A Generic Framework for Side-Channel Attacks against LWE-based Cryptosystems

Julius Hermelink[1] Silvan Streit[2, 3] Erik Mårtensson [4, 5] Richard Petri[1]

[1]Max Planck Institute for Security and Privacy, Bochum, Germany,

[2]Fraunhofer AISEC, Garching, Germany,

[3]Technical University of Munich (TUM), Munich, Germany

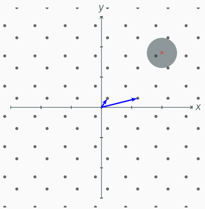
[4]Lund University, Lund, Sweden

[5]Advenica AB, Malmö, Sweden

How to deal with side information in lattice-based schemes?

Primal attack:

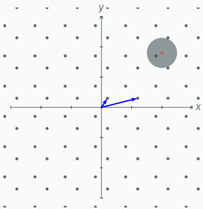
E.g., [DDGR20; DGHK23; MN23]



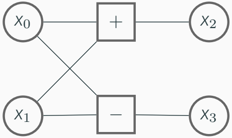
Side Information in Lattice-Based Schemes

How to deal with side information in lattice-based schemes?

Primal attack:
E.g., [DDGR20; DGHK23; MN23]



Soft-analytic [VGS14]:
E.g., [PPM17; HPP21; BAE+24]



Attacks: often noisy information on Hamming weights.

Context: Inequalities in ML-KEM's secret key arising from information on the noise term.

Solving $\langle \mathbf{v}, \mathbf{x} \rangle \leq b$ for $\mathbf{x}$.

Context: Inequalities in ML-KEM's secret key arising from information on the noise term.

Solving $\langle \mathbf{v}, \mathbf{x} \rangle \leq b$ for $\mathbf{x}$.

BP Solver [HPP21]

Update probabilities $x_j = x_j'$ using partial sum $\sum_{i \neq j} v_i x_i$:

$$P(x_j = x_j') = \sum_a \delta_{a + v_j x_j' \leq b} \cdot P(\sum_{i \neq j} v_i x_i = a)$$

Belief Propagation and Greedy Solvers

Context: Inequalities in ML-KEM's secret key arising from information on the noise term.

Solving $\langle \mathbf{v}, \mathbf{x} \rangle \leq b$ for $\mathbf{x}$.

BP Solver [HPP21]

Update probabilities $x_j = x'_j$ using partial sum $\sum_{i \neq j} v_i x_i$:

$$P(x_j = x'_j) = \sum_a \delta_{a+v_j x'_j \leq b} \cdot \; P(\sum_{i \neq j} v_i x_i = a)$$

Greedy Solver [RPJ+24]

Update guess $\mathbf{x}'$ by $x'_j + c$ using scores:

$$s_j(c) = \max(\sum_i v_i x_i + v_j c - b, 0)$$

Belief Propagation and Greedy Solvers

Context: Inequalities in ML-KEM's secret key arising from information on the noise term.

Solving $\langle \mathbf{v}, \mathbf{x} \rangle \leq b$ for $\mathbf{x}$.

BP Solver [HPP21]

Update probabilities $x_j = x'_j$ using partial sum $\sum_{i \neq j} v_i x_i$:

$$P(x_j = x'_j) = \sum_a \delta_{a + v_j x'_j \leq b} \cdot P(\sum_{i \neq j} v_i x_i = a)$$

Greedy Solver [RPJ+24]

Update guess $\mathbf{x}'$ by $x'_j + c$ using scores:

$$s_j(c) = \max(\sum_i v_i x_i + v_j c - b, 0)$$

Attack actually learns HW of noise term.

Belief Propagation and Greedy Solvers

Context: Inequalities in ML-KEM's secret key arising from information on the noise term.

Solving $\langle \mathbf{v}, \mathbf{x} \rangle \leq b$ for $\mathbf{x}$.

