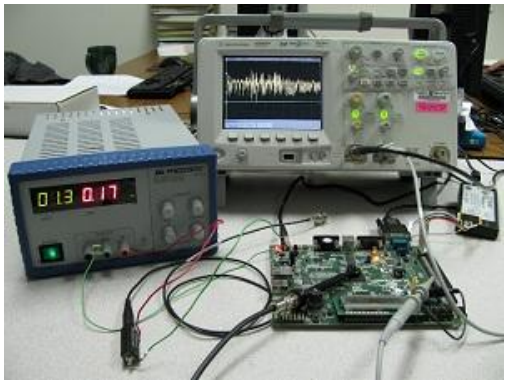
Prime Field Masking and Hard Physical Learning Problems: *Design and (Crypt)Analysis Challenges*



François-Xavier Standaert

UCLouvain (Belgium)

SPRING/GEMS, Roma, May 2026

Outline

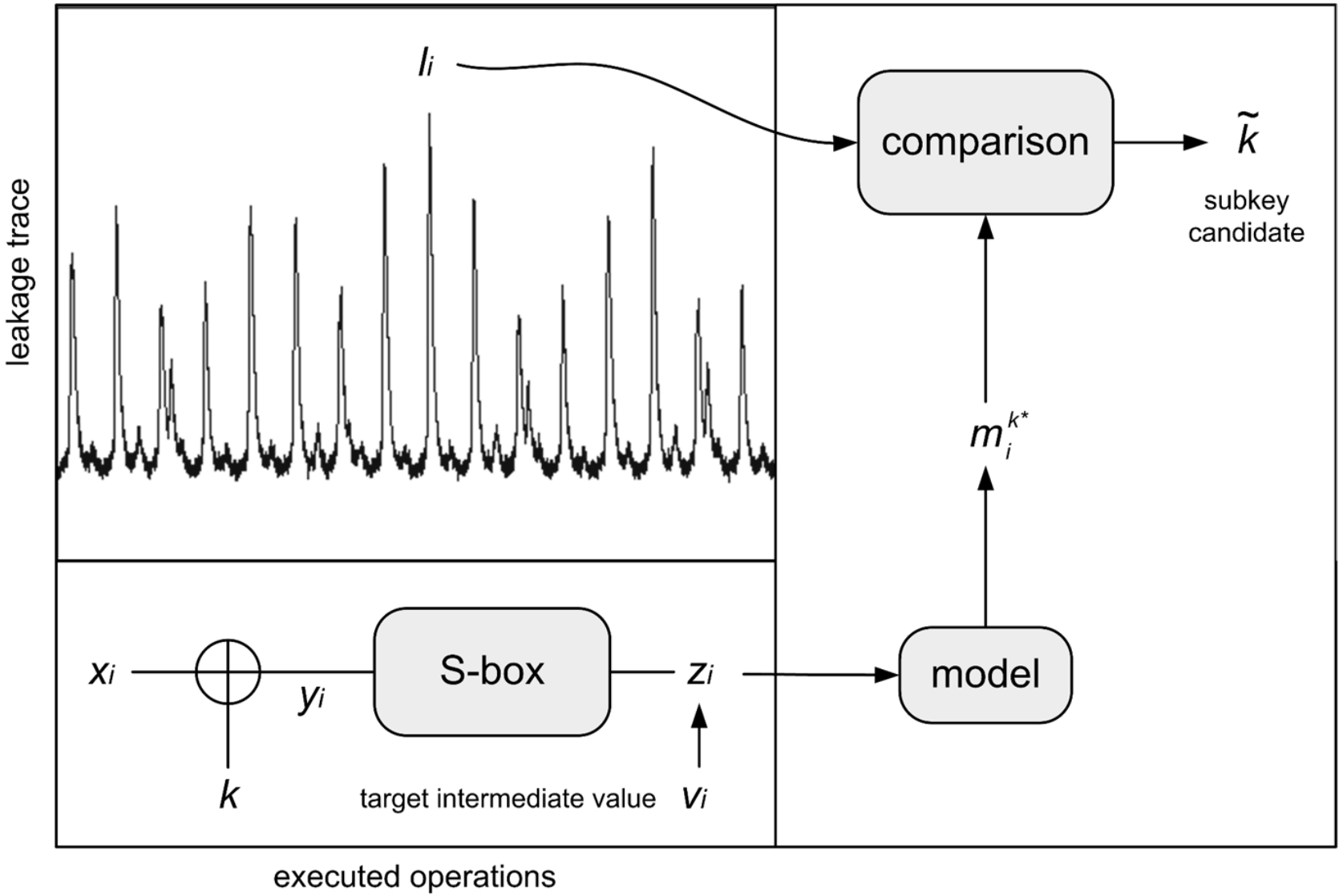
- Background & problem statement
  - Side-channel attacks & Boolean masking
  - Masking-friendly ciphers
  - Leakage-resistant modes of operation

  ⇒ The (lack of) implementation noise issue

- Prime field masking (and cipher design)

- Re-keying: hard physical learning problems

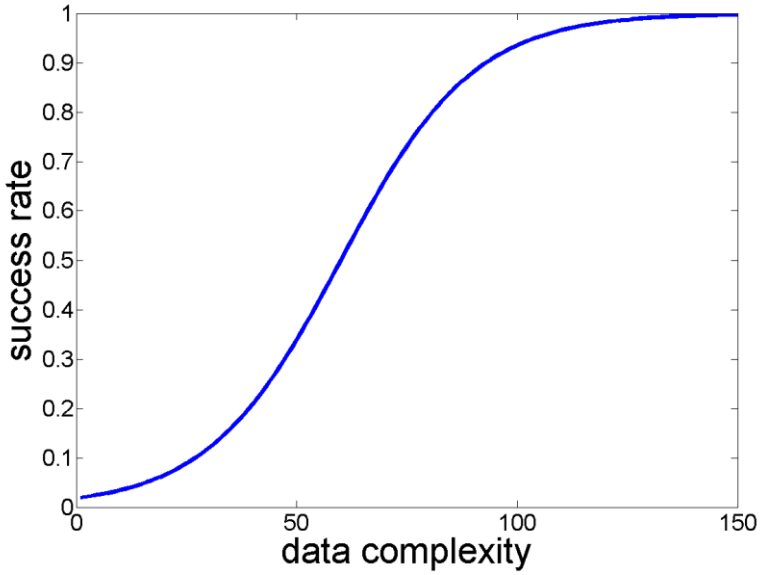
Power Analysis Attacks



DPA vs. SPA taxonomy

- Differential Power Analysis (many-traces attacks)

$$\Pr\left[A_{\mathrm{KR}}\left(x_1, \boldsymbol{L}(x_1, K), \ldots, x_q, \boldsymbol{L}\left(x_q, K\right)\right) \rightarrow K | K \leftarrow \$\right] \approx 2^{-128+q\cdot\lambda}$$

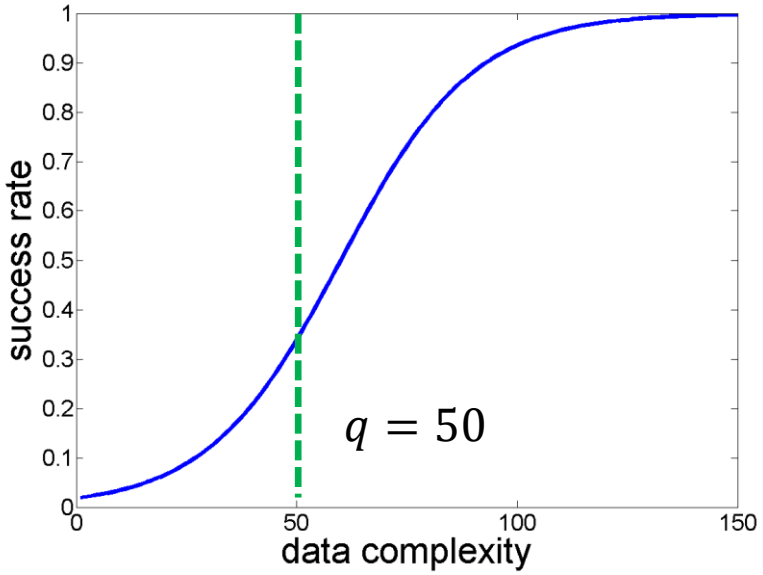


$$\lambda \approx \mathrm{MI}(Z; \boldsymbol{L})$$

DPA vs. SPA taxonomy

- Differential Power Analysis (many-traces attacks)

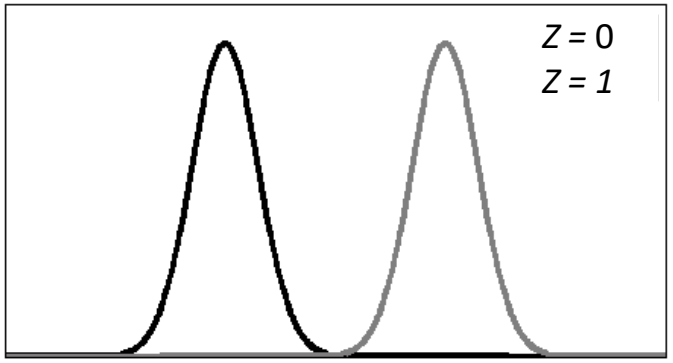
$$\Pr\left[A_{\mathrm{KR}}\left(x_1, \boldsymbol{L}(x_1, K), \ldots, x_q, \boldsymbol{L}(x_q, K)\right) \rightarrow K | K \leftarrow \$\right] \approx 2^{-128+q\cdot\lambda}$$

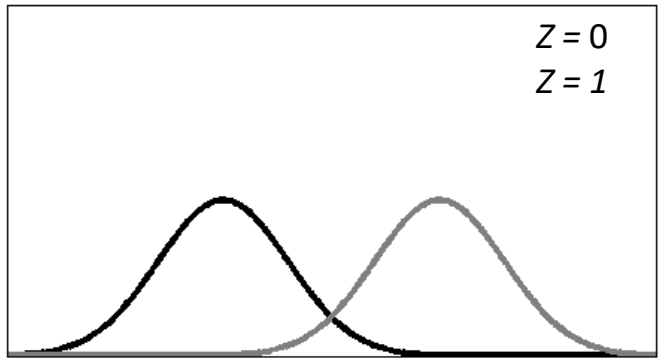


$$\lambda \approx \mathrm{MI}(Z; \boldsymbol{L})$$

- Simple Power Analysis (≈ bounded leakage)

