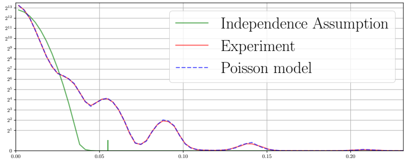
# Rigorous Foundations for Dual Attacks in Coding Theory

Charles Meyer-Hilfiger, Jean-Pierre Tillich

Journée C2 - 17/10/2023



# Dual attacks in codes and lattices

## Dual attacks solve

Decoding Problem (Codes) | Shortest Vector Problem (Lattices)

$\rightarrow$ Heart of security of cryptographic primitives

Lattices : Dual attacks impact Kyber (NIST standard)

# Dual attacks in codes and lattices

## Dual attacks solve

| Decoding Problem (Codes) | Shortest Vector Problem (Lattices) |
|---|---|

→ Heart of security of cryptographic primitives

Lattices : Dual attacks impact Kyber (NIST standard)

**Independence** assumptions to analyse dual attacks

⇓ (**Valid?**)

## Not so much

| Codes | Lattices |
|---|---|
| [CDMT22]<br>↓<br>Notice experimental differences | [DP23]<br>↓<br>Show the model cannot hold in some regimes |

# Goal of this talk

- 1) Why independence assumptions does not hold.
- 2) Give rigorous foundations for analyzing dual attacks.

# 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 $t$ (sparse)

- **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

# Dual attacks 1.0 (Statistical decoding [Al-Jabri, 2001])

- Compute all $\mathbf{h} \in \mathscr{C}_w^\perp \subset \mathscr{C}^\perp = \boxed{w \text{ (sparse)}}$

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

$$\mathbf{bias}_{\mathbf{h} \in \mathscr{C}_w^\perp} (\langle \mathbf{e}, \mathbf{h} \rangle) \triangleq \frac{\left| \left\{ \mathbf{h} \in \mathscr{C}_w^\perp \; : \; \langle \mathbf{e}, \mathbf{h} \rangle = 0 \right\} \right|}{|\mathscr{C}_w^\perp|} \, 2 - 1$$

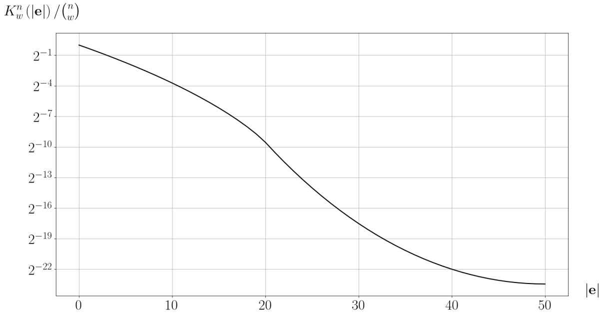
If $\left| \mathscr{C}_w^\perp \right| > \left( \frac{1}{\mathbf{bias}_{\mathbf{h} \in \mathscr{C}_w^\perp} (\langle \mathbf{e}, \mathbf{h} \rangle)} \right)^2 \Rightarrow$ Distinguish $\mathbf{y} = \mathbf{c} + \mathbf{e}$ from random $\mathbf{y} \in \mathbb{F}_2^n$

# Estimate of $\mathbf{bias}_{\mathbf{h} \in \mathscr{C}_w^\perp}(\langle \mathbf{e}, \mathbf{h} \rangle)$ ($\mathscr{C}$ is random)

**Theorem [CDMT22]**

$$\mathbf{bias}_{\mathbf{h} \in \mathscr{C}_w^\perp}(\langle \mathbf{e}, \mathbf{h} \rangle) \approx \mathbf{bias}_{\mathbf{h}' \in \mathcal{S}_w^n}(\langle \mathbf{e}, \mathbf{h}' \rangle) = \frac{K_w^{(n)}(|\mathbf{e}|)}{\binom{n}{w}} \quad (K_w^{(n)} \text{ Krawtchouk poly.})$$

Where $\mathscr{C}_w^\perp \subset \mathcal{S}_w^n \stackrel{\triangle}{=} \{\mathbf{h}' \in \mathbb{F}_2^n : |\mathbf{h}'| = w\}$



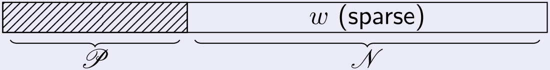

$n = 100,$
$w = 10$

Hold if: $\mathbb{E}\left[\left|\mathscr{C}_w^\perp\right|\right] > \left(\frac{1}{\mathbf{bias}_{\mathbf{h}' \in \mathcal{S}_w^n}(\langle \mathbf{e}, \mathbf{h}' \rangle)}\right)^2$

