



COSIC

mUOV: Masking the Unbalanced Oil and Vinegar Digital Signature Algorithm at First- and Higher-Order

ACM CCS 2025



S. Kundu*, Q. Norga*, A. Karmakar, U.K. Ojha, A. Ganguly, I. Verbauwhede

COSIC, KU Leuven

15 October 2025

Focus of This Presentation

Masking UOV

- 🛡 Countermeasure against Side Channel Attacks (SCAs)
- 📌 Applicable to other Multivariate DSAs (MAYO, QR-UOV, SNOVA ...)

Focus of This Presentation

Masking UOV

- 🛡 Countermeasure against Side Channel Attacks (SCAs)
- 📌 Applicable to other Multivariate DSAs (MAYO, QR-UOV, SNOVA ...)

In this work, we found that UOV is relatively **easy** and **efficient** to mask

- ▶ $GF(256)$ & matrix-vector arithmetic
- ▶ **NO Arithmetic-to-Boolean or Boolean-to-Arithmetic** conversions

Post-Quantum Cryptography

Need to anticipate the **Quantum Threat**, replace vulnerable public-key crypto:

- ▶ Key Encapsulation Mechanisms (KEM)
- ▶ Digital Signature Algorithms (DSA)

PQC Standardization

-  NIST: ML-KEM, ML-DSA, SLH-DSA, FN-DSA, HQC-KEM...
-  BSI: FrodoKEM, Classic McEliece, ML-KEM, ML-DSA, SLH-DSA
-  NIS/NSR: HAETAE, AImer, SMAUG-T, NTRU+

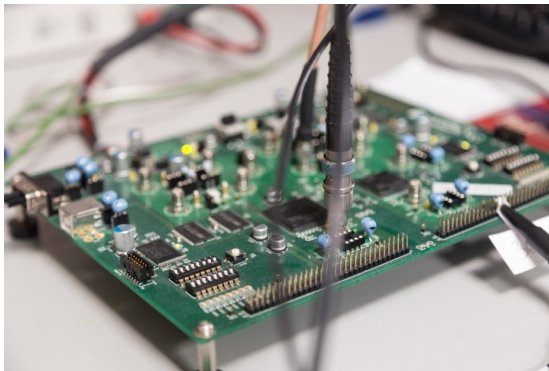
The Unbalanced Oil and Vinegar DSA

Based on **Multivariate Quadratic Equations**

- ▶ Candidate in Ongoing NIST PQC Standardization Process
- + short signatures, fast SigGen() & Verify()
- large public key
- ✦ Embedded (RC) Devices (w/ pre-distributed keys)

Algorithm	EC-DSA	ML-DSA <i>FIPS 204</i> [NIS24a]	SLH-DSA <i>FIPS 205</i> [NIS24b]	FN-DSA <i>FIPS 206</i> [FHK ⁺ 20]	UOV [BCD ⁺ 25]
Signature [Bytes]	128	4 627 (36.1×)	29 792 (232.8×)	1 280 (10.0×)	260 (2.0×)
Public Key [Bytes]	66	2 592 (39.3×)	64 (0.97×)	1 793 (27.2×)	446 992 (461.0×)
Implementation Complexity					