Noise is not enough for DPA security



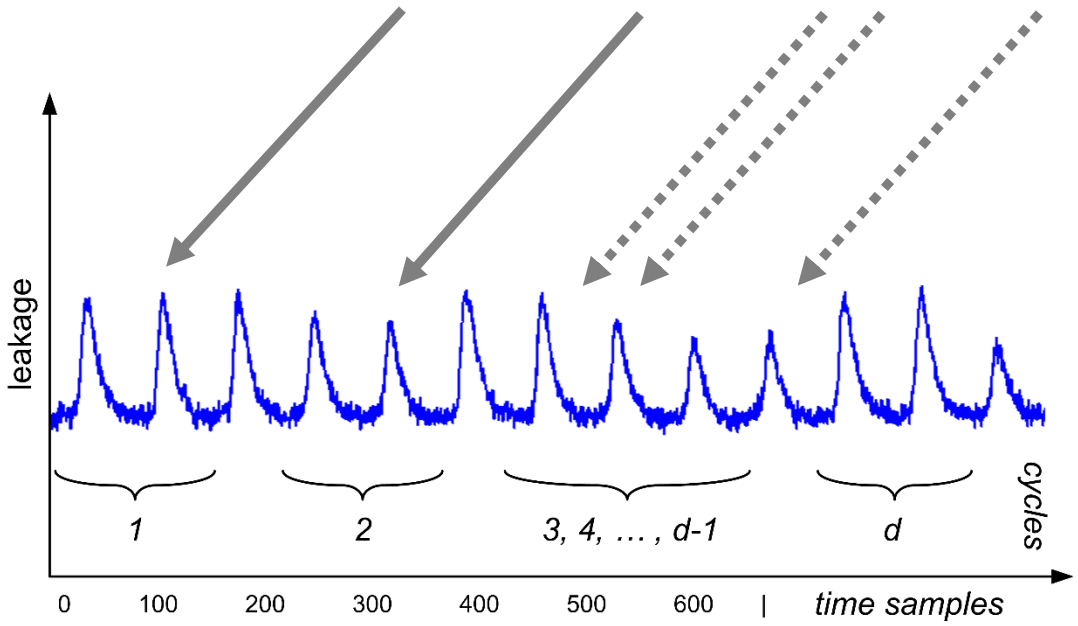


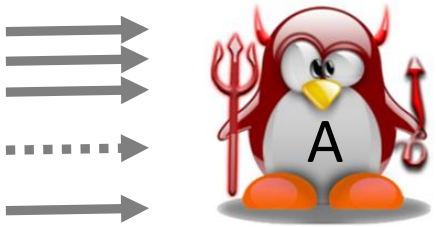
- Additive noise $\approx$ cost $\times 2 \Rightarrow$ security $\times 2$
  $\Rightarrow$ not a good (crypto) security parameter
- $\approx$ same holds for all hardware countermeasures

Masking (≈ uncertainty amplification)

- Private circuits / probing security [ISW03]

$$z = z_1 \oplus z_2 \oplus \cdots \oplus z_{d-1} \oplus z_d$$





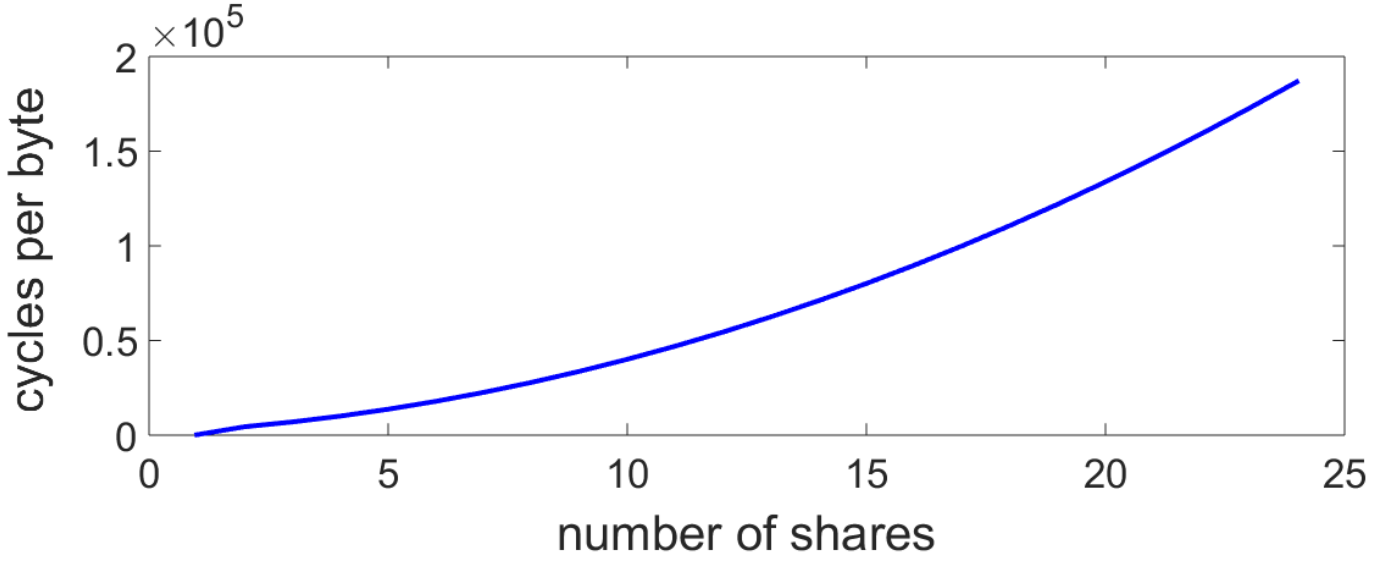
serial implementation.

- Goal: bounded information $\mathrm{MI}(Z; \boldsymbol{L}) < \mathrm{MI}(Z_i; \boldsymbol{L}_{Z_i})^d$

Masking is expensive (e.g., ARM Cortex-M4)

- Multiplications ≈ quadratic overheads

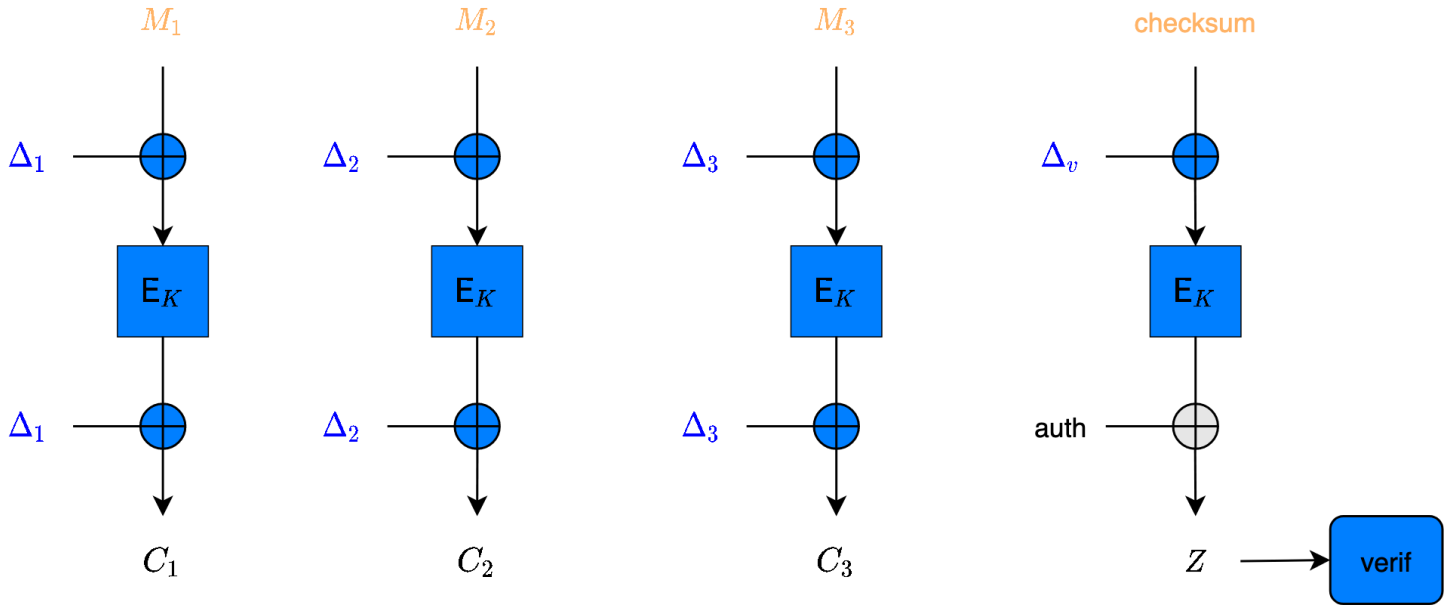
$$\begin{bmatrix} a_1b_1 & a_1b_2 & a_1b_3 \\ a_2b_1 & a_2b_2 & a_2b_3 \\ a_3b_1 & a_3b_2 & a_3b_3 \end{bmatrix} + \begin{bmatrix} 0 & r_1 & r_2 \\ -r_1 & 0 & r_3 \\ -r_2 & -r_3 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$$



⇒ Motivates a scarce use of multiplications!

Leakage-unaware modes

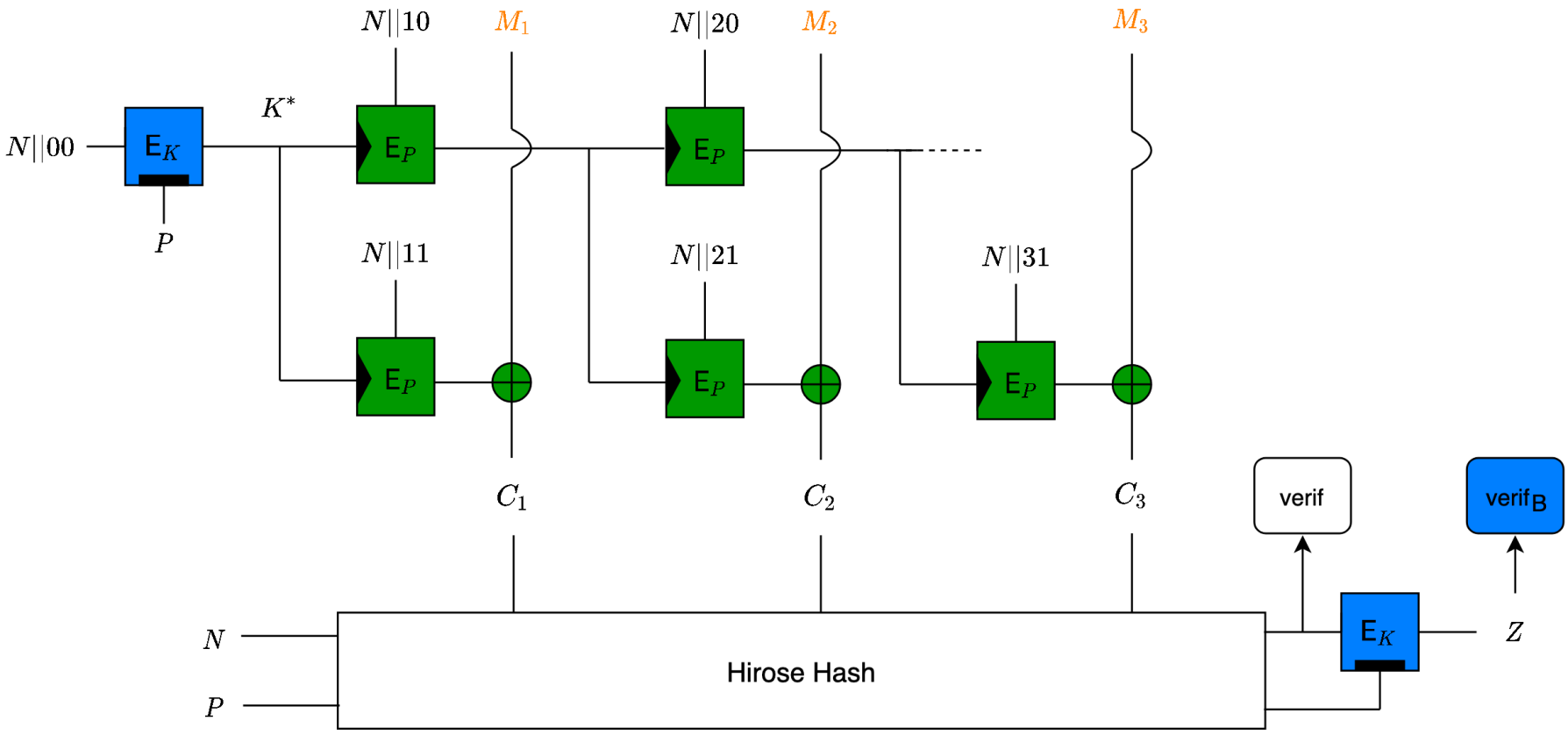
- OCB: DPA possible for all block cipher calls