# Dual attacks 2.0 [CDMT, 2022]

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

- Compute $\mathbf{h} \in \mathscr{C}_w^{\perp} \subset \mathscr{C}^{\perp} =$




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

$$\Downarrow$$

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

- Find $\mathbf{x} \in \mathbb{F}_2^{|\mathscr{P}|}$ s.t $\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle$ is the most biased toward $0$

  $\rightarrow$ Hope maximum for $\mathbf{x} = \mathbf{e}_{\mathscr{P}}$

# Recovering $\mathbf{e}_{\mathscr{P}}$

If maximum $\mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle\right)$ given by $\mathbf{x} = \mathbf{e}_{\mathscr{P}}$

$$\Downarrow$$

Can recover $\mathbf{e}_{\mathscr{P}}$

- **1)** How big is $\mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{e}_{\mathscr{P}},\mathbf{h}_{\mathscr{P}}\rangle\right)$?
- **2)** How big is $\mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle\right)$ for all other $\mathbf{x} \neq \mathbf{e}_{\mathscr{P}}$'s?

# 1) Estimate of $\mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{e}_{\mathscr{P}},\mathbf{h}_{\mathscr{P}}\rangle\right)$

**Theorem [CDMT22]**

$$\mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{e}_{\mathscr{P}},\mathbf{h}_{\mathscr{P}}\rangle\right) \approx \frac{K_w^{(|\mathscr{N}|)}\left(|\mathbf{e}_{\mathscr{N}}|\right)}{\binom{|\mathscr{N}|}{w}}$$

$$\mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{e}_{\mathscr{P}},\mathbf{h}_{\mathscr{P}}\rangle\right) = \mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle\right)$$

$$\approx \mathbf{bias}_{\mathbf{h}'_{\mathscr{N}}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{e}_{\mathscr{N}},\mathbf{h}'_{\mathscr{N}}\rangle\right)$$

$$= \frac{K_w^{(|\mathscr{N}|)}\left(|\mathbf{e}_{\mathscr{N}}|\right)}{\binom{|\mathscr{N}|}{w}}$$

$\rightarrow$ Hold if: $\mathbb{E}\left[\left|\mathscr{C}_w^\perp\right|\right] > \left(\frac{1}{\mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle\right)}\right)^2$

# 2) Estimate of $\mathrm{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle\right)$, $\quad \mathbf{x} \neq \mathbf{e}_{\mathscr{P}}$

$$\begin{aligned}\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle &= \langle \mathbf{e},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle \\ &= \langle \mathbf{e}_{\mathscr{P}},\mathbf{h}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle + \langle \mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle \\ &= \langle \mathbf{e}_{\mathscr{P}}+\mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle + \langle \mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle\end{aligned}$$

**Independence Assumption**

Assume $\langle \mathbf{e}_{\mathscr{P}}+\mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle$ and $\langle \mathbf{e}_{\mathscr{N}},\mathbf{h}_{\mathscr{N}}\rangle$ independent when $\mathbf{h}$ uniform in $\mathscr{C}_w^\perp$

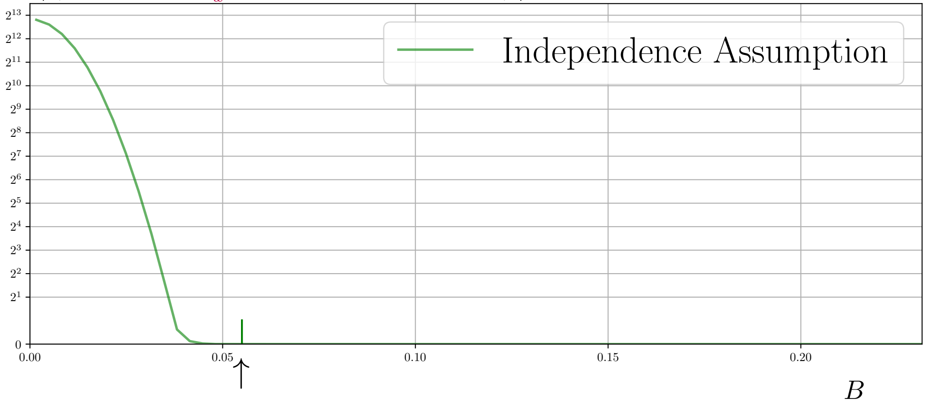
$$\Downarrow$$

$$\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle \sim \mathrm{Bern}\left(\frac{1}{2}\right), \qquad \mathbf{x} \neq \mathbf{e}_{\mathscr{P}}$$

