Side-Channel Analysis of Post-Quantum Schemes

Julius Hermelink

April 1, 2025

Who am I?

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.
- Formal models 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.

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.

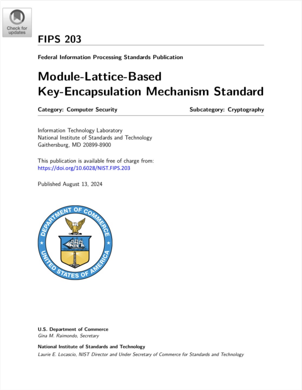
Therefore, we need:

- 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.



Check for updates

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

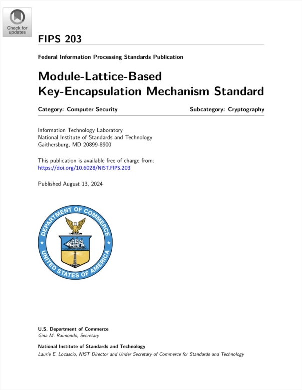
National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

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.

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



Check for updates

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

DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA

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.

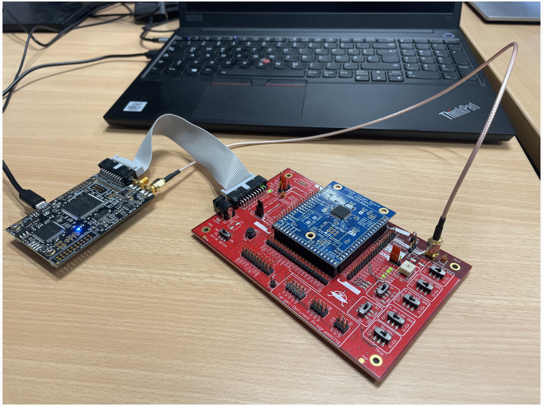
- Five candidates already selected.
- Three are lattice-based.
- ML-KEM and ML-DSA standardized.

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

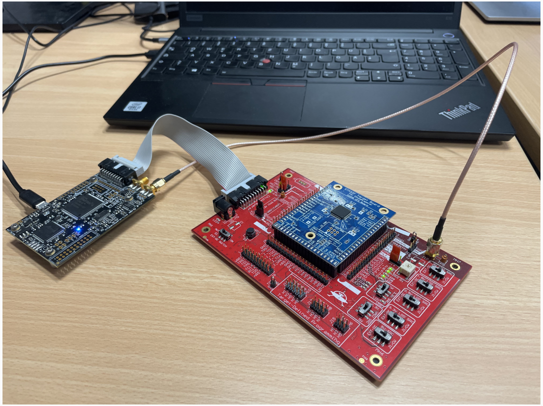
NIST FIPS 203, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf, accessed March 31, 2025.

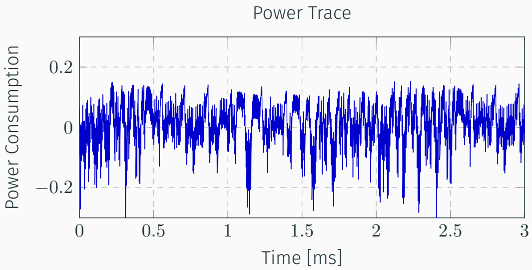
Attacks on Embedded Devices

Embedded devices may be particularly vulnerable to side-channel and fault attacks.



Embedded devices may be particularly vulnerable to side-channel and fault attacks.





The Insecurity of Masked Comparisons

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*. Ed. by Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie. ACM Press, Oct. 2024, pp. 2430–2444

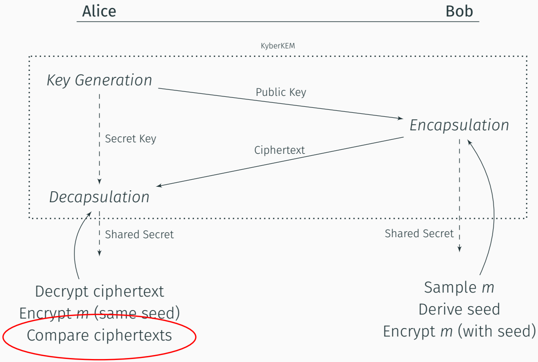
Fujisaki-Okamoto Transform Comparisons

In ML-KEM:

- Comparison $\texttt{ct}' == \texttt{ct}$.
- Checks if honestly generated.
- Comparison is sensitive operation.

