On the Soundness of Algebraic Attacks against Code-based Assumptions

Miguel Cueto Noval[1] Simon-Philipp Merz[2] Patrick Stählin[1]
Akin Ünal[2]

[1]Institute of Science and Technology Austria

[2]ETH Zurich, Switzerland

October 20, 2025

Table of Contents

Syndrome Decoding

Let $\mathbb{F}$ be a field. Let $n, k, w \in \mathbb{N}$, $w \leq n$.

Syndrome Decoding

Let $\mathbb{F}$ be a field. Let $n, k, w \in \mathbb{N}$, $w \leq n$.

Definition (Syndrome Decoding Problem)

Extract e out of

$$(H, s = H \cdot e)$$

where $H \in \mathbb{F}^{(n-k)\times n}$ is a **parity-check matrix** and $e \in \mathbb{F}^n$ a noise vector of **Hamming-weight** w $\quad (\mathrm{hw}(e) = \# \{i \in [n] \mid e_i \neq 0\})$.

Syndrome Decoding

Let $\mathbb{F}$ be a field. Let $n, k, w \in \mathbb{N}$, $w \leq n$.

Definition (Syndrome Decoding Problem)

Extract e out of

$$(H, s = H \cdot e)$$

where $H \in \mathbb{F}^{(n-k)\times n}$ is a **parity-check matrix** and $e \in \mathbb{F}^n$ a noise vector of **Hamming-weight** w $\quad (\mathrm{hw}(e) = \#\{i \in [n] \mid e_i \neq 0\})$.

Definition (Learning Parity with Noise)

Extract x out of

$$(G, y = Gx + e)$$

where $G \in \mathbb{F}^{n\times k}$ is a **generator matrix**, $e \in \mathbb{F}^n$ of **Hamming-weight** w, and $x \in \mathbb{F}^k$.

Regular Syndrome Decoding

Let $n = bw$ for $b \in \mathbb{N}$.

Regular Syndrome Decoding

Let $n = bw$ for $b \in \mathbb{N}$.
$e \in \mathbb{F}^n$ is called *b*-**regular** if it can be subdivided into consecutive chunks

$$e = (e^{(1)}, \ldots, e^{(w)})$$

such that $e^{(i)} \in \mathbb{F}^b$ and $\mathrm{hw}(e^{(i)}) \leq 1$.

Regular Syndrome Decoding

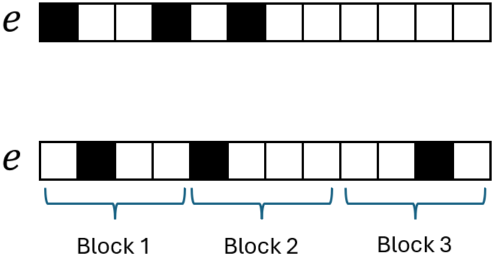
Let $n = bw$ for $b \in \mathbb{N}$.
$e \in \mathbb{F}^n$ is called b-**regular** if it can be subdivided into consecutive chunks

$$e = (e^{(1)}, \dots, e^{(w)})$$

such that $e^{(i)} \in \mathbb{F}^b$ and $\mathrm{hw}(e^{(i)}) \leq 1$.

Non-regular noise
$(n = 12, w = 3)$

Regular noise
$(n = 12, w = 3, b = 4)$



Regular Syndrome Decoding

Let $n = bw$ for $b \in \mathbb{N}$.
$e \in \mathbb{F}^n$ is called b-**regular** if it can be subdivided into chunks

$$e = (e^{(1)}, \ldots, e^{(w)})$$

such that $e^{(i)} \in \mathbb{F}^b$ and $\mathrm{hw}(e^{(i)}) \leq 1$.

Definition (Regular Syndrome Decoding Problem)

Extract e out of

$$(H, s = H \cdot e)$$

where $H \in \mathbb{F}^{(n-k)\times n}$ is a parity-check matrix and $e \in \mathbb{F}^n$ is b-**regular**.

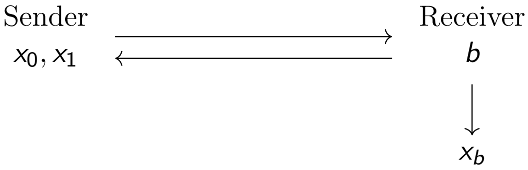
Regular Syndrome Decoding: Application

Regular Syndrome Decoding: Application

Oblivious Transfers (OT) are an essential building block for private 2-Party Computation protocols.

Regular Syndrome Decoding: Application

Oblivious Transfers (OT) are an essential building block for private 2-Party Computation protocols.



Regular Syndrome Decoding: Application

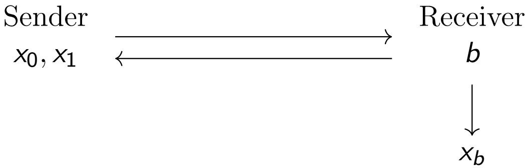
Oblivious Transfers (OT) are an essential building block for private 2-Party Computation protocols.

$$\begin{tikzcd} \text{Sender} & & \text{Receiver} \\ x_0, x_1 \arrow[rr, shift left] & & b \arrow[ll, shift left] \arrow[d] \\ & & x_b \end{tikzcd}$$

Preparing OTs is costly, as both parties need to share correlated randomness.

Regular Syndrome Decoding: Application

Oblivious Transfers (OT) are an essential building block for private 2-Party Computation protocols.



Preparing OTs is costly, as both parties need to share correlated randomness.

Pseudorandom Correlation Generators (PCGs) allow for OT-extension, i.e., they stretch short strings of correlated random bits to longer strings of correlated pseudorandom bits [BCGI18, BCG+19, BCG+20].

Regular Syndrome Decoding: Application

Oblivious Transfers (OT) are an essential building block for private 2-Party Computation protocols.

$$
\begin{tikzcd}
\text{Sender} & & \text{Receiver} \\
x_0, x_1 \arrow[rr, shift left] & & b \arrow[ll, shift left] \arrow[d] \\
& & x_b
\end{tikzcd}
$$

Preparing OTs is costly, as both parties need to share correlated randomness.

Pseudorandom Correlation Generators (PCGs) allow for OT-extension, i.e., they stretch short strings of correlated random bits to longer strings of correlated pseudorandom bits [BCGI18, BCG$^+$19, BCG$^+$20].

There are also other applications (signature schemes and local pseudorandom generators).

The Attack of Briaud and Øygarden [BØ23]

Consider $(H, s = He)$, $H \in \mathbb{F}^{(n-k)\times n}$, $e = (e^{(1)}, \ldots, e^{(w)}) \in \mathbb{F}^n$, $e^{(1)}, \ldots, e^{(w)} \in \mathbb{F}^b$ of HW ≤ 1.

The Attack of Briaud and Øygarden [BØ23]

Consider $(H, s = He)$, $H \in \mathbb{F}^{(n-k)\times n}$, $e = (e^{(1)}, \dots, e^{(w)}) \in \mathbb{F}^n$, $e^{(1)}, \dots, e^{(w)} \in \mathbb{F}^b$ of HW ≤ 1.

Idea: Model RSD as a system of quadratic equations:

The Attack of Briaud and Øygarden [BØ23]

Consider $(H, s = He)$, $H \in \mathbb{F}^{(n-k)\times n}$, $e = (e^{(1)}, \dots, e^{(w)}) \in \mathbb{F}^n$, $e^{(1)}, \dots, e^{(w)} \in \mathbb{F}^b$ of HW ≤ 1.

Idea: Model RSD as a system of quadratic equations:

1. Variables $E_\alpha^{(i)}$, $i \in [w]$, $\alpha \in [b]$, for e with equations

$$E_\alpha^{(i)} \cdot E_\beta^{(i)} = 0 \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b.$$

The Attack of Briaud and Øygarden [BØ23]

Consider $(H, s = He)$, $H \in \mathbb{F}^{(n-k)\times n}$, $e = (e^{(1)}, \ldots, e^{(w)}) \in \mathbb{F}^n$, $e^{(1)}, \ldots, e^{(w)} \in \mathbb{F}^b$ of HW ≤ 1.

Idea: Model RSD as a system of quadratic equations:

1. Variables $E_\alpha^{(i)}$, $i \in [w]$, $\alpha \in [b]$, for e with equations

$$E_\alpha^{(i)} \cdot E_\beta^{(i)} = 0 \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b.$$

2. For every row

$$(h_{j,1}^{(1)}, \ldots, h_{j,b}^{(1)}, \ldots, h_{j,1}^{(w)}, \ldots, h_{j,b}^{(w)},)$$

of H and $s = He$, a parity check equation

$$s_j = \sum_{i\in[w],\alpha\in[b]} h_{j,\alpha}^{(i)} \cdot E_\alpha^{(i)} \qquad \text{for } j \in [n-k].$$

The Attack of Briaud and Øygarden [BØ23]

Consider $(H, s = He)$, $H \in \mathbb{F}^{(n-k)\times n}$, $e = (e^{(1)}, \dots, e^{(w)}) \in \mathbb{F}^n$, $e^{(1)}, \dots, e^{(w)} \in \mathbb{F}^b$ of HW ≤ 1.