BP Solver [HPP21]

Update probabilities $x_j = x'_j$ using partial sum $\sum_{i \neq j} v_i x_i$:

$$P(x_j = x'_j) = \sum_a \delta_{a + v_j x'_j \leq b} \cdot P(\sum_{i \neq j} v_i x_i = a)$$

Greedy Solver [RPJ+24]

Update guess $\mathbf{x}'$ by $x'_j + c$ using scores:

$$s_j(c) = \max(\sum_i v_i x_i + v_j c - b, 0)$$

Attack actually learns HW of noise term.

Relation? Greedy requires less information? No information loss?

Distribution Hints

Various proposals to define and deal with side information.

Previous hint definitions [DDGR20; DGHK23]:

For known $\mathbf{v}, l, k$:

- $\langle \mathbf{v}, \mathbf{x} \rangle = l$
- $\langle \mathbf{v}, \mathbf{x} \rangle = l \mod k$
- $\langle \mathbf{v}, \mathbf{x} \rangle = l + \mathcal{N}$
- $\langle \mathbf{v}, \mathbf{x} \rangle \leq l$
- short $\mathbf{v} \in \Lambda$

Distribution Hints

Various proposals to define and deal with side information.

Previous hint definitions [DDGR20; DGHK23]:
For known $\mathbf{v}, l, k$:

- $\langle \mathbf{v}, \mathbf{x} \rangle = l$
- $\langle \mathbf{v}, \mathbf{x} \rangle = l \mod k$
- $\langle \mathbf{v}, \mathbf{x} \rangle = l + \mathcal{N}$
- $\langle \mathbf{v}, \mathbf{x} \rangle \leq l$
- ~~short $\mathbf{v} \in \Lambda$~~

$\longrightarrow$

Distribution hints:
For known $\mathbf{v}$, distribution $\mathcal{D}$:

$$\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$$

Distribution Hints

Various proposals to define and deal with side information.

Previous hint definitions [DDGR20; DGHK23]:

For known $\mathbf{v}, l, k$:

- $\langle \mathbf{v}, \mathbf{x} \rangle = l$
- $\langle \mathbf{v}, \mathbf{x} \rangle = l \mod k$
- $\langle \mathbf{v}, \mathbf{x} \rangle = l + \mathcal{N}$
- $\langle \mathbf{v}, \mathbf{x} \rangle \leq l$
- ~~short~~ $\cancel{\mathbf{v} \in \Lambda}$

$\longrightarrow$

Distribution hints:

For known $\mathbf{v}$, distribution $\mathcal{D}$:

$$\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$$

Information from [RPJ+24] without loss!

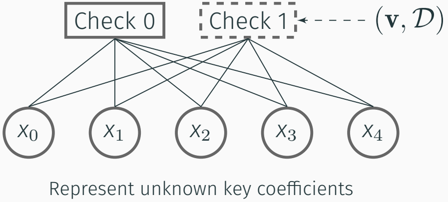
$$\mathrm{HW}(\langle \mathbf{v}, \mathbf{x} \rangle) \sim \mathcal{D}$$

Solving Distribution Hints

Two different solvers: BP and Greedy

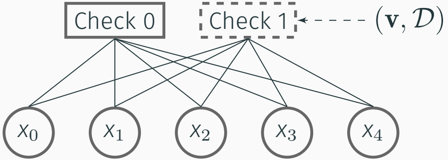
Solving Distribution Hints

Two different solvers: BP and Greedy; hint: $\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$



Solving Distribution Hints

Two different solvers: **BP and Greedy**; hint: $\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$

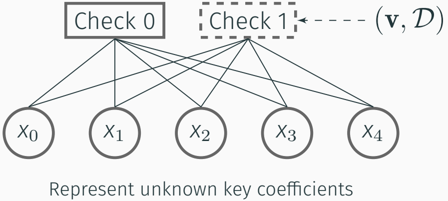


Represent unknown key coefficients

Update for $x_j = x_j'$:

$$P(x_j = x_j') = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P(\sum_{i \neq j} v_i x_i = a - v_j x_j')$$

