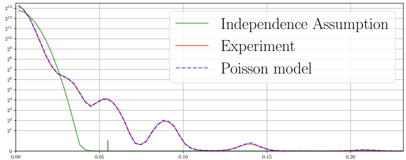
Rigorous Foundations for Dual Attacks in Coding Theory

Charles Meyer-Hilfiger, Jean-Pierre Tillich

TCC 2023



Dual attacks in codes and lattices

Dual attacks solve

Decoding Problem in Codes and Lattices

→ Heart of security of cryptographic primitives

Lattices : Dual attacks would impact Kyber (NIST standard)

Independence assumptions to analyze dual attacks

Not valid

Codes	Lattices
Carrier, Debris-Alazard, Meyer-Hilfiger, Tillich. 2022 : "Statistical decoding 2.0" ↓ Notice experimental differences	Ducas, Pulles. 2023 : "Does the Dual-Sieve Attack on Learning with Errors even Work?" ↓ Seriously question dual attacks

Contributions of the paper

- Explain why independence assumptions does not hold
- Give rigorous foundations for analyzing dual attacks $\leftarrow$ **This talk**
- Show that dual attacks in coding theory work

Table of Contents

Setting for **Dual** attacks in Coding Theory

Linear code

$\mathscr{C}$ a binary $[n, k]$ linear code: linear subspace of $\mathbb{F}_2^n$ of dimension k.

Decoding problem at distance t (small)

- **Input:** $\mathbf{y} \in \mathbb{F}_2^n$ where $\mathbf{y} = \mathbf{c} + \mathbf{e}$ with $\mathbf{c} \in \mathscr{C}$ and $|\mathbf{e}| = t$
- **Output:** $\mathbf{e} \in \mathbb{F}_2^n$ such that $|\mathbf{e}| = t$ and $\mathbf{y} + \mathbf{e} \in \mathscr{C}$.

$|\mathbf{x}|$ is Hamming weight of $\mathbf{x}$: number of non-zero coordinates.

Dual code

$\mathscr{C}^{\perp} = \{\mathbf{h} \in \mathbb{F}_2^n \ : \ \langle \mathbf{h}, \mathbf{c} \rangle = 0 \quad \forall \mathbf{c} \in \mathscr{C}\} \rightarrow \mathscr{C}^{\perp}$ is $[n, n-k]$ linear code

$\langle \mathbf{x}, \mathbf{z} \rangle \in \mathbb{F}_2$ usual inner product for $\mathbb{F}_2^n$

Idea of Dual attacks (Al-Jabri, 2001)

- $\mathbf{h} = \boxed{\quad w \text{ (small)} \quad} \in \mathscr{C}^\perp$

- $\langle \mathbf{y}, \mathbf{h} \rangle = \langle \mathbf{c}, \mathbf{h} \rangle + \langle \mathbf{e}, \mathbf{h} \rangle = \langle \mathbf{e}, \mathbf{h} \rangle = \sum_{i=1}^{n} \mathbf{e}_i \, \mathbf{h}_i \quad \rightarrow$ Biased toward 0

Distinguisher ($\mathbf{y}$ random v.s $\mathbf{y} = \mathbf{c} + \mathbf{e}$)

- Compute all parity-checks of weight w

$$\mathscr{C}_w^\perp \triangleq \{\mathbf{h} \in \mathscr{C}^\perp \ : \ |\mathbf{h}| = w\}$$

- Compute **bias**

$$\mathbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{y}) \triangleq \frac{1}{|\mathscr{C}_w^\perp|} \sum_{\mathbf{h} \in \mathscr{C}_w^\perp} (-1)^{\langle \mathbf{y}, \mathbf{h} \rangle} \in [-1 \ , \ 1]$$

- Make decision:

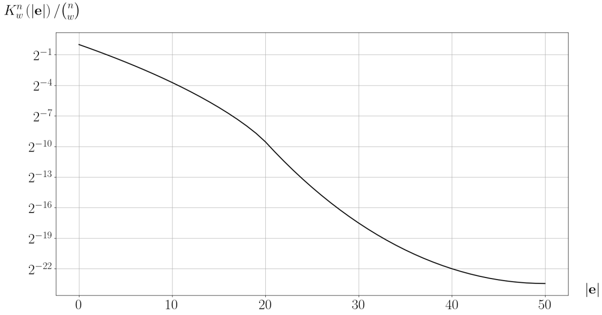
$\mathbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{y})$ is **big** enough $\rightarrow$ decide $\mathbf{y} = \mathbf{c} + \mathbf{e}$

