A New Algebraic Approach to the Regular Syndrome Decoding Problem and Implications for PCG Constructions

Pierre Briaud[1], joint work with Morten Øygarden[2]

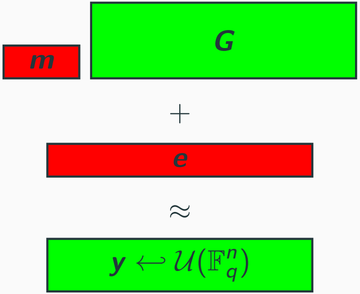
Eurocrypt 2023, April 27

[1]Inria Paris & Sorbonne Université
[2]Simula UiB

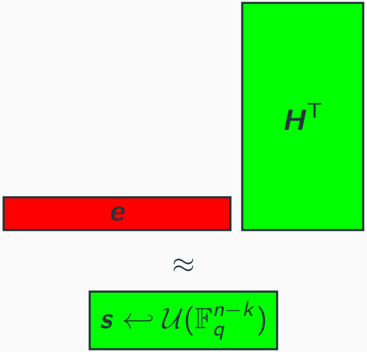
Decoding Problem over $\mathbb{F}_q$

$\boldsymbol{G} \hookleftarrow \mathcal{U}(\mathbb{F}_q^{k\times n})$ full-rank, $\boldsymbol{m} \hookleftarrow \mathcal{U}(\mathbb{F}_q^{k})$

Error $\boldsymbol{e}$, $t \stackrel{def}{=} \mathrm{HW}(\boldsymbol{e})$ small



Parity-check $\boldsymbol{H} \hookleftarrow \mathcal{U}(\mathbb{F}_q^{(n-k)\times n})$ full-rank



LPN ?

Secret size k, number of samples $n = k^{1+\alpha}$, $0 < \alpha < 1$, tiny noise

Regular Syndrome Decoding (RSD)

Assume $n = N \times t$ for some $N \in \mathbb{N}$ (blocksize)

Regular error [AFS05]

- For $1 \leq i \leq t$, random $\boldsymbol{e}_i \in \mathbb{F}_q^N$, $\mathrm{HW}(\boldsymbol{e}_i) = 1$
- Error is $\boldsymbol{e} \stackrel{def}{=} (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_t) \in \mathbb{F}_q^n$

Use case: Secure Computation [Haz+18]

Pseudorandom Correlation Generators (PCGs) [Boy+19]

$\rightarrow$ Correlated randomness

[AFS05] Augot, Finiasz, and Sendrier. "A Family of Fast Syndrome Based Cryptographic Hash Functions". *MYCRYPT 2005*.

[Haz+18] Hazay et al. *TinyKeys: A New Approach to Efficient Multi-Party Computation*.

[Boy+19] Boyle et al. *Compressing Vector OLE*.

PCG for Vector OLE [Boy+19]

Want shares of long pseudorandom $\boldsymbol{u}$

1. Function Secret Sharing $\rightarrow$ t-sparse vector $\boldsymbol{e}$
2. Decoding/LPN $\rightarrow$ final $\boldsymbol{u}$

LPN, 2 ways !

Code rate $R \stackrel{def}{=} k/n$

Primal	Dual
$\boldsymbol{u} = \boldsymbol{m}\boldsymbol{G} + \boldsymbol{e}$	$\boldsymbol{u} = \boldsymbol{e}\boldsymbol{H}^\top$
Very low R	Constant R

Regular $\boldsymbol{e}$ $\rightarrow$ reduce FSS cost

Known attacks on RSD

Do NOT exploit regular noise !

- "Folklore": guess k error-free positions in $\boldsymbol{e}$ + Gauss
- ISD (cf. Andre's talk), Statistical Decoding...

$\rightarrow$ Tiny noise: "Folklore" is better

Contribution

1st algebraic attack on RSD

- Tailored to regular noise
- Can beat "Folklore"/ISD for low code rates (Primal)

(Naive) algebraic system for $q = 2$

Modeling regular structure

Polynomial ring $R \stackrel{def}{=} \mathbb{F}_2[(e_{i,j})_{i,j}]$, n variables, block $\boldsymbol{e}_i \stackrel{def}{=} (e_{i,1}, \ldots, e_{i,N}) \in \mathbb{F}_2^N$

Coordinates $\in \mathbb{F}_2$ (field equations)

$$\forall i,\ \forall j,\ e_{i,j}^2 - e_{i,j} = 0. \tag{1}$$

One $\neq 0$ coordinate per block

$$\forall i,\ \forall j_1 \neq j_2,\ e_{i,j_1} e_{i,j_2} = 0. \tag{2}$$

Over $\mathbb{F}_2$, this coordinate is 1

$$\forall i,\ \textstyle\sum_{j=1}^{N} e_{i,j} = 1. \tag{3}$$

We consider $\mathcal{Q} \stackrel{def}{=} (1) \cup (2) \cup (3)$

Parity-checks $\boldsymbol{e}\boldsymbol{H}^{\mathsf{T}} = \boldsymbol{s}$

Linear equations ($\boldsymbol{h}_i$ i-th row in $\boldsymbol{H}$)

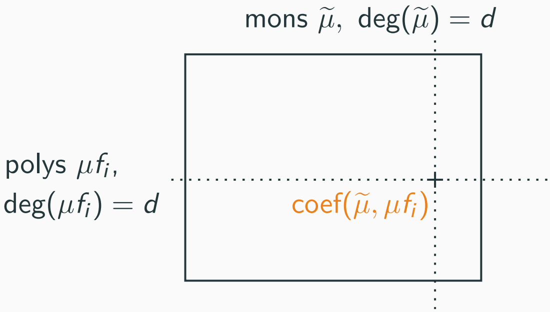
Parity-checks

$$\mathcal{P} \stackrel{def}{=} \{\forall i \in \{1..n-k\},\ \langle \boldsymbol{h}_i, \boldsymbol{e} \rangle - s_i\}$$

More when R small:

$$\boxed{\#\mathcal{P} = n - k = n(1 - R)}$$

1) $\times$ monomials $\rightarrow$ Macaulay matrix $\boldsymbol{M}_d$ (here, homogeneous)



2) RowEchelon($\boldsymbol{M}_d$) for $d \leq D$

Cost $\exp(D)$, but which D ?

