Side-Channel Analysis of Post-Quantum Schemes

Julius Hermelink – Postdoc

July 8, 2025

Max Planck Institute for Security and Privacy

Who am I?

Julius Hermelink

Short CV:

- Postdoc at MPI-SP in Bochum.
- PhD from UniBw in Munich in 2024.
- Master's in Mathematics from LMU in 2020.

Research interests:

- Implementation attacks on post-quantum schemes.
- Soft-analytic side-channel attacks.
- Cryptanalysis (under side information).
- Information theory.
- How (not) to use formal methods for side-channel security.

The Quantum Threat

Quantum computers threaten currently used asymmetric cryptography.

We have to assume that:

- Large-scale quantum computer break commonly used asymmetric schemes.
- Adversaries: harvest now, decrypt later.

IBM Research, https://www.flickr.com/photos/ibm_research_zurich/51248690716/, unmodified, license: CC BY 2.0

The Quantum Threat

Quantum computers threaten currently used asymmetric cryptography.

We have to assume that:

- Large-scale quantum computer break commonly used asymmetric schemes.
- Adversaries: harvest now, decrypt later.

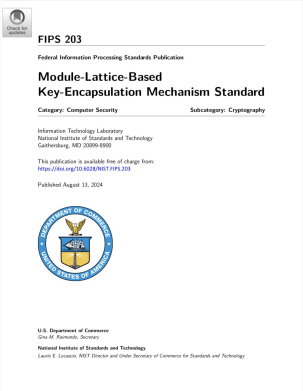
Therefore, we need:

- Post-quantum asymmetric cryptography.
- Most pressingly key exchanges.

IBM Research, https://www.flickr.com/photos/ibm_research_zurich/51248690716/, unmodified, license: CC BY 2.0

The NIST Standardization Process

NIST is in the process of standardizing post-quantum cryptography.



FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security — Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

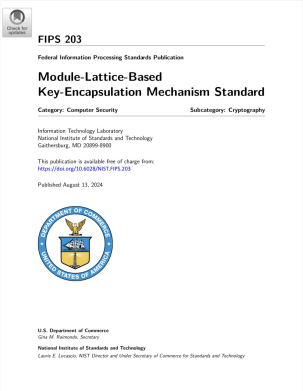
NIST started a standardization process in 2016.

- Five candidates already selected.
- Three are lattice-based.
- ML-KEM and ML-DSA standardized.

NIST FIPS 203, `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf`, accessed March 31, 2025.

The NIST Standardization Process

NIST is in the process of standardizing post-quantum cryptography.



FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security — Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST started a standardization process in 2016.

- Five candidates already selected.
- Three are lattice-based.
- ML-KEM and ML-DSA standardized.

ML-KEM used in Signal, Chrome, iMessage, ...

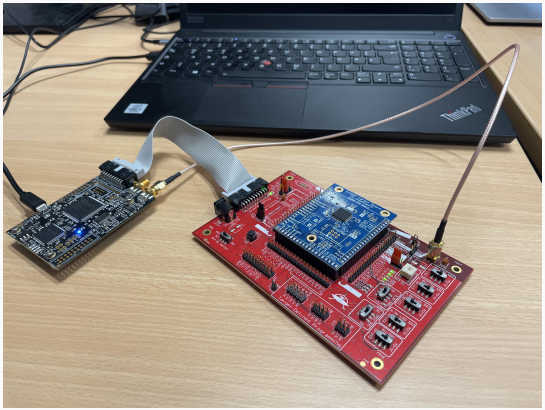
NIST FIPS 203, `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf`, accessed March 31, 2025.

Side-Channel Attacks

Devices may be vulnerable to side-channel and fault attacks.

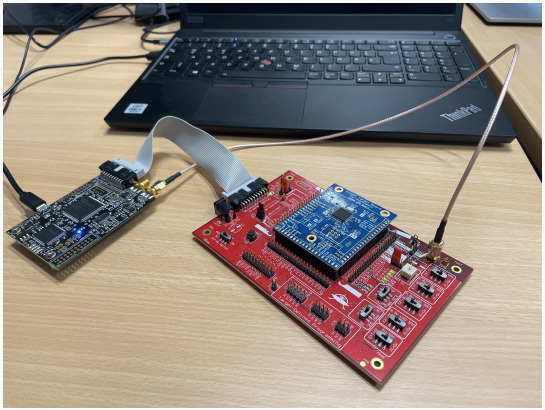
Side-Channel Attacks

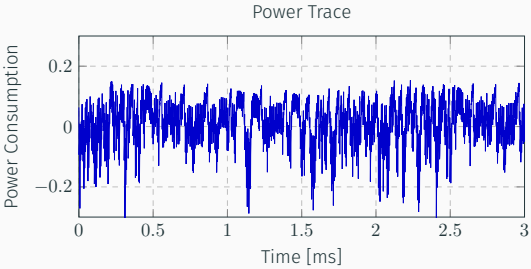
Devices may be vulnerable to side-channel and fault attacks.