Estimate of $\mathbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{y})$ $\quad (\mathbf{y} = \mathbf{c} + \mathbf{e},$ w.t $|\mathbf{e}|$ small $)$

Theorem [CDMT22]

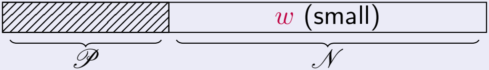
Under certain conditions:

$$\mathbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{y}) \approx \frac{K_w^{(n)}(|\mathbf{e}|)}{\binom{n}{w}} \qquad (K_w^{(n)} \text{ Krawtchouk polynomial})$$



$n = 100,$
$w = 10$

Idea of Dual Attacks 2.0 [CDMT, 2022]

- Split support in arbitrary complementary part $\mathscr{P}$ and $\mathscr{N}$ $\rightarrow$ Recover $\mathbf{e}_{\mathscr{P}}$?
- Compute $\mathbf{h} =$ 

$\in \mathscr{C}^{\perp}$

$$\langle \mathbf{y}, \mathbf{h} \rangle \;=\; \langle \mathbf{e}, \mathbf{h} \rangle \;=\; \langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}} \rangle + \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle$$

$$\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}} \rangle \;=\; \langle \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle \quad \rightarrow \quad \text{biased toward } 0$$

Algorithm : return $\mathbf{x}$ s.t $\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle$ most biased tower 0

- Compute set of parity-checks $\mathscr{C}_w^{\perp} \stackrel{\triangle}{=} \{\mathbf{h} \in \mathscr{C}^{\perp} \; : \; |\mathbf{h}_{\mathscr{N}}| = w\}$
- Compute **bias** for each $\mathbf{x}$

$$\textbf{bias}_{\mathscr{C}_w^{\perp}}(\mathbf{x}) \stackrel{\triangle}{=} \frac{1}{|\mathscr{C}_w^{\perp}|} \sum_{\mathbf{h} \in \mathscr{C}_w^{\perp}} (-1)^{\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle} \in [-1 \,,\, 1]$$

- Return $\mathbf{x}$ such that $\textbf{bias}_{\mathscr{C}_w^{\perp}}(\mathbf{x})$ maximum $\rightarrow$ Hope max given by $\mathbf{e}_{\mathscr{P}}$

Analysis of Dual Attack 2.0

Recall $\quad \textbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{x}) \triangleq \frac{1}{|\mathscr{C}_w^\perp|} \sum_{\mathbf{h} \in \mathscr{C}_w^\perp} (-1)^{\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle}$

Study probability that $\textbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{e}_{\mathscr{P}}) > \textbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{x})$ for all $\mathbf{x} \neq \mathbf{e}_{\mathscr{P}}$

bias for $\mathbf{e}_{\mathscr{P}}$: Theorem [CDMT22]

Under certain conditions:

$$\textbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{e}_{\mathscr{P}}) \approx \frac{K_w^{(|\mathscr{N}|)}(|\mathbf{e}_{\mathscr{N}}|)}{\binom{|\mathscr{N}|}{w}}$$

bias for others $\mathbf{x} \neq \mathbf{e}_{\mathscr{P}}$

Independence Assumption

$$\Downarrow$$

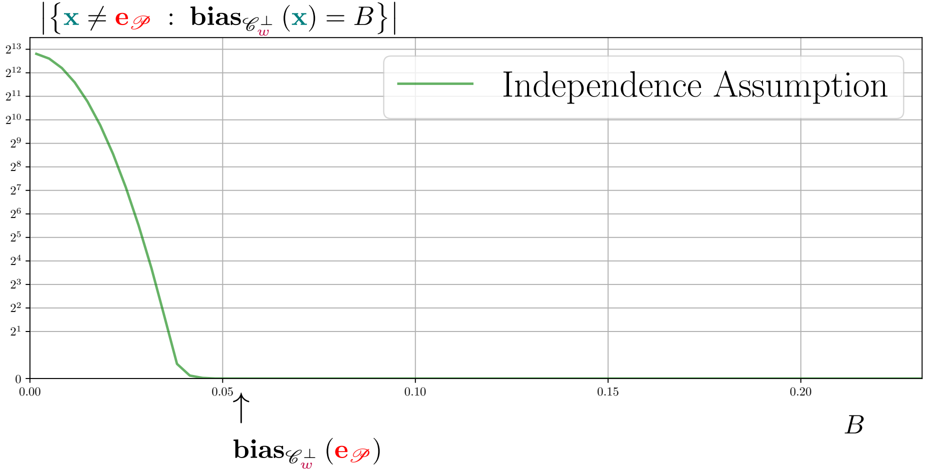
$$\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle \sim \text{Bernouilli}(1/2) \qquad \mathbf{h} \text{ sampled in } \mathscr{C}_w^\perp \text{ and } \mathbf{x} \neq \mathbf{e}_{\mathscr{P}}$$

$$\Downarrow$$

$$\textbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{x}) \approx \text{centered Normal}$$

Sum up in a plot!