Idea: Model RSD as a system of quadratic equations:

1. Variables $E_\alpha^{(i)}$, $i \in [w]$, $\alpha \in [b]$, for e with equations

$$E_\alpha^{(i)} \cdot E_\beta^{(i)} = 0 \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b.$$

2. For every row

$$(h_{j,1}^{(1)}, \dots, h_{j,b}^{(1)}, \dots, h_{j,1}^{(w)}, \dots, h_{j,b}^{(w)},)$$

of H and $s = He$, a parity check equation

$$s_j = \sum_{i \in [w], \alpha \in [b]} h_{j,\alpha}^{(i)} \cdot E_\alpha^{(i)} \qquad \text{for } j \in [n-k].$$

Strategy: Use an XL-style algorithm to solve this equation system.

XL-Algorithm (Macaulay Matrices)

Consider a set of equations over $\mathbb{F}[X_1, \ldots, X_k]$

$$f_1(X) = f_2(X) = \cdots = f_m(X) = 0.$$

XL-Algorithm (Macaulay Matrices)

Consider a set of equations over $\mathbb{F}[X_1, \ldots, X_k]$

$$f_1(X) = f_2(X) = \cdots = f_m(X) = 0.$$

1. **Populate** the set of equations until some degree D

$$X_1^{a_1} \cdots X_k^{a_k} \cdot f_j(X) = 0$$

   for $j \in [m]$ and $a_1 + \cdots + a_k + \deg(f_j) \leq D$.

XL-Algorithm (Macaulay Matrices)

Consider a set of equations over $\mathbb{F}[X_1, \ldots, X_k]$

$$f_1(X) = f_2(X) = \cdots = f_m(X) = 0.$$

1. **Populate** the set of equations until some degree D

$$X_1^{a_1} \cdots X_k^{a_k} \cdot f_j(X) = 0$$

   for $j \in [m]$ and $a_1 + \cdots + a_k + \deg(f_j) \leq D$.

2. **Relinearize**: Write coefficients of all equations into a matrix

$$M_D = \begin{pmatrix} \mathrm{coeff}(g_1) \\ \vdots \\ \mathrm{coeff}(g_L). \end{pmatrix}$$

   Columns correspond to monomials and are sorted according to some degree-preserving monomial ordering.

XL-Algorithm (Macaulay Matrices)

Consider a set of equations over $\mathbb{F}[X_1, \ldots, X_k]$

$$f_1(X) = f_2(X) = \cdots = f_m(X) = 0.$$

1. **Populate** the set of equations until some degree D

$$X_1^{a_1} \cdots X_k^{a_k} \cdot f_j(X) = 0$$

   for $j \in [m]$ and $a_1 + \cdots + a_k + \deg(f_j) \leq D$.

2. **Relinearize**: Write coefficients of all equations into a matrix

$$M_D = \begin{pmatrix} \mathrm{coeff}(g_1) \\ \vdots \\ \mathrm{coeff}(g_L). \end{pmatrix}$$

   Columns correspond to monomials and are sorted according to some degree-preserving monomial ordering.

3. **Reduce** M_D, by bringing it into RRNF.

XL-Algorithm (Macaulay Matrices)

Consider a set of equations over $\mathbb{F}[X_1, \ldots, X_k]$

$$f_1(X) = f_2(X) = \cdots = f_m(X) = 0.$$

1. **Populate** the set of equations until some degree D

$$X_1^{a_1} \cdots X_k^{a_k} \cdot f_j(X) = 0$$

   for $j \in [m]$ and $a_1 + \cdots + a_k + \deg(f_j) \leq D$.
2. **Relinearize**: Write coefficients of all equations into a matrix

$$M_D = \begin{pmatrix} \mathrm{coeff}(g_1) \\ \vdots \\ \mathrm{coeff}(g_L). \end{pmatrix}$$

   Columns correspond to monomials and are sorted according to some degree-preserving monomial ordering.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Extract** a Groebner basis from the rows of M_D.

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Extract** a Groebner basis from the rows of M_D.

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Extract** a Groebner basis from the rows of M_D.

This algorithm succeeds if D is large enough.

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Extract** a Groebner basis from the rows of M_D.

This algorithm succeeds if D is large enough.
Question: How high do we need to set D?

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Extract** a Groebner basis from the rows of M_D.

This algorithm succeeds if D is large enough.
Question: How high do we need to set D?
Lazard: $D = \Theta(n)$ is good enough for most cases.

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Extract** a Groebner basis from the rows of M_D.

This algorithm succeeds if D is large enough.
Question: How high do we need to set D?
Lazard: $D = \Theta(n)$ is good enough for most cases.
Salizzoni: $D = \mathrm{d}_{\mathrm{reg}}(f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}) + 1$ suffices for **Mutant**-XL.

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Mutant-Step**: If a row of M_D corresponds to a polynomial g with $\deg(g) < D$ and

$$X_i \cdot g \notin \mathrm{span}\{X_1^{a_1} \cdots X_k^{a_k} \cdot f_j(X)\} \text{ for some } i \in [k],$$

   then add $g(X) = 0$ to the set of initial equations and go back to step 1.
5. **Extract** a Groebner basis from the rows of M_D.

This algorithm succeeds if D is large enough.
Question: How high do we need to set D?
Lazard: $D = \Theta(n)$ is good enough for most cases.
Salizzoni: $D = \mathrm{d}_{\mathrm{reg}}(f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}) + 1$ suffices for **Mutant**-XL.

Table of Contents

Degree of Regularity

Let $R = R^0 \oplus R^1 \oplus \ldots$ be a graded $\mathbb{F}$-algebra.

Degree of Regularity

Let $R = R^0 \oplus R^1 \oplus \dots$ be a graded $\mathbb{F}$-algebra.
(For example, $R = \mathbb{F}[X_1, \dots, X_k]$ is graded with

$$\mathbb{F}[X]^d = \text{Space of homogeneous polynomials of degree} d.)$$

Degree of Regularity

Let $R = R^0 \oplus R^1 \oplus \dots$ be a graded $\mathbb{F}$-algebra.
The **Hilbert series** of R is defined by

$$\mathcal{H}_R(T) := \sum_{d=0}^{\infty} \dim_{\mathbb{F}}(R^d) \cdot T^d.$$

Degree of Regularity

Let $R = R^0 \oplus R^1 \oplus \dots$ be a graded $\mathbb{F}$-algebra.
The **Hilbert series** of R is defined by

$$\mathcal{H}_R(T) := \sum_{d=0}^{\infty} \dim_{\mathbb{F}}(R^d) \cdot T^d.$$

The **degree of regularity** of a series $\mathcal{H} = \sum_d c_d \cdot T^d$ is defined by

$$\mathrm{d}_{\mathrm{reg}}(\mathcal{H}) := \inf\{d \in \mathbb{N} \mid c_d \leq 0\}.$$

Degree of Regularity

Let $R = R^0 \oplus R^1 \oplus \dots$ be a graded $\mathbb{F}$-algebra.
The **Hilbert series** of R is defined by

$$\mathcal{H}_R(T) := \sum_{d=0}^{\infty} \dim_{\mathbb{F}}(R^d) \cdot T^d.$$

The **degree of regularity** of a series $\mathcal{H} = \sum_d c_d \cdot T^d$ is defined by

$$d_{\text{reg}}(\mathcal{H}) := \inf\{d \in \mathbb{N} \mid c_d \leq 0\}.$$

The degree of regularity of homogeneous $f_1, \dots, f_m \in \mathbb{F}[X_1, \dots, X_n]$ is defined by $d_{\text{reg}}(f_1, \dots, f_m) = d_{\text{reg}}(\mathcal{H}_{\mathbb{F}[X]/(f_1,\dots,f_m)})$.

Degree of Regularity

Let $R = R^0 \oplus R^1 \oplus \ldots$ be a graded $\mathbb{F}$-algebra.
The **Hilbert series** of R is defined by

$$\mathcal{H}_R(T) := \sum_{d=0}^{\infty} \dim_{\mathbb{F}}(R^d) \cdot T^d.$$

The **degree of regularity** of a series $\mathcal{H} = \sum_d c_d \cdot T^d$ is defined by

$$\mathrm{d_{reg}}(\mathcal{H}) := \inf\{d \in \mathbb{N} \mid c_d \leq 0\}.$$

The degree of regularity of homogeneous $f_1, \ldots, f_m \in \mathbb{F}[X_1, \ldots, X_n]$ is defined by $\mathrm{d_{reg}}(f_1, \ldots, f_m) = \mathrm{d_{reg}}(\mathcal{H}_{\mathbb{F}[X]/(f_1,\ldots,f_m)})$.
Given a series $\mathcal{H} = \sum_d c_d \cdot T^d$, its truncation is given by

$$[\mathcal{H}]_+ = \sum_{d=0}^{\mathrm{d_{reg}}(\mathcal{H})-1} c_d \cdot T^d.$$

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Mutant-Step**: Extract degree-falls.
5. **Extract** a Groebner basis from the rows of M_D.