Side-Channel Attacks

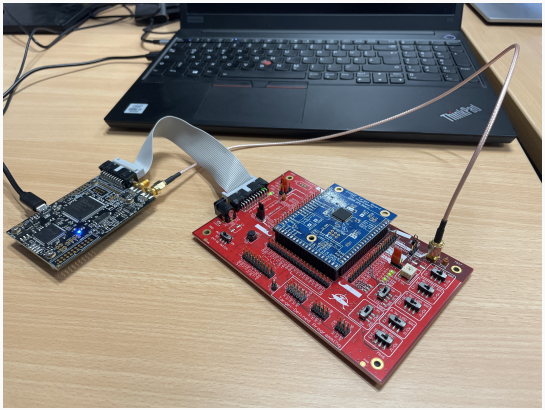
Devices may be vulnerable to side-channel and fault attacks.

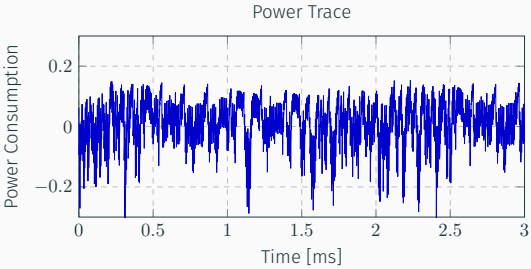




Side-Channel Attacks

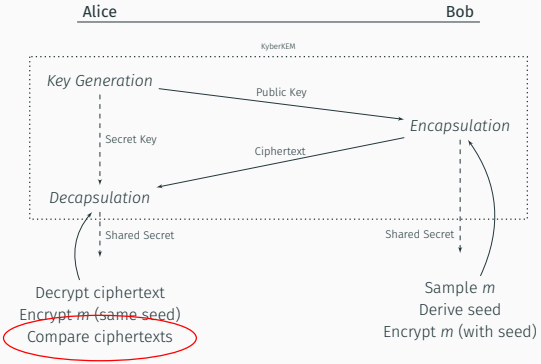
Devices may be vulnerable to side-channel and fault attacks.



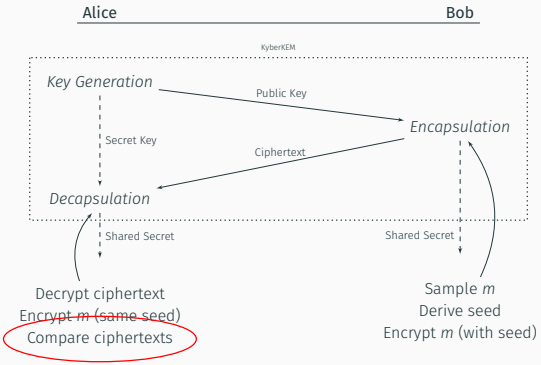


Lattice-based schemes/post-quantum cryptography comes with different challenges.

New Standards, New Challenges



New Standards, New Challenges



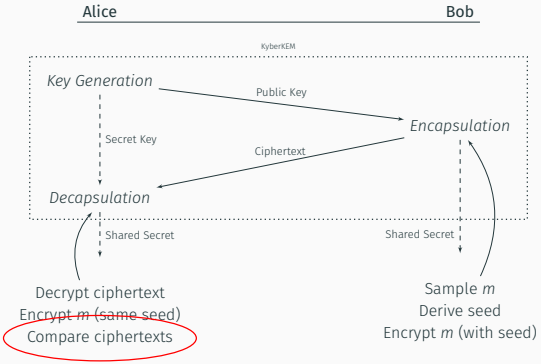
In ML-KEM:

- Comparison $\mathtt{ct}' == \mathtt{ct}$.
- Comparison is sensitive operation.

Adversary observes comparison:

- Enables chosen-ciphertext attack.
- Gives inequalities in the secret key.
- Solving using our prior work.

New Standards, New Challenges



In ML-KEM:

- Comparison $\mathtt{ct}' == \mathtt{ct}$.
- Comparison is sensitive operation.

