On the Soundness of Algebraic Attacks against Code-based Assumptions

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

Eurocrypt 2025

ISTA, Klosterneuburg, Austria

ETH Zurich, Zurich, Switzerland

Institute of Science and Technology Austria

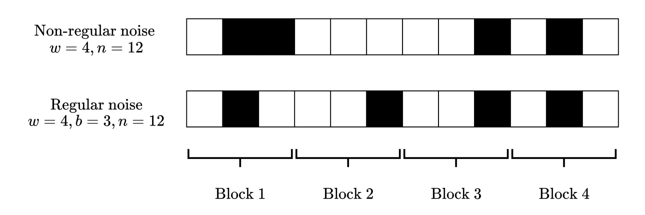
Introduction

Introduction: Regular Syndrome Decoding

- Syndrome Decoding Problem: given a parity-check matrix $\mathbf{H} \in \mathbb{F}^{n-k,n}$ and a syndrome $\mathbf{s} = \mathbf{He} \in \mathbb{F}^{n-k}$ such that $\mathrm{hw}(\mathbf{e}) \leq w$, find $\mathbf{e} \in \mathbb{F}^n$.

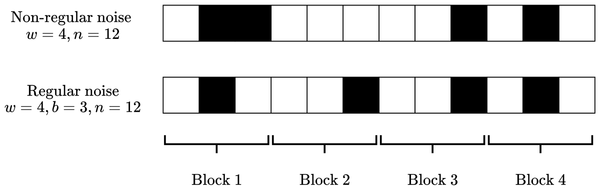
Introduction: Regular Syndrome Decoding

- Syndrome Decoding Problem: given a parity-check matrix $\mathbf{H} \in \mathbb{F}^{n-k,n}$ and a syndrome $\mathbf{s} = \mathbf{He} \in \mathbb{F}^{n-k}$ such that $\mathrm{hw}(\mathbf{e}) \leq w$, find $\mathbf{e} \in \mathbb{F}^n$.
- Regular Syndrome Decoding (RSD) Problem: given a parity-check matrix $\mathbf{H} \in \mathbb{F}^{n-k,n}$ and a syndrome $\mathbf{s} = \mathbf{He} \in \mathbb{F}^{n-k}$ such that $\mathbf{e}^\mathsf{T} = ((\mathbf{e}^{(1)})^\mathsf{T}, \ldots, (\mathbf{e}^{(w)})^\mathsf{T})$ and $\mathbf{e}^{(i)} \in \mathbb{F}^b$ and $\mathrm{hw}(\mathbf{e}^{(i)}) \leq 1$ for all i, find $\mathbf{e} \in \mathbb{F}^n$.



Introduction: Regular Syndrome Decoding

- Syndrome Decoding Problem: given a parity-check matrix $\mathbf{H} \in \mathbb{F}^{n-k,n}$ and a syndrome $\mathbf{s} = \mathbf{He} \in \mathbb{F}^{n-k}$ such that $\mathrm{hw}(\mathbf{e}) \leq w$, find $\mathbf{e} \in \mathbb{F}^n$.
- Regular Syndrome Decoding (RSD) Problem: given a parity-check matrix $\mathbf{H} \in \mathbb{F}^{n-k,n}$ and a syndrome $\mathbf{s} = \mathbf{He} \in \mathbb{F}^{n-k}$ such that $\mathbf{e}^\mathsf{T} = ((\mathbf{e}^{(1)})^\mathsf{T}, \ldots, (\mathbf{e}^{(w)})^\mathsf{T})$ and $\mathbf{e}^{(i)} \in \mathbb{F}^b$ and $\mathrm{hw}(\mathbf{e}^{(i)}) \leq 1$ for all i, find $\mathbf{e} \in \mathbb{F}^n$.



- Applications of RSD in cryptography: MPC [Haz+18], signatures [CCJ23], Vector Oblivious Linear Evaluation [Boy+18], Pseudorandom Correlation Generators [Boy+19].

- The analysis of the best known attack [BØ23] relies on unproven assumptions.
- Question: *Do algebraic attacks on RSD actually work?*

- The analysis of the best known attack [BØ23] relies on unproven assumptions.
- Question: *Do algebraic attacks on RSD actually work?*

Theorem

NO for $w = 2, b < k$ and $w = 3, b < 2k/3$.
YES for $w \cdot \binom{b}{2} > 6 \cdot \binom{k+1}{2}$ and $w \geq 4$ and $\mathbb{F}$ large enough.
Here $b =$ block length, $w =$ number of blocks, $k =$ code dimension.