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Mutant-Step**: Extract degree-falls.
5. **Extract** a Groebner basis from the rows of M_D.

Theorem ([Sal25])

The above algorithm solves[a] the system $f_1(X) = \cdots = f_m(X) = 0$ in time $O(k^{4D})$ where $D = \mathrm{d}_{\mathrm{reg}}(f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}) + 1$.

[a] I.e., it computes a Groebner basis for some degree-preserving monomial ordering.

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Mutant-Step**: Extract degree-falls.
5. **Extract** a Groebner basis from the rows of M_D.

Theorem ([Sal25])

The above algorithm solves[a] *the system* $f_1(X) = \cdots = f_m(X) = 0$ *in time* $O(k^{4D})$ *where* $D = \mathrm{d}_{\mathrm{reg}}(f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}) + 1$.

[a] I.e., it computes a Groebner basis for some degree-preserving monomial ordering.

$\mathrm{d}_{\mathrm{reg}}$ constant $\implies$ poly-time attack.

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Mutant-Step**: Extract degree-falls.
5. **Extract** a Groebner basis from the rows of M_D.

Theorem ([Sal25])

The above algorithm solves[a] *the system* $f_1(X) = \cdots = f_m(X) = 0$ *in time* $O(k^{4D})$ *where* $D = \mathrm{d_{reg}}(f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}) + 1$.

[a] I.e., it computes a Groebner basis for some degree-preserving monomial ordering.

$\mathrm{d_{reg}}$ constant $\implies$ poly-time attack.

$\mathrm{d_{reg}}$ sublinear $\implies$ subexponential-time attack.

XL-Algorithm (Macaulay Matrices)

1. **Populate** the set of equations until some degree D.
2. **Relinearize**: Write coefficients of all equations into a matrix M_D.
3. **Reduce** M_D, by bringing it into RRNF.
4. **Mutant-Step**: Extract degree-falls.
5. **Extract** a Groebner basis from the rows of M_D.

Theorem ([Sal25])

The above algorithm solves[a] *the system* $f_1(X) = \cdots = f_m(X) = 0$ *in time* $O(k^{4D})$ *where* $D = \mathrm{d}_{\mathrm{reg}}(f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}) + 1$.

[a] I.e., it computes a Groebner basis for some degree-preserving monomial ordering.

$\mathrm{d}_{\mathrm{reg}}$ constant $\implies$ poly-time attack.
$\mathrm{d}_{\mathrm{reg}}$ sublinear $\implies$ subexponential-time attack.
Problem: How do we bound $\mathrm{d}_{\mathrm{reg}}(f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$?

Semi-Regularity

Semi-Regularity

The concept of semi-regularity goes back to a conjecture of Fröberg on generic sequences [Frö85, Par10].

Semi-Regularity

The concept of semi-regularity goes back to a conjecture of Fröberg on generic sequences [Frö85, Par10].
There are 4 different definitions of semi-regular sequences (depending on the size of the field and if mathematical/cryptographic).

Semi-Regularity

The concept of semi-regularity goes back to a conjecture of Fröberg on generic sequences [Frö85, Par10].

There are 4 different definitions of semi-regular sequences (depending on the size of the field and if mathematical/cryptographic).

Definition (Mathematical Semi-Regularity Over Large Fields)

A sequence of homogeneous elements $f_1, \ldots, f_m \in R$ is **semi-regular** if

$$\begin{aligned} (R/(f_1, \ldots, f_{i-1}))^d &\longrightarrow (R/(f_1, \ldots, f_{i-1}))^{d+\deg(f_i)} \\ z &\longmapsto z \cdot f_i \end{aligned}$$

has full rank for all $i \in [m]$, $d \in \mathbb{N}_0$.

Semi-Regularity

The concept of semi-regularity goes back to a conjecture of Fröberg on generic sequences [Frö85, Par10].
There are 4 different definitions of semi-regular sequences (depending on the size of the field and if mathematical/cryptographic).

Definition (Mathematical Semi-Regularity Over Large Fields)

A sequence of homogeneous elements $f_1, \dots, f_m \in R$ is **semi-regular** if

$$\begin{aligned}(R/(f_1, \dots, f_{i-1}))^d &\longrightarrow (R/(f_1, \dots, f_{i-1}))^{d+\deg(f_i)} \\ z &\longmapsto z \cdot f_i\end{aligned}$$

has full rank for all $i \in [m]$, $d \in \mathbb{N}_0$.

Lemma

If $f_1, \dots, f_m \in R$ is semi-regular, we have

$$\mathcal{H}_{R/(f_1,\dots,f_m)}(T) = \left[(1 - T^{\deg(f_1)}) \cdots (1 - T^{\deg(f_m)}) \cdot \mathcal{H}_R(T)\right]_+ .$$

The Attack of Briaud and Øygarden [BØ23]

1. Variables $E_\alpha^{(i)}$, $i \in [w]$, $\alpha \in [b]$, for e with equations

$$E_\alpha^{(i)} \cdot E_\beta^{(i)} = 0 \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b.$$

2. Parity check equations

$$s_j = \sum_{i \in [w], \alpha \in [b]} h_{j,\alpha}^{(i)} \cdot E_\alpha^{(i)} \qquad \text{for } j \in [n-k].$$

The Attack of Briaud and Øygarden [BØ23]

1. Variables $E_\alpha^{(i)}$, $i \in [w]$, $\alpha \in [b]$, for e with equations

$$E_\alpha^{(i)} \cdot E_\beta^{(i)} = 0 \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b.$$

2. Parity check equations

$$s_j = \sum_{i \in [w], \alpha \in [b]} h_{j,\alpha}^{(i)} \cdot E_\alpha^{(i)} \qquad \text{for } j \in [n-k].$$

To bound the degree of regularity, Briaud and Øygarden need that parity-check polynomials $h_1, \ldots, h_{n-k}$ form a semi-regular sequence in $\mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)} \mid i \in [w], 1 \leq \alpha < \beta \leq b)$.

The Attack of Briaud and Øygarden [BØ23]

1. Variables $E_\alpha^{(i)}$, $i \in [w]$, $\alpha \in [b]$, for e with equations

$$E_\alpha^{(i)} \cdot E_\beta^{(i)} = 0 \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b.$$

2. Parity check equations

$$s_j = \sum_{i \in [w], \alpha \in [b]} h_{j,\alpha}^{(i)} \cdot E_\alpha^{(i)} \qquad \text{for } j \in [n-k].$$

To bound the degree of regularity, Briaud and Øygarden need that parity-check polynomials $h_1, \ldots, h_{n-k}$ form a semi-regular sequence in $\mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)} \mid i \in [w], 1 \leq \alpha < \beta \leq b)$.
Solution: Semi-Regularity Heuristic! Just assume that $h_1, \ldots, h_{n-k}$ are semi-regular.

Semi-Regularity Heuristic

Semi-Regularity Heuristic

Hypothesis

A sequence of polynomials $f_1, \ldots, f_m$ from **some** distribution in **some** graded ring R will be semi-regular with **some** probability for **some** parameters.

Semi-Regularity Heuristic

Hypothesis

A sequence of polynomials $f_1, \ldots, f_m$ from **some** distribution in **some** graded ring R will be semi-regular with **some** probability for **some** parameters.

Correctness of heuristic depends on various factors!

Table of Contents

Our Results [NMSÜ25]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Our Results [NMSÜ25]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Theorem

The semi-regularity hypothesis of [BØ23] is ***wrong*** *for $w \in \{2, 3\}$.*
However, it is true for w large enough and $w \cdot \binom{b}{2} \geq 2\binom{k+1}{2}$.

Our Results [NMSÜ25]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Theorem

*The semi-regularity hypothesis of [BØ23] is **wrong** for $w \in \{2, 3\}$. However, it is true for w large enough and $w \cdot \binom{b}{2} \geq 2\binom{k+1}{2}$.*

Corollary

There is a PPT algorithm for the Regular Syndrome Decoding problem whenever $w \cdot \binom{b}{2} \geq 2\binom{k+1}{2}$.

Semi-Regularity for the Attack of [BØ23]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Semi-Regularity for the Attack of [BØ23]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Hypothesis

A sequence of uniformly random linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)})$ is semi-regular with **overwhelming** probability.

Semi-Regularity for the Attack of [BØ23]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Hypothesis

A sequence of uniformly random linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)})$ is semi-regular with **overwhelming** probability.

We consider huge fields ($\# \mathbb{F} = 2^{256}$).