Adversary observes comparison:

- Enables chosen-ciphertext attack.
- Gives inequalities in the secret key.
- Solving using our prior work.

$$(-1)^{\mathtt{obs}}(\mathbf{r}^\top \mathbf{e} - \mathbf{s}^\top(\mathbf{e}_1 + \Delta\mathbf{u}) + e_2 + \Delta v) \leq 0$$

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 Transactions on Cryptographic Hardware and Embedded Systems* 2023.4 (2023), pp. 287–317

Most Recent Secure Proposal

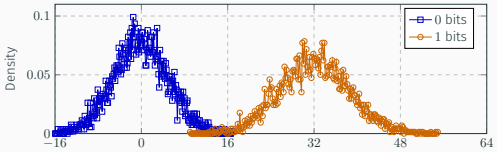
Recent secure proposal: we suspected signal amplification.

Julius Hermelink, Kai-Chun Ning, Richard Petri, and Emanuele Strieder. "The Insecurity of Masked Comparisons: SCAs on ML-KEM's FO-Transform". In: *ACM CCS 2024: 31st Conference on Computer and Communications Security*. Ed. by Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie. ACM Press, Oct. 2024, pp. 2430–2444

Most Recent Secure Proposal

Recent secure proposal: we suspected signal amplification.

Our model (simulation for $\sigma = 5$):



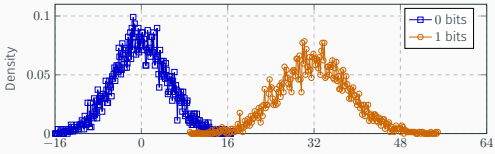
Power consumption of processing a single shared bit.

Julius Hermelink, Kai-Chun Ning, Richard Petri, and Emanuele Strieder. "The Insecurity of Masked Comparisons: SCAs on ML-KEM's FO-Transform". In: *ACM CCS 2024: 31st Conference on Computer and Communications Security*. Ed. by Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie. ACM Press, Oct. 2024, pp. 2430–2444

Most Recent Secure Proposal

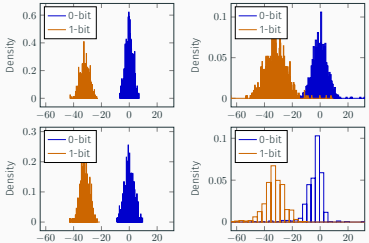
Recent secure proposal: we suspected signal amplification.

Our model (simulation for $\sigma = 5$):



Power consumption of processing a single shared bit.

Actual leakage confirms our model:

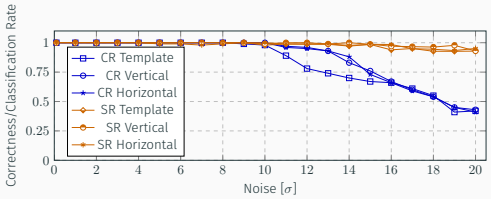


Julius Hermelink, Kai-Chun Ning, Richard Petri, and Emanuele Strieder. "The Insecurity of Masked Comparisons: SCAs on ML-KEM's FO-Transform". In: *ACM CCS 2024: 31st Conference on Computer and Communications Security*. Ed. by Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie. ACM Press, Oct. 2024, pp. 2430–2444

Highly Noise-Tolerant Attacks

Leads to highly noise-tolerant attacks.

Simulated results with 4 shares:



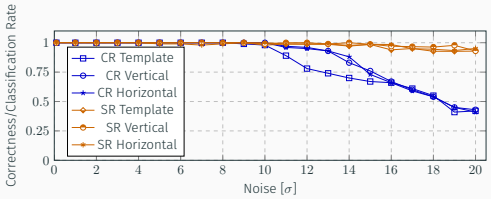
Julius Hermelink, Kai-Chun Ning, Richard Petri, and Emanuele Strieder. "The Insecurity of Masked Comparisons: SCAs on ML-KEM's FO-Transform". In: *ACM CCS 2024: 31st Conference on Computer and Communications Security*. Ed. by Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie. ACM Press, Oct. 2024, pp. 2430–2444

Dina Hesse, Jakob Feldtkeller, Tim Güneysu, **Julius Hermelink**, Markus Krausz, and Georg Land. *t-Probing (In-)Security: Pitfalls on Noise Assumptions*. Cryptology ePrint Archive, Report 2025/1202. 2025. URL: https://eprint.iacr.org/2025/1202

Highly Noise-Tolerant Attacks

Leads to highly noise-tolerant attacks.

Simulated results with 4 shares:



Why do these attacks work so well?

- Slight advantage enough.
- Amplified leakage.

$\rightarrow$ High noise requirements
– analysis in [HFG+25].