Main Theorem

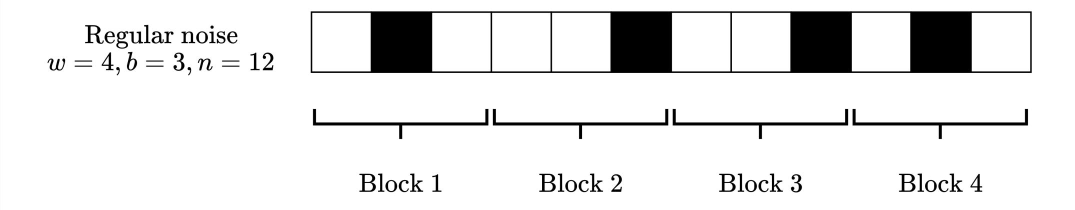
Let $\mathbb{F}$ be a large enough field. There is a PPT algorithm that can solve RSD over $\mathbb{F}$ with $w \geq 4$ blocks and block length b with high probability (over the randomness of $\mathbf{H} \leftarrow \mathbb{F}^{n-k,n}$) if

$$w \cdot \binom{b}{2} \geq 6 \cdot \binom{k+1}{2}.$$

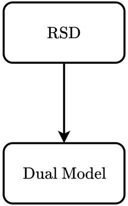
Proof Sketch

Recap

Let $(\mathbf{H}, \mathbf{s} = \mathbf{He}) \in \mathbb{F}^{n-k,n} \times \mathbb{F}^{n-k}$ be a RSD instance.



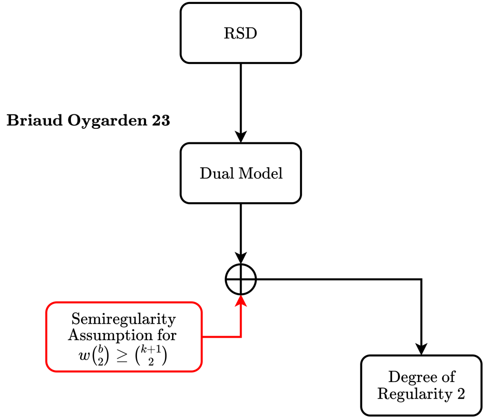
Overview



Briaud Oygarden 23

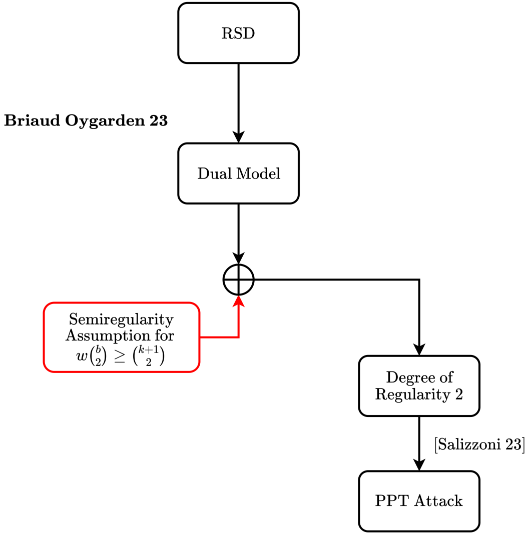
This Work

Overview

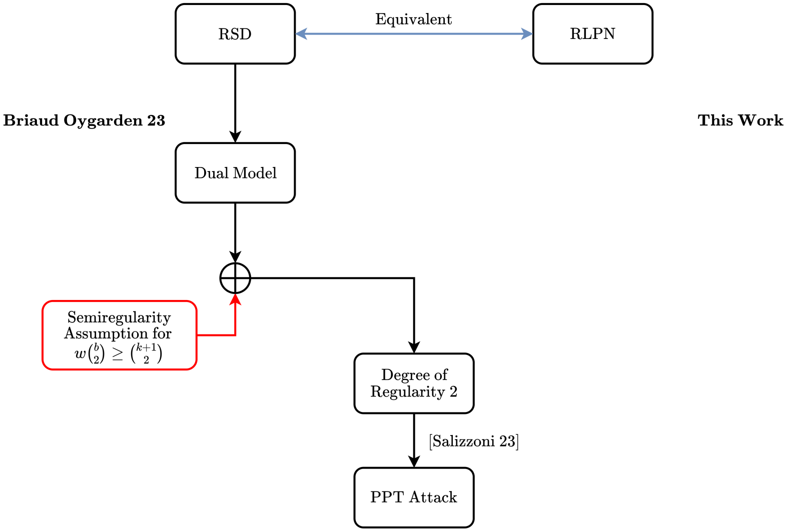


RSD
Briaud Oygarden 23
This Work
Dual Model
Semiregularity Assumption for $w\binom{b}{2} \geq \binom{k+1}{2}$
Degree of Regularity 2