Semi-Regularity for the Attack of [BØ23]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Hypothesis

A sequence of uniformly random linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)})$ is semi-regular with **overwhelming** probability.

We consider huge fields ($\# \mathbb{F} = 2^{256}$).

Lemma (Schwartz-Zippel)

For $f \in \mathbb{F}[X]$, $f \neq 0$

$$\Pr_{x \leftarrow \mathbb{F}^k}[f(x) = 0] \leq \frac{\deg(f)}{\# \mathbb{F}}$$

Semi-Regularity for the Attack of [BØ23]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Hypothesis

A sequence of uniformly random linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)})$ is semi-regular with **overwhelming** probability.

We consider huge fields ($\# \mathbb{F} = 2^{256}$).
By a Schwartz-Zippel argument, the above hypothesis is equivalent to:

Semi-Regularity for the Attack of [BØ23]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Hypothesis

A sequence of uniformly random linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)})$ is semi-regular with **overwhelming** probability.

We consider huge fields ($\# \mathbb{F} = 2^{256}$).
By a Schwartz-Zippel argument, the above hypothesis is equivalent to:

Hypothesis

There **exists** a semi-regular sequence of linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)})$.

Semi-Regularity for the Attack of [BØ23]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Hypothesis

A sequence of uniformly random linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)})$ is semi-regular wop.

Semi-Regularity for the Attack of [BØ23]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Hypothesis

A sequence of uniformly random linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)})$ is semi-regular wop.

$$\begin{aligned}
\mathcal{H}_{\mathbb{F}[E]/(h_1,\ldots,h_{n-k},E_\alpha^{(i)}\cdot E_\beta^{(i)})}(T) =& (1-T)^{n-k} \cdot \mathcal{H}_{\mathbb{F}[E]/(E_\alpha^{(i)}\cdot E_\beta^{(i)})}(T) \\
=& (1-T)^{n-k} \cdot (1 + bT + bT^2 + \cdots)^w \\
=& 1 + kT + \left(\binom{k+1}{2} - w\binom{b}{2}\right) T^2 + \cdots
\end{aligned}$$

Semi-Regularity for the Attack of [BØ23]

Let $k, n, w \in \mathbb{N}$, $n = bw$.

Hypothesis

A sequence of uniformly random linear forms $h_1, \ldots, h_{n-k} \in \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)})$ is semi-regular wop.

$$\begin{aligned}
\mathcal{H}_{\mathbb{F}[E]/(h_1,\ldots,h_{n-k},E_\alpha^{(i)}\cdot E_\beta^{(i)})}(T) &= (1-T)^{n-k} \cdot \mathcal{H}_{\mathbb{F}[E]/(E_\alpha^{(i)}\cdot E_\beta^{(i)})}(T) \\
&= (1-T)^{n-k} \cdot (1 + bT + bT^2 + \cdots)^w \\
&= 1 + kT + \left(\binom{k+1}{2} - w\binom{b}{2}\right) T^2 + \cdots
\end{aligned}$$

According to semi-regularity hypothesis, we have

$$\mathrm{d}_{\mathrm{reg}} \leq 2 \iff \binom{k+1}{2} \leq w \cdot \binom{b}{2}.$$

Primal-Dual Equivalence

For $(H, s = He)$, [BØ23] considered a **dual** modeling

$$\begin{aligned} E_\alpha^{(i)} \cdot E_\beta^{(i)} &= 0 && \text{for } i \in [w], 1 \leq \alpha < \beta \leq b, \\ s_j = \sum_{i \in [w], \alpha \in [b]} h_{j,\alpha}^{(i)} \cdot E_\alpha^{(i)} & && \text{for } j \in [n-k]. \end{aligned}$$

Primal-Dual Equivalence

For $(H, s = He)$, [BØ23] considered a **dual** modeling

$$\begin{aligned} E_\alpha^{(i)} \cdot E_\beta^{(i)} &= 0 && \text{for } i \in [w], 1 \leq \alpha < \beta \leq b, \\ s_j &= \sum_{i \in [w], \alpha \in [b]} h_{j,\alpha}^{(i)} \cdot E_\alpha^{(i)} && \text{for } j \in [n-k]. \end{aligned}$$

For the LPN version $(G, y = Gx + e)$, $G \in \mathbb{F}^{n \times k}$, $x \in \mathbb{F}^k$, there is also a **primal** modeling over $\mathbb{F}[X_1, \ldots, X_k]$

Primal-Dual Equivalence

For $(H, s = He)$, [BØ23] considered a **dual** modeling

$$E_\alpha^{(i)} \cdot E_\beta^{(i)} = 0 \qquad \text{for } i \in [w], 1 \le \alpha < \beta \le b,$$

$$s_j = \sum_{i \in [w], \alpha \in [b]} h_{j,\alpha}^{(i)} \cdot E_\alpha^{(i)} \qquad \text{for } j \in [n-k].$$

For the LPN version $(G, y = Gx + e)$, $G \in \mathbb{F}^{n \times k}$, $x \in \mathbb{F}^k$, there is also a **primal** modeling over $\mathbb{F}[X_1, \ldots, X_k]$

$$(y_\alpha^i - \sum_{j=1}^{k} g_{\alpha,j}^{(i)} \cdot X_j) \cdot (y_\beta^i - \sum_{j=1}^{k} g_{\beta,j}^{(i)} \cdot X_j) = 0 \quad \text{for } i \in [w], 1 \le \alpha < \beta \le b$$

where every row of G is given by

$$g_\alpha^{(i)} = (g_{\alpha,1}^{(i)}, \ldots, g_{\alpha,k}^{(i)}).$$

Primal-Dual Equivalence

Let $(H, s = He)$ and $(G, y = Gx + e)$ be equivalent formulations of the same code-based problem instance.

Primal-Dual Equivalence

Let $(H, s = He)$ and $(G, y = Gx + e)$ be equivalent formulations of the same code-based problem instance.

Lemma

The dual modeling for $(H, s = He)$ and the primal modeling for $(G, y = Gx + e)$ are equivalent, in the sense that both have the same degree of regularity.

Primal-Dual Equivalence

Let $(H, s = He)$ and $(G, y = Gx + e)$ be equivalent formulations of the same code-based problem instance.

Lemma

The dual modeling for $(H, s = He)$ and the primal modeling for $(G, y = Gx + e)$ are equivalent, in the sense that both have the same degree of regularity.

Proof (High-Level Idea):

Primal-Dual Equivalence

Let $(H, s = He)$ and $(G, y = Gx + e)$ be equivalent formulations of the same code-based problem instance.

Lemma

The dual modeling for $(H, s = He)$ and the primal modeling for $(G, y = Gx + e)$ are equivalent, in the sense that both have the same degree of regularity.

Proof (High-Level Idea): We have a short exact sequence

$$0 \longrightarrow \mathbb{F}^k \xrightarrow{G} \mathbb{F}^n \xrightarrow{H} \mathbb{F}^{n-k} \longrightarrow 0.$$

Primal-Dual Equivalence

Let $(H, s = He)$ and $(G, y = Gx + e)$ be equivalent formulations of the same code-based problem instance.

Lemma

The dual modeling for $(H, s = He)$ and the primal modeling for $(G, y = Gx + e)$ are equivalent, in the sense that both have the same degree of regularity.

Proof (High-Level Idea): We have a short exact sequence

$$0 \longrightarrow \mathbb{F}^k \xrightarrow{G} \mathbb{F}^n \xrightarrow{H} \mathbb{F}^{n-k} \longrightarrow 0.$$

For RSD, this sequence induces an isomorphism

$$\begin{aligned}\mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)}, h_1(E), \ldots, h_{n-k}(E)) &\longrightarrow \mathbb{F}[X]/(g_\alpha^{(i)}(X) \cdot g_\beta^{(i)}(X)) \\ E_\alpha^{(i)} &\longmapsto g_\alpha^{(i)}(X).\end{aligned}$$

Primal-Dual Equivalence

Let $(H, s = He)$ and $(G, y = Gx + e)$ be equivalent formulations of the same code-based problem instance.

Lemma

The dual modeling for $(H, s = He)$ and the primal modeling for $(G, y = Gx + e)$ are equivalent, in the sense that both have the same degree of regularity.

