Variants of the Syndrome Decoding Problem and algebraic cryptanalysis

Pierre Briaud¹, joint work with Morten Øygarden²

Crypto Reading Club meeting, September 6, 2023

¹Inria Paris & Sorbonne Université
²Simula UiB
Syndrome Decoding Problem (SDP)

Code-based crypto
Secure Computation ("LPN")

McEliece, BIKE, HQC, etc.
Indistinguishability obfuscation

\[ G \leftarrow \mathcal{U}(\mathbb{F}_q^{k \times n}) \text{ full-rank}, \quad m \leftarrow \mathcal{U}(\mathbb{F}_q^k) \]

Error \( e, \; t \overset{\text{def}}{=} \text{HW}(e) \) small

\[ y \leftarrow \mathcal{U}(\mathbb{F}_q^n) \]
\[ m \cdot G + e \approx y \]

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

\[ e \approx \mathcal{U}(\mathbb{F}_q^n) \]

\[ s \leftarrow \mathcal{U}(\mathbb{F}_q^{n-k}) \]
SDP variants

What to change?

- Public code: sparse, quasi-cyclic, ...
- Error distribution
- Metric: $\mathbb{F}_q$ $\rightarrow$ rank metric, Lee metric

Goal

Efficiency gain! (at least)
## Known attacks

### On plain version

| Information Set Decoding (ISD), Statistical Decoding | → combinatorial |

More structure here!

- Improve generic solvers?
- Other attack types?
Algebraic cryptanalysis

- Reduction to polynomial system solving
- Applies to some variants

Regular Syndrome Decoding [BØ23] + Ongoing work

---

Solving $S = \{s_1, \ldots, s_m\}$

1) $\times$ monomials: (Homogeneous) Macaulay matrix $M_d$

- mons $\tilde{\mu}$, $\deg(\tilde{\mu}) = d$

- polys $\mu s_i$, $\deg(\mu s_i) = d$

- coef($\tilde{\mu}, \mu s_i$)

2) Linear algebra: $\text{RowEchelon}(M_d)$ for $d \leq D$, solving degree
Regular Syndrome Decoding
### Regular noise [AFS05]

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

- For \( 1 \leq i \leq t \), random \( e_i \in \mathbb{F}_q^N \), \( \text{HW}(e_i) = 1 \)
- Error is \( e \overset{\text{def}}{=} (e_1, \ldots, e_t) \in \mathbb{F}_q^n \)

#### Secure Computation

**Pseudorandom Correlation Generators (PCGs) [Boy+19]**

---


B., Øygarden SDP variants and algebraic cryptanalysis

Crypto Reading Club meeting 7 / 21
PCG for Vector OLE [Boy+19]

Want shares of long pseudorandom $u$

1. Function Secret Sharing (FSS) $\rightarrow$ $t$-sparse vector $e$
2. Decoding Problem $\rightarrow$ final $u$

2 ways!

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

<table>
<thead>
<tr>
<th>Primal</th>
<th>Dual</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u = mG + e$</td>
<td>$u = eH^T$</td>
</tr>
<tr>
<td>Very low $R$</td>
<td>Constant $R$</td>
</tr>
</tbody>
</table>

Regular $e \rightarrow$ reduce FSS cost
Contribution

Algebraic attack on Reg-SDP

- Tailored to noise distribution
- Can beat ISDs for low code rates (Primal)
Algebraic system for Reg-SDP
Modeling regular structure \((q = 2)\)

Polynomial ring \(R \overset{\text{def}}{=} \mathbb{F}_2[(e_{i,j})_{i,j}],\) \(n\) variables, block \(e_i \overset{\text{def}}{=} (e_{i,1}, \ldots, e_{i,N}) \in \mathbb{F}_2^N\)

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

\[
\forall i, \forall j, \quad e^2_{i,j} - e_{i,j} = 0 \tag{1}
\]

One \(\neq 0\) coordinate per block

\[
\forall i, \forall j_1 \neq j_2, \quad e_{i,j_1} e_{i,j_2} = 0 \tag{2}
\]