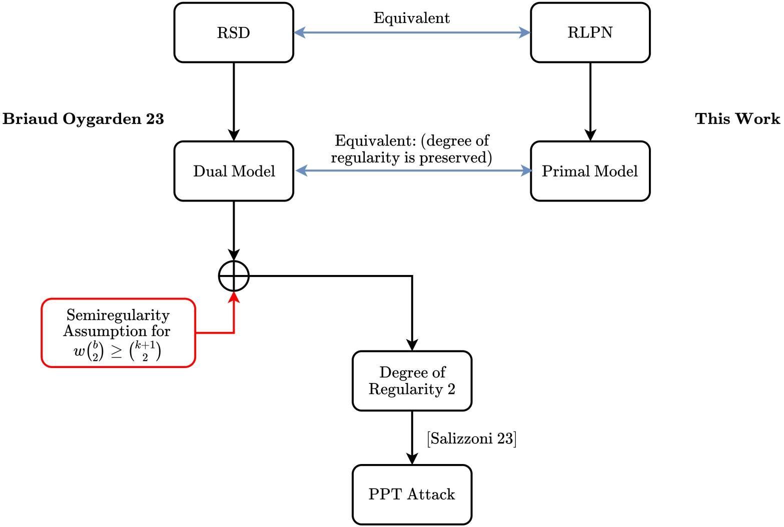
Overview


RSD
Briaud Oygarden 23
This Work
Dual Model
Semiregularity Assumption for $w\binom{b}{2} \geq \binom{k+1}{2}$
Degree of Regularity 2
[Salizzoni 23]
PPT Attack

Overview

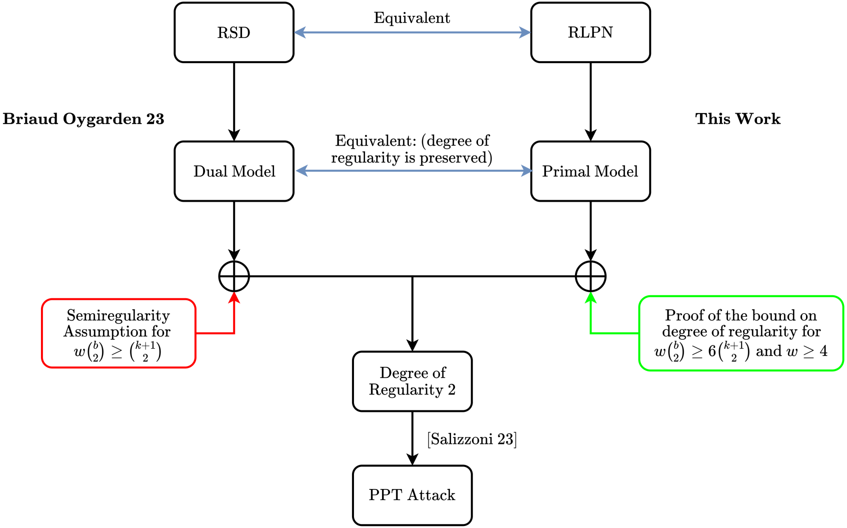

RSD
Equivalent
RLPN
Briaud Oygarden 23
This Work
Dual Model
Semiregularity Assumption for $w\binom{b}{2} \geq \binom{k+1}{2}$
Degree of Regularity 2
[Salizzoni 23]
PPT Attack

Overview



RSD
Equivalent
RLPN
Briaud Oygarden 23
This Work
Dual Model
Equivalent: (degree of regularity is preserved)
Primal Model
Semiregularity Assumption for $w\binom{b}{2} \geq \binom{k+1}{2}$
Degree of Regularity 2
[Salizzoni 23]
PPT Attack

Overview



RSD
Equivalent
RLPN
Briaud Oygarden 23
This Work
Equivalent: (degree of regularity is preserved)
Dual Model
Primal Model
Semiregularity Assumption for $w\binom{b}{2} \geq \binom{k+1}{2}$
Proof of the bound on degree of regularity for $w\binom{b}{2} \geq 6\binom{k+1}{2}$ and $w \geq 4$
Degree of Regularity 2
[Salizzoni 23]
PPT Attack