Adversary observes comparison:

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



Fujisaki-Okamoto Transform Comparisons

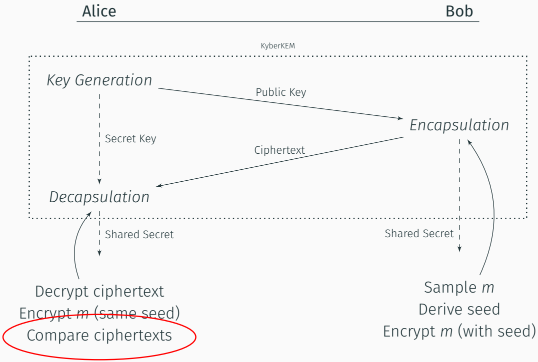
In ML-KEM:

- Comparison $\texttt{ct}' == \texttt{ct}$.
- Checks if honestly generated.
- Comparison is sensitive operation.

Adversary observes comparison:

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

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

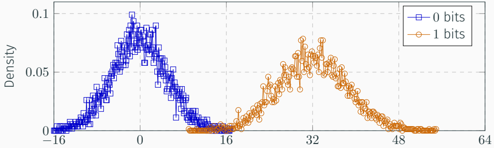


Leakage Model

Recent masked t-probing secure proposal: We suspected signal amplification.

Masking countermeasures share information over multiple variables, e.g., $s = s_0 \oplus s_1$.

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



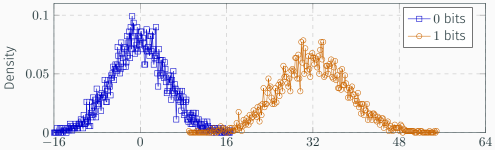
Power consumption of processing a single shared bit.

Leakage Model

Recent masked t-probing secure proposal: We suspected signal amplification.

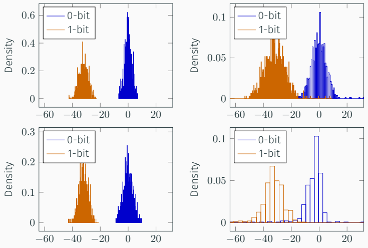
Masking countermeasures share information over multiple variables, e.g., $s = s_0 \oplus s_1$.

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



Power consumption of processing a single shared bit.

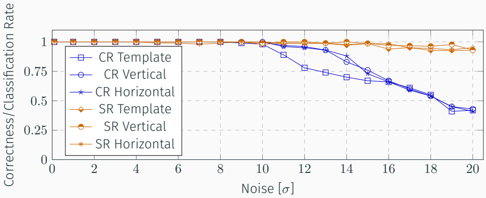
Actual leakage confirms our model:



Results

Carried out in practice and simulated for different noise levels.

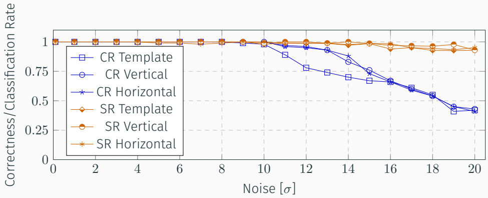
Simulated results with 4 shares:



Results

Carried out in practice and simulated for different noise levels.

Simulated results with 4 shares:



Why do these attacks work so well?

- Slight advantage enough.
- Amplified leakage.

→ High noise requirements.

Noise/masking order necessary to prevent attacks extraordinarily high.

A Generic Framework for Side-Channel Attacks against LWE

Julius Hermelink, Silvan Streit, Erik Mårtensson, and Richard Petri. "A Generic Framework for Side-Channel Attacks against LWE-based Cryptosystems". In: *To appear in Eurocrypt*. LNCS. Springer, 2025. URL: https://eprint.iacr.org/2024/1211

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

Distribution Hints

The secret often has to be recovered from side information.

Adversary may learn, e.g.,:

- $\langle \mathbf{v}, \mathbf{x} \rangle = l$
- $\langle \mathbf{v}, \mathbf{x} \rangle \equiv l \mod p$
- $\langle \mathbf{v}, \mathbf{x} \rangle = l + \mathcal{N}(0, \sigma)$
- $\langle \mathbf{v}, \mathbf{x} \rangle \leq l$
- $\mathrm{HW}(\langle \mathbf{v}, \mathbf{x} \rangle) = h + \mathcal{N}(0, \sigma)$
- ...

for known $\mathbf{v}, l, h, p, \sigma$; called hints.

Distribution Hints

The secret often has to be recovered from side information.