Proof (High-Level Idea): We have a short exact sequence

$$0 \longrightarrow \mathbb{F}^k \xrightarrow{G} \mathbb{F}^n \xrightarrow{H} \mathbb{F}^{n-k} \longrightarrow 0.$$

For RSD, this sequence induces an isomorphism

$$\begin{aligned} \mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)}, h_1(E), \ldots, h_{n-k}(E)) &\longrightarrow \mathbb{F}[X]/(g_\alpha^{(i)}(X) \cdot g_\beta^{(i)}(X)) \\ E_\alpha^{(i)} &\longmapsto g_\alpha^{(i)}(X). \end{aligned}$$

$$\mathrm{d}_{\mathrm{reg}}(\mathcal{H}_{\mathbb{F}[E]/(E_\alpha^{(i)} \cdot E_\beta^{(i)}, h_1(E), \ldots, h_{n-k}(E))}) = \mathrm{d}_{\mathrm{reg}}(\mathcal{H}_{\mathbb{F}[X]/(g_\alpha^{(i)}(X) \cdot g_\beta^{(i)}(X))}).$$

Primal Modeling

For the Regular LPN problem $(G, y = Gx + e)$, consider the polynomial system over $\mathbb{F}[X_1, \ldots, X_k]$

$$(y_\alpha^{(i)} - g_\alpha^{(i)}(X)) \cdot (y_\beta^{(i)} - g_\beta^{(i)}(X)) = 0 \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b$$

where the (i, α)-th row of G is evaluated by the linear form

$$g_\alpha^{(i)}(X) = \sum_{j=1}^{k} g_{\alpha,j}^{(i)} \cdot X_j.$$

Primal Modeling

For the Regular LPN problem $(G, y = Gx + e)$, consider the polynomial system over $\mathbb{F}[X_1, \ldots, X_k]$

$$(y_\alpha^{(i)} - g_\alpha^{(i)}(X)) \cdot (y_\beta^{(i)} - g_\beta^{(i)}(X)) = 0 \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b$$

where the (i, α)-th row of G is evaluated by the linear form

$$g_\alpha^{(i)}(X) = \sum_{j=1}^{k} g_{\alpha,j}^{(i)} \cdot X_j.$$

This system has $\mathrm{d_{reg}} \leq 2$ iff

$$\mathrm{span}\{g_\alpha^{(i)}(X) \cdot g_\beta^{(i)}(X) \mid \text{for } i \in [w], 1 \leq \alpha < \beta \leq b\} = \mathbb{F}[X_1, \ldots, X_k]^2.$$

Primal Modeling

For the Regular LPN problem $(G, y = Gx + e)$, consider the polynomial system over $\mathbb{F}[X_1, \ldots, X_k]$

$$(y_\alpha^{(i)} - g_\alpha^{(i)}(X)) \cdot (y_\beta^{(i)} - g_\beta^{(i)}(X)) = 0 \qquad \text{for } i \in [w], 1 \leq \alpha < \beta \leq b$$

where the (i, α)-th row of G is evaluated by the linear form

$$g_\alpha^{(i)}(X) = \sum_{j=1}^{k} g_{\alpha,j}^{(i)} \cdot X_j.$$

This system has $\mathrm{d}_{\mathrm{reg}} \leq 2$ iff

$$\mathrm{span}\{g_\alpha^{(i)}(X) \cdot g_\beta^{(i)}(X) \mid \text{for } i \in [w], 1 \leq \alpha < \beta \leq b\} = \mathbb{F}[X_1, \ldots, X_k]^2.$$

The semi-regularity hypothesis implies that this holds whenever $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$.

Refuting Semi-Regularity for $w = 2$ and $b = k - 1$

Refuting Semi-Regularity for $w = 2$ and $b = k - 1$

For $w = 2, b = k - 1$, the inequality $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$ does hold.
Hence, the semi-regularity heuristic would imply that there are linear forms $g_1^{(1)}, \dots, g_{k-1}^{(1)}, g_1^{(2)}, \dots, g_{k-1}^{(2)} \in \mathbb{F}[X]^1$ such that

$$\mathrm{span}\{g_\alpha^{(1)} \cdot g_\beta^{(1)}\} + \mathrm{span}\{g_\alpha^{(2)} \cdot g_\beta^{(2)}\} = \mathbb{F}[X_1, \dots, X_k]^2.$$

Refuting Semi-Regularity for $w = 2$ and $b = k - 1$

For $w = 2, b = k - 1$, the inequality $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$ does hold.
Hence, the semi-regularity heuristic would imply that there are linear forms $g_1^{(1)}, \ldots, g_{k-1}^{(1)}, g_1^{(2)}, \ldots, g_{k-1}^{(2)} \in \mathbb{F}[X]^1$ such that

$$\mathrm{span}\{g_\alpha^{(1)} \cdot g_\beta^{(1)}\} + \mathrm{span}\{g_\alpha^{(2)} \cdot g_\beta^{(2)}\} = \mathbb{F}[X_1, \ldots, X_k]^2.$$

Disproof: Write $V^{(1)} = \mathrm{span}\{g_1^{(1)}, \ldots, g_{k-1}^{(1)}\}$
and $V^{(2)} = \mathrm{span}\{g_1^{(2)}, \ldots, g_{k-1}^{(2)}\}$.

Refuting Semi-Regularity for $w = 2$ and $b = k - 1$

For $w = 2, b = k - 1$, the inequality $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$ does hold.
Hence, the semi-regularity heuristic would imply that there are linear forms $g_1^{(1)}, \ldots, g_{k-1}^{(1)}, g_1^{(2)}, \ldots, g_{k-1}^{(2)} \in \mathbb{F}[X]^1$ such that

$$\mathrm{span}\{g_\alpha^{(1)} \cdot g_\beta^{(1)}\} + \mathrm{span}\{g_\alpha^{(2)} \cdot g_\beta^{(2)}\} = \mathbb{F}[X_1, \ldots, X_k]^2.$$

Disproof: Write $V^{(1)} = \mathrm{span}\{g_1^{(1)}, \ldots, g_{k-1}^{(1)}\}$
and $V^{(2)} = \mathrm{span}\{g_1^{(2)}, \ldots, g_{k-1}^{(2)}\}$.
Wlog. $\dim V^{(1)} = \dim V^{(2)} = k - 1$ and $V^{(1)} \neq V^{(2)}$.

Refuting Semi-Regularity for $w = 2$ and $b = k - 1$

For $w = 2, b = k - 1$, the inequality $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$ does hold.
Hence, the semi-regularity heuristic would imply that there are linear forms $g_1^{(1)}, \ldots, g_{k-1}^{(1)}, g_1^{(2)}, \ldots, g_{k-1}^{(2)} \in \mathbb{F}[X]^1$ such that

$$\mathrm{span}\{g_\alpha^{(1)} \cdot g_\beta^{(1)}\} + \mathrm{span}\{g_\alpha^{(2)} \cdot g_\beta^{(2)}\} = \mathbb{F}[X_1, \ldots, X_k]^2.$$

Disproof: Write $V^{(1)} = \mathrm{span}\{g_1^{(1)}, \ldots, g_{k-1}^{(1)}\}$
and $V^{(2)} = \mathrm{span}\{g_1^{(2)}, \ldots, g_{k-1}^{(2)}\}$.
Wlog. $\dim V^{(1)} = \dim V^{(2)} = k - 1$ and $V^{(1)} \neq V^{(2)}$.
Since $V^{(1)}, V^{(2)} \subset \mathbb{F}[X]^1$, the dimension of $C = V^{(1)} \cap V^{(2)}$ is $k - 2$.

Refuting Semi-Regularity for $w = 2$ and $b = k - 1$

For $w = 2, b = k - 1$, the inequality $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$ does hold.
Hence, the semi-regularity heuristic would imply that there are linear forms $g_1^{(1)}, \ldots, g_{k-1}^{(1)}, g_1^{(2)}, \ldots, g_{k-1}^{(2)} \in \mathbb{F}[X]^1$ such that

$$\mathrm{span}\{g_\alpha^{(1)} \cdot g_\beta^{(1)}\} + \mathrm{span}\{g_\alpha^{(2)} \cdot g_\beta^{(2)}\} = \mathbb{F}[X_1, \ldots, X_k]^2.$$

Disproof: Write $V^{(1)} = \mathrm{span}\{g_1^{(1)}, \ldots, g_{k-1}^{(1)}\}$
and $V^{(2)} = \mathrm{span}\{g_1^{(2)}, \ldots, g_{k-1}^{(2)}\}$.
Wlog. $\dim V^{(1)} = \dim V^{(2)} = k - 1$ and $V^{(1)} \neq V^{(2)}$.
Since $V^{(1)}, V^{(2)} \subset \mathbb{F}[X]^1$, the dimension of $C = V^{(1)} \cap V^{(2)}$ is $k - 2$. In particular, there are $g_1, g_2 \in \mathbb{F}[X]^1$ such that

$$V^{(1)} = C + \mathrm{span}\{g_1\}, \qquad V^{(2)} = C + \mathrm{span}\{g_2\}.$$

Refuting Semi-Regularity for $w = 2$ and $b = k - 1$

For $w = 2, b = k - 1$, the inequality $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$ does hold.
Hence, the semi-regularity heuristic would imply that there are linear forms $g_1^{(1)}, \ldots, g_{k-1}^{(1)}, g_1^{(2)}, \ldots, g_{k-1}^{(2)} \in \mathbb{F}[X]^1$ such that

$$\mathrm{span}\{g_\alpha^{(1)} \cdot g_\beta^{(1)}\} + \mathrm{span}\{g_\alpha^{(2)} \cdot g_\beta^{(2)}\} = \mathbb{F}[X_1, \ldots, X_k]^2.$$