Two different solvers: **BP and Greedy**; hint: $\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$

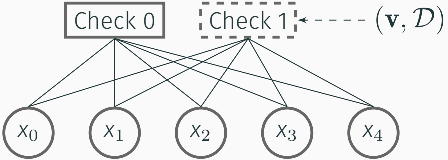


Update for $x_j = x_j'$:

$$P(x_j = x_j') = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P\Big(\sum_{i \neq j} v_i x_i = a - v_j x_j'\Big)$$

Solving Distribution Hints

Two different solvers: BP and Greedy; hint: $\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$

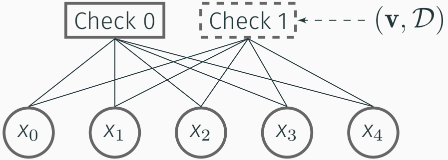


Represent unknown key coefficients

Update for $x_j = x_j'$:

$$P(x_j = x_j') = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P\Big(\sum_{i \neq j} v_i x_i = a - v_j x_j'\Big)$$

Two different solvers: BP and Greedy; hint: $\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$



Represent unknown key coefficients

Update for $x_j = x_j'$:

$$P(x_j = x_j') = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P(\sum_{i \neq j} v_i x_i = a - v_j x_j')$$

Greedy: $\mathbf{x}'$ and change $x_j + c$.

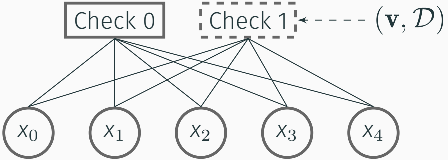
Change scores for coefficients j:

$$s_j(c) = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) |\langle \mathbf{v}, \mathbf{x}' \rangle + v_j c - a|,$$

and perform k best updates on guess $\mathbf{x}'$.

Solving Distribution Hints

Two different solvers: BP and Greedy; hint: $\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$



Represent unknown key coefficients

Update for $x_j = x_j'$:

$$P(x_j = x_j') = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P(\sum_{i \neq j} v_i x_i = a - v_j x_j')$$

Greedy: $\mathbf{x}'$ and change $x_j + c$.

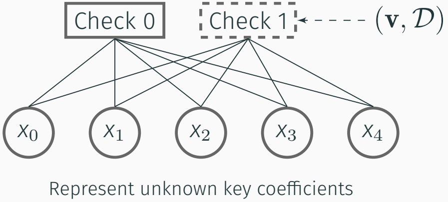
Change scores for coefficients j:

$$s_j(c) = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) |\langle \mathbf{v}, \mathbf{x}' \rangle + v_j c - a|,$$

and perform k best updates on guess $\mathbf{x}'$.

Solving Distribution Hints

Two different solvers: BP and Greedy; hint: $\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$



Update for $x_j = x_j'$:

$$P(x_j = x_j') = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P(\sum_{i \neq j} v_i x_i = a - v_j x_j')$$

Greedy: $\mathbf{x}'$ and change $x_j + c$.

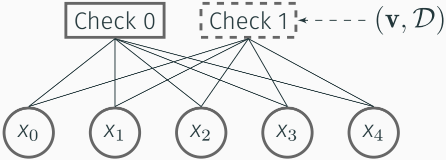
Change scores for coefficients j:

$$s_j(c) = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) |\langle \mathbf{v}, \mathbf{x}' \rangle + v_j c - a|,$$

and perform k best updates on guess $\mathbf{x}'$.

Solving Distribution Hints

Two different solvers: BP and Greedy; hint: $\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$



Represent unknown key coefficients

Update for $x_j = x_j'$:

$$P(x_j = x_j') = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P\Big(\sum_{i \neq j} v_i x_i = a - v_j x_j'\Big)$$

Greedy: $\mathbf{x}'$ and change $x_j + c$.

