A Side Channel Attack on Masked ML-DSA

Find the Weakest Spot

Julius Hermelink, Kai-Chun Ning, Richard Petri

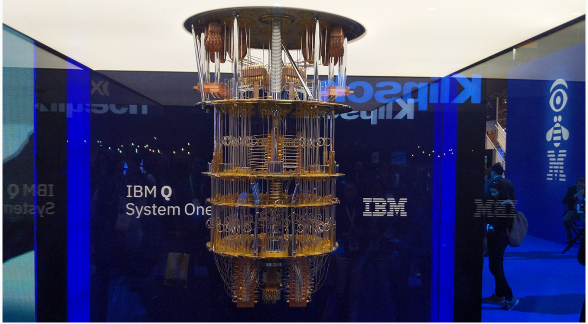
`firstname.lastname@mpi-sp.org`

Max Planck Institute for Security and Privacy, Bochum, Germany

August 18, 2025

Intro

Post-quantum Cryptography



- Breaks asymmetric cryptography
- Long term PKI

https://www.extremetech.com/extreme/283427-quantum-computing-goes-commercial-with-ibms-q-system-one

Intro
Dilithium/ML-DSA


FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature 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.204

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

- Module-Lattice-based Digital Signature
- Standardized in 2024
- Dilithium: original proposal
- Fiat-Shamir with aborts

https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

Intro

Dilithium/ML-DSA Signing

Algorithm 1 Simplified Signing Algorithm

procedure SIGN(secret s_1, public A, message m)
  while no valid signature **do**
    $y \leftarrow$ random sample
    $c \leftarrow$ hash of m and part of Ay
    $z \leftarrow y + cs_1$
    Try again if z leaks sensitive info
  end while
  return signature $\leftarrow (z, c)$
end procedure

- No SCA assessment on masked ML-DSA!
- Many attacks do not tolerate noise well

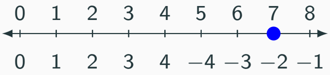
- SASCA on seed of PRNG [KPP20]
- Distinguish zero coefficients in y [Uli+24]
- CPA on cs_1 in NTT domain
  - Software [Che+21]
  - Hardware (FPGA) [Ste+23]
- Find noise-free equations $cs_1 = x + \delta$ [Qia+24]
- SASCA framework on cs_1 [Bro+24]

Boolean and Arithmetic Masking

- Boolean
  - Xor'ing shares
  - $0101_2 \oplus 0111_2 = 0010_2$
- Arithmetic over modulus q
  - Sum of shares mod q
  - $5 + 7 \bmod 9 = 3$
- Masking order
  - Memory and cycle overhead
  - In practice small

Signed and Unsigned Representation

- To represent 7 mod 9:

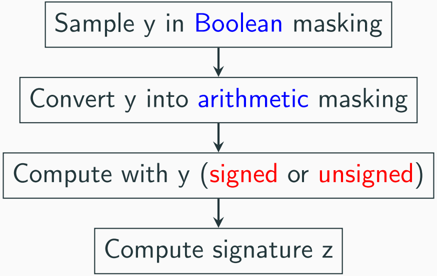


- Unsigned: canonical
- Signed: centered

Signed representation usually leaks more [TMS24]

Intro
Masked Dilithium/ML-DSA

Figure 1: Simplified Masked ML-DSA



State of the art:

- 2023: Closed source masked Dilithium [Azo+23]
- 2023: Gadgets for Dilithium [Cor+23]
- 2024: Extended for ML-DSA [Cor+24]

Can we still target y? If so, how?

- Boolean or Arithmetic?
- Signed or Unsigned?

Information Theoretic Analysis
Methodology

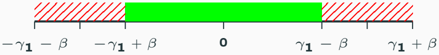
Setup:

- First-order masking
- Hamming weight (HW) leakage model
- Noise-free and noisy (Gaussian)

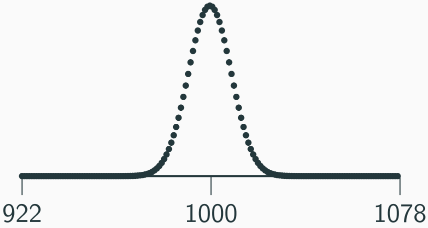
- Leaked Info: mutual info between random variables
- Our case:
  - $x = cs_1$
  - Defined by leakage function L on shares m
- How to compute $I(x; L(\mathrm{m}) \mid z)$?