Noise/masking order necessary to prevent attacks extraordinarily high.

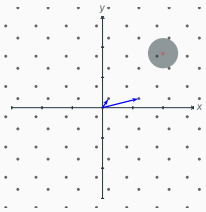
Julius Hermelink, Kai-Chun Ning, Richard Petri, and Emanuele Strieder. "The Insecurity of Masked Comparisons: SCAs on ML-KEM's FO-Transform". In: *ACM CCS 2024: 31st Conference on Computer and Communications Security*. Ed. by Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie. ACM Press, Oct. 2024, pp. 2430–2444

Dina Hesse, Jakob Feldtkeller, Tim Güneysu, **Julius Hermelink**, Markus Krausz, and Georg Land. *t-Probing (In-)Security: Pitfalls on Noise Assumptions*. Cryptology ePrint Archive, Report 2025/1202. 2025. URL: https://eprint.iacr.org/2025/1202

Side Information in Lattice-Based Schemes

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

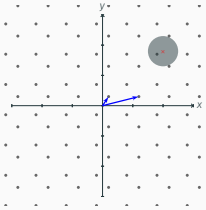
Primal attack:
E.g., [DDGR20; DGHK23; MN23]



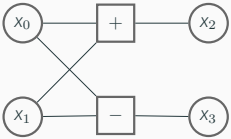
Side Information in Lattice-Based Schemes

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

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



Soft-analytic [VGS14]:
E.g., [PPM17; tPP21; BAE+24]



Attacks: often noisy information on Hamming weights.

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 $\mathbf{v} \in \Lambda$

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32

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:

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

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

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32

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:

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

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

Information from [RPJ+24] without loss!

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

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32

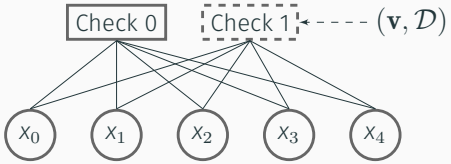
Solving Distribution Hints

Two different solvers: BP and Greedy

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32

Solving Distribution Hints

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

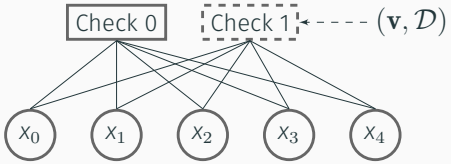


Represent unknown key coefficients

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32

Solving Distribution Hints

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



Represent unknown key coefficients

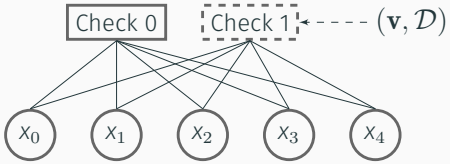
Update for $x_j = x'_j$:

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

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32

Solving Distribution Hints

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



Represent unknown key coefficients

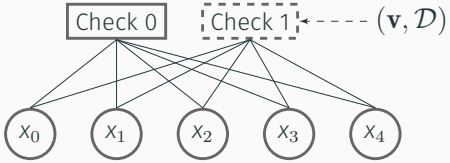
Update for $x_j = x'_j$:

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

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32

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:

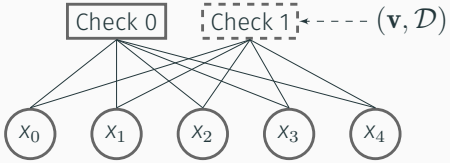
$$s_j(c) = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) |\langle \mathbf{v}, \mathbf{x}' \rangle + v_j c - a|,$$

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

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32

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 $\mathbf{x}'$.

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

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32

Side-Channel Attacks on Masked ML-DSA

A more conceptual approach to side-channel attacks on ML-DSA.

Masked ML-DSA:

- Different types of masking.
- Choice of signed and unsigned integers.
- Several attacks on unmasked ML-DSA.

How to target masked ML-DSA?

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 (To Appear at Crypto 2025). 2025. URL: https://eprint.iacr.org/2025/276

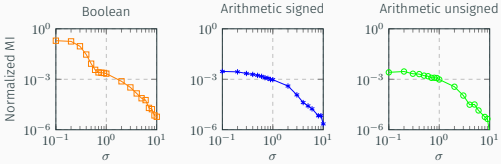
A more conceptual approach to side-channel attacks on ML-DSA.

Masked ML-DSA:

- Different types of masking.
- Choice of signed and unsigned integers.
- Several attacks on unmasked ML-DSA.

How to target masked ML-DSA?