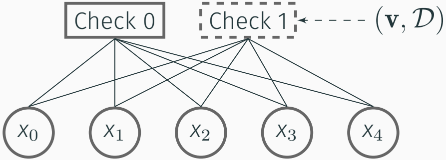
Change scores for coefficients j:

$$s_j(c) = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) \left| \langle \mathbf{v}, \mathbf{x}' \rangle + v_j c - a \right|,$$

and perform k best updates on guess $\mathbf{x}'$.

Solving Distribution Hints

Two different solvers: BP and Greedy; hint: $\langle \mathbf{v}, \mathbf{x} \rangle \sim \mathcal{D}$



Represent unknown key coefficients

Update for $x_j = x'_j$:

$$P(x_j = x'_j) = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P\Big(\sum_{i \neq j} v_i x_i = a - v_j x'_j\Big)$$

Greedy: $\mathbf{x}'$ and change $x_j + c$.

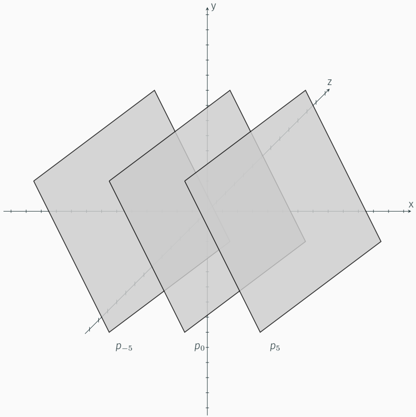
Change scores for coefficients j:

$$s_j(c) = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) |\langle \mathbf{v}, \mathbf{x}' \rangle + v_j c - a|,$$

and perform k best updates on guess $\mathbf{x}'$.

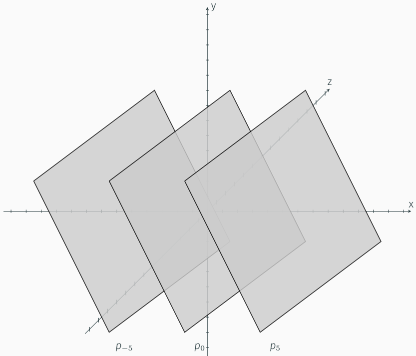
$P(\sum_{i \neq j} v_i x_i = a - v_j x'_j) \to |\mathbf{v}^\top \mathbf{x}' + v_j c - a|$

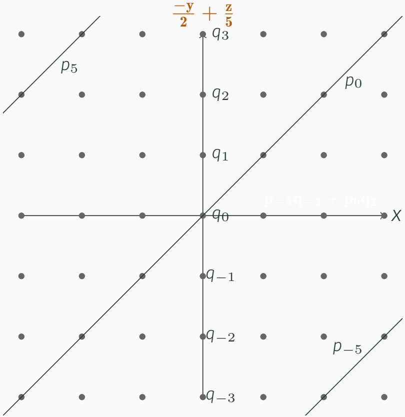
Solving Process



$$-x + \frac{\mathbf{-y}}{\mathbf{2}} + \frac{\mathbf{z}}{\mathbf{5}} \sim \{-5 : p_{-5}, 0 : p_0, 5 : p_5\}$$