Information Theoretic Analysis
Computing MI

- $y : [-\gamma_1 + 1, \gamma_1]$, $x : [-\beta, \beta], \gamma_1 = 2^{17}, \beta = 78$
- $z = y + x$

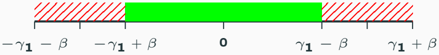


Distribution of y conditioned on z



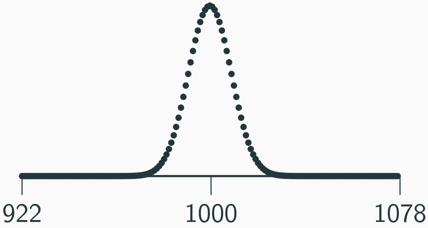
Information Theoretic Analysis
Computing MI

- $y : [-\gamma_1 + 1, \gamma_1]$, $x : [-\beta, \beta], \gamma_1 = 2^{17}, \beta = 78$
- $z = y + x$



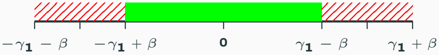
- Fixing $z \to$ small range of y
  - x has $2\beta + 1 = 157$ possible values
  - y is uniquely determined by x

Distribution of y conditioned on z



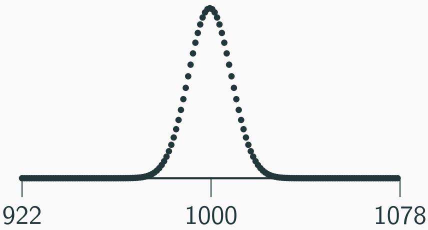
Information Theoretic Analysis
Computing MI

- $y : [-\gamma_1 + 1, \gamma_1]$, $x : [-\beta, \beta], \gamma_1 = 2^{17}, \beta = 78$
- $z = y + x$



- Fixing $z \rightarrow$ small range of y
  - x has $2\beta + 1 = 157$ possible values
  - y is uniquely determined by x
  - Boolean: $m_0 \in [0, 2^{18} - 1], m_1 = y \oplus m_0$
  - Arithmetic: $m_0 \in [0, q - 1], m_1 = y - m_0 \mod q$

Distribution of y conditioned on z

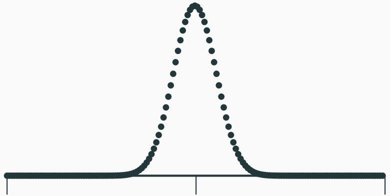


Information Theoretic Analysis
Computing MI

- $y : [-\gamma_1 + 1, \gamma_1]$, $x : [-\beta, \beta], \gamma_1 = 2^{17}, \beta = 78$
- $z = y + x$

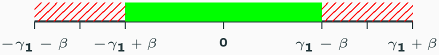
- Fixing $z \rightarrow$ small range of y
  - x has $2\beta + 1 = 157$ possible values
  - y is uniquely determined by x
  - Boolean: $m_0 \in [0, 2^{18} - 1], m_1 = y \oplus m_0$
  - Arithmetic: $m_0 \in [0, q - 1], m_1 = y - m_0 \mod q$
- $I(x; L(\mathrm{m}) \mid z) = \frac{1}{2(\gamma_1 - \beta)} \sum_{z=z'} I(x; L(\mathrm{m}) \mid z = z')$

Distribution of y conditioned on z



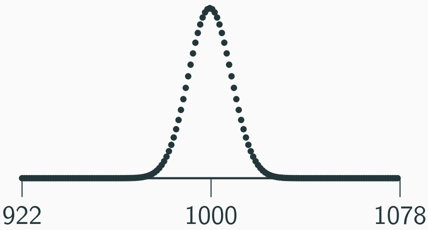
Information Theoretic Analysis
Computing MI

