



COSIC

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

6th PQC Standardization Conference



Quinten Norga

COSIC, KU Leuven

24 September 2025

Techniques for Masking UOV (and variants)

Synthesis presentation of two works:

Masking Gaussian Elimination at Arbitrary Order

Q. Norga, S. Kundu, U.K. Ojha, A. Ganguly, A. Karmakar, I. Verbauwhede. Topics in Cryptology – CT-RSA 2025. [NKO⁺25]

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

S. Kundu*, Q. Norga*, A. Karmakar, U.K. Ojha, A. Ganguly, I. Verbauwhede. ACM SIGSAC Conference on Computer and Communications Security - ACM CCS 2025. [KNKO⁺25]

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

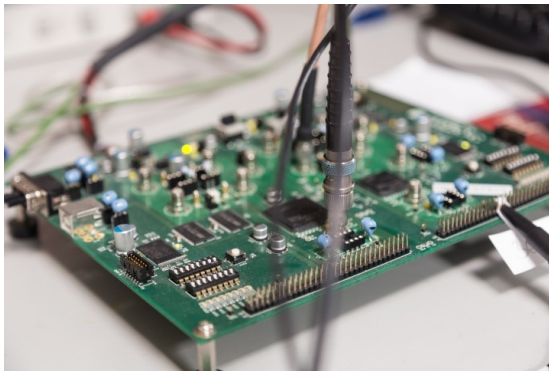
Masking UOV

- 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

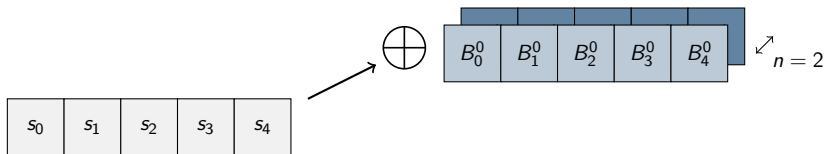
Differential Power Analysis



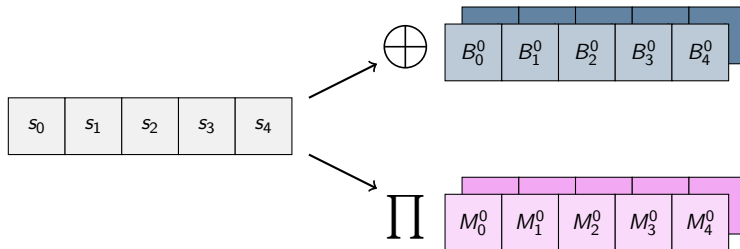
Masking as countermeasure

Secret sharing

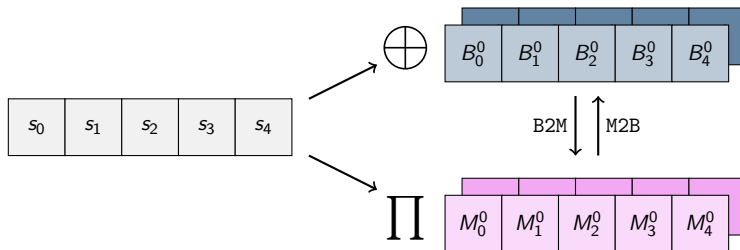
Types of Masking



Types of Masking



Types of Masking



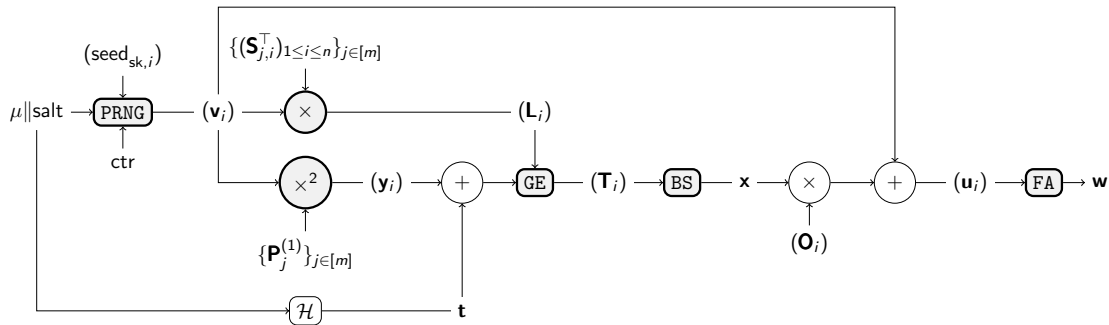
UOV

Properties:

- + short signatures, fast SigGen() & Verify()
- large public key
- ✦ Embedded (RC) Devices (w/ pre-distributed keys)

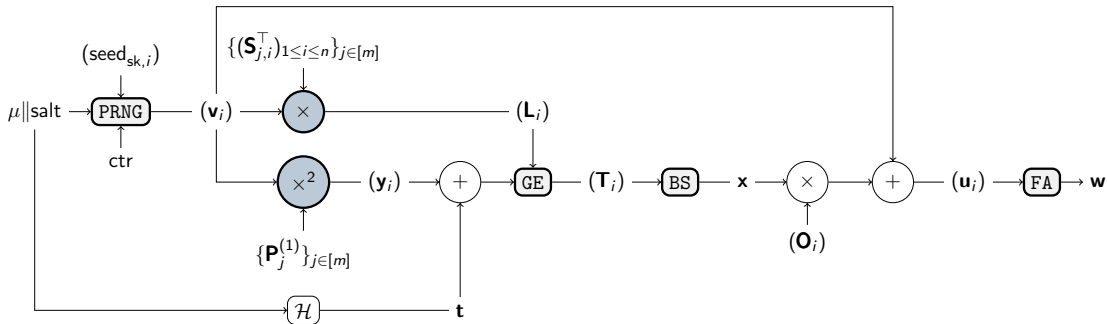
Algorithm	EC-DSA	ML-DSA <i>FIPS 204</i> [NIS24a]	SLH-DSA <i>FIPS 205</i> [NIS24b]	FN-DSA <i>FIPS 206</i> [FHK ⁺ 20]	UOV [BCD ⁺ 25]
Signature [Bytes]	128	4 627 (36.1×)	29 792 (232.8×)	1 280 (10.0×)	260 (2.0×)
Public Key [Bytes]	66	2 592 (39.3×)	64 (0.97×)	1 793 (27.2×)	446 992 (461.0×)
Implementation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

Signature Generation



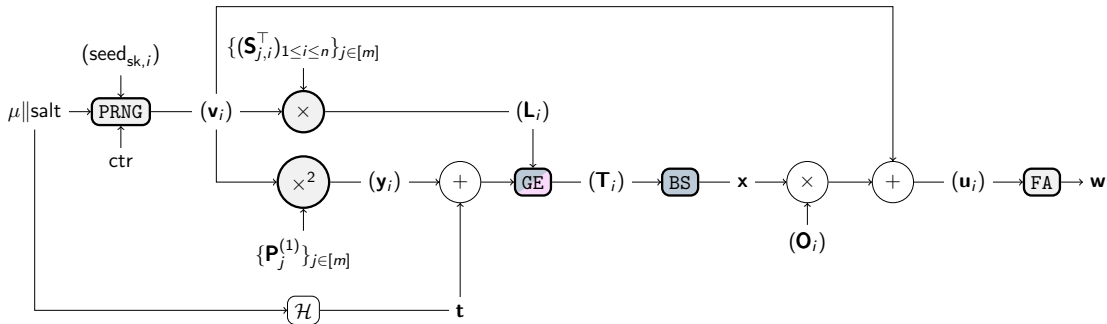
Signature Generation

► Vector-Matrix Arithmetic (Boolean)