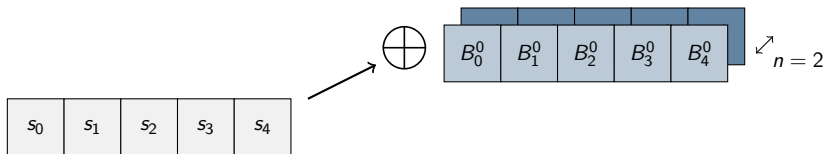
Differential Power Analysis



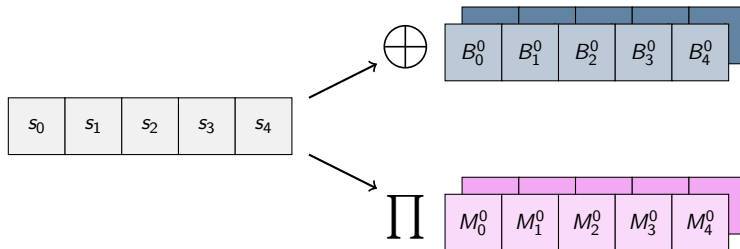
Masking as countermeasure

Secret sharing

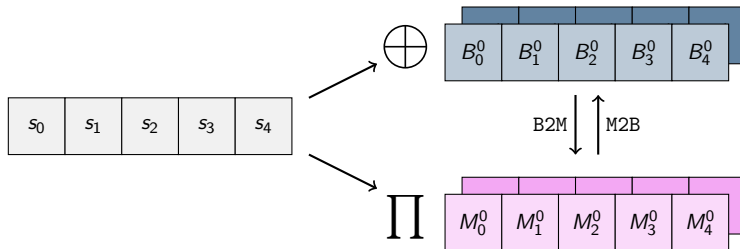
Types of Masking



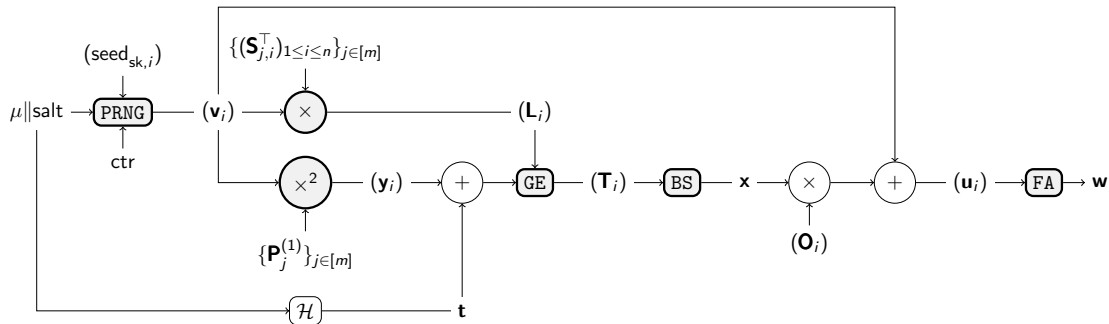
Types of Masking



Types of Masking

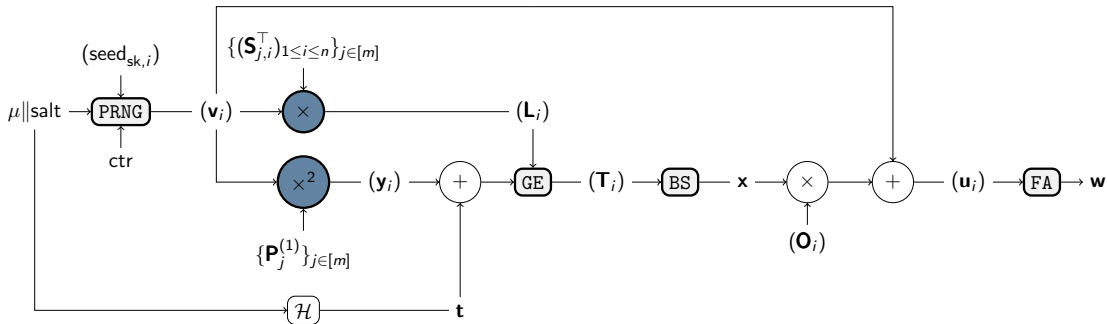


Signature Generation



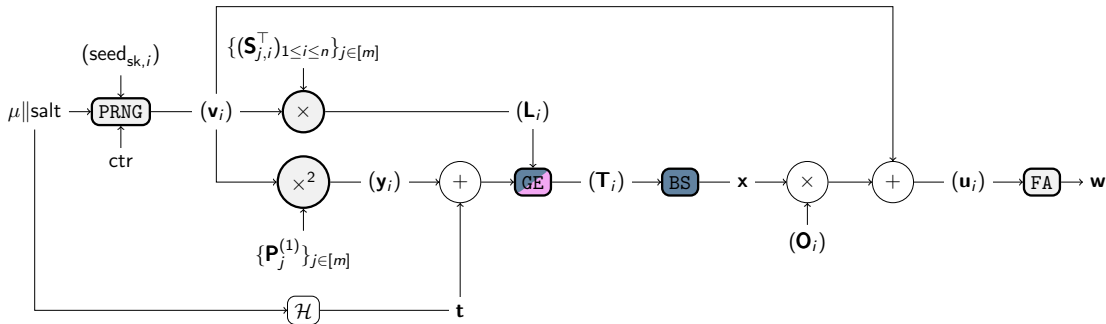
Signature Generation

► Vector-Matrix Arithmetic (Boolean)