# Sum up in a plot!

Under Independence assumption:

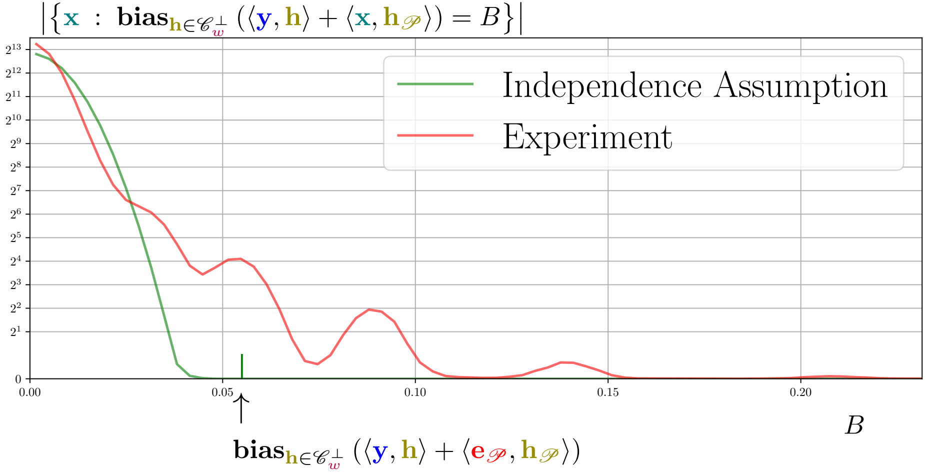
$$\left|\left\{\mathbf{x} \;:\; \mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{x},\mathbf{h}_{\mathscr{P}}\rangle\right) = B\right\}\right|$$




$$\mathbf{bias}_{\mathbf{h}\in\mathscr{C}_w^\perp}\left(\langle \mathbf{y},\mathbf{h}\rangle + \langle \mathbf{e}_{\mathscr{P}},\mathbf{h}_{\mathscr{P}}\rangle\right)$$

# Sum up in a plot!

Under Independence assumption:

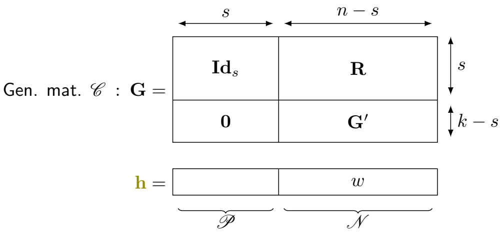


# Table of Contents

# Why independence assumption is false

## Indepence assumption

$$\Rightarrow \langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle \sim \mathrm{Bern}(1/2)$$




## Linear dependency $\mathbf{h}_{\mathscr{P}}$ and $\mathbf{h}_{\mathscr{N}}$

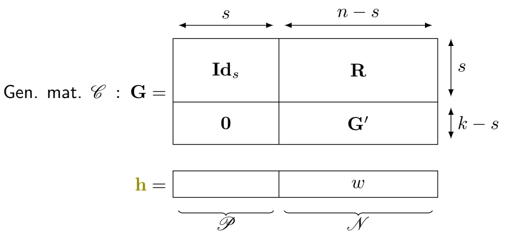
$$\mathbf{h}_{\mathscr{P}}^{\top} = \mathbf{R}\, \mathbf{h}_{\mathscr{N}}^{\top}$$

$$\mathbf{h} \in \mathscr{C}^{\perp}$$
$$\Downarrow$$
$$\mathbf{G}\, \mathbf{h}^{\top} = \mathbf{0}$$
$$\Downarrow$$
$$\mathbf{h}_{\mathscr{P}}^{\top} + \mathbf{R}\mathbf{h}_{\mathscr{N}}^{\top} = \mathbf{0} \text{ and } \mathbf{G}'\mathbf{h}_{\mathscr{N}}^{\top} = \mathbf{0}$$

$$\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle = \langle (\mathbf{x} + \mathbf{e}_{\mathscr{P}})\, \mathbf{R} + \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle$$

$\rightarrow$ Assumption cannot hold!