- $y : [-\gamma_1 + 1, \gamma_1]$, $x : [-\beta, \beta], \gamma_1 = 2^{17}, \beta = 78$
- $z = y + x$



- Fixing $z \rightarrow$ small range of y
  - x has $2\beta + 1 = 157$ possible values
  - y is uniquely determined by x
  - Boolean: $m_0 \in [0, 2^{18} - 1], m_1 = y \oplus m_0$
  - Arithmetic: $m_0 \in [0, q - 1], m_1 = y - m_0 \mod q$
- $I(x; L(\mathrm{m}) \mid z) = \frac{1}{2(\gamma_1 - \beta)} \sum_{z=z'} I(x; L(\mathrm{m}) \mid z = z')$
- $L(\mathrm{m})$ depends on signed/unsigned representation

Distribution of y conditioned on z



Information Theoretic Analysis
Noise-free

Figure 2: Boolean

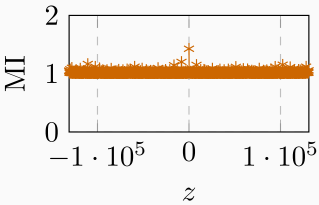


Figure 3: Arithmetic

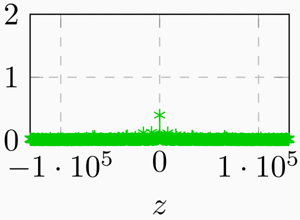


Table 1: $I(x; L(\mathrm{m}) \mid z)$.

Variant	MI
Arith. cen. ($t = 2$)	0.01363
Arith. can. ($t = 2$)	0.01317
Boolean ($t = 2$)	1.01949
Boolean ($t = 1$)	2.16538
Arith. cen. ($t = 1$)	0.17219
Arith. can. ($t = 1$)	0.16708

Not much difference b/w signed and unsigned

- z provides info on y already
- Signed representation leaks slightly more

Accidental leakage for arithmetic masking:

- $y = \mathrm{m}_0 + \mathrm{m}_1 \bmod q$
- $\mathrm{HW}(\mathrm{m}_0 \oplus \mathrm{m}_1) \neq \mathrm{HW}(y)$

Figure 4: Boolean

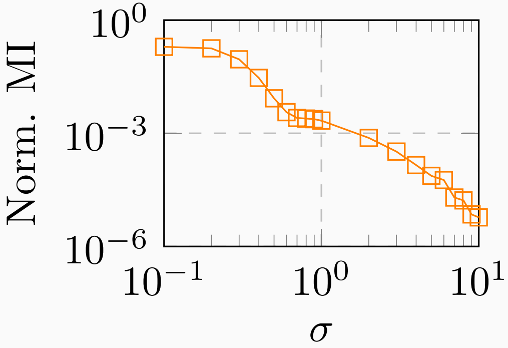
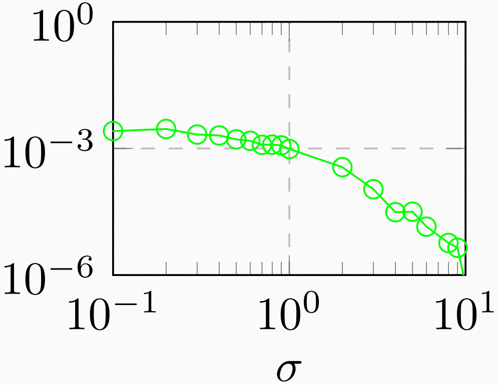


Figure 5: Arithmetic



Not much difference b/w signed and unsigned

What is belief propagation?