Solving Process

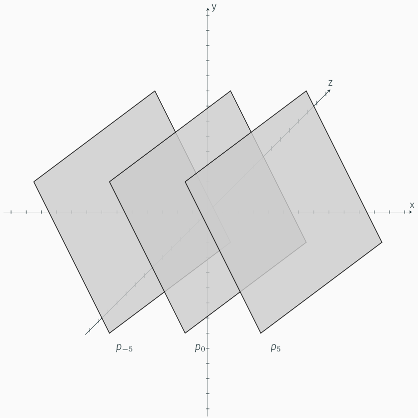




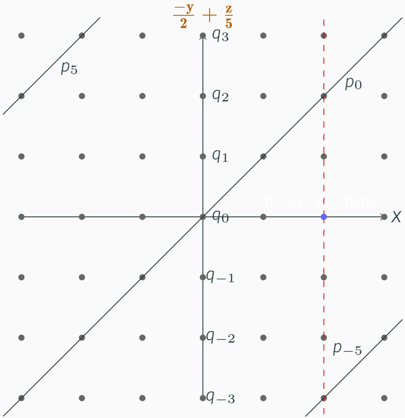
$$-x + \frac{-\mathbf{y}}{\mathbf{2}} + \frac{\mathbf{z}}{\mathbf{5}} \sim \{-5 : p_{-5}, 0 : p_0, 5 : p_5\}$$

Update for x

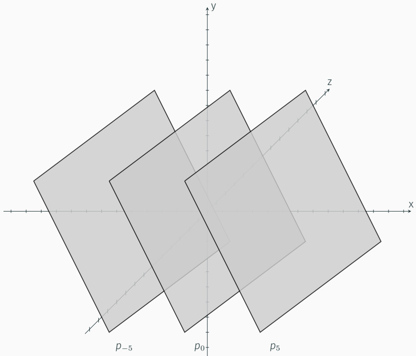
Solving Process



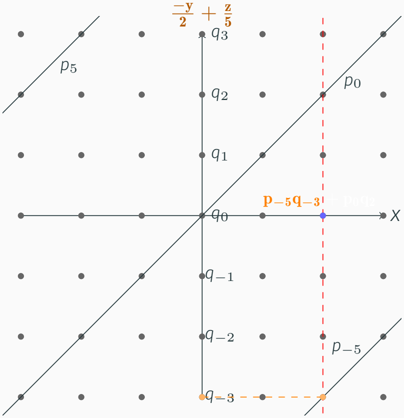
$$-x + \frac{-y}{2} + \frac{z}{5} \sim \{-5 : p_{-5}, 0 : p_0, 5 : p_5\}$$



Update for x

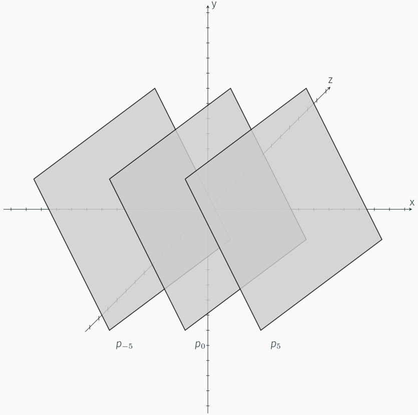


$$-x + \frac{-\mathbf{y}}{\mathbf{2}} + \frac{\mathbf{z}}{\mathbf{5}} \sim \{-5 : p_{-5}, 0 : p_0, 5 : p_5\}$$

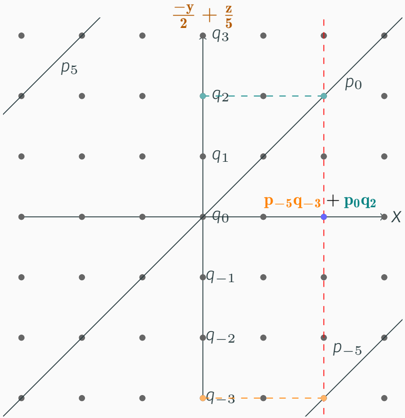


Update for x

Solving Process



$-x + \frac{-y}{2} + \frac{z}{5} \sim \{-5 : p_{-5}, 0 : p_0, 5 : p_5\}$



Update for x

Comparison of Solvers

Greedy may be seen as “collapsed” BP.

$$(\{-1 : 0.2, 0 : 0.1, 1 : 0.7\}, \{-1 : 0.3, 0 : 0.7\}), \ldots,) \quad \rightarrow \qquad (1, 0, \ldots,)$$

Comparison of Solvers

Greedy may be seen as "collapsed" BP.

