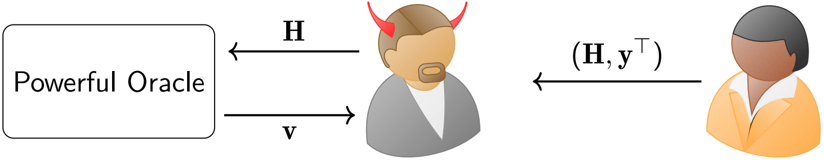
Goal. Find $\mathbf{e} = (\mathbf{e}_1, \ldots, \mathbf{e}_\ell) \in \mathbb{F}_q[G]^\ell$ with $|\mathbf{e}_i| = t$ and $\mathbf{H}\mathbf{e}^\top = \mathbf{s}$.

Decision version

Data. Random $\mathbf{H} \leftarrow \mathbb{F}_q[G]^{(\ell-k)\times\ell}$, a target weight $t \leqslant n$ and $\mathbf{y} \in \mathbb{F}_q[G]^{\ell-k}$.

Question. Is $\mathbf{y}$ uniform or of the form $\mathbf{H}\mathbf{e}^\top$ with $|\mathbf{e}_i| = t$?

Essentially all known [5] distinguishers can be expressed as a *linear* function $\mathbf{v} \cdot \mathbf{y}^\top$.



$\mathbf{v} \cdot \mathbf{H}\mathbf{e}^\top = \langle \mathbf{v}\mathbf{H}, \mathbf{e} \rangle$ is biased towards 0 if $\mathbf{v}\mathbf{H}$ is *sparse*.

[5] Information Set Decoding, Statistical Decoding, folding ...

Security against linear attacks

No low-weight (non-zero) $\mathbf{vH} \iff \mathcal{C}^{\perp}$ has good minimum distance

Gilbert-Varshamov bound [FL15][6]

Random QA codes have minimum distance linear in their length.

[6] *Thresholds of Random Quasi-Abelian Codes*, Fan, Lin - IEEE-IT

Strong caveat

Consider $\mathbf{H} \stackrel{\text{def}}{=} (\mathbf{a}_1 \ \mathbf{a}_2) \in \mathbb{F}_q[G]^{1\times 2}$ and $\mathbf{e} = (\mathbf{e}_1 \ \mathbf{e}_2) \in \mathbb{F}_q[G]^2$.

$$\mathbf{H}\mathbf{e}^\top = \mathbf{a}_1 \cdot \mathbf{e}_1 + \mathbf{a}_2 \cdot \mathbf{e}_2 \in \langle \mathbf{a}_1, \mathbf{a}_2 \rangle = \text{ Ideal generated by } \mathbf{a}_1 \text{ and } \mathbf{a}_2.$$

$\langle \mathbf{a}_1, \mathbf{a}_2 \rangle$ might be *strictly smaller* than $\mathbb{F}_q[G]$.

Restrict to matrices in systematic form:

$$\mathbf{H} = (\mathbf{H}' \mid \mathbf{I}_k).$$

Standard assumption for quasi-cyclic decoding problem (e.g. NIST).

A relevant example

Consider $G = \mathbb{Z}/n\mathbb{Z}$, so that $\mathcal{R} = \mathbb{F}_q[G] = \mathbb{F}_q[X]/(X^n - 1)$.

Let $\mathbf{a} \leftarrow \mathcal{R}$ be uniformly random, and $\mathbf{e}, \mathbf{f} \in \mathcal{R}$ sparse.

$$\mathbf{a} \cdot \mathbf{e} + \mathbf{f} = (\mathbf{a} \mid 1) \begin{pmatrix} \mathbf{e} \\ \mathbf{f} \end{pmatrix} = \mathbf{H} \begin{pmatrix} \mathbf{e} \\ \mathbf{f} \end{pmatrix}$$

$(\mathbf{a}, \mathbf{a} \cdot \mathbf{e} + \mathbf{f})$ is pseudorandom under the hardness of QA-SD.

What happens if not a quasi-group code?

Consider the ring $\mathcal{R} = \mathbb{F}_q[X]/(X^q - X) \simeq \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{q \text{ copies}}$.

- $\mathbf{a} \leftarrow \mathcal{R}$
- $\mathbf{e}, \mathbf{f}$ sparse
- $\mathbf{y} \stackrel{\text{def}}{=} \mathbf{a} \cdot \mathbf{e} + \mathbf{f}$

$$\mathbf{y}(0) = \mathbf{a}(0) \cdot \mathbf{e}(0) + \mathbf{f}(0) \mod (X^q - X)$$

A simple linear attack

- $\mathbf{e}, \mathbf{f}$ sparse $\Rightarrow \mathbf{y}(0) = 0$ with high probability.
- Compatible with reduction $\mod (X^q - X)$

Not possible over $\mathbb{F}_q[X]/(X^{q-1} - 1) = \mathbb{F}_q[\mathbb{Z}/(q-1)\mathbb{Z}]$!

A multivariate setting

Goal. Find G such that $\mathbb{F}_q[G] \simeq \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{N \text{ copies}}$ with $N \gg 1$.

A multivariate setting

Goal. Find G such that $\mathbb{F}_q[G] \simeq \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{N \text{ copies}}$ with $N \gg 1$.