Analysis

Hilbert series (HS)

Homogeneous ideal I, $R_d \overset{def}{=} \text{span}\{\mu, \deg(\mu) = d\}$, $I_d \overset{def}{=} I \cap R_d$

HS are nice

But unknown in general :(

$$\boxed{\mathcal{H}_{R/I}(z) \overset{def}{=} \sum_{d\in\mathbb{N}} \dim\left(R_d/I_d\right)z^d = \sum_{d\in\mathbb{N}} \dim\left(R_d\right)z^d - \sum_{d\in\mathbb{N}} \text{Rank}(\boldsymbol{M}_d)z^d}$$

- Highest degree parts in $\mathcal{S} \overset{def}{=} \mathcal{P} \cup \mathcal{Q}$

$$I \overset{def}{=} \langle \mathcal{S}^{(h)} \rangle = \langle \mathcal{P}^{(h)} \rangle + \langle \mathcal{Q}^{(h)} \rangle$$

- I zero-dimensional:

$$\mathcal{H}_{R/I}(z) \text{ polynomial of degree } D-1$$

Structural part $\mathcal{Q}$

Easy to handle

$$\mathcal{Q}^{(h)} = \underbrace{\{\forall i \in \{1..t\}, \forall j \in \{1..N\},\ e_{i,j}^2\}}_{(1)} \cup \underbrace{\{\forall i, \forall j_1 \neq j_2,\ e_{i,j_1} e_{i,j_2}\}}_{(2)} \cup \underbrace{\{\forall i,\ \sum_{j=1}^{N} e_{i,j}\}}_{(3)}$$

HS 1

Combinatorics $\rightarrow$ $\boxed{\dim(R_d/\langle \mathcal{Q}^{(h)} \rangle_d) = \binom{t}{d}(N-1)^d}$

$$\boxed{\mathcal{H}_{R/\langle \mathcal{Q}^{(h)} \rangle}(z) = (1 + (N-1)z)^t}$$

Parity-checks $\mathcal{P}$

Require assumption. Hope: HS known for random systems

Assumption ($\approx$ semi-regularity)

$\mathcal{P}^{(h)}$ behaves randomly in quotient $R/\langle \mathcal{Q}^{(h)} \rangle$

We have $\langle \mathcal{S}^{(h)} \rangle = \langle \mathcal{P}^{(h)} \rangle + \langle \mathcal{Q}^{(h)} \rangle$. Under Assumption, we get

$$\mathcal{H}_{R/\langle \mathcal{S}^{(h)} \rangle}(z) = \left[\frac{\mathcal{H}_{R/\langle \mathcal{Q}^{(h)} \rangle}(z)}{(1+z)^{n-k}} \right]_+ ,$$

$[.]_+$: truncation after first < 0 coef.

HS 2 (under Assumption + using HS 1)

$$\boxed{\mathcal{H}_{R/\langle \mathcal{S}^{(h)} \rangle}(z) = \left[\frac{(1+(N-1)z)^t}{(1+z)^{n-k}} \right]_+}$$

Final cost

Estimate for D

We had $D = \deg(\mathcal{H}_{R/\langle \mathcal{S}^{(h)} \rangle}) + 1$

$\rightarrow$ 1st < 0 coef. in generating series

- Linear algebra on Macaulay matrix $\boldsymbol{M}_D$, $2 \leq \omega < 3$

$$\boxed{T_{\text{solve}}(\mathcal{S}) = \mathcal{O}(\#\text{cols}(\boldsymbol{M}_D)^{\omega}) = \mathcal{O}\left(\binom{t}{D}^{\omega}(N-1)^{\omega D}\right)}$$

Improvements

Standard tricks

- **Hybrid approach**
- **XL-Wiedemann**

Cost with improvements

Parameters from Boyle *et al.* [Boy+19], updated analysis by Liu *et al.* [Liu+22]

Large field: no more $\{\forall i,\ \sum_{j=1}^{N} e_{i,j} = 1\}$, high degree field eqs

n	k	t	$\mathbb{F}_2$ [Liu+22]	This work $\mathbb{F}_2$	$\mathbb{F}_{2^{128}}$ [Liu+22]	This work $\mathbb{F}_{2^{128}}$
2^{22}	64770	4788	147	**104**	156	**111**
2^{20}	32771	2467	143	**126**	155	**131**
2^{18}	15336	1312	139	**123**	153	**133**
2^{16}	7391	667	135	141	151	151
2^{14}	3482	338	132	140	150	152
2^{12}	1589	172	131	136	155	**152**
2^{10}	652	106	176	**146**	194	**180**

[Liu+22] Liu et al. *The Hardness of LPN over Any Integer Ring and Field for PCG Applications.*