Disproof: Write $V^{(1)} = \mathrm{span}\{g_1^{(1)}, \ldots, g_{k-1}^{(1)}\}$
and $V^{(2)} = \mathrm{span}\{g_1^{(2)}, \ldots, g_{k-1}^{(2)}\}$.
Wlog. $\dim V^{(1)} = \dim V^{(2)} = k - 1$ and $V^{(1)} \neq V^{(2)}$.
Since $V^{(1)}, V^{(2)} \subset \mathbb{F}[X]^1$, the dimension of $C = V^{(1)} \cap V^{(2)}$ is $k - 2$. In particular, there are $g_1, g_2 \in \mathbb{F}[X]^1$ such that

$$V^{(1)} = C + \mathrm{span}\{g_1\}, \qquad V^{(2)} = C + \mathrm{span}\{g_2\}.$$

If the hypothesis was true, then

$$\mathbb{F}[X]^2 = (V^{(1)})^2 + (V^{(2)})^2 = C^2 + g_1 \cdot C + C^2 + g_2 \cdot C + \mathrm{span}\{g_1^2, g_2^2\}.$$

Refuting Semi-Regularity for $w = 2$ and $b = k - 1$

For $w = 2, b = k - 1$, the inequality $w \cdot \binom{b}{2} \geq \binom{k+1}{2}$ does hold.
Hence, the semi-regularity heuristic would imply that there are linear forms $g_1^{(1)}, \dots, g_{k-1}^{(1)}, g_1^{(2)}, \dots, g_{k-1}^{(2)} \in \mathbb{F}[X]^1$ such that

$$\mathrm{span}\{g_\alpha^{(1)} \cdot g_\beta^{(1)}\} + \mathrm{span}\{g_\alpha^{(2)} \cdot g_\beta^{(2)}\} = \mathbb{F}[X_1, \dots, X_k]^2.$$

Disproof: Write $V^{(1)} = \mathrm{span}\{g_1^{(1)}, \dots, g_{k-1}^{(1)}\}$
and $V^{(2)} = \mathrm{span}\{g_1^{(2)}, \dots, g_{k-1}^{(2)}\}$.
Wlog. $\dim V^{(1)} = \dim V^{(2)} = k - 1$ and $V^{(1)} \neq V^{(2)}$.
Since $V^{(1)}, V^{(2)} \subset \mathbb{F}[X]^1$, the dimension of $C = V^{(1)} \cap V^{(2)}$ is $k - 2$. In particular, there are $g_1, g_2 \in \mathbb{F}[X]^1$ such that

$$V^{(1)} = C + \mathrm{span}\{g_1\}, \qquad V^{(2)} = C + \mathrm{span}\{g_2\}.$$

If the hypothesis was true, then

$$\mathbb{F}[X]^2 = (V^{(1)})^2 + (V^{(2)})^2 = C^2 + g_1 \cdot C + C^2 + g_2 \cdot C + \mathrm{span}\{g_1^2, g_2^2\}.$$

However, $\binom{k+1}{2} > \binom{k-1}{2} + 2(k-1) + 2$.

Proving Semiregularity for $b\binom{w}{2} \geq 2\binom{k+1}{2}$

Proving Semiregularity for $b\binom{w}{2} \geq 2\binom{k+1}{2}$

Idea: Prove hypothesis for $w = a^2$ and $b \geq \frac{k}{a} + 1$ by constructing linear forms $(g_1^{(i)}, \ldots, g_b^{(i)})_{i=1}^{w} \in \mathbb{F}[X]$ such that

$$\operatorname{span}\left\{ g_\alpha^{(i)} \cdot g_\beta^{(i)} \;\middle|\; i \in [w], 1 \leq \alpha < \beta \leq b \right\} = \mathbb{F}[X]^2.$$

Proving Semiregularity for $b\binom{w}{2} \geq 2\binom{k+1}{2}$

Idea: Prove hypothesis for $w = a^2$ and $b \geq \frac{k}{a} + 1$ by constructing linear forms $(g_1^{(i)}, \ldots, g_b^{(i)})_{i=1}^{w} \in \mathbb{F}[X]$ such that

$$\mathrm{span}\left\{ g_\alpha^{(i)} \cdot g_\beta^{(i)} \;\middle|\; i \in [w], 1 \leq \alpha < \beta \leq b \right\} = \mathbb{F}[X]^2.$$

Prove hypothesis for $w \cdot \binom{b}{2} \geq 2\binom{k+1}{2}$ by noticing that

$$w \geq a^2 \text{ and } b \geq \frac{k}{a} + 1$$

for $a = \left\lceil \frac{k}{b-1} \right\rceil$.

Conclusion

Theorem

The semi-regularity hypothesis of [BØ23] is wrong for $w \in \{2, 3\}$*. However, if* $w \cdot \binom{b}{2} \geq 2\binom{k+1}{2}$*, then the dual and primal modelings of RSD have a degree of regularity of 2.*

Corollary

If $w \cdot \binom{b}{2} \geq 2\binom{k+1}{2}$*, then we can solve an RSD instance* (H, He) *in time* $O(n^{12})$ *with probability* $1 - O(k^2/|\mathbb{F}|)$ *over the randomness of* $H \leftarrow \mathbb{F}^{(n-k)\times n}$*.*

Table of Contents

Learning With Bounded Errors

Let $G \in \mathbb{Z}_q^{n \times k}$ be some generator matrix.

Learning With Bounded Errors

Let $G \in \mathbb{Z}_q^{n \times k}$ be some generator matrix.

Definition (Learning With Errors (LWE) Problem)

Extract x from

$$(G, Gx + e \bmod q)$$

where $x \leftarrow \mathbb{Z}_q^k$ and $e \leftarrow D_\sigma^n$.

Learning With Bounded Errors

Let $G \in \mathbb{Z}_q^{n \times k}$ be some generator matrix.

Definition (Learning With Errors (LWE) Problem)

Extract x from

$$(G, Gx + e \bmod q)$$

where $x \leftarrow \mathbb{Z}_q^k$ and $e \leftarrow D_\sigma^n$.

Definition (Learning With Bounded Errors (LWBE) Problem)

Extract x from

$$(G, Gx + e \bmod q)$$

where $x \leftarrow \mathbb{Z}_q^k$ and $e \leftarrow \{0, \ldots, d-1\}^n$.

Arora-Ge: Primal Modeling

Let $G \in \mathbb{Z}_q^{n \times k}$, $x \in \mathbb{Z}_q^k$, $e \in \{0, \ldots, d-1\}^n$.

Arora-Ge: Primal Modeling

Let $G \in \mathbb{Z}_q^{n\times k}$, $x \in \mathbb{Z}_q^k$, $e \in \{0, \ldots, d-1\}^n$.
Arora-Ge [AG11] algorithm for solving $(G, y = Gx + e)$:

Arora-Ge: Primal Modeling

Let $G \in \mathbb{Z}_q^{n \times k}$, $x \in \mathbb{Z}_q^k$, $e \in \{0, \dots, d-1\}^n$.
Arora-Ge [AG11] algorithm for solving $(G, y = Gx + e)$:

1. Define $f(Z) := Z \cdot (Z-1) \cdot (Z-2) \cdots (Z-d+1)$.

Arora-Ge: Primal Modeling

Let $G \in \mathbb{Z}_q^{n \times k}$, $x \in \mathbb{Z}_q^k$, $e \in \{0, \ldots, d-1\}^n$.
Arora-Ge [AG11] algorithm for solving $(G, y = Gx + e)$:

1. Define $f(Z) := Z \cdot (Z-1) \cdot (Z-2) \cdots (Z-d+1)$.
2. Collect degree-d equations

$$f(y_i - \sum_{j=1}^{k} g_{i,j} \cdot X_j) = 0.$$

Arora-Ge: Primal Modeling

Let $G \in \mathbb{Z}_q^{n \times k}$, $x \in \mathbb{Z}_q^k$, $e \in \{0, \ldots, d-1\}^n$.
Arora-Ge [AG11] algorithm for solving $(G, y = Gx + e)$:

1. Define $f(Z) := Z \cdot (Z-1) \cdot (Z-2) \cdots (Z-d+1)$.
2. Collect degree-d equations

$$f(y_i - \sum_{j=1}^{k} g_{i,j} \cdot X_j) = 0.$$

3. Relinearize and solve the system once enough equations have been collected.

Arora-Ge: Primal Modeling

Let $G \in \mathbb{Z}_q^{n \times k}$, $x \in \mathbb{Z}_q^k$, $e \in \{0, \ldots, d-1\}^n$.
Arora-Ge [AG11] algorithm for solving $(G, y = Gx + e)$:

1. Define $f(Z) := Z \cdot (Z-1) \cdot (Z-2) \cdots (Z-d+1)$.
2. Collect degree-d equations

$$f(y_i - \sum_{j=1}^{k} g_{i,j} \cdot X_j) = 0.$$

3. Relinearize and solve the system once enough equations have been collected.

Arora-Ge: We need $n = O(\log(q) \cdot q \cdot k^d)$ samples.