Dual Model [BØ23]

Let $(\mathbf{H}, \mathbf{s} = \mathbf{H}\mathbf{e}) \in \mathbb{F}^{n-k,n} \times \mathbb{F}^{n-k}$ be a RSD instance. Recall that $\mathbf{e}^\mathsf{T} = ((\mathbf{e}^{(1)})^\mathsf{T}, \ldots, (\mathbf{e}^{(w)})^\mathsf{T})$ and $\mathbf{e}^{(i)} \in \mathbb{F}^b$ and $\mathrm{hw}(\mathbf{e}^{(i)}) \leq 1$ for all i.

Dual Model [BØ23]

Let $(\mathbf{H}, \mathbf{s} = \mathbf{He}) \in \mathbb{F}^{n-k,n} \times \mathbb{F}^{n-k}$ be a RSD instance. Recall that $\mathbf{e}^\mathsf{T} = ((\mathbf{e}^{(1)})^\mathsf{T}, \dots, (\mathbf{e}^{(w)})^\mathsf{T})$ and $\mathbf{e}^{(i)} \in \mathbb{F}^b$ and $\mathrm{hw}(\mathbf{e}^{(i)}) \leq 1$ for all i.

Consider:

- $n = wb$ variables for the errors $E = (E_\alpha^{(i)})_{\alpha \in [b], i \in [w]}$ and
- the rows $\mathbf{h}_1^\mathsf{T}, \dots, \mathbf{h}_{n-k}^\mathsf{T}$ of $\mathbf{H}$.

Dual Model [BØ23]

Let $(\mathbf{H}, \mathbf{s} = \mathbf{He}) \in \mathbb{F}^{n-k,n} \times \mathbb{F}^{n-k}$ be a RSD instance. Recall that $\mathbf{e}^\mathsf{T} = ((\mathbf{e}^{(1)})^\mathsf{T}, \ldots, (\mathbf{e}^{(w)})^\mathsf{T})$ and $\mathbf{e}^{(i)} \in \mathbb{F}^b$ and $\mathrm{hw}(\mathbf{e}^{(i)}) \leq 1$ for all i.

Consider:

- $n = wb$ variables for the errors $E = (E_\alpha^{(i)})_{\alpha \in [b], i \in [w]}$ and
- the rows $\mathbf{h}_1^\mathsf{T}, \ldots, \mathbf{h}_{n-k}^\mathsf{T}$ of $\mathbf{H}$.

Dual Model:

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

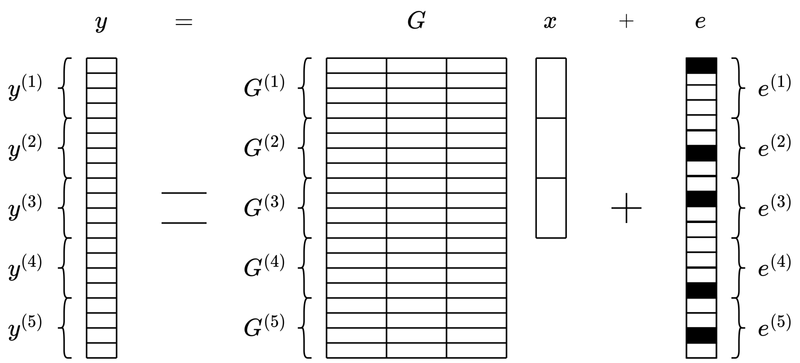
$$h_j(E) := \mathbf{h}_j^\mathsf{T} \cdot E = s_j, \qquad \text{for } j \in [n-k].$$

Primal Model [AG11]

The Regular LPN problem: given $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e}) \in \mathbb{F}^{n,k} \times \mathbb{F}^{n}$, find $\mathbf{x} \in \mathbb{F}^{k}$ and $\mathbf{e}^{\mathsf{T}} = ((\mathbf{e}^{(1)})^{\mathsf{T}}, \ldots, (\mathbf{e}^{(w)})^{\mathsf{T}}) \in \mathbb{F}^{n}$ where $\mathbf{e}^{(i)} \in \mathbb{F}^{b}$ and $\mathrm{hw}(\mathbf{e}^{(i)}) \leq 1$.