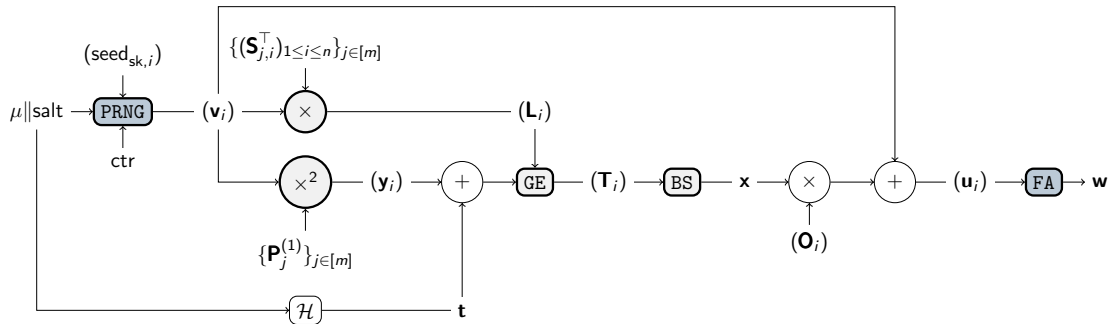
Signature Generation

► Solving System of Linear Equations (Boolean & Multiplicative)

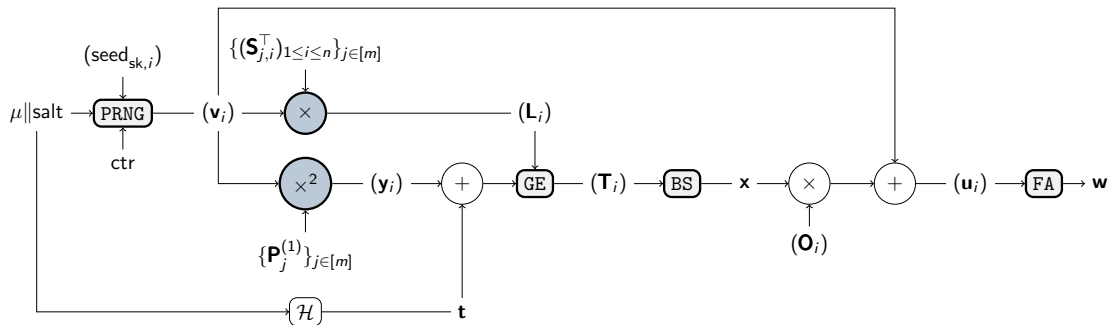


Signature Generation

- Other: PRNG, linear operations (Boolean)



Vector-Matrix Arithmetic



Vector-Matrix Arithmetic

(Masked) Matrix-Vector Multiplication & Quadratic Form Evaluation

- ▶ $S^T v$
- ▶ $xP^T x$

Repeated Masked GF(256) Multiplication

- ▶ **optimized** (masked) dot product: *lazy compression*
- ▶ Minimize overhead of large m, l

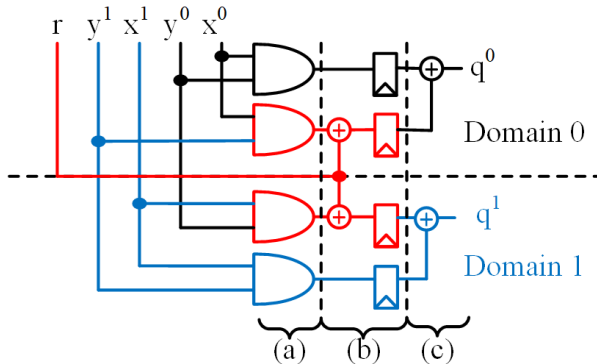
(Repeated) Masked Multiplication

Masked Multiplication = Calculation (a) + Compression (b, c) [GMK16]

NAÏVE

k multiplications:

- (a) k cross-products
- (b) k fresh randoms & registers
- (c) k ADD's



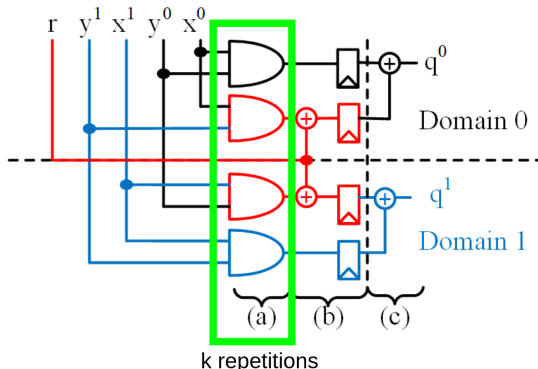
Lazy Compression

$$k \text{ Masked Multiplications} = k \times (a) + 1 \times (b, c)$$

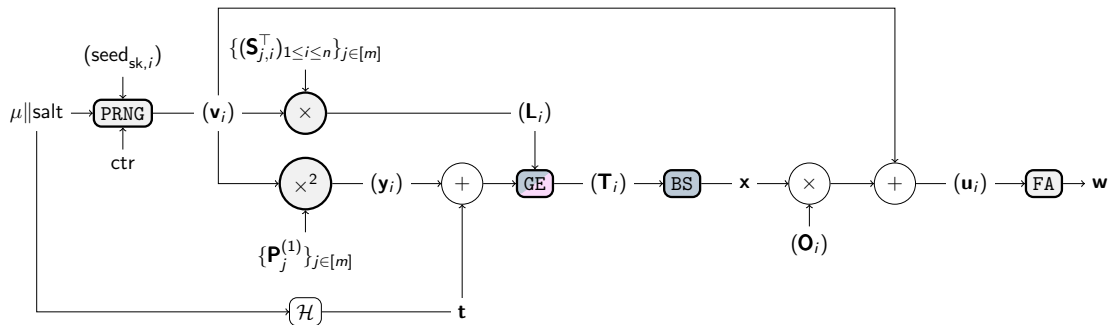
DELAYED COMPRESSION

k multiplications:

- (a) k cross-products
- (b) 1 fresh randoms & register
- (c) $2k$ ADD's



Masked Gaussian Elimination



Masked Gaussian Elimination

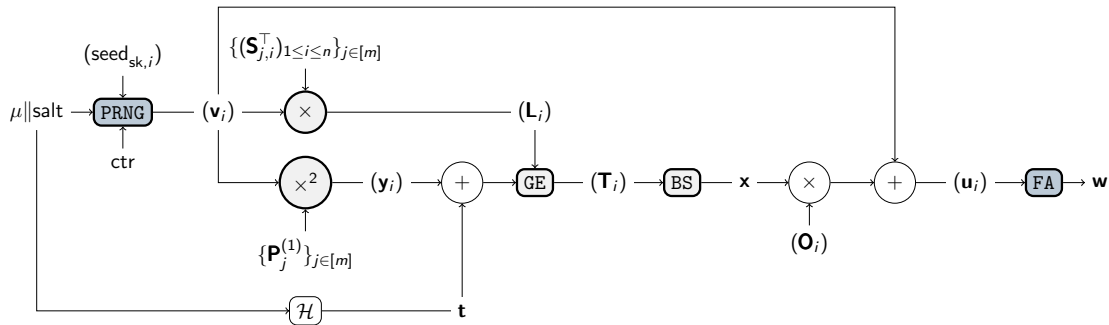
Row-Echelon Conversion w/ Back Substitution

Steps:

- (1) Make pivot $\neq 0 \rightarrow$ timing side-channel!
- (2) Make pivot $= 1 \rightarrow$ multiply with inverse (B2M)
- (3) Make elements below pivot $= 0 \rightarrow$ multiply & subtract

Step 3 is bottleneck ($\pm 80\%$)

Other Components



Other Components

PRNG: mExpand_v

- ▶ SHA-3 (shake256)
- ▶ Boolean Masking [[BDPVA10](#), [BBD⁺16](#)]