Arora-Ge: Primal Modeling

Let $G \in \mathbb{Z}_q^{n \times k}$, $x \in \mathbb{Z}_q^k$, $e \in \{0, \ldots, d-1\}^n$.
Arora-Ge [AG11] algorithm for solving $(G, y = Gx + e)$:

1. Define $f(Z) := Z \cdot (Z-1) \cdot (Z-2) \cdots (Z-d+1)$.
2. Collect degree-d equations

$$f(y_i - \sum_{j=1}^{k} g_{i,j} \cdot X_j) = 0.$$

3. Relinearize and solve the system once enough equations have been collected.

Arora-Ge: We need $n = O(\log(q) \cdot q \cdot k^d)$ samples.
Our Work [NMSÜ25]: If $q > d$ is prime, $n = \binom{k+d-1}{d}$ samples are enough.

Semiregularity by Vandermonde Matrices

Lemma

Let $\operatorname{char} \mathbb{F} > d$ *and* $n = \binom{k+d-1}{d}$*. When sampling* $g_1, \ldots, g_n \leftarrow \mathbb{F}[X]^1$*, we have wop.*

$$\operatorname{span}_{\mathbb{F}}\{g_1(X)^d, \ldots, g_n(X)^d\} = \mathbb{F}[X]^d.$$

Semiregularity by Vandermonde Matrices

Lemma

Let $\operatorname{char}\mathbb{F} > d$ *and* $n = \binom{k+d-1}{d}$. ***There are*** $g_1, \ldots, g_n \in \mathbb{F}[X]^1$ *such that*

$$\operatorname{span}_{\mathbb{F}}\{g_1(X)^d, \ldots, g_n(X)^d\} = \mathbb{F}[X]^d.$$

Semiregularity by Vandermonde Matrices

Lemma

Let $\operatorname{char} \mathbb{F} > d$ *and* $n = \binom{k+d-1}{d}$. ***There are*** $g_1, \ldots, g_n \in \mathbb{F}[X]^1$ *such that*

$$\operatorname{span}_{\mathbb{F}}\{g_1(X)^d, \ldots, g_n(X)^d\} = \mathbb{F}[X]^d.$$

Let $\alpha(1), \ldots, \alpha(n)$ be an enumeration of

$$\left\{\beta \in \mathbb{N}_0^{k-1} \;\middle|\; \beta_1 + \cdots + \beta_{k-1} \leq d\right\}.$$

Semiregularity by Vandermonde Matrices

Lemma

Let $\operatorname{char}\mathbb{F} > d$ *and* $n = \binom{k+d-1}{d}$. ***There are*** $g_1, \dots, g_n \in \mathbb{F}[X]^1$ *such that*

$$\operatorname{span}_{\mathbb{F}}\{g_1(X)^d, \dots, g_n(X)^d\} = \mathbb{F}[X]^d.$$

Let $\alpha(1), \dots, \alpha(n)$ be an enumeration of

$$\left\{\beta \in \mathbb{N}_0^{k-1} \;\middle|\; \beta_1 + \dots + \beta_{k-1} \le d\right\}.$$

The **multivariate Vandermonde matrix** on $\alpha(1), \dots, \alpha(n)$ is given by

$$V = \begin{pmatrix} \alpha(1)_1^{\alpha(1)_1} \cdots \alpha(1)_{k-1}^{\alpha(1)_{k-1}} & \cdots & \alpha(1)_1^{\alpha(n)_1} \cdots \alpha(1)_{k-1}^{\alpha(n)_{k-1}} \\ \vdots & \ddots & \vdots \\ \alpha(n)_1^{\alpha(1)_1} \cdots \alpha(n)_{k-1}^{\alpha(1)_{k-1}} & \cdots & \alpha(n)_1^{\alpha(n)_1} \cdots \alpha(n)_{k-1}^{\alpha(n)_{k-1}} \end{pmatrix} \in \mathbb{F}^{n \times n}.$$

Semiregularity by Vandermonde Matrices

Lemma

Let $\operatorname{char}\mathbb{F} > d$ *and* $n = \binom{k+d-1}{d}$. ***There are*** $g_1, \ldots, g_n \in \mathbb{F}[X]^1$ *such that*

$$\mathrm{span}_{\mathbb{F}}\{g_1(X)^d, \ldots, g_n(X)^d\} = \mathbb{F}[X]^d.$$

Let $\alpha(1), \ldots, \alpha(n)$ be an enumeration of

$$\left\{\beta \in \mathbb{N}_0^{k-1} \;\middle|\; \beta_1 + \cdots + \beta_{k-1} \le d\right\}.$$

The **multivariate Vandermonde matrix** on $\alpha(1), \ldots, \alpha(n)$ is given by

$$V = \begin{pmatrix} \alpha(1)_1^{\alpha(1)_1} \cdots \alpha(1)_{k-1}^{\alpha(1)_{k-1}} & \cdots & \alpha(1)_1^{\alpha(n)_1} \cdots \alpha(1)_{k-1}^{\alpha(n)_{k-1}} \\ \vdots & \ddots & \vdots \\ \alpha(n)_1^{\alpha(1)_1} \cdots \alpha(n)_{k-1}^{\alpha(1)_{k-1}} & \cdots & \alpha(n)_1^{\alpha(n)_1} \cdots \alpha(n)_{k-1}^{\alpha(n)_{k-1}} \end{pmatrix} \in \mathbb{F}^{n \times n}.$$

For $f \in \mathbb{F}[X_1, \ldots, X_{k-1}]^d$: $\quad V \cdot \mathrm{coeff}(f) = (f(\alpha(1)), \ldots, f(\alpha(n)))$

Semiregularity by Vandermonde Matrices

$$V = \begin{pmatrix} \alpha(1)_1^{\alpha(1)_1} \cdots \alpha(1)_{k-1}^{\alpha(1)_{k-1}} & \cdots & \alpha(1)_1^{\alpha(n)_1} \cdots \alpha(1)_{k-1}^{\alpha(n)_{k-1}} \\ \vdots & \ddots & \vdots \\ \alpha(n)_1^{\alpha(1)_1} \cdots \alpha(n)_{k-1}^{\alpha(1)_{k-1}} & \cdots & \alpha(n)_1^{\alpha(n)_1} \cdots \alpha(n)_{k-1}^{\alpha(n)_{k-1}} \end{pmatrix} \in \mathbb{F}^{n \times n}.$$

Semiregularity by Vandermonde Matrices

$$V = \begin{pmatrix} \alpha(1)^{\alpha(1)} & \cdots & \alpha(1)^{\alpha(n)} \\ \vdots & \ddots & \vdots \\ \alpha(n)^{\alpha(1)} & \cdots & \alpha(n)^{\alpha(n)} \end{pmatrix} \in \mathbb{F}^{n \times n}.$$

Semiregularity by Vandermonde Matrices

$$V = \begin{pmatrix} \alpha(1)^{\alpha(1)} & \cdots & \alpha(1)^{\alpha(n)} \\ \vdots & \ddots & \vdots \\ \alpha(n)^{\alpha(1)} & \cdots & \alpha(n)^{\alpha(n)} \end{pmatrix} \in \mathbb{F}^{n \times n}.$$

One can show: $\det V = \prod_{i=1}^{d} (d + 1 - i)^{i \cdot \binom{k-2+i}{i}}$.

Semiregularity by Vandermonde Matrices

$$V = \begin{pmatrix} \alpha(1)^{\alpha(1)} & \cdots & \alpha(1)^{\alpha(n)} \\ \vdots & \ddots & \vdots \\ \alpha(n)^{\alpha(1)} & \cdots & \alpha(n)^{\alpha(n)} \end{pmatrix} \in \mathbb{F}^{n \times n}.$$

One can show: $\det V = \prod_{i=1}^{d} (d+1-i)^{i \cdot \binom{k-2+i}{i}}$.
Set for $i \in [n]$

$$g_i(X) := X_k + \sum_{j=1}^{k-1} \alpha(i)_j \cdot X_j.$$

Semiregularity by Vandermonde Matrices

$$V = \begin{pmatrix} \alpha(1)^{\alpha(1)} & \cdots & \alpha(1)^{\alpha(n)} \\ \vdots & \ddots & \vdots \\ \alpha(n)^{\alpha(1)} & \cdots & \alpha(n)^{\alpha(n)} \end{pmatrix} \in \mathbb{F}^{n \times n}.$$

One can show: $\det V = \prod_{i=1}^{d} (d+1-i)^{i \cdot \binom{k-2+i}{i}}$.
Set for $i \in [n]$

$$g_i(X) := X_k + \sum_{j=1}^{k-1} \alpha(i)_j \cdot X_j.$$

We have

$$(g_i(X))^d = \sum_{j=1}^{n} \gamma_j \cdot \alpha(i)^{\alpha(j)} \cdot X_1^{\alpha(j)_1} \cdots X_{k-1}^{\alpha(j)_{k-1}} \cdot X_k^{d-\alpha(j)_1-\cdots-\alpha(j)_{k-1}}$$

for $\gamma_1, \ldots, \gamma_n \in \mathbb{F}$ not zero.