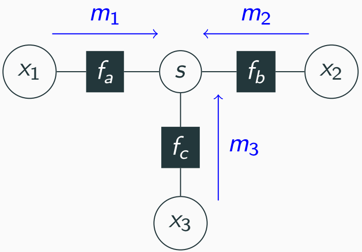
- "Gossiping neighbors"
- Pass distributions

Generic framework for LWE [Her+25]:

- Uses belief propagation
- Instantiated for ML-KEM as an example
- Open source

Example:

$$f(s, x_1, x_1, x_3) = f_a(x_1, s) f_b(x_2, s) f_c(x_3, s)$$



SASCA
Filtering

Drop equations with the highest entropy

- Numerical instability
- Efficiency

Figure 6: Less uniform

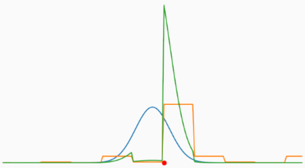


Figure 7: More uniform

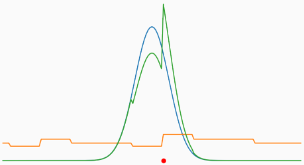
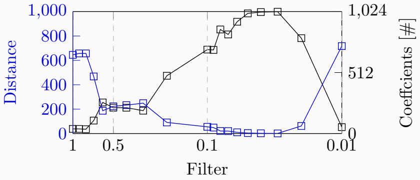


Figure 8: Effect of Filtering



Overview of simulated attacks:

- Signed and unsigned
- 1st order: HW(y), HW(y) + HW(x), LSBs of y
- 2nd order: HW(m), Boolean and Arithmetic

Figure 9: Boolean

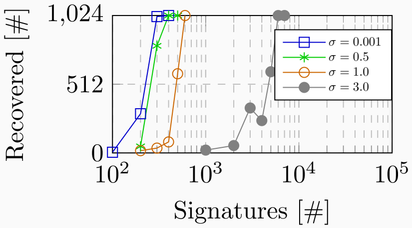
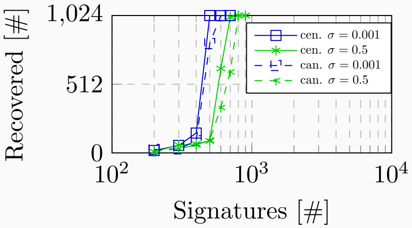


Figure 10: Arithmetic



Setup:

- Ported implementation from [Cor+24]
- Cortex-M3 and M4
- Target Boolean shares of y

Overview of physical attacks:

- 1^{st} order: HW(y), LSBs of y
- 2^{nd} order: HW(m)

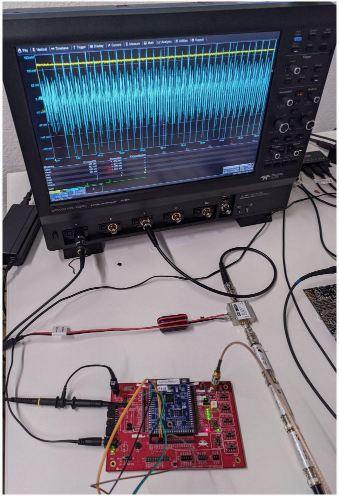


Figure 11: LSBs of y, 1st order

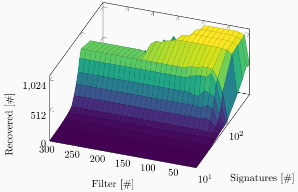


Figure 13: HW(m), 2nd order

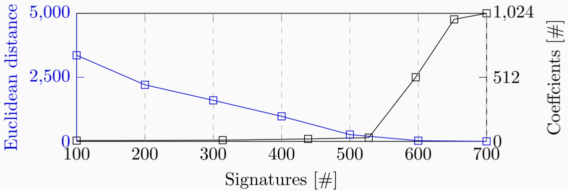


Figure 12: HW(m), 2nd order, simulated

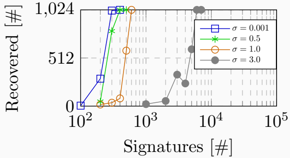


Table 2: Summary of Physical Attacks

Leakage function	Order	σ	Signatures
LSBs of y	1	12	250
HW(y)	1	4.74	300
HW(m)	2	1.47, 1.65	700

Takeaways

- Signed vs Unsigned: not much diff. in this case
- Boolean masking:
  - More likely to have strong accidental leakage
  - Leaks more for all orders
- Noise tolerant 2^{nd} order attacks
- Filters matter: drop dist. with high entropy

Our paper: `https://eprint.iacr.org/2025/276`

Table 3: Summary of Our Attacks

Order	Type	HW(y)	HW(y) + HW(x)	LSBs of y
1	Simulated	✓	✓	✓
	Physical	✓	✗	✓
		HW(m), Boolean	HW(m), Arithmetic	
2	Simulated	✓	✓	
	Physical	✓	✗	

Thank you for your attention!