FullAdd [[CGV14](#)]

- ▶ Public output $\rightarrow$ Secure unmasking
- ▶ Free- t -SNI refresh [[CGMZ22](#), [BBD⁺16](#), [CGTZ23](#)]

Results

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

Scheme	Key-generation (kcycles)				Sign (kcycles or seconds)			
	unmasked	Masked			unmasked	Masked		
		1st	2nd	3rd		1st	2nd	3rd
UOV-Ip [TW]	58,772	791,871 (13×)	2,215,190 (38×)	36,616,77 (62×)	1,268	15,490 (12×)	61,420 (48×)	99,469 (78×)
UOV-III [TW]	370,483	5,670,203 (15×)	16,241,454 (44×)	25,509,566 (69×)	5,064	62,110 (12×)	259,969 (51×)	415,293 (82×)

Results

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

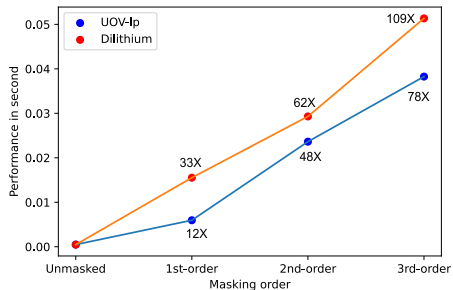
Scheme	Key-generation (kcycles)				Sign (kcycles or seconds)			
	unmasked	1st	Masked 2nd	3rd	unmasked	1st	Masked 2nd	3rd
UOV-Ip [TW]	58,772	791,871 (13×)	2,215,190 (38×)	36,616,77 (62×)	1,268	15,490 (12×)	61,420 (48×)	99,469 (78×)
Dilithium2 [CGL ⁺ 24]	-	-	-	-	1,228	40,368 (33×)	76,173 (62×)	133,508 (109×)
Falcon 512** [BPT ⁺ 24]	-	-	-	-	-	3.199 s	6.368 s	-
UOV-III [TW]	370,483	5,670,203 (15×)	16,241,454 (44×)	25,509,566 (69×)	5,064	62,110 (12×)	259,969 (51×)	415,293 (82×)

**: No processor frequency provided.

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

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

Performance Comparison



... and *easier*

- ▶ GF(256) arithmetic → AES-like masking
- ▶ Many optimizations possible!

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)

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.

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
- ▶ Future Work: Gaussian Elimination, FIA/combined protection ...

Thank you. Questions?



ePrint 2024/1777



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.



Pierre-Augustin Berthet, Justine Paillet, Cédric Tavernier, Lilian Bossuet, and Brice Colombier. Masked computation of the floor function and its application to the FALCON signature. *IACR Commun. Cryptol.*, 1(4):9, 2024.



Jean-Sébastien Coron, François Gérard, Tancrede Lepoint, Matthias Trannoy, and Rina Zeitoun. Improved high-order masked generation of masking vector and rejection sampling in dilithium. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2024(4):335–354, 2024.



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.



Jean-Sébastien Coron, Johann Großschädl, and Praveen Kumar Vadnala. Secure conversion between boolean and arithmetic masking of any order. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 188–205. Springer, 2014.



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>.



Hannes Gross, Stefan Mangard, and Thomas Korak.
Domain-oriented masking: Compact masked hardware implementations with arbitrary protection order.
In *Proceedings of the 2016 ACM Workshop on Theory of Implementation Security*, TIS '16, page 3, New York, NY, USA, 2016. Association for Computing Machinery.



Suparna Kundu, Quinten Norga, Uttam Kumar Ojha, Anindya Ganguly, Angshuman Karmakar, and Ingrid Verbauwhede.
muov: Masking the unbalanced oil and vinegar digital signature scheme at first- and higher-order.
In *Proceedings of the 2025 on ACM SIGSAC Conference on Computer and Communications Security*, CCS '25, New York, NY, USA, 2025. Association for Computing Machinery.



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.