$$(\{-1:0.2, 0:0.1, 1:0.7\}, \{-1:0.3, 0:0.7\}), \ldots,) \quad \rightarrow \quad (1, 0, \ldots,)$$

update probabilities for values of coefficients $\rightarrow$ scores for changes of coefficients

Comparison of Solvers

Greedy may be seen as “collapsed” BP.

$$(\{-1:0.2, 0:0.1, 1:0.7\}, \{-1:0.3, 0:0.7\}), \ldots,) \quad \to \quad (1, 0, \ldots,)$$

update probabilities for values of coefficients $\to$ scores for changes of coefficients

$$P(\textstyle\sum_{i \neq j} v_i x_i = a - v_j x_j') \quad \to \quad |\mathbf{v}^\top \mathbf{x}' + v_j c - a|$$

Comparison of Solvers

Greedy may be seen as “collapsed” BP.

$$(\{-1:0.2, 0:0.1, 1:0.7\}, \{-1:0.3, 0:0.7\}), \ldots,) \quad \rightarrow \quad (1, 0, \ldots,)$$

update probabilities for values of coefficients $\rightarrow$ scores for changes of coefficients

$$P(\textstyle\sum_{i \neq j} v_i x_i = a - v_j x_j') \quad \rightarrow \quad |\mathbf{v}^\top \mathbf{x}' + v_j c - a|$$

Loses information but gains performance.

Relation to Previous Solvers

Several previous solvers are (almost) special cases of ours.

Some instantiations give previous solvers:

- Inequalities (BP): [HPP21].
- Inequalities (GR): close to [RPJ+24].
- Targeting ML-DSA: [BAE+24] with different computation (FFT).

Relation to Previous Solvers

Several previous solvers are (almost) special cases of ours.

Some instantiations give previous solvers:

- Inequalities (BP): [HPP21].
- Inequalities (GR): close to [RPJ+24].
- Targeting ML-DSA: [BAE+24] with different computation (FFT).

Explains conceptual relations;

Relation to Previous Solvers

Several previous solvers are (almost) special cases of ours.

Some instantiations give previous solvers:

- Inequalities (BP): [HPP21].
- Inequalities (GR): close to [RPJ+24].
- Targeting ML-DSA: [BAE+24] with different computation (FFT).

Additionally:

- Improves attack of [RPJ+24].
- Covers most hints of [DDGR20].
- Applies to information on linear intermediates.
- Combined with lattice reduction by adapting [HMS+23].

Explains conceptual relations;

Relation to Previous Solvers

Several previous solvers are (almost) special cases of ours.

Some instantiations give previous solvers:

- Inequalities (BP): [HPP21].
- Inequalities (GR): close to [RPJ+24].
- Targeting ML-DSA: [BAE+24] with different computation (FFT).

Additionally:

- Improves attack of [RPJ+24].
- Covers most hints of [DDGR20].
- Applies to information on linear intermediates.
- Combined with lattice reduction by adapting [HMS+23].

Explains conceptual relations; used for second-order attacks [HNP25].

Conclusion

Our framework:

- Generic and efficient.
- Generalizes previous solvers.
- Explains relation greedy $\leftrightarrow$ BP.
- Complements lattice-based frameworks.
- Also applies to other types of schemes.

Open source:

Easy to use!

```
bp = PyBP(vs, distributions)
greedy = PyGreedy(vs, distributions)
greedy.set_nthreads(4)
bp.set_nthreads(4)

greedy.solve(k)
guess = greedy.get_guess()
bp.propagate()
dists = bp.get_results()
```

Thank you for your attention!

References (1)

[BAE+24] Olivier Bronchain, Melissa Azouaoui, Mohamed ElGhamrawy, Joost Renes, and Tobias Schneider. "Exploiting Small-Norm Polynomial Multiplication with Physical Attacks Application to CRYSTALS-Dilithium". In: *IACR TCHES* 2024.2 (2024), pp. 359–383.