Semiregularity by Vandermonde Matrices

We have

$$(g_i(X))^d = \sum_{j=1}^{n} \gamma_j \cdot \alpha(i)^{\alpha(j)} \cdot X_1^{\alpha(j)_1} \cdots X_{k-1}^{\alpha(j)_{k-1}} \cdot X_k^{d-\alpha(j)_1-\cdots-\alpha(j)_{k-1}}$$

for $\gamma_1, \ldots, \gamma_n \in \mathbb{F}$ not zero.

Semiregularity by Vandermonde Matrices

We have

$$(g_i(X))^d = \sum_{j=1}^{n} \gamma_j \cdot \alpha(i)^{\alpha(j)} \cdot X_1^{\alpha(j)_1} \cdots X_{k-1}^{\alpha(j)_{k-1}} \cdot X_k^{d-\alpha(j)_1-\cdots-\alpha(j)_{k-1}}$$

for $\gamma_1, \ldots, \gamma_n \in \mathbb{F}$ not zero.

Hence,

$$\begin{pmatrix} \mathrm{coeff}(g_1^d) \\ \vdots \\ \mathrm{coeff}(g_n^d) \end{pmatrix} = \begin{pmatrix} \alpha(1)^{\alpha(1)} & \cdots & \alpha(1)^{\alpha(n)} \\ \vdots & \ddots & \vdots \\ \alpha(n)^{\alpha(1)} & \cdots & \alpha(n)^{\alpha(n)} \end{pmatrix} \cdot \begin{pmatrix} \gamma_1 & & \\ & \ddots & \\ & & \gamma_n \end{pmatrix}.$$

Semiregularity by Vandermonde Matrices

We have

$$(g_i(X))^d = \sum_{j=1}^{n} \gamma_j \cdot \alpha(i)^{\alpha(j)} \cdot X_1^{\alpha(j)_1} \cdots X_{k-1}^{\alpha(j)_{k-1}} \cdot X_k^{d-\alpha(j)_1-\cdots-\alpha(j)_{k-1}}$$

for $\gamma_1, \ldots, \gamma_n \in \mathbb{F}$ not zero.
Hence,

$$\begin{pmatrix} \mathrm{coeff}(g_1^d) \\ \vdots \\ \mathrm{coeff}(g_n^d) \end{pmatrix} = \begin{pmatrix} \alpha(1)^{\alpha(1)} & \cdots & \alpha(1)^{\alpha(n)} \\ \vdots & \ddots & \vdots \\ \alpha(n)^{\alpha(1)} & \cdots & \alpha(n)^{\alpha(n)} \end{pmatrix} \cdot \begin{pmatrix} \gamma_1 & & \\ & \ddots & \\ & & \gamma_n \end{pmatrix}.$$

Lemma

Let $\mathrm{char}\,\mathbb{F} > d$ *and* $n = \binom{k+d-1}{d}$. *There are* $g_1, \ldots, g_n \in \mathbb{F}[X]^1$ *such that*

$$\mathrm{span}_{\mathbb{F}}\{g_1(X)^d, \ldots, g_n(X)^d\} = \mathbb{F}[X]^d.$$

Semiregularity by Vandermonde Matrices

We have

$$(g_i(X))^d = \sum_{j=1}^{n} \gamma_j \cdot \alpha(i)^{\alpha(j)} \cdot X_1^{\alpha(j)_1} \cdots X_{k-1}^{\alpha(j)_{k-1}} \cdot X_k^{d-\alpha(j)_1-\cdots-\alpha(j)_{k-1}}$$

for $\gamma_1, \ldots, \gamma_n \in \mathbb{F}$ not zero.
Hence,

$$\begin{pmatrix} \mathrm{coeff}(g_1^d) \\ \vdots \\ \mathrm{coeff}(g_n^d) \end{pmatrix} = \begin{pmatrix} \alpha(1)^{\alpha(1)} & \cdots & \alpha(1)^{\alpha(n)} \\ \vdots & \ddots & \vdots \\ \alpha(n)^{\alpha(1)} & \cdots & \alpha(n)^{\alpha(n)} \end{pmatrix} \cdot \begin{pmatrix} \gamma_1 & & \\ & \ddots & \\ & & \gamma_n \end{pmatrix}.$$

Lemma

Let char $\mathbb{F} > d$ *and* $n = \binom{k+d-1}{d}$. *When* ***sampling*** $g_1, \ldots, g_n \leftarrow \mathbb{F}[X]^1$, *we have with probability* $\geq 1 - nd/|\mathbb{F}|$

$$\mathrm{span}_{\mathbb{F}}\{g_1(X)^d, \ldots, g_n(X)^d\} = \mathbb{F}[X]^d.$$

Overview of Runtimes

		Samples	Time	Heuristical?
[AG11]	**d**	$O\left(\log(q)\cdot q\cdot k^{d}\right)$	$O\left(\log(q)\cdot q\cdot k^{\omega d}\right)$	NO
[ACFP14]	2	$O\left(k\log\log k\right)$	$O\left(k^2\cdot 2^{\frac{\omega k\log\log\log k}{8\log\log k}}\right)$	NO
[ACFP14]	2	$c\cdot k$	$2^{O(k)}$	YES
[STA20]	2	$c\cdot k^2$	$k^{O(1/c)}$	YES
[STA20]	2	$k^{1+\alpha}$	$2^{\widetilde{O}\left(n^{1-\alpha}\right)}$	YES
[Ste24]	**d**	$> k$	$2^{O(k)}$	NO
[Ste24]	**d**	$O\left(\binom{k+d-1}{d}\right)$	$O\left(d^3\cdot c_d^{(k-1)^{1-1/\ln(4)}}\right)$	YES
[Ste24]	2	$O\left(k^2\right)$	$O\left(k^2\cdot\binom{k+3}{3}^{\omega+2}\right)$	YES
[NMSÜ25]	**d**	$\binom{k+d-1}{d}$	$O\left(dk^{1+d\omega}\right)$	NO

References I

Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, and Ludovic Perret.
Algebraic algorithms for LWE.
Cryptology ePrint Archive, Report 2014/1018, 2014.

Sanjeev Arora and Rong Ge.
New algorithms for learning in presence of errors.
In Luca Aceto, Monika Henzinger, and Jiri Sgall, editors, *ICALP 2011, Part I*, volume 6755 of *LNCS*, pages 403–415. Springer, Berlin, Heidelberg, July 2011.

Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Peter Rindal, and Peter Scholl.
Efficient two-round OT extension and silent non-interactive secure computation.

References II

In Lorenzo Cavallaro, Johannes Kinder, XiaoFeng Wang, and Jonathan Katz, editors, *ACM CCS 2019*, pages 291–308. ACM Press, November 2019.

Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl.
Efficient pseudorandom correlation generators from ring-LPN.
In Daniele Micciancio and Thomas Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 387–416. Springer, Cham, August 2020.

Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai.
Compressing vector OLE.
In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 896–912. ACM Press, October 2018.

References III

Pierre Briaud and Morten Øygarden.
A new algebraic approach to the regular syndrome decoding problem and implications for PCG constructions.
In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 391–422. Springer, Cham, April 2023.

Ralf Fröberg.
An inequality for hilbert series of graded algebras.
MATHEMATICA SCANDINAVICA, 56:117–144, 12 1985.

Miguel Cueto Noval, Simon-Philipp Merz, Patrick Stählin, and Akin Ünal.
On the soundness of algebraic attacks against code-based assumptions.

References IV

In Serge Fehr and Pierre-Alain Fouque, editors, *EUROCRYPT 2025, Part VI*, volume 15606 of *LNCS*, pages 385–415. Springer, Cham, May 2025.

Keith Pardue.
Generic sequences of polynomials.
Journal of Algebra, 324(4):579–590, 2010.

Flavio Salizzoni.
An upper bound for the solving degree in terms of the degree of regularity.
Transactions on Mathematical Cryptology, 5(1):1–7, Sep. 2025.

Chao Sun, Mehdi Tibouchi, and Masayuki Abe.
Revisiting the hardness of binary error LWE.
In Joseph K. Liu and Hui Cui, editors, *ACISP 20*, volume 12248 of *LNCS*, pages 425–444. Springer, Cham, November / December 2020.

References V

Matthias Johann Steiner.
The complexity of algebraic algorithms for LWE.
In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part III*, volume 14653 of *LNCS*, pages 375–403. Springer, Cham, May 2024.