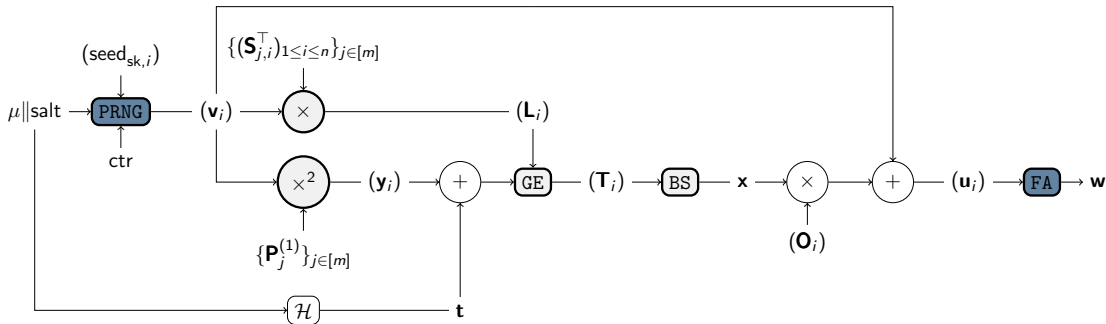
Signature Generation

► Solving System of Linear Equations (Boolean & Multiplicative)



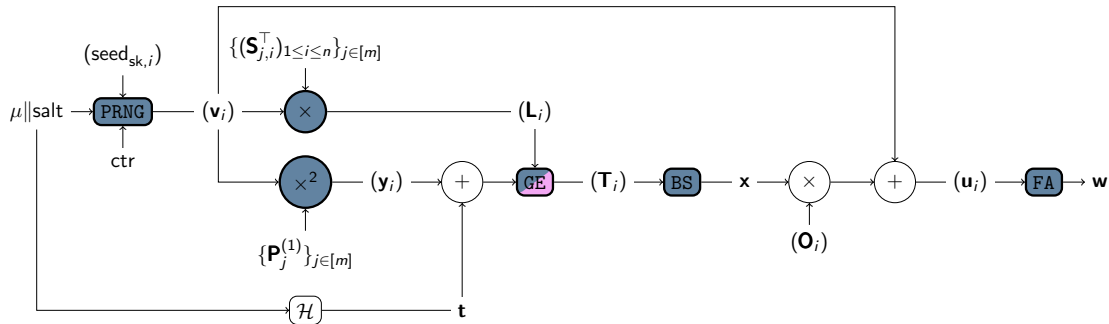
Signature Generation

- Other: PRNG, linear operations (Boolean)



Signature Generation

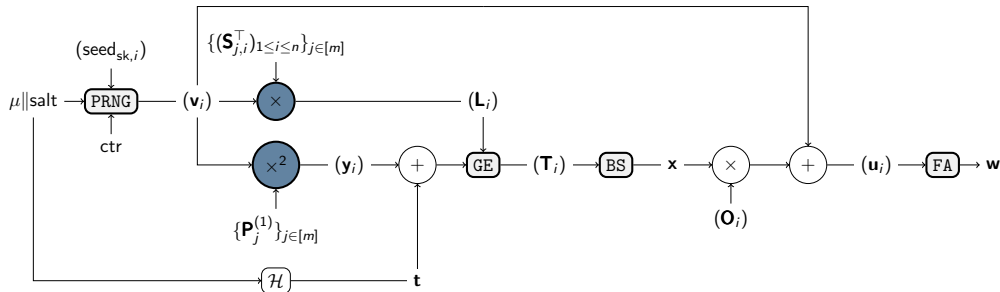
► Mainly Boolean Masking



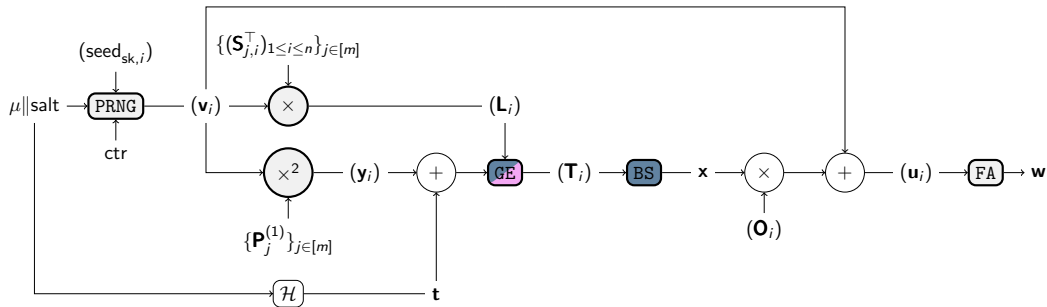
Vector-Matrix Arithmetic

(Masked) Matrix-Vector Multiplication & Quadratic Form Evaluation

- **Repeated** masked GF(256) multiplication
- *Lazy Compression* → reduce fresh randomness