⇒ Masking everywhere (uniform protection)

Mode-level optimizations

- TEDT: DPA against key / tag generation only



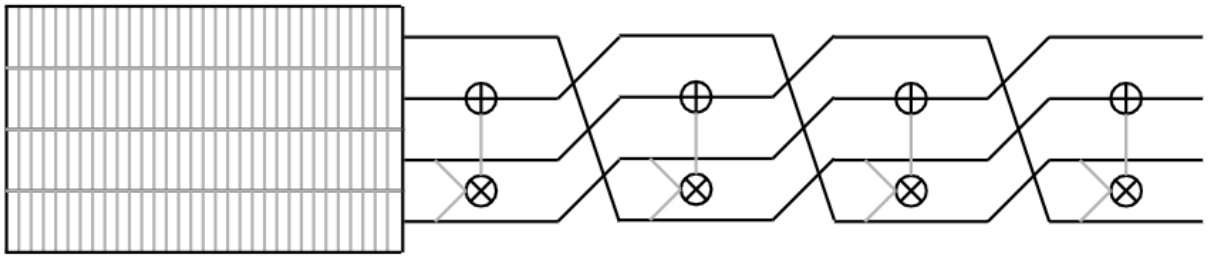
⇒ Limited masking (leveled implementations)

Primitive-level optimizations

- Without leakage: Boolean operations are cheaper (& lower latency) than arithmetic ones

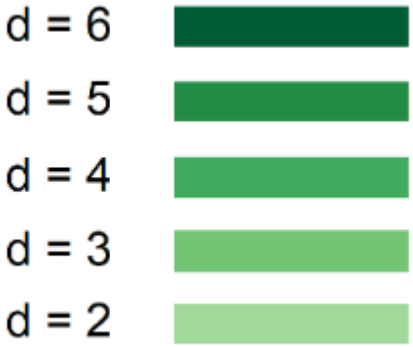
⇒ With leakage: minimize the # of AND gates

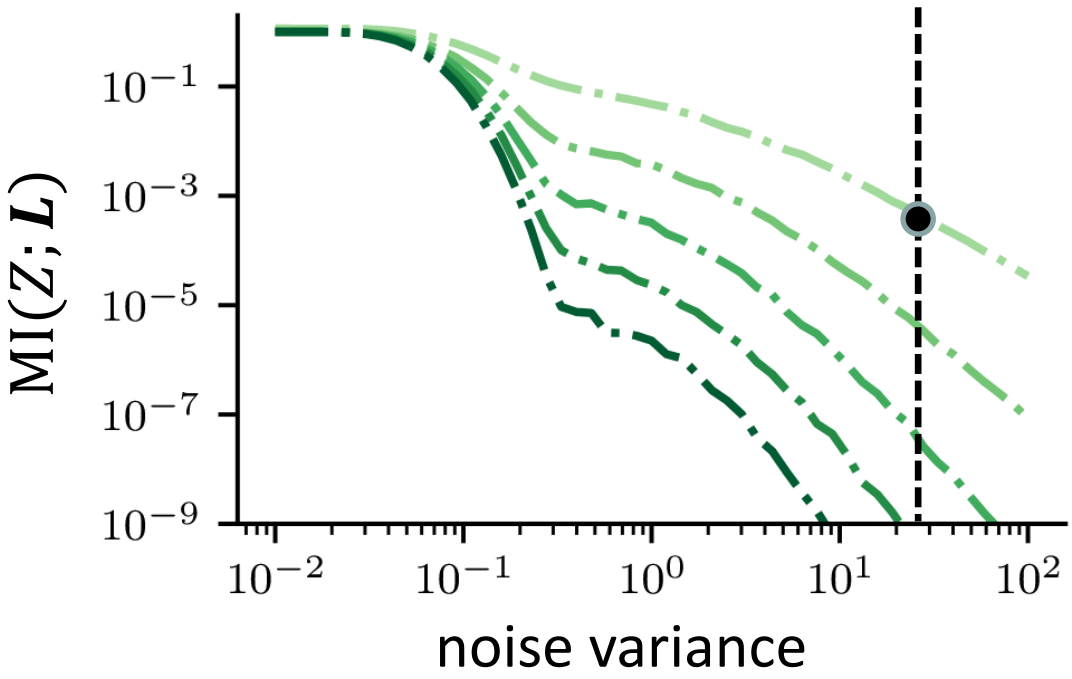
- Standard approach: bitslice ciphers
  - Typical: 4-bit S-box, 32-bit linear layer