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

\[
\forall i, \quad \sum_{j=1}^{N} e_{i,j} = 1 \tag{3}
\]

We consider \(Q \overset{\text{def}}{=} (1) \cup (2) \cup (3)\)
Parity-checks $eH^T = s$

Linear equations ($h_i$ $i$-th row in $H$)

Parity-checks

$$\mathcal{P} \overset{\text{def}}{=} \{ \forall i \in \{1..n-k\}, \langle h_i, e \rangle - s_i \}$$

More when $R$ small:

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

Final system $S \overset{\text{def}}{=} \mathcal{P} \cup Q$
Estimating solving degree
Hilbert series (HS)

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

\[
\mathcal{H}_{R/I}(z) \overset{\text{def}}{=} \sum_{d \in \mathbb{N}} \dim (R_d/I_d)z^d = \sum_{d \in \mathbb{N}} \dim (R_d)z^d - \sum_{d \in \mathbb{N}} \text{Rank}(M_d)z^d
\]

Typical case in crypto: \( I \) zero-dimensional

Consequence

HS polynomial of degree \( D - 1 \)

- Recover solving degree from HS !
- HS unknown in general :( \[\rightarrow\] need to estimate it
Structural part $Q$

Easy to handle

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

HS 1

Combinatorics:

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

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

Require assumption. Hope: HS known for random systems

**Assumption ($\approx$ semi-regularity)**

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

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

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

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

**HS 2 (under Assumption + using HS 1)**

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

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

$\rightarrow$ First < 0 coef in $\frac{(1 + (N - 1)z)^t}{(1 + z)^{n-k}}$

- Linear algebra on Macaulay matrix $M_D$, $2 \leq \omega < 3$

\[ T_{\text{solve}}(S) = \mathcal{O} \left( \#\text{cols}(M_D)^\omega \right) = \mathcal{O} \left( \binom{t}{D}^\omega (N - 1)^{\omega D} \right) \]
Improvements

- **Hybrid approach**
  - fix variables *(here, in a structured way)*

- **XL-Wiedemann**
  - exploit sparse Macaulay matrix
Cost with improvements

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

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


SDP variants and algebraic cryptanalysis
Other SDP variants
Restricted Syndrome Decoding Problem (R-SDP)

CROSS signature scheme [Bal+23] \[ \rightarrow \text{new NIST call} \]

Constrained coefs

- Full Hamming weight

\[ \text{HW}(e) = n \]

- Coefs \( e_i \in \mathbb{F}_q^\times \) restricted to subgroup

\[ E = \langle g \rangle, \ g \in \mathbb{F}_q^\times \text{ of order } z \]

Level 1 parameters \( q = 127, \ n = 127, \ k = 76, \ z = 7 \)

Permuted Kernel Problem (PKP)

Introduced by Shamir in 1989

- PKP-DSS [Beu+18] → Chinese PQC competition
- PERK → new NIST call

Formulation

Parity-check $H \in \mathbb{F}_q^{(n-k) \times n}$, public vector $y \in \mathbb{F}^n_q$.

Find secret $\sigma \in S_n$ s.t.

$$y_\sigma H^T = 0,$$

where $y_\sigma = (y_\sigma(1), \ldots, y_\sigma(n))$

Level 1 PKP-DSS $q = 251$, $n = 69$, $n - k = 41$

$(n! \approx q^{n-k})$

[Beu+18] Beullens et al. PKP-Based Signature Scheme.

B., Øygarden
SDP variants and algebraic cryptanalysis

Crypto Reading Club meeting
## Algebraic systems

<table>
<thead>
<tr>
<th>Parity-checks</th>
<th>( n - k ) linear eqs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra structure</td>
<td>higher degree eqs</td>
</tr>
<tr>
<td>R-SDP:</td>
<td>( \forall i \in {1..n}, e_i^z - 1 = 0 )</td>
</tr>
<tr>
<td>PKP:</td>
<td>Model permutation matrix ( P_\sigma = (p_{i,j}) )</td>
</tr>
</tbody>
</table>
Ongoing work

Same approach for Hilbert series?

- Seems fine for R-SDP
- Much more complicated for PKP