Adversary may learn, e.g.,:

- $\langle \mathbf{v}, \mathbf{x} \rangle = l$
- $\langle \mathbf{v}, \mathbf{x} \rangle \equiv l \mod p$
- $\langle \mathbf{v}, \mathbf{x} \rangle = l + \mathcal{N}(0, \sigma)$
- $\langle \mathbf{v}, \mathbf{x} \rangle \leq l$
- $\mathrm{HW}(\langle \mathbf{v}, \mathbf{x} \rangle) = h + \mathcal{N}(0, \sigma)$
- ...

for known $\mathbf{v}, l, h, p, \sigma$; called hints.

Distribution Hints:

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

for known vector $\mathbf{v}$, distribution $\mathcal{D}$, and secret $\mathbf{x}$.

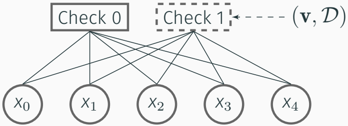
The definition:

- Generalizes all but one previous hints.
- Complements lattice-based frameworks.

Solver for Distribution Hints

We present two solvers working on distribution hints.

Belief propagation-based solver:



Represent unknown key coefficients

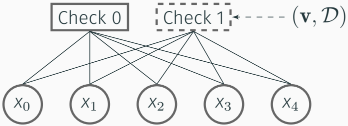
Update for $x_j = x_j'$ where $s_j = \sum_{i \neq j} v_i x_i$:

$$P(x_j = x_j') = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P(s_j = a - v_j x_j')$$

Solver for Distribution Hints

We present two solvers working on distribution hints.

Belief propagation-based solver:



Represent unknown key coefficients

Update for $x_j = x_j'$ where $s_j = \sum_{i \neq j} v_i x_i$:

$$P(x_j = x_j') = \sum_{a \in \operatorname{supp} \mathcal{D}} P_{\mathcal{D}}(a) P(s_j = a - v_j x_j')$$

Greedy solver:

Compute change scores for coefficients j:

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

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

$P(s_j = a - v_j x_j')$ replaced by $|\mathbf{v}^\top \mathbf{x}' + v_j c - a|$.

A more conceptual approach to side-channel attacks.

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?

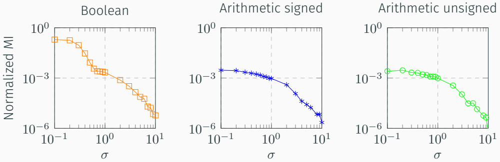
A more conceptual approach to side-channel attacks.

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:



Side-Channel Attacks on Masked ML-DSA

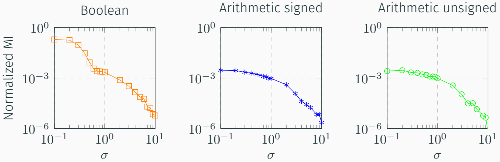
A more conceptual approach to side-channel attacks.

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.

Future Directions

Real-world security largely an open question.

- Improved cryptanalysis under side-information.
- Non-standard side-channel.
- Impacts of leakage on protocol level.
- Conceptual information-theoretic approaches to (previous) attacks.
- Formal models/verification.
- Other PQC schemes.
- Cryptanalysis.
- ...

Future Directions

Real-world security largely an open question.

- Improved cryptanalysis under side-information.
- Non-standard side-channel.
- Impacts of leakage on protocol level.
- Conceptual information-theoretic approaches to (previous) attacks.
- Formal models/verification.
- Other PQC schemes.
- Cryptanalysis.
- ...

Why Birmingham?

- **Elisabeth Oswald**: side-channel analysis and applied cryptography
- **David Oswald**: embedded security and side-channel analysis.
- **Christophe Petit**: cryptanalysis and isogeny-based cryptography.
- **Mihai Ordean**: system security, protocol security and privacy.
- ...

Future Directions

Real-world security largely an open question.

- Improved cryptanalysis under side-information.
- Non-standard side-channel.
- Impacts of leakage on protocol level.
- Conceptual information-theoretic approaches to (previous) attacks.
- Formal models/verification.
- Other PQC schemes.
- Cryptanalysis.
- ...

Why Birmingham?

- **Elisabeth Oswald**: side-channel analysis and applied cryptography
- **David Oswald**: embedded security and side-channel analysis.
- **Christophe Petit**: cryptanalysis and isogeny-based cryptography.
- **Mihai Ordean**: system security, protocol security and privacy.
- ...

Thank you for your attention!