Primal Model [AG11]

The Regular LPN problem: given $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e}) \in \mathbb{F}^{n,k} \times \mathbb{F}^{n}$, find $\mathbf{x} \in \mathbb{F}^{k}$ and $\mathbf{e}^{\mathsf{T}} = ((\mathbf{e}^{(1)})^{\mathsf{T}}, \ldots, (\mathbf{e}^{(w)})^{\mathsf{T}}) \in \mathbb{F}^{n}$ where $\mathbf{e}^{(i)} \in \mathbb{F}^{b}$ and $\mathrm{hw}(\mathbf{e}^{(i)}) \leq 1$.



Primal Model [AG11]

The Regular LPN problem: given $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e}) \in \mathbb{F}^{n,k} \times \mathbb{F}^n$, find $\mathbf{x} \in \mathbb{F}^k$ and $\mathbf{e}^\mathsf{T} = ((\mathbf{e}^{(1)})^\mathsf{T}, \ldots, (\mathbf{e}^{(w)})^\mathsf{T}) \in \mathbb{F}^n$ where $\mathbf{e}^{(i)} \in \mathbb{F}^b$ and $\mathrm{hw}(\mathbf{e}^{(i)}) \leq 1$.

Decompose $\mathbf{G}$ into blocks

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}^{(1)} \\ \vdots \\ \mathbf{G}^{(w)} \end{pmatrix} \quad \text{of shape } b \times k \text{ where} \quad \mathbf{G}^{(i)} = \begin{pmatrix} (\mathbf{g}_1^{(i)})^\mathsf{T} \\ \vdots \\ (\mathbf{g}_b^{(i)})^\mathsf{T} \end{pmatrix}.$$

Decompose $\mathbf{y}^\mathsf{T} = ((\mathbf{y}^{(1)})^\mathsf{T}, \ldots, (\mathbf{y}^{(w)})^\mathsf{T}) = ((y_1^{(1)}, \ldots, y_b^{(1)}), \ldots, (y_1^{(w)}, \ldots, y_b^{(w)}))$.

Primal Model [AG11]

The Regular LPN problem: given $(\mathbf{G}, \mathbf{y} = \mathbf{G}\mathbf{x} + \mathbf{e}) \in \mathbb{F}^{n,k} \times \mathbb{F}^{n}$, find $\mathbf{x} \in \mathbb{F}^{k}$ and $\mathbf{e}^{\mathsf{T}} = ((\mathbf{e}^{(1)})^{\mathsf{T}}, \ldots, (\mathbf{e}^{(w)})^{\mathsf{T}}) \in \mathbb{F}^{n}$ where $\mathbf{e}^{(i)} \in \mathbb{F}^{b}$ and $\mathrm{hw}(\mathbf{e}^{(i)}) \leq 1$.

Decompose $\mathbf{G}$ into blocks

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}^{(1)} \\ \vdots \\ \mathbf{G}^{(w)} \end{pmatrix} \quad \text{of shape } b \times k \text{ where} \quad \mathbf{G}^{(i)} = \begin{pmatrix} (\mathbf{g}_1^{(i)})^{\mathsf{T}} \\ \vdots \\ (\mathbf{g}_b^{(i)})^{\mathsf{T}} \end{pmatrix}.$$

Decompose $\mathbf{y}^{\mathsf{T}} = ((\mathbf{y}^{(1)})^{\mathsf{T}}, \ldots, (\mathbf{y}^{(w)})^{\mathsf{T}}) = ((y_1^{(1)}, \ldots, y_b^{(1)}), \ldots, (y_1^{(w)}, \ldots, y_b^{(w)}))$.

Primal Model:

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

where $g_\alpha^{(i)}(X) \coloneqq (\mathbf{g}_\alpha^{(i)})^{\mathsf{T}} \cdot X$.

Proof Strategy

1. The two models are equivalent; they have the same degree of regularity.

Proof Strategy

1. The two models are equivalent; they have the same degree of regularity.
2. We want to show that for $g_\alpha^{(i)}(X) \leftarrow \mathbb{F}[X]^{=1}$ for $i \in [w], \alpha \in [b]$ it holds with high probability that

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

Proof Strategy

1. The two models are equivalent; they have the same degree of regularity.
2. We want to show that for $g_\alpha^{(i)}(X) \leftarrow \mathbb{F}[X]^{=1}$ for $i \in [w], \alpha \in [b]$ it holds with high probability that

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

3. Over large fields, it suffices to show existence! There exist $g_\alpha^{(i)}(X) \in \mathbb{F}[X]^{=1}$ for $i \in [w], \alpha \in [b]$ such that