Under Independence assumption:



Sum up in a plot!

Under Independence assumption:

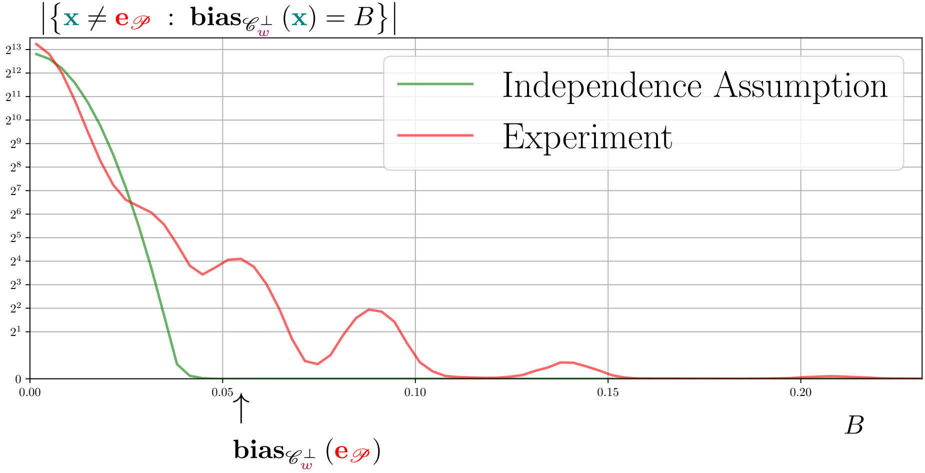


Table of Contents

A dual expression for $\mathbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{x})$

Theorem

$$\mathbf{bias}_{\mathscr{C}_w^\perp}(\mathbf{x}) \approx \sum_i N_i \; \frac{K_w(i)}{\binom{|\mathscr{N}|}{w}}$$

- N_i is number of word of $\mathscr{C}_{\mathbf{x}}$ at distance i of $\mathbf{e}_{\mathscr{N}}$
- $\mathscr{C}_{\mathbf{x}}$ $\triangleq \{\mathbf{c}_{\mathscr{N}} \;:\; \mathbf{c} \in \mathscr{C}$ and $\mathbf{c}_{\mathscr{P}} = \mathbf{x} + \mathbf{e}_{\mathscr{P}}\}$

Proof: Poisson formula

$\rightarrow$ Dominated by lowest term i s.t $N_i \neq 0$

Model for the N_i

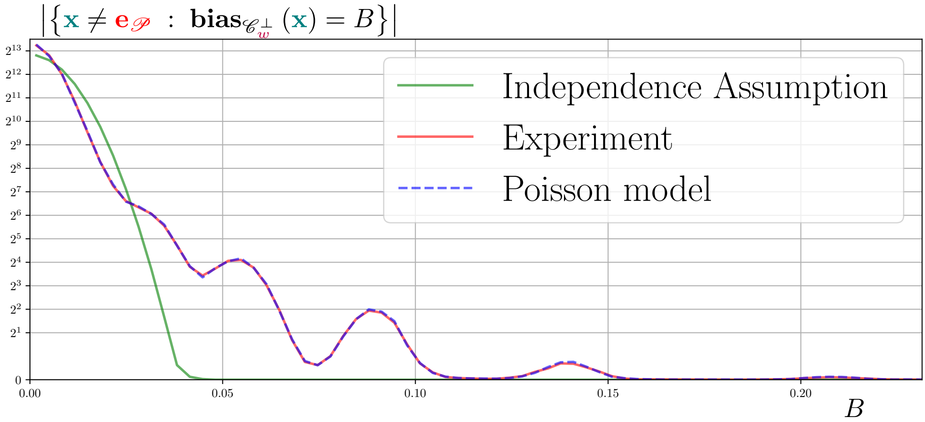
Poisson model

$$N_i \sim \mathrm{Poisson}\left(\, \mathbb{E}\left[N_i\right] \,\right)$$

$\rightarrow$ The expression of $\mathbb{E}\left[N_i\right]$ is known

Experimental Results

Under Poisson model:



Conclusion

- This model can be used to analyze dual attacks
- [CDMT22] with a tweak $\rightarrow$ originally claimed complexities!

  $\rightarrow$ **Dual attacks in Coding Theory work!**
- Can be adapted to Lattices

Thank you!