[DDGR20] Dana Dachman-Soled, Léo Ducas, Huijing Gong, and Mélissa Rossi. "LWE with Side Information: Attacks and Concrete Security Estimation". In: *CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. LNCS. Springer, Cham, Aug. 2020, pp. 329–358.

[DGHK23] Dana Dachman-Soled, Huijing Gong, Tom Hanson, and Hunter Kippen. "Revisiting Security Estimation for LWE with Hints from a Geometric Perspective". In: *CRYPTO 2023, Part V*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14085. LNCS. Springer, Cham, Aug. 2023, pp. 748–781.

[HMS+23] Julius Hermelink, Erik Mårtensson, Simona Samardjiska, Peter Pessl, and Gabi Dreo Rodosek. "Belief Propagation Meets Lattice Reduction: Security Estimates for Error-Tolerant Key Recovery from Decryption Errors". In: *IACR TCHES* 2023.4 (2023), pp. 287–317.

[HNP25] Julius Hermelink, Kai-Chun Ning, and Richard Petri. *Finding and Protecting the Weakest Link: On Side-Channel Attacks on Masked ML-DSA*. Cryptology ePrint Archive, Report 2025/276. 2025. URL: `https://eprint.iacr.org/2025/276`.

[HPP21] Julius Hermelink, Peter Pessl, and Thomas Pöppelmann. "Fault-Enabled Chosen-Ciphertext Attacks on Kyber". In: *INDOCRYPT 2021*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. LNCS. Springer, Cham, Dec. 2021, pp. 311–334.

References (2)

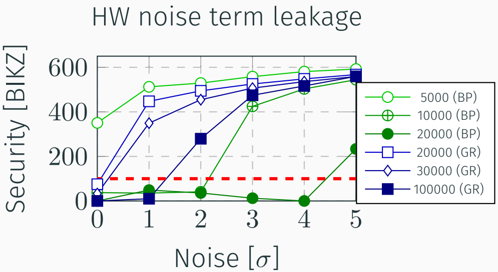
[MN23] Alexander May and Julian Nowakowski. “Too Many Hints - When LLL Breaks LWE”. In: *ASIACRYPT 2023, Part IV*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14441. LNCS. Springer, Singapore, Dec. 2023, pp. 106–137.

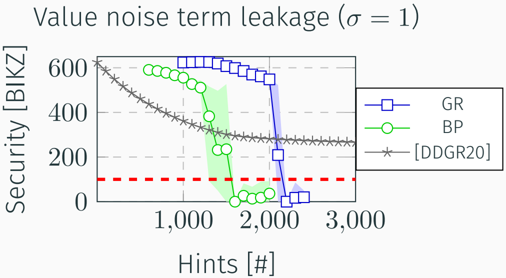
[PPM17] Robert Primas, Peter Pessl, and Stefan Mangard. “Single-Trace Side-Channel Attacks on Masked Lattice-Based Encryption”. In: *CHES 2017*. Ed. by Wieland Fischer and Naofumi Homma. Vol. 10529. LNCS. Springer, Cham, Sept. 2017, pp. 513–533.

[RPJ+24] Prasanna Ravi, Thales Paiva, Dirmanto Jap, Jan-Pieter D’Anvers, and Shivam Bhasin. “Defeating Low-Cost Countermeasures against Side-Channel Attacks in Lattice-based Encryption A Case Study on Crystals-Kyber”. In: *IACR TCHES* 2024.2 (2024), pp. 795–818.

[VGS14] Nicolas Veyrat-Charvillon, Benoît Gérard, and François-Xavier Standaert. “Soft Analytical Side-Channel Attacks”. In: *ASIACRYPT 2014, Part I*. Ed. by Palash Sarkar and Tetsu Iwata. Vol. 8873. LNCS. Springer, Berlin, Heidelberg, Dec. 2014, pp. 282–296.

Results for leakage on ML-KEM's noise term





Follow-up work: Targeting $\mathbf{y}$ in masked ML-DSA using our solver [HNP25].