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

Proof Strategy

1. The two models are equivalent; they have the same degree of regularity.
2. We want to show that for $g_\alpha^{(i)}(X) \leftarrow \mathbb{F}[X]^{=1}$ for $i \in [w], \alpha \in [b]$ it holds with high probability that
$$\sum_{i \in [w]} \mathrm{span}_{\mathbb{F}}\{g_\alpha^{(i)}(X) g_\beta^{(i)}(X) \mid 1 \leq \alpha < \beta \leq b\} = \mathbb{F}[X_1, \ldots, X_k]^{=2}.$$
3. Over large fields, it suffices to show existence! There exist $g_\alpha^{(i)}(X) \in \mathbb{F}[X]^{=1}$ for $i \in [w], \alpha \in [b]$ such that
$$\sum_{i \in [w]} \mathrm{span}_{\mathbb{F}}\{g_\alpha^{(i)}(X) g_\beta^{(i)}(X) \mid 1 \leq \alpha < \beta \leq b\} = \mathbb{F}[X_1, \ldots, X_k]^{=2}.$$
4. Result of [Salizzoni23] implies PPT algorithm.

Learning with Bounded Errors

Learning with Bounded Errors

Learning with Bounded Errors (LWBE) Problem: given a generator matrix $\mathbf{G} \in \mathbb{F}^{n \times k}$ and $\mathbf{b} = \mathbf{G}\mathbf{x} + \mathbf{e}$, where $\mathbf{e} \in \{0, \ldots, d-1\}^n$, find $\mathbf{x} \in \mathbb{F}^k$.

Learning with Bounded Errors

Learning with Bounded Errors (LWBE) Problem: given a generator matrix $\mathbf{G} \in \mathbb{F}^{n \times k}$ and $\mathbf{b} = \mathbf{G}\mathbf{x} + \mathbf{e}$, where $\mathbf{e} \in \{0, \ldots, d-1\}^n$, find $\mathbf{x} \in \mathbb{F}^k$.

Main Theorem

Let $n = \binom{k+d-1}{d}$ and $\mathbb{F}$ be large enough with characteristic $> d$. There is an algorithm that solves LWBE with high probability (over the randomness of $\mathbf{G} \leftarrow \mathbb{F}^{n,k}$) and has time complexity $O(dk^{1+d\omega})$.[a]

[a] Recall $2 \leq \omega \leq 2.38$.

Learning with Bounded Errors

Learning with Bounded Errors (LWBE) Problem: given a generator matrix $\mathbf{G} \in \mathbb{F}^{n \times k}$ and $\mathbf{b} = \mathbf{G}\mathbf{x} + \mathbf{e}$, where $\mathbf{e} \in \{0, \ldots, d-1\}^n$, find $\mathbf{x} \in \mathbb{F}^k$.

Main Theorem

Let $n = \binom{k+d-1}{d}$ and $\mathbb{F}$ be large enough with characteristic $> d$. There is an algorithm that solves LWBE with high probability (over the randomness of $\mathbf{G} \leftarrow \mathbb{F}^{n,k}$) and has time complexity $O(dk^{1+d\omega})$.[a]

[a] Recall $2 \leq \omega \leq 2.38$.

Learning with Rounding (LWR) with primes $q > p$ can be broken in time $O(qk^{1+\omega q/p}/p)$ when given $O(k^{q/p})$ samples.

Cryptanalysis of LWBE

Work	Size of Errors	Number of Samples n	Time Complexity
AG11	d	$O\left(\log(q) \cdot q \cdot k^d\right)$	$O\left(\log(q) \cdot q \cdot k^{\omega d}\right)$
Steiner 24	d	$> k$	$O\left(n \cdot d \cdot k \cdot 2^{O(k)}\right)$
This Work	d	$\binom{k+d-1}{d}$	$O\left(dk^{1+d\omega}\right)$

Table 1: An overview of attacks on LWBE that do not rely on heuristics. Recall $2 \leq \omega \leq 2.38$.

Conclusion

Conclusion

- Verified some of the assumptions in [BØ23] and obtained a PPT algorithm for RSD/RLPN when $w \cdot \binom{b}{2} \geq 6 \cdot \binom{k+1}{2}$.
- We apply the same framework in order to obtain attacks against other problems like
  - LWBE with $O(k^d)$ samples and in time $O(dk^{1+2.38d})$,
  - LWR with $O(k^{q/p})$ samples and in time $O(qk^{1+2.38q/p}/p)$.

Thanks

`https://eprint.iacr.org/2025/415`