# About $\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle$




$$\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle = \langle (\mathbf{x} + \mathbf{e}_{\mathscr{P}})\,\mathbf{R} + \mathbf{e}_{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle$$

## Definition

$\mathscr{C}^{\mathscr{N}}$ is $[n-s, k-s]$ code of gen. mat. $\mathbf{G}'$

$$\rightarrow \mathbf{h}_{\mathscr{N}} \in \left(\mathscr{C}^{\mathscr{N}}\right)^{\perp}$$

$$\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle = \langle (\mathbf{x} + \mathbf{e}_{\mathscr{P}})\,\mathbf{R} + \mathbf{e}_{\mathscr{N}} + \mathbf{c}^{\mathscr{N}}, \mathbf{h}_{\mathscr{N}} \rangle \qquad \forall \mathbf{c}^{\mathscr{N}} \in \mathscr{C}^{\mathscr{N}}$$

# An expression for $\mathbf{bias}\left(\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle\right)$

**Theorem of bias of error terms in RLPN**

$$\mathbf{bias}_{\mathbf{h} \in \mathscr{C}_w^{\perp}}\left(\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle\right) = \sum_{i=0}^{n-s} N_i \; \frac{K_w^{(n-s)}(i)}{\binom{n-s}{w}}$$

where $N_i \triangleq \left| (\mathbf{x} + \mathbf{e}_{\mathscr{P}}) \mathbf{R} + \mathbf{e}_{\mathscr{N}} + \mathscr{C}^{\mathscr{N}} \bigcap \mathcal{S}_i^{n-s} \right|$ is weight enumerator

**Proof:** Poisson formula

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

$$\rightarrow \mathbf{bias}_{\mathbf{h} \in \mathscr{C}_w^{\perp}}\left(\langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{e}_{\mathscr{P}}, \mathbf{h}_{\mathscr{P}} \rangle\right) \approx \frac{1}{\binom{n-s}{w}} K_w^{(n-s)}\left(|\mathbf{e}_{\mathscr{N}}|\right)$$

# Table of Contents

# Model for the bias

$\rightarrow \mathscr{C}$ is random $[n, k]$ linear code,

$$\mathbf{bias}_{\mathbf{h} \in \mathscr{C}_w^\perp} \left( \langle \mathbf{y}, \mathbf{h} \rangle + \langle \mathbf{x}, \mathbf{h}_{\mathscr{P}} \rangle \right) = \sum_{i=0}^{n-s} N_i \; \frac{K_w^{(n-s)}(i)}{\binom{n-s}{w}}$$

where $N_i \stackrel{\triangle}{=} \left| (\mathbf{x} + \mathbf{e}_{\mathscr{P}}) \, \mathbf{R} + \mathbf{e}_{\mathscr{N}} + \mathscr{C}^{\mathscr{N}} \bigcap \mathcal{S}_i^{n-s} \right|$ is weight enumerator

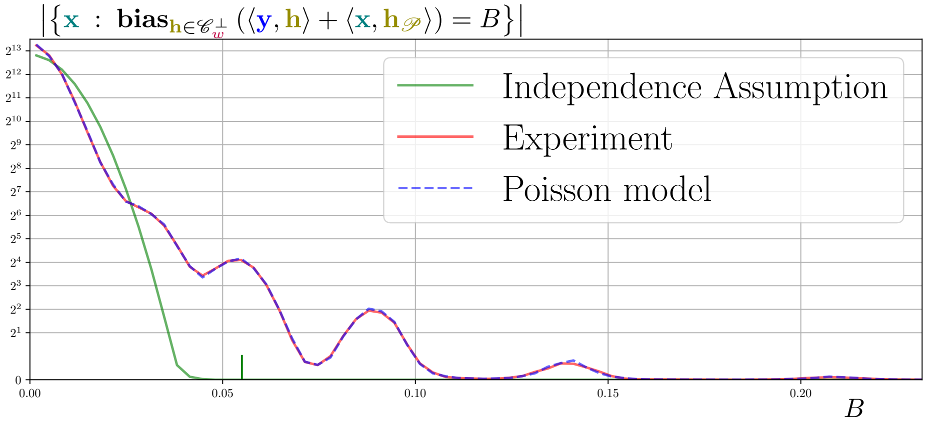
$$\Downarrow$$

## Model

$$N_i \sim \text{Poisson} \left( \frac{\binom{n-s}{i}}{2^{n-k}} \right)$$

# Experimental Results

Under Poisson model:



# Conclusion

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

Thank you!