Idea. Take $G = (\mathbb{Z}/(q-1)\mathbb{Z})^t$ for some $t \geqslant 1$.

$$\begin{aligned}
\mathbb{F}_q[G] = &\quad \mathbb{F}_q[X_1, \ldots, X_t]/(X_1^{q-1} - 1, \ldots, X_t^{q-1} - 1) \\
= &\quad \prod_{(\zeta_1, \ldots, \zeta_t) \in (\mathbb{F}_q^\times)^t} \mathbb{F}_q[X_1, \ldots, X_t]/(X_1 - \zeta_1, \ldots, X_t - \zeta_t) \\
= &\quad \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{(q-1)^t \text{ copies}}
\end{aligned}$$

With $q = 3$, choose $t = 20$ to get $N = 2^{20}$ OLE correlations over $\mathbb{F}_3$.

Efficiency

- The codes have *huge* length $N = |G|$, but we need a *fast* encoding algorithm.
- This amounts to efficiently computing products in $\mathbb{F}_q[G]$ (need $\tilde{O}(N)$).

$\implies$ FFT algorithm in $\mathbb{F}_q[G]$. Depends on the Jordan-Hölder series of G.

Products in $\mathbb{F}_q[(\mathbb{Z}/(q-1)\mathbb{Z})^t]$: $O(t \times (q-1)^t) = O(N \log(N))$ operations in $\mathbb{F}_q$.

Outline

- Is it possible to go to $\mathbb{F}_2$?
- Obviously, we cannot set $q = 2$ in the above construction.
- Most natural approach would be using the ring of boolean functions

$$\mathcal{R} = \mathbb{F}_2[X_1, \ldots, X_t]/(X_1^2 - X_1, \ldots, X_t^2 - X_t).$$

⚠This is NOT a group algebra.

Vulnerable to a simple attack.

The curious case of $\mathbb{F}_2$

In fact we have the following theorem

There is no group G such that $\mathbb{F}_2[G] = \underbrace{\mathbb{F}_2 \times \cdots \times \mathbb{F}_2}_{N \text{ times}}$ unless $G = \{1\}$ and $N = 1$.

Proof. $G \subset \mathbb{F}_2[G]^\times$ and $|(\mathbb{F}_2 \times \cdots \times \mathbb{F}_2)^\times| = 1$.

Towards $\mathbb{F}_2$?

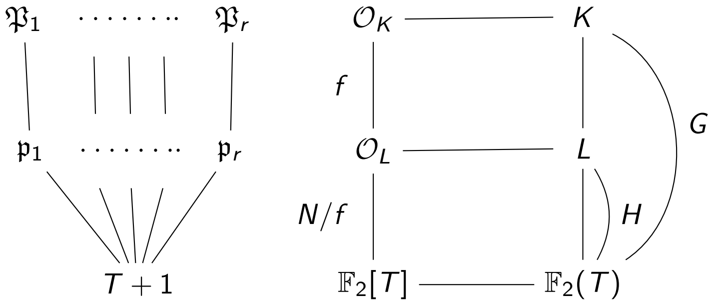
- There exists G and a ring $\mathcal{R}$ endowed with an action of G such that

$$\mathbb{F}_2[G] \underbrace{\simeq}_{\textit{As modules}} \mathcal{R} \underbrace{\simeq}_{\textit{As algebras}} \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$$

- G identifies as the Galois group of some Carlitz extension of $\mathbb{F}_2(T)$.
- Needs more work on the MPC side....
- Additive FFT in $\mathbb{F}_2[G]$?

A proposed construction

Set $K_\ell \overset{\text{def}}{=} \mathbb{F}_2(T)[\Lambda_{T^{\ell+1}}]$, and $\mathcal{O}_{K_\ell} \overset{\text{def}}{=} \mathbb{F}_2[T][\Lambda_{T^{\ell+1}}]$,



- $\mathcal{O}_L$ has a Local normal integral basis at $T+1$
- $\mathcal{O}_L / (T+1)\mathcal{O}_L \simeq \mathbb{F}_2 \times \cdots \times \mathbb{F}_2$

Explicit Example with Magma ($\ell = 25$)

$$\mathcal{O}_K / (T+1)\mathcal{O}_K \simeq \mathbb{F}_2[X] / (P(X)) \simeq \underbrace{\mathbb{F}_{2^{32}} \times \cdots \times \mathbb{F}_{2^{32}}}_{2^{20} \text{ copies}}$$

with

$$P(X) = 1 + X + X^2 + X^{256} + X^{512} + X^{2^{16}} + X^{2^{17}} + X^{2^{24}} + X^{2^{25}}$$

and

$$\begin{aligned} \mathcal{O}_L / (T+1)\mathcal{O}_L &= \left\{ F(X) \in \mathbb{F}_2[X] / (P(X)) \,\middle|\, F(X^2) = F(X) \right\} \\ &= \underbrace{\mathbb{F}_2 \times \cdots \times \mathbb{F}_2}_{2^{20} \text{ copies}} \end{aligned}$$

Galois Structure

(Chebolu, Lockridge, 2017)

$G \stackrel{\text{def}}{=} \mathrm{Gal}(K/\mathbb{F}_2(T)) = \left({\mathbb{F}_2[T]}/{(T^n)} \right)^{\times}$ is isomorphic to

$$\bigoplus_{1 \leqslant k < \lceil \log(n) \rceil} \left({\mathbb{Z}}/{2^k\mathbb{Z}} \right)^{\left\lceil \frac{n}{2^{k-1}} \right\rceil - 2\left\lceil \frac{n}{2^k} \right\rceil + \left\lceil \frac{n}{2^{k+1}} \right\rceil}.$$