Mutual information per measurement:



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 (To Appear at Crypto 2025). 2025. URL: https://eprint.iacr.org/2025/276

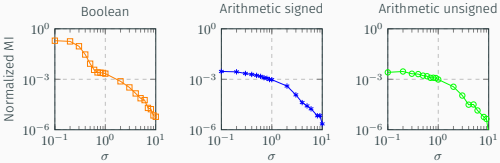
A more conceptual approach to side-channel attacks on ML-DSA.

Masked ML-DSA:

- Different types of masking.
- Choice of signed and unsigned integers.
- Several attacks on unmasked ML-DSA.

How to target masked ML-DSA?

Mutual information per measurement:



Our framework can be applied with hint-filtering technique.

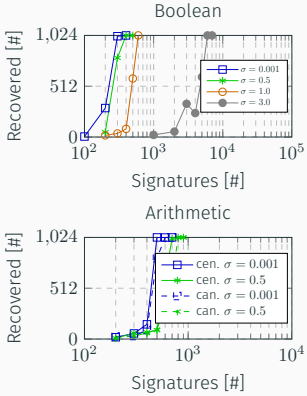
Julius Hermelink, Kai-Chun Ning, and Richard Petri. *Finding and Protecting the Weakest Link: On Side-Channel Attacks on Masked ML-DSA*. Cryptology ePrint Archive, Report 2025/276 (To Appear at Crypto 2025). 2025. URL: `https://eprint.iacr.org/2025/276`

Targeting ML-DSA

First attacks against masked ML-DSA targeting $\mathbf{y}$ in several representations.

Practical attacks:

- Replicates previous attack.
- New reasonably noise-tolerant second-order attacks.
- Concrete practical recommendations for future implementation.



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 (To Appear at Crypto 2025). 2025. URL: `https://eprint.iacr.org/2025/276`

Conclusion

Conclusion:

- Protecting ML-KEM is challenging.
- Efficient and generic framework.
- Attacks on masked ML-DSA.
- Works well with info-theoretic analysis.
- Framework applies more generally.

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 Transactions on Cryptographic Hardware and Embedded Systems* 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: *Advances in Cryptology – CRYPTO 2020, Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. 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: *Advances in Cryptology – CRYPTO 2023, Part V*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14085. Lecture Notes in Computer Science. Springer, Cham, Aug. 2023, pp. 748–781.

[HFG+25] Dina Hesse, Jakob Feldtkeller, Tim Güneysu, **Julius Hermelink**, Markus Krausz, and Georg Land. *t-Probing (In-)Security: Pitfalls on Noise Assumptions*. Cryptology ePrint Archive, Report 2025/1202. 2025. URL: `https://eprint.iacr.org/2025/1202`.

[MN23] Alexander May and Julian Nowakowski. “Too Many Hints - When LLL Breaks LWE”. In: *Advances in Cryptology – ASIACRYPT 2023, Part IV*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14441. Lecture Notes in Computer Science. 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: *Cryptographic Hardware and Embedded Systems – CHES 2017*. Ed. by Wieland Fischer and Naofumi Homma. Vol. 10529. Lecture Notes in Computer Science. Springer, Cham, Sept. 2017, pp. 513–533.

References (2)

[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 Transactions on Cryptographic Hardware and Embedded Systems* 2024.2 (2024), pp. 795–818.

[tMS+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 Transactions on Cryptographic Hardware and Embedded Systems* 2023.4 (2023), pp. 287–317.

[tNP25] **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 (To Appear at Crypto 2025). 2025. URL: https://eprint.iacr.org/2025/276.

[tNPS24] **Julius Hermelink**, Kai-Chun Ning, Richard Petri, and Emanuele Strieder. "The Insecurity of Masked Comparisons: SCAs on ML-KEM's FO-Transform". In: *ACM CCS 2024: 31st Conference on Computer and Communications Security*. Ed. by Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie. ACM Press, Oct. 2024, pp. 2430–2444.

[tPP21] **Julius Hermelink**, Peter Pessl, and Thomas Pöppelmann. "Fault-Enabled Chosen-Ciphertext Attacks on Kyber". In: *Progress in Cryptology - INDOCRYPT 2021: 22nd International Conference in Cryptology in India*. Ed. by Avishek Adhikari, Ralf Küsters, and Bart Preneel. Vol. 13143. Lecture Notes in Computer Science. Springer, Cham, Dec. 2021, pp. 311–334.

[tSMP25] **Julius Hermelink**, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *Advances in Cryptology – EUROCRYPT 2025, Part VIII*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. Lecture Notes in Computer Science. Springer, Cham, May 2025, pp. 3–32.

References (3)

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