References

[Azo+23] Melissa Azouaoui et al. "Protecting Dilithium against Leakage Revisited Sensitivity Analysis and Improved Implementations". In: *IACR TCHES* 2023.4 (2023), pp. 58–79. DOI: 10.46586/tches.v2023.i4.58-79.

[Bro+24] Olivier Bronchain et al. "Exploiting Small-Norm Polynomial Multiplication with Physical Attacks Application to CRYSTALS-Dilithium". In: *IACR TCHES* 2024.2 (2024), pp. 359–383. DOI: 10.46586/tches.v2024.i2.359-383.

[Che+21] Zhaohui Chen et al. "An Efficient Non-Profiled Side-Channel Attack on the CRYSTALS-Dilithium Post-Quantum Signature". In: *2021 IEEE 39th International Conference on Computer Design (ICCD)*. 2021, pp. 583–590. DOI: 10.1109/ICCD53106.2021.00094.

[Cor+23] Jean-Sébastien Coron et al. "Improved Gadgets for the High-Order Masking of Dilithium". In: *IACR TCHES* 2023.4 (2023), pp. 110–145. DOI: 10.46586/tches.v2023.i4.110-145.

References

[Cor+24] Jean-Sébastien Coron et al. *Improved High-Order Masked Generation of Masking Vector and Rejection Sampling in Dilithium*. Cryptology ePrint Archive, Report 2024/1149. 2024. URL: https://eprint.iacr.org/2024/1149.

[Han+21] Jaeseung Han et al. "Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-Based Profiling". In: *IEEE Access* 9 (2021), pp. 166283–166292. DOI: 10.1109/ACCESS.2021.3135600. URL: https://doi.org/10.1109/ACCESS.2021.3135600.

[Her+25] Julius Hermelink et al. "A Generic Framework for Side-Channel Attacks Against LWE-Based Cryptosystems". In: *EUROCRYPT 2025, Part VIII*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15608. LNCS. Springer, Cham, May 2025, pp. 3–32. DOI: 10.1007/978-3-031-91101-9_1.

[KPP20] Matthias J. Kannwischer, Peter Pessl, and Robert Primas. "Single-Trace Attacks on Keccak". In: *IACR TCHES* 2020.3 (2020), pp. 243–268. ISSN: 2569-2925. DOI: 10.13154/tches.v2020.i3.243-268. URL: https://tches.iacr.org/index.php/TCHES/article/view/8590.

References

[PP19] Peter Pessl and Robert Primas. "More Practical Single-Trace Attacks on the Number Theoretic Transform". In: *LATINCRYPT 2019*. Ed. by Peter Schwabe and Nicolas Thériault. Vol. 11774. LNCS. Springer, Cham, Oct. 2019, pp. 130–149. DOI: 10.1007/978-3-030-30530-7_7.

[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. DOI: 10.1007/978-3-319-66787-4_25.

[Qia+24] Zehua Qiao et al. *Single Trace is All It Takes: Efficient Side-channel Attack on Dilithium*. Cryptology ePrint Archive, Report 2024/512. 2024. URL: https://eprint.iacr.org/2024/512.

[Ste+23] Hauke Malte Steffen et al. "Breaking and Protecting the Crystal: Side-Channel Analysis of Dilithium in Hardware". In: *Post-Quantum Cryptography - 14th International Workshop, PQCrypto 2023*. Ed. by Thomas Johansson and Daniel Smith-Tone. Springer, Cham, Aug. 2023, pp. 688–711. DOI: 10.1007/978-3-031-40003-2_25.