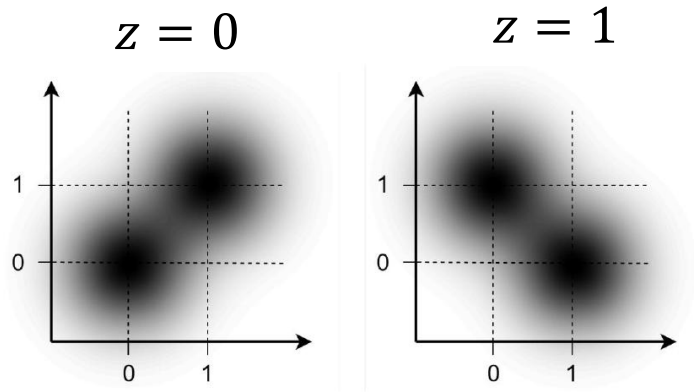


  - ***Is it the best/only optimization criteria?***

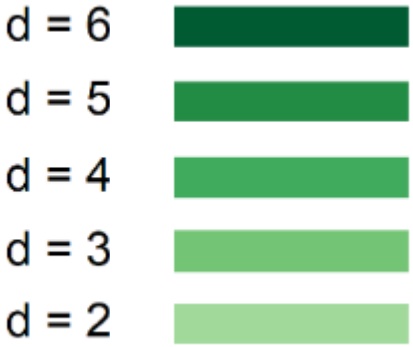
Boolean masking with noise: OK

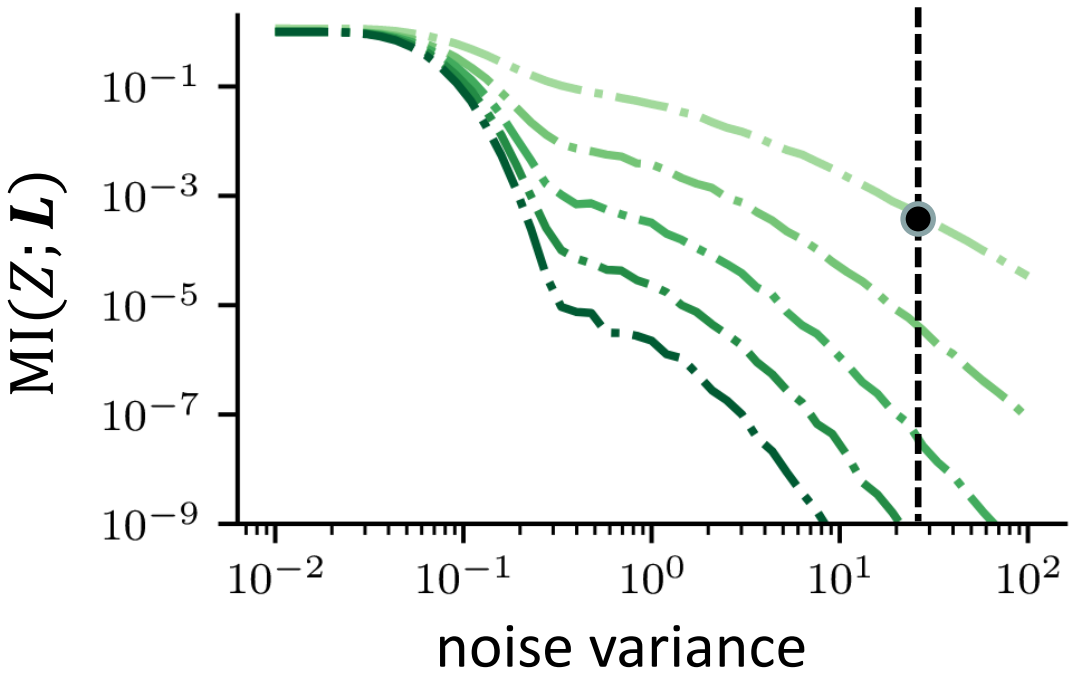


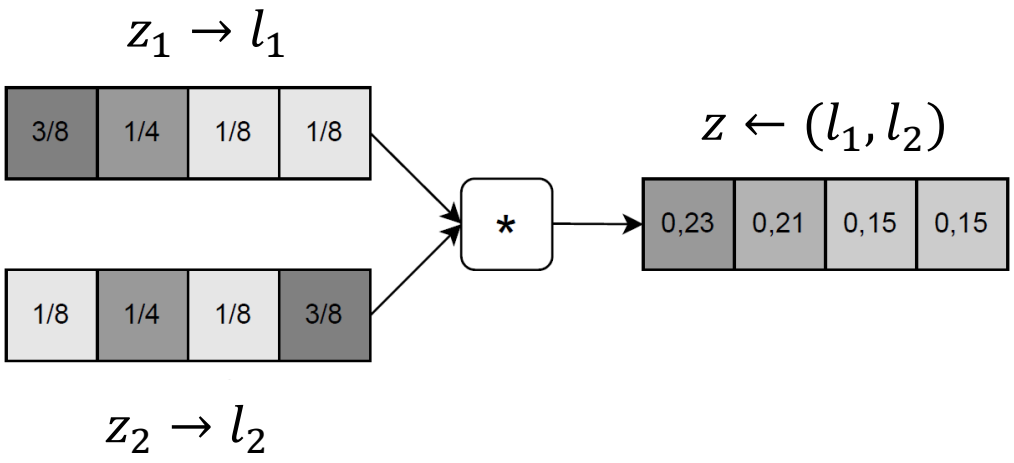


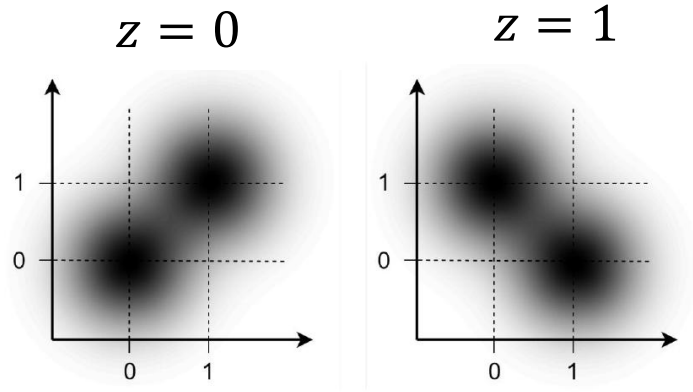


Boolean masking with noise: OK

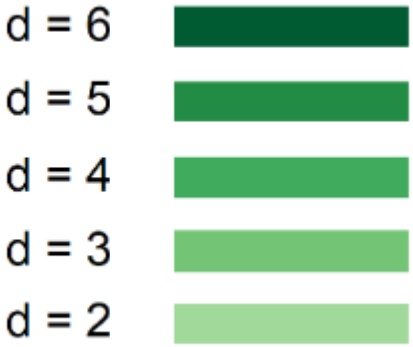


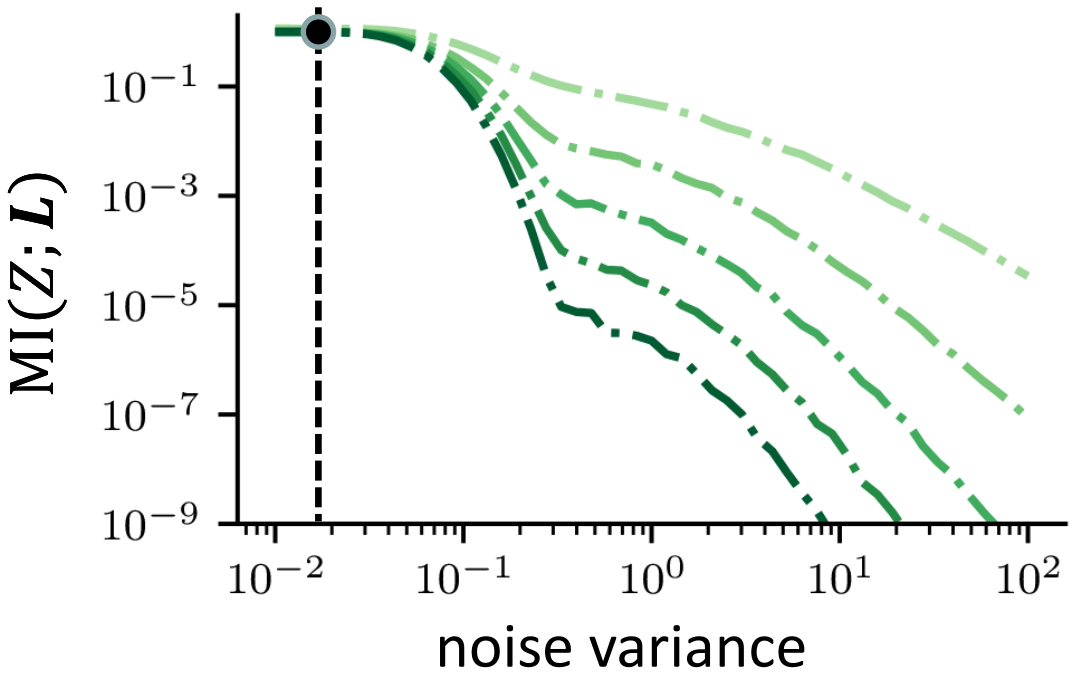


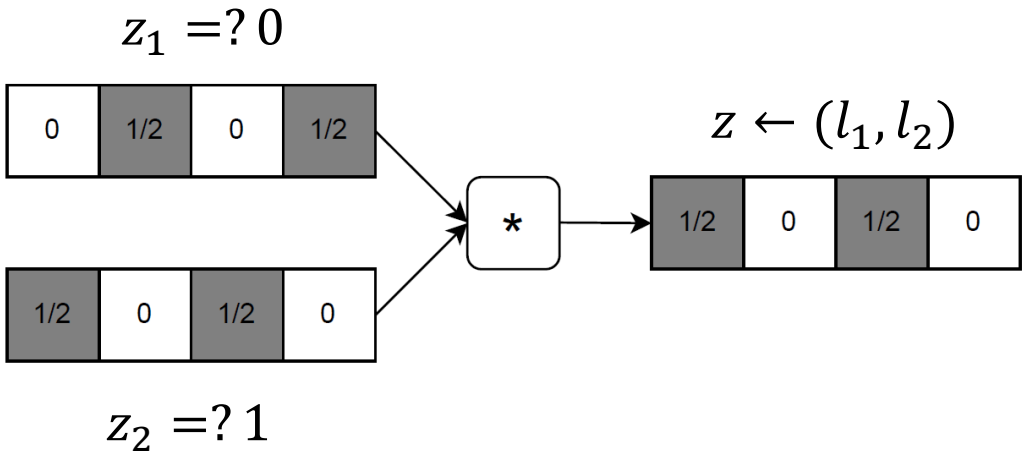


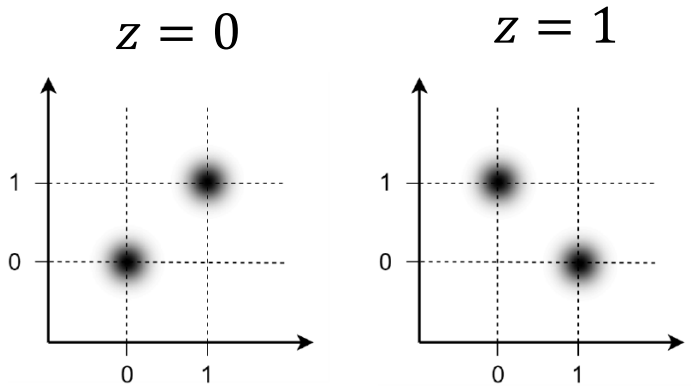


Boolean masking without noise: not OK



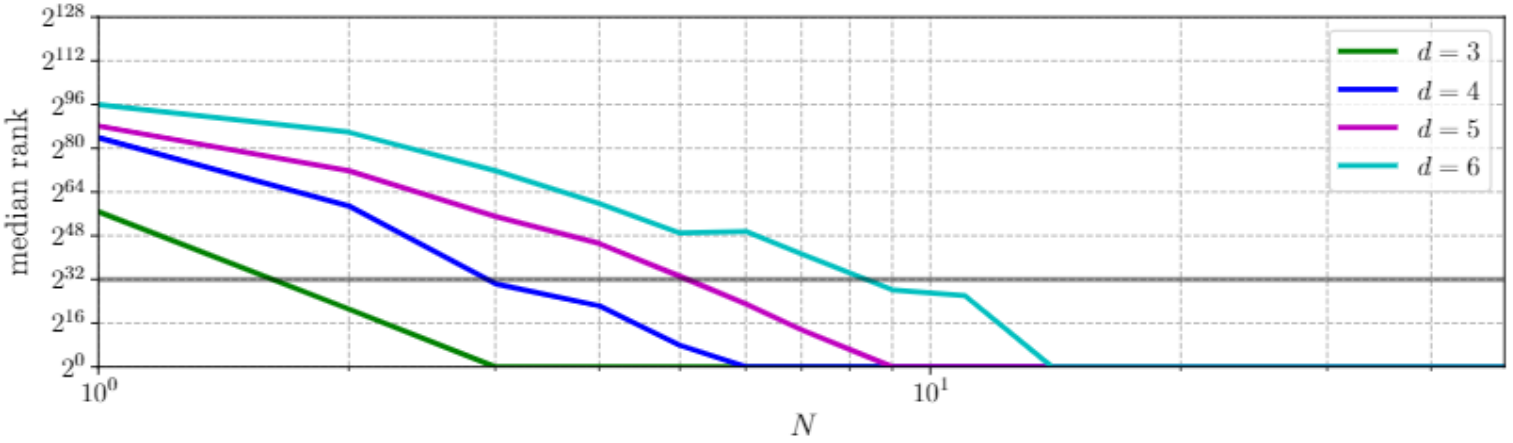




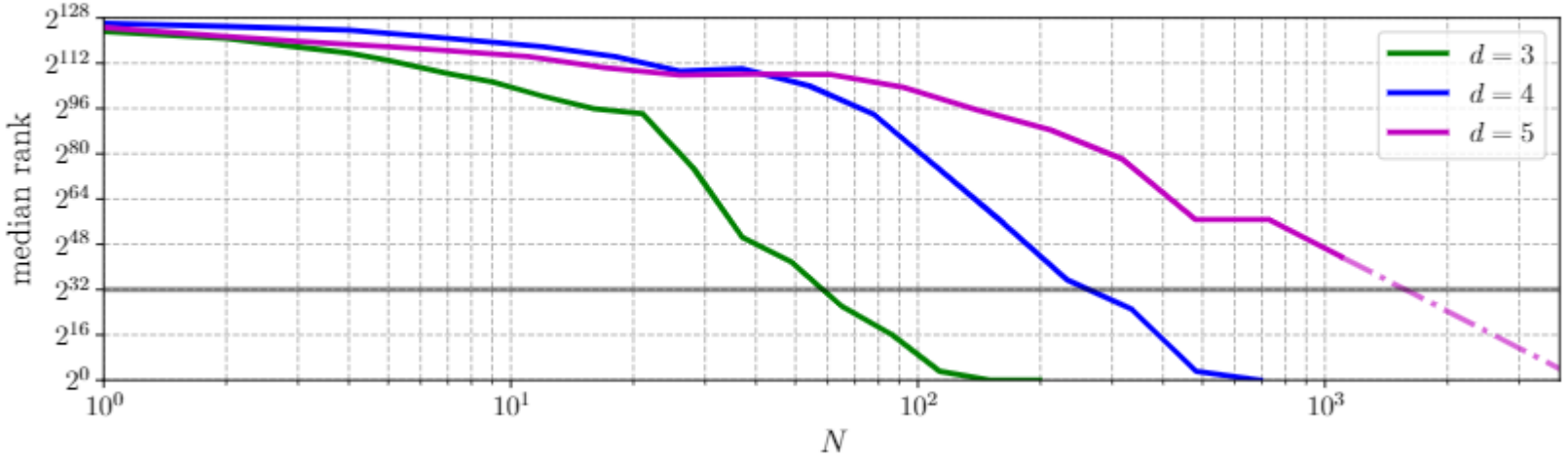


Noise issue in practice

- Masked bitslice AES implementation
  - ARM Cortex-M0



  - ARM Cortex-M3



Outline

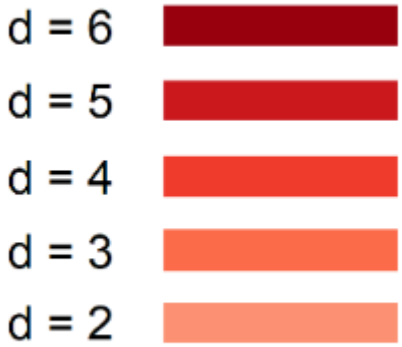
- Background & problem statement
  - Side-channel attacks & Boolean masking
  - Masking-friendly ciphers
  - Leakage-resistant modes of operation

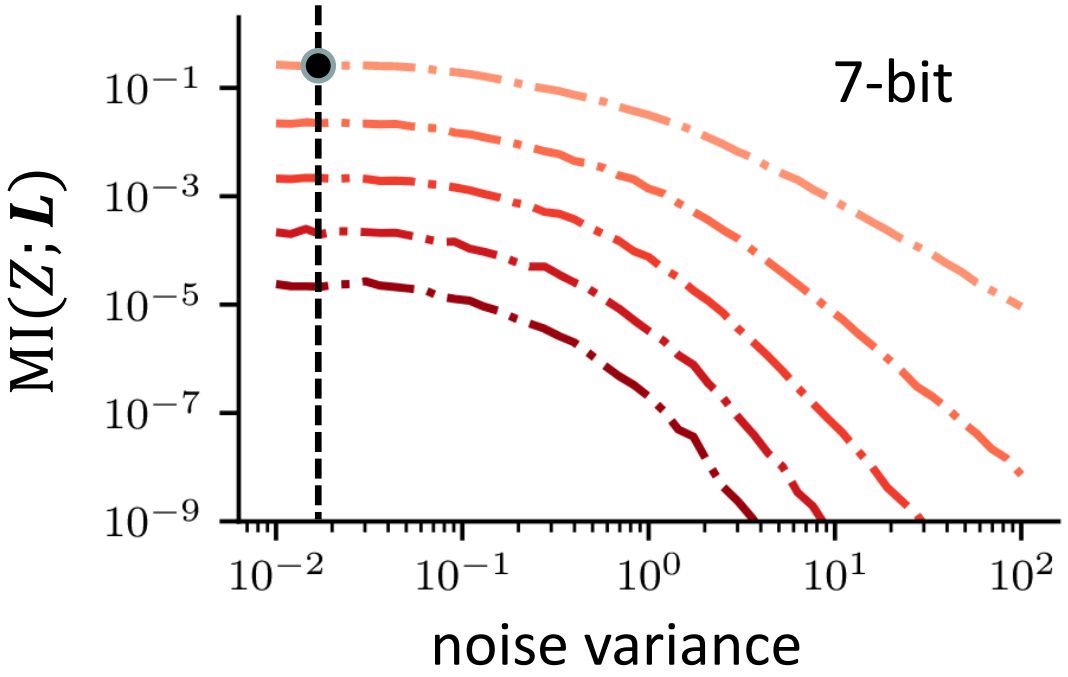
  ⇒ The (lack of) implementation noise issue

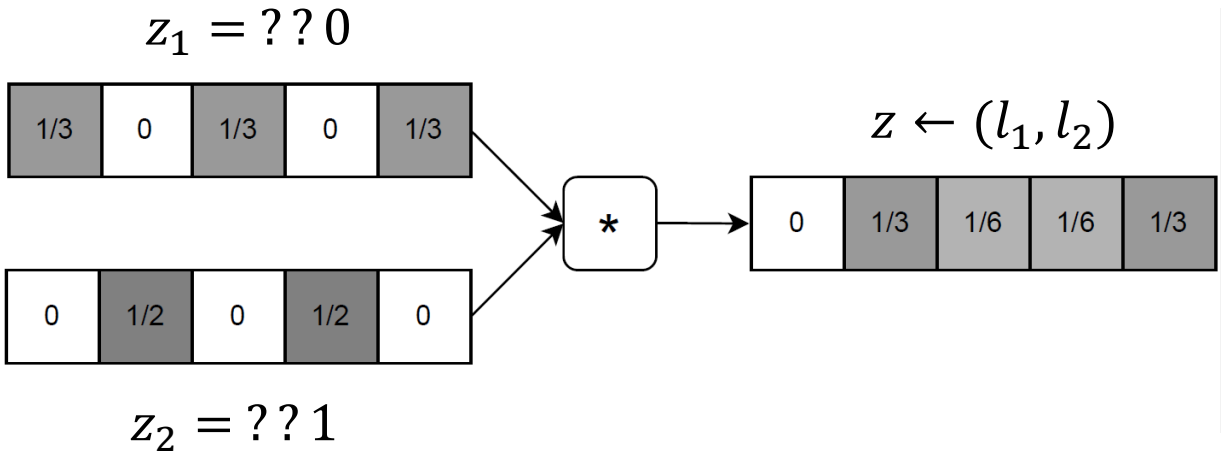
- Prime field masking (and cipher design)

- Re-keying: hard physical learning problems

Prime masking without noise: better

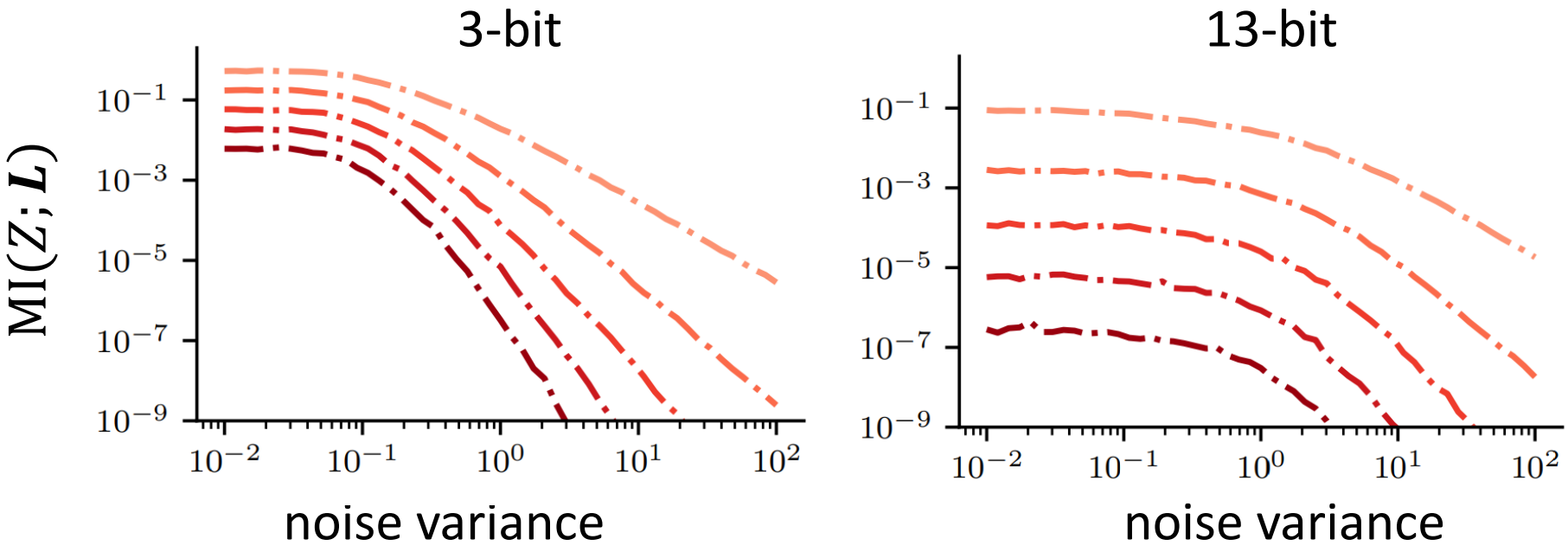






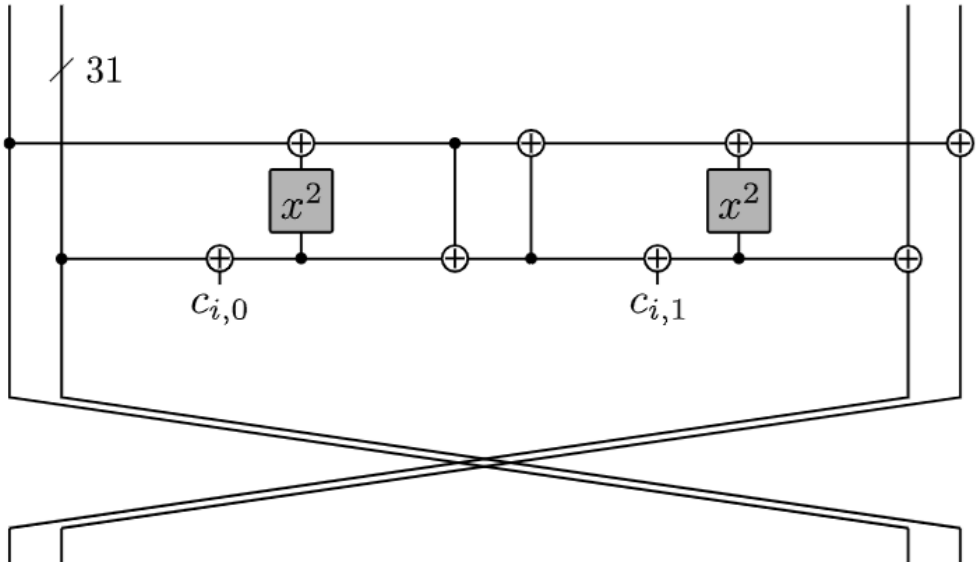
Cost vs. security tradeoff

- Increasing the field size (sometimes) helps
  - Example for Hamming weight leakages
  - And Mersenne primes for efficiency



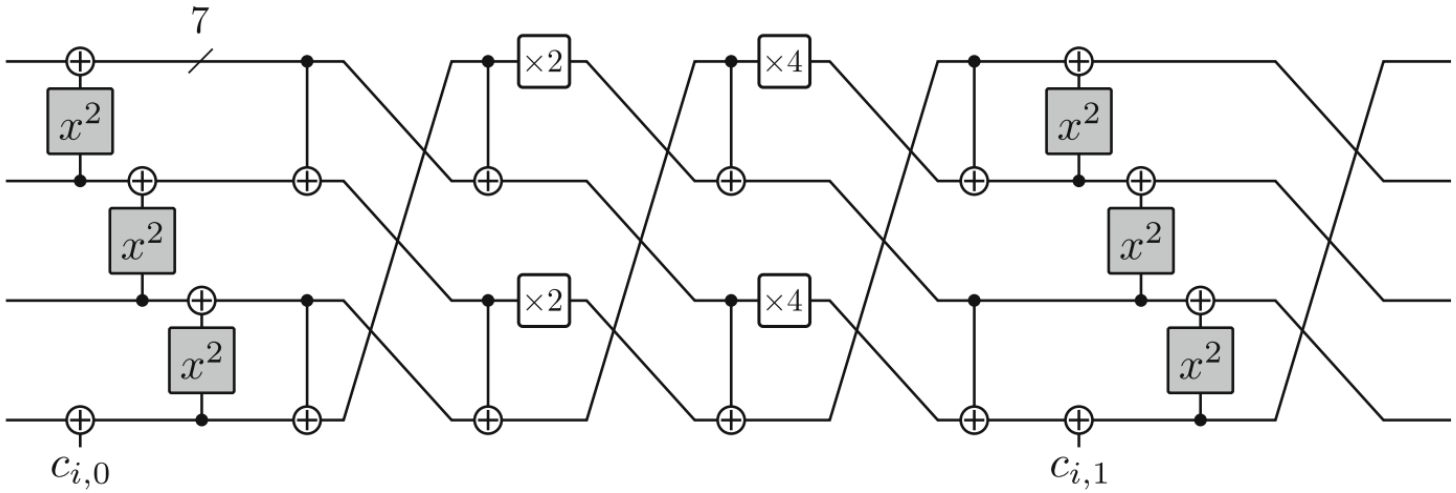
Challenge #1: cipher design & analysis

- Need ciphers mod *p* with low mult. complexity
- Cheapest non-linear power map: square
  - Easier to mask (than mult.), but non-bijective
- First attempt: Feistel for Prime Masking (FPM)
  - Example: mid-pSquare (software) 31-bit square

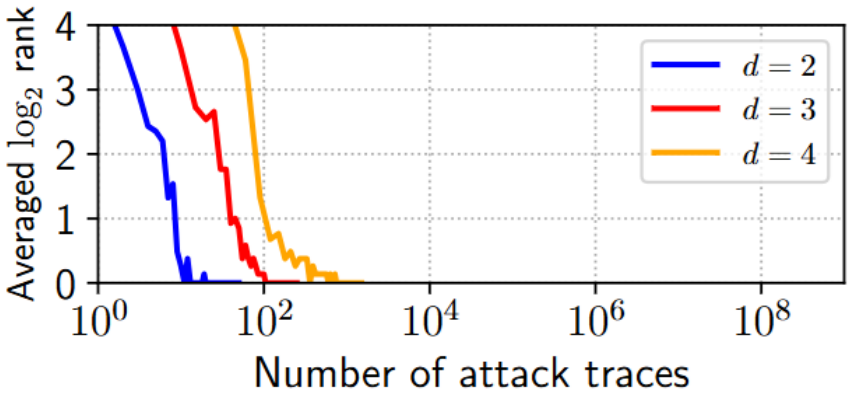


Challenge #1: cipher design & analysis

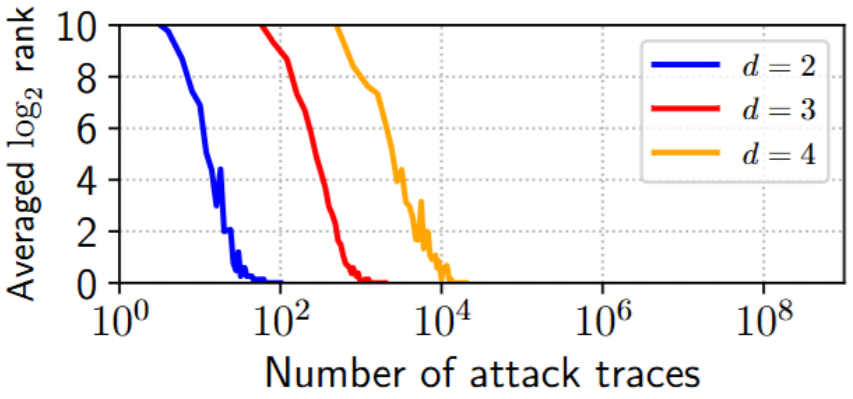
- Need ciphers mod *p* with low mult. complexity
- Cheapest non-linear power map: square
  - Easier to mask (than mult.), but non-bijective
- First attempt: Feistel for Prime Masking (FPM)
  - Example: mid-pSquare (software) 31-bit square



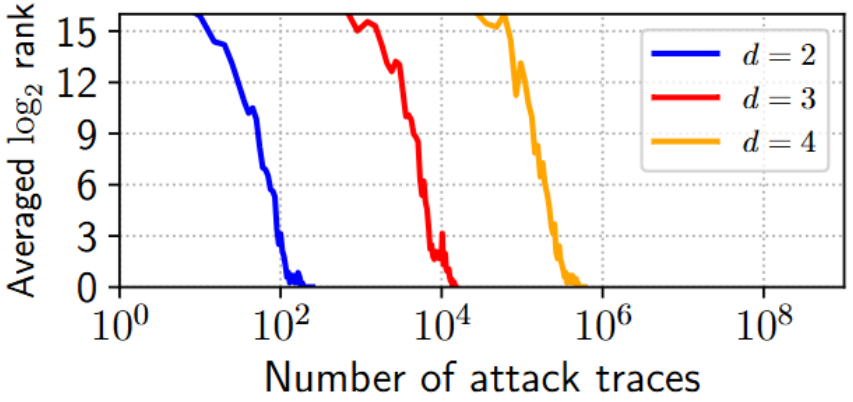
Side-channel security (mid-pSquare, software)



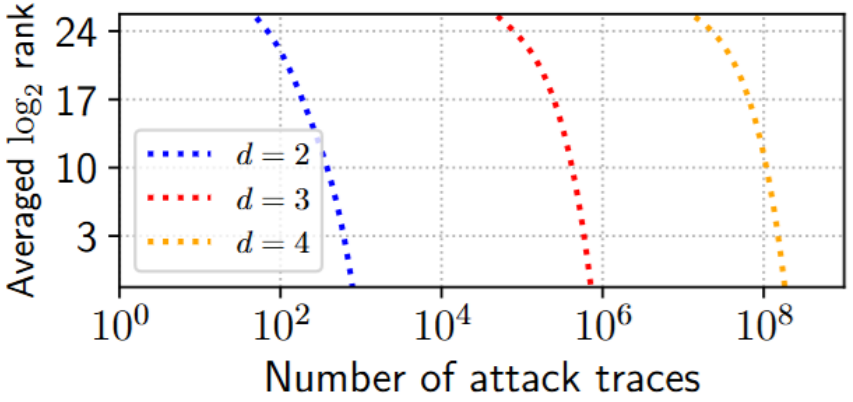
(a) $p = 2^7 - 1$



(b) $p = 2^{13} - 1$



(c) $p = 2^{19} - 1$



(d) $p = 2^{31} - 1$

- Security of binary ciphers ≈ small primes

Performances (Cortex-M4)

Primitive		$d=1$	$d=2$		$d=4$		$d=8$		$d=16$		$d=32$	
			TRNG		TRNG		TRNG		TRNG		TRNG	
			off	on	off	on	off	on	off	on	off	on
SKINNY-128-128	E	6.9k	17.7k	20.0k	62.9k	77.9k	186.2k	244.6k	830.8k	1.11M	2.56M	3.86M
	D	6.9k	17.8k	20.4k	63.5k	78.5k	188.0k	246.4k	790.2k	1.07M	2.56M	3.86M
small-pSquare $\tau=0$	E	10.3k	35.1k	56.4k	110.0k	227.0k	557.2k	1.01M	1.91M	3.92M	7.03M	15.4M
	D	10.8k	35.9k	57.4k	108.8k	227.5k	557.0k	1.00M	1.95M	3.92M	7.05M	15.4M
mid-pSquare $\tau=0$	E	2.9k	11.0k	14.1k	30.8k	55.4k	165.9k	263.2k	574.4k	990.0k	2.08M	3.84M
	D	2.9k	10.8k	14.0k	31.4k	55.3k	163.7k	258.3k	579.5k	992.9k	2.16M	3.82M
SKINNY-128-256	E	8.4k	21.3k	24.1k	75.8k	93.8k	223.6k	293.6k	996.8k	1.33M	3.06M	4.63M
	D	8.4k	21.4k	24.6k	76.4k	94.4k	225.7k	295.8k	954.5k	1.29M	3.06M	4.63M
small-pSquare $\tau=1$	E	23.6k	67.6k	102.5k	197.3k	405.9k	988.9k	1.80M	3.43M	6.97M	12.7M	27.5M
	D	24.8k	69.1k	106.0k	199.7k	409.5k	990.1k	1.80M	3.45M	6.95M	12.5M	27.5M
mid-pSquare $\tau=1$	E	5.1k	14.5k	17.7k	37.7k	63.2k	189.5k	300.8k	653.9k	1.14M	2.38M	4.36M
	D	5.1k	13.9k	18.2k	37.6k	65.1k	187.1k	299.3k	668.4k	1.13M	2.46M	4.36M
SKINNY-128-384	E	10.4k	25.4k	28.7k	89.1k	110.2k	261.4k	343.1k	1.16M	1.55M	3.57M	5.41M
	D	10.3k	25.5k	29.2k	89.8k	110.9k	263.9k	345.6k	1.10M	1.49M	3.57M	5.41M
small-pSquare $\tau=2$	E	30.7k	88.6k	135.2k	258.4k	532.2k	1.30M	2.36M	4.50M	9.15M	16.6M	36.1M
	D	32.1k	90.2k	138.6k	261.5k	537.0k	1.30M	2.34M	4.53M	9.12M	16.4M	36.1M
mid-pSquare $\tau=2$	E	7.4k	17.5k	22.4k	44.5k	73.3k	215.6k	340.4k	753.3k	1.28M	2.77M	4.92M
	D	7.3k	17.6k	22.2k	44.6k	72.8k	216.4k	337.2k	744.2k	1.28M	2.67M	4.92M

The GEMS slide

- Unprotected mid-pSquare fast in software
- Masking ⇒ square as only non-linear operation
  - Algebraic attacks set the # of rounds of mid-pSquare
  - Implies dealing with a non-bijective mapping
- Side observation: ∃ bit permutations that have high algebraic degree and are bijective in $\mathbb{F}_p$
  - Only used in the mid-pSquare's tweak schedule
- ***For GPUs: SPNs with mid-size Mersennes primes (or even 61- or 127-bit primes), using bijective power maps & bit-level operations ?***

Intermediate conclusions & challenges

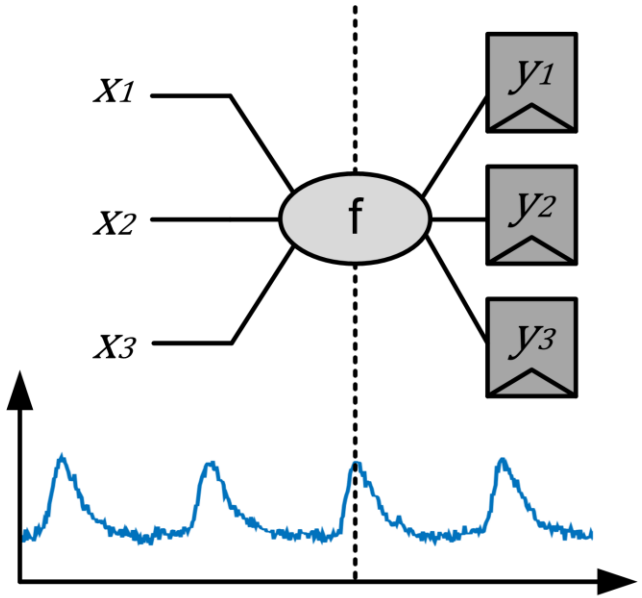
- FHE/MPC: primarily cost-driven optimizations
- Leakage: algebraic structure impacts security
  - Cost-driven optimizations come as a bonus

Intermediate conclusions & challenges

- FHE/MPC: primarily cost-driven optimizations
- Leakage: algebraic structure impacts security
  - Cost-driven optimizations come as a bonus
- First cipher designs (to show conceptual feasibility)
  - *Need more mathematical cryptanalysis*
    - There are good margins to cover improvements
  - *Need more (further optimized) cipher designs?*
  - *Is full-key security a meaningful goal?*
- *Need to formally understand prime masking*
  - And to compare with more complex encodings
- *Need to concretely analyze large (32-bit) models*

Going further?

- Lower noise but complexity still ≈ quadratic in *d*
- Physical defaults “recombining” the shares



$$L = f(x_1, x_2, x_3) + N$$

- Addressed if we only mask linear operations!

Outline

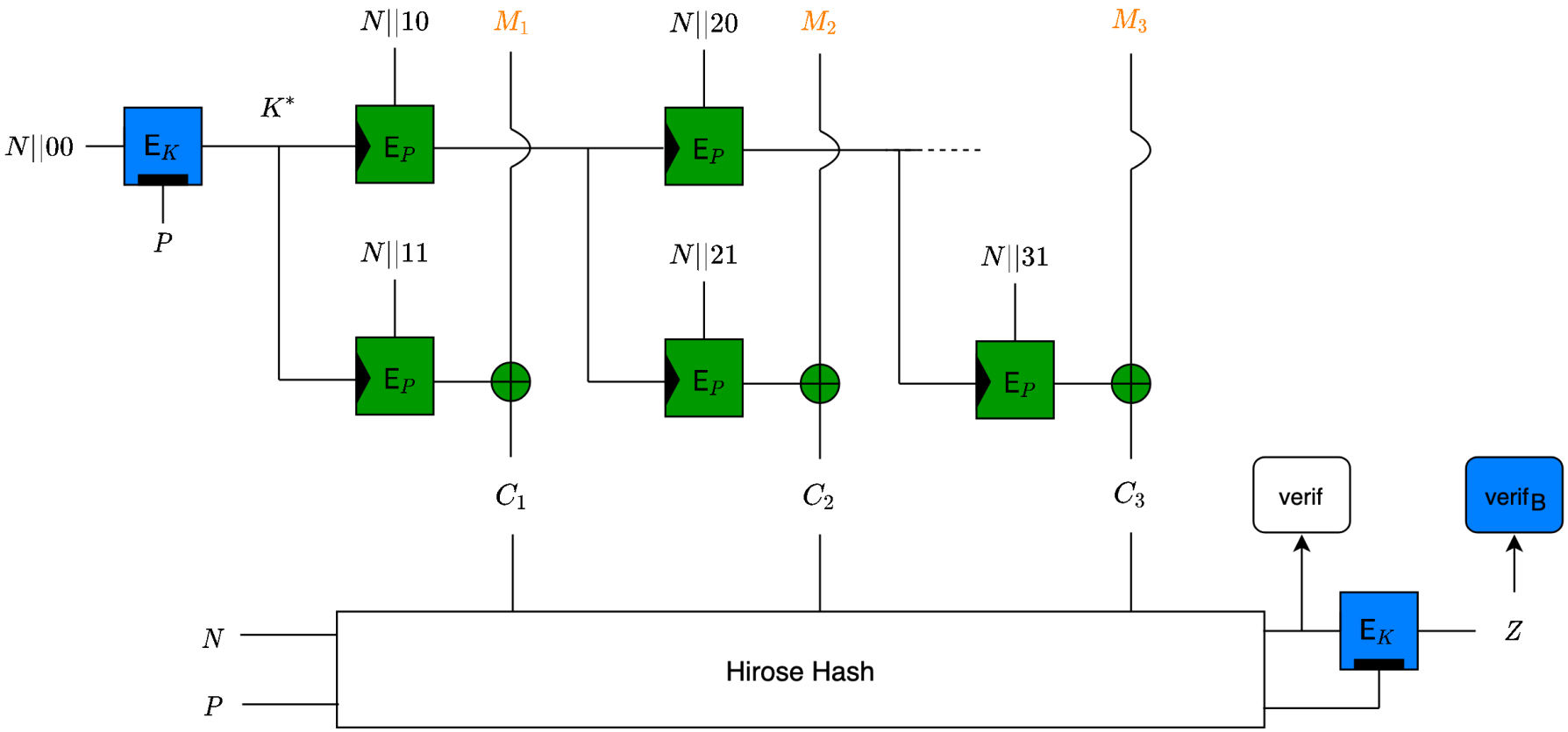
- Background & problem statement
  - Side-channel attacks & Boolean masking
  - Masking-friendly ciphers
  - Leakage-resistant modes of operation

  ⇒ The (lack of) implementation noise issue

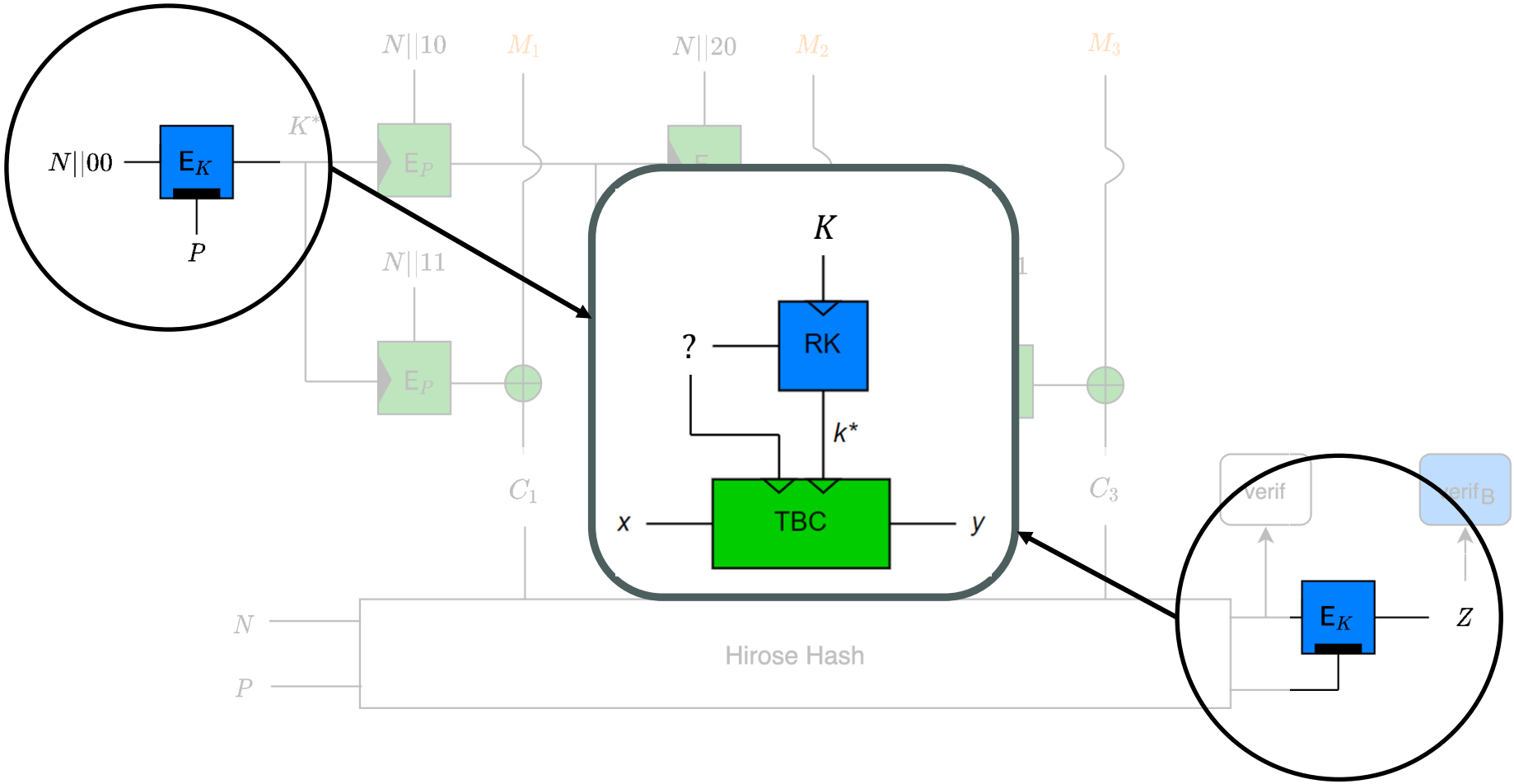
- Prime field masking (and cipher design)

- Re-keying: hard physical learning problems

TEDT, revisited

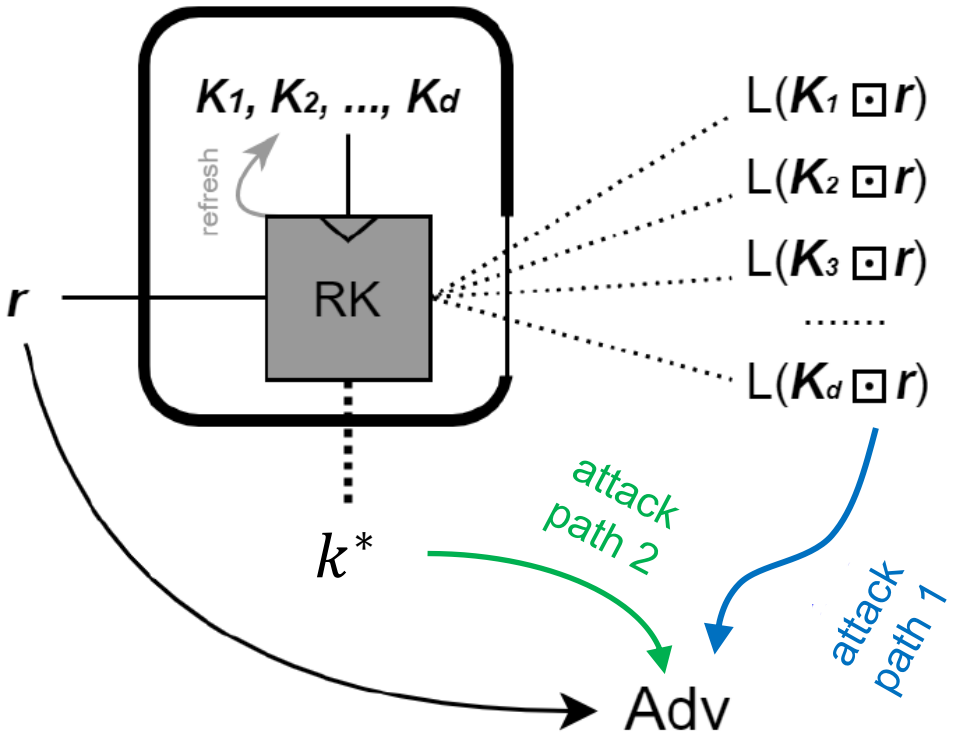


TEDT, revisited



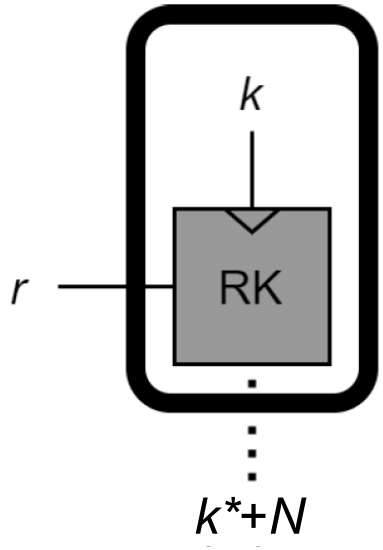
- RK: key-homomorphic re-keying (e.g. mult.)

Security requirements



- Avoiding attack path #1 is well understood
- Avoiding attack path #2 much less (≠ models)

Model 1: Medwed et al. 2010



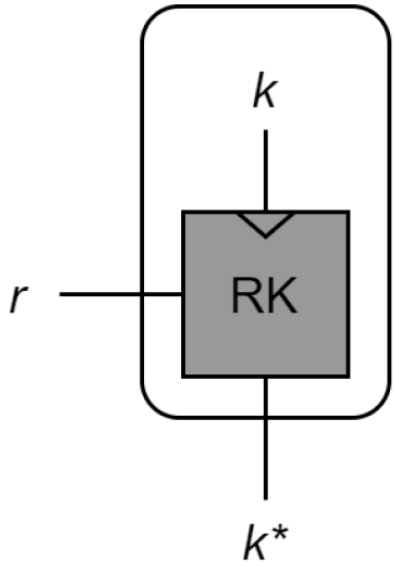
- Started from a concrete instance
  - $k^* = r \cdot k$ over $\mathbb{F}_{2^\kappa}$
- Insecure w/o noise

$\Rightarrow$ Noisy leakage model only

- Beware of decryption leakages!

- Somewhat similar to Boolean masking
  - LSB of Hamming weight = linear equation of *k* bits
- Formally: "Learning Parity with Leakage" (LPL) in $\mathbb{F}_2$
  - Security reduction from LPL to standard LPN

Model 2: Dziembowski et al. 2016



- Unbounded leakages on k^*
- Proposed instance (wPRF)
  - $k^* = \lfloor \langle r, k \rangle \rceil_p$, with $k, r \in \mathbb{Z}_{2^q}^n$
  - Nearly key-homomorphic

$\Rightarrow$ Needs $\log(d)$ bits of error correction

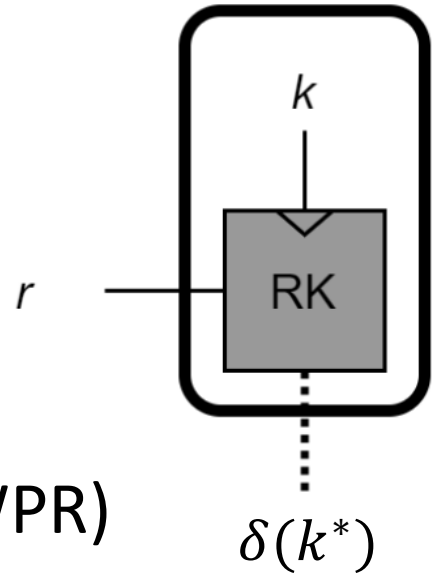
- Significantly larger key requirements
  - Worse performances in software (& hardware?)
  - Despite nearly linear masking overheads

Model 3: Duval et al. 2021

- Noise-free (compressive) leakages
- Similar to "crypto dark matter"
  - $\mathrm{F}_K(r) = \mathrm{map}(r \cdot K)$

  ≈ security by combining different fields
- But assumes a physical mapping δ

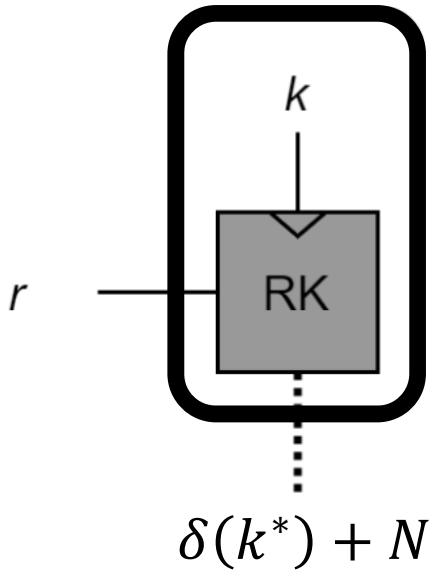
  ⇒ Learning With Physical Rounding (LWPR)



- *Interest for re-keying (vs. wPRF):* δ never has to be computed (& masked) explicitly by the leaking device, physics does it. *Challenge:* δ *(e.g., HW) is not controlled by the designer*

Model 4: Hoffmann et al. 2026

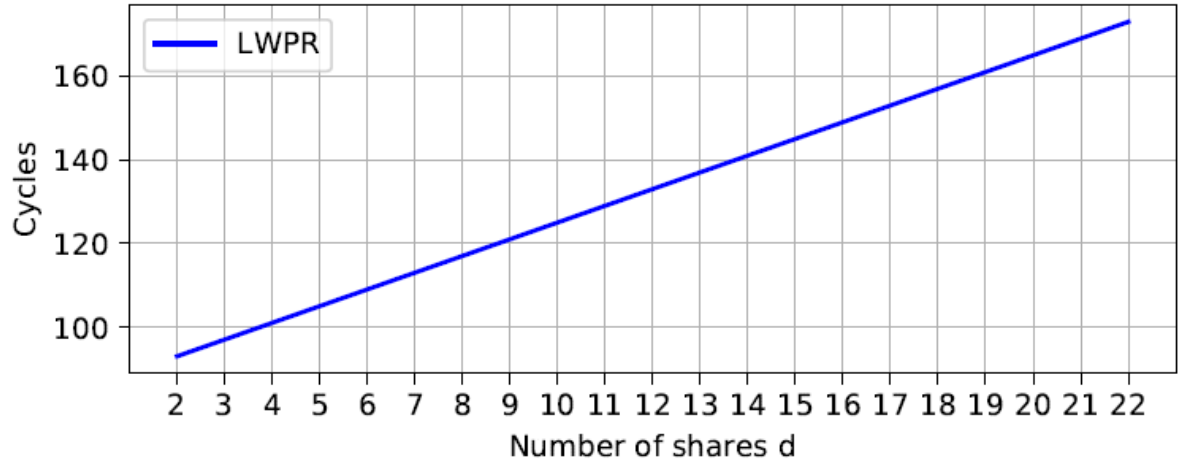
- Same with physical noise
  - Learning With Physical Rounding & Noise (LWPRN)
- Beware of decryption leakages!

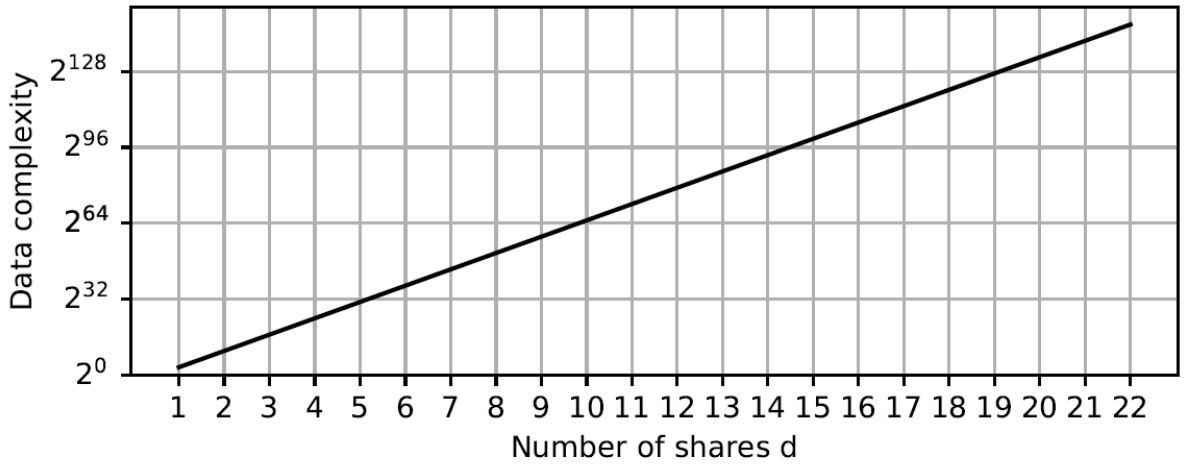


- One could also define “Learning with Physical Noise” only (LWPN) ≈ LPL in large fields
  - Which also corresponds to LWPRN with δ(.)=Id(.)
- Less realistic (& requires more noise than LWPRN)

High risk / high gain

- 128-bit FPGA implementation





Intermediate conclusions & challenges

- Deterministic version: LWPR
  - Only