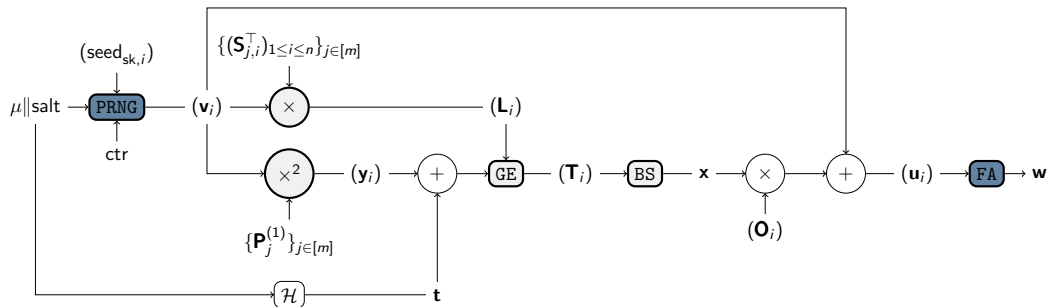


Masked Gaussian Elimination

Row-Echelon Conversion w/ Back Substitution [NKO⁺25]

Other Components

- ▶ Masked SHA-3 [BDPVA10, BBD⁺16]
- ▶ Secure unmasking [CGMZ22, BBD⁺16, CGTZ23]



Security Evaluation

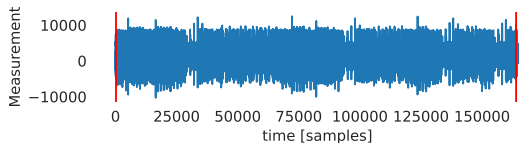
Formal

- ✍ Proofs in t -probing model
- ⚙ Verified mechanically (maskVerif)

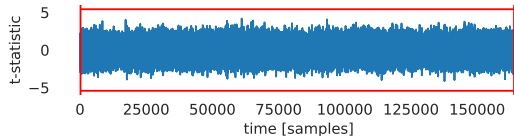
Practical/Experimental

- 📊 NewAE CW308 UFO w/ STM32F415RG Arm Cortex-M4 + PicoScope (@ 125 MS/s)
- ▶ TVLA fix vs. random t -test (up to **1M** traces)

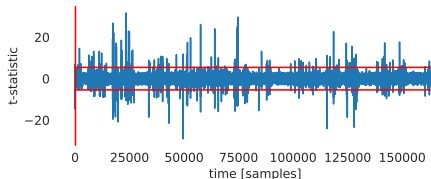
Security Evaluation



(a) Mean Trace



(b) RNG ON



(c) RNG OFF

Micro-Architectural Effects & Compiler Optimization

Transitional (Hamming Weight) Leakages in CPUs

- ▶ Register overwrites
- ▶ Sequential datapath/ALU access
- ▶ ...

Need to take care off these to ensure **countermeasure is effective!**

Micro-Architectural Effects & Compiler Optimization

Transitional (Hamming Weight) Leakages in CPUs

- ▶ Register overwrites
- ▶ Sequential datapath/ALU access
- ▶ ...

Need to take care off these to ensure **countermeasure is effective!**

To make matters worse:

- ▶ manually mitigate leakages (ASM, RND ...)
- ▶ compiler might optimize away [BGG⁺14, ZM24]

🔍 Possible solution: **disable compiler optimization** (-o0)

Proposed Solution

✓ Enable **aggressive** compiler optimization (`-O3`)

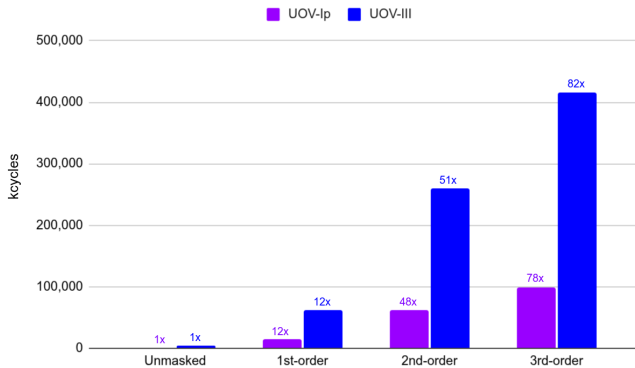
A combination of:

- ▶ Masking countermeasure (written in C)
- ▶ interleaved ASM routines (clear ALU, pre-load RND ...)
- ▶ `-fno-schedule-insns` and `-fno-schedule-insns2` : **no re-ordering**

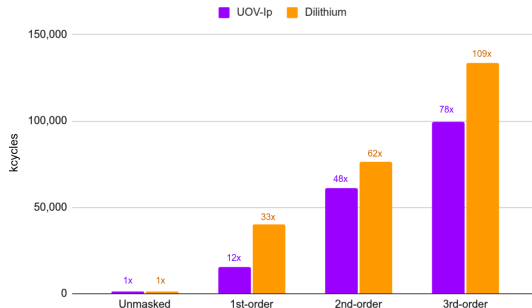
From our experiments, this is sufficient for practical security w low impact on performance.

Results

Intel (R) Core (TM) i7-6600 CPU (2.60 GHz) w GCC 6.5



Performance Comparison



Masking MQE-based seems more efficient than lattice-based equivalents

- ▶ no A2B/B2A
- ▶ (relatively) nice scaling

Summary

PQC in the Real World requires protection against SCAs

- ▶ mUOV protects against t -order DPAs
- ▶ Masking UOV seems easier than lattice-based schemes
- ▶ Mitigation of micro-architectural leakages at low cost

Thank you. Questions?



ePrint 2024/1875



 mUOV Code



Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, and Rébecca Zucchini.

Strong non-interference and type-directed higher-order masking.

In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 2016*, pages 116–129. ACM Press, October 2016.



Ward Beullens, Ming-Shing Chen, Jintai Ding, Boru Gong, Matthias J. Kannwischer, Jacques Patarin, Bo-Yuan Peng, Dieter Schmidt, Cheng-Jhih Shih, Chengdong Tao, and Bo-Yin Yang.

Uov: Unbalanced oil and vinegar algorithm specifications and supporting documentation version 2.0, 2025.



Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.

Building power analysis resistant implementations of Keccak.

In *Second SHA-3 candidate conference*, volume 142, 2010.



Josep Balasch, Benedikt Gierlichs, Vincent Grosso, Oscar Reparaz, and François-Xavier Standaert.

On the cost of lazy engineering for masked software implementations.

In Marc Joye and Amir Moradi, editors, *Smart Card Research and Advanced Applications - 13th International Conference, CARDIS 2014, Paris, France, November 5-7, 2014. Revised Selected Papers*, volume 8968 of *Lecture Notes in Computer Science*, pages 64–81. Springer, 2014.



Jean-Sébastien Coron, François Gérard, Simon Montoya, and Rina Zeitoun.
High-order polynomial comparison and masking lattice-based encryption.
IACR Trans. Cryptogr. Hardw. Embed. Syst., pages 153–192, 11 2022.



Jean-Sébastien Coron, François Gérard, Matthias Trannoy, and Rina Zeitoun.
Improved gadgets for the high-order masking of dilithium.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2023(4):110—145, Aug. 2023.



Pierre-Alain Fouque, Jeffrey Hoffstein, Paul Kirchner, Vadim Lyubashevsky, Thomas Pornin, Thomas Prest, Thomas Ricosset, Gregor Seiler, William Whyte, and Zhenfei Zhang.
Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU, 2020.
<https://falcon-sign.info/falcon.pdf>.



NIST.
FIPS 204 Module-Lattice-Based Digital Signature Standard.
Online. Accessed 10th November, 2024, 2024.



NIST.
FIPS 205 Stateless Hash-Based Digital Signature Standard.
Online. Accessed 10th November, 2024, 2024.



Quinten Norga, Suparna Kundu, Uttam Kumar Ojha, Anindya Ganguly, Angshuman Karmakar, and Ingrid Verbauwhede.

Masking gaussian elimination at arbitrary order with application to multivariate-and code-based pqc. In Arpita Patra, editor, *Topics in Cryptology – CT-RSA 2025*, pages 249–272, Cham, 2025. Springer Nature Switzerland.



Jannik Zeitschner and Amir Moradi.

Pommes: Prevention of micro-architectural leakages in masked embedded software.

IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(3):342–376, Jul. 2024.