References

[TMS24] Tolun Tosun, Amir Moradi, and Erkay Savas. "Exploiting the Central Reduction in Lattice-Based Cryptography". In: *IEEE Access* 12 (2024), pp. 166814–166833. DOI: 10.1109/ACCESS.2024.3494593. URL: https://doi.org/10.1109/ACCESS.2024.3494593.

[Uli+24] Vincent Quentin Ulitzsch et al. "Profiling Side-Channel Attacks on Dilithium - A Small Bit-Fiddling Leak Breaks It All". In: *SAC 2022*. Ed. by Benjamin Smith and Huapeng Wu. Vol. 13742. LNCS. Springer, Cham, Aug. 2024, pp. 3–32. DOI: 10.1007/978-3-031-58411-4_1.

Extra

Dilithium/ML-DSA Key Generation

Algorithm 2 Simplified Key Generation

procedure KEYGEN
    $A \leftarrow$ random sample
    $(s_1, s_2) \leftarrow$ random short samples
    $t \leftarrow As_1 + s_2$
    $(t_1, t_0) \leftarrow$ split t into t_1 and t_0
    return pk $\leftarrow (A, t_1)$, sk $\leftarrow (t_0, s_1, s_2)$
end procedure

- SASCA on ML-KEM key in NTT domain [PP19; PPM17]; *Maybe* s_1?
- SASCA on seed of PRNG [KPP20]
- Target s_1 in normal domain with neural network [Han+21]

Due to compiler optimization, unexpected microarchitectural effects

Figure 14: HW(y)

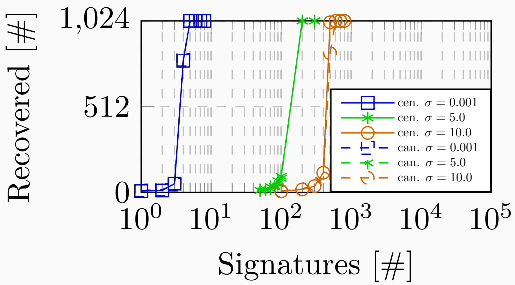
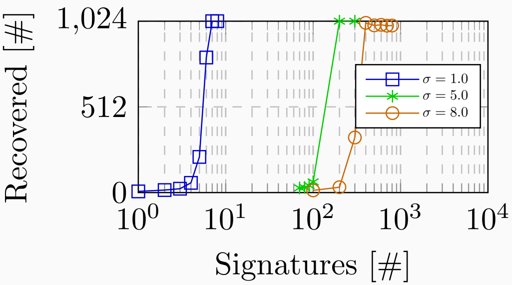


Figure 15: 8 LSBs of y



Extra
Naïve Template Attack

20 PoIs in 1 million gadget calls ($\sim$ 1000 traces)

- Cortex-M3 ($\sigma = 2.5$): 9% advantage per bit
- Cortex-M4 ($\sigma = 12$) : 5% advantage per bit

Table 4: Accuracy targeting individual bits of y.

Bit Index	0	1	2	3	4	5	6	7
Cortex-M4								
σ	38.79	11.72	11.89	11.65	12.84	13.40	12.78	13.06
SNR_{max}	0.000166	0.001818	0.001767	0.001839	0.001514	0.001390	0.001528	0.001465
Accuracy (%)	49.98	50.64	53.80	54.73	54.21	54.39	54.97	54.19
Cortex-M3								
σ	2.37	2.84	2.66	2.46	2.51	2.47	2.52	2.40
SNR_{max}	0.044281	0.030956	0.035102	0.041014	0.039497	0.040864	0.039298	0.043089
Accuracy (%)	59.10	57.62	58.05	58.84	58.34	58.21	58.12	58.61

Table 5: Overhead of Our Countermeasure (in cycles)

	Total signing	masked_sample_y	seed_y
Original	39118662.27	5488094 (14.02%)	175083 (0.44%)
With Countermeasure	52031577.69	17779727 (34.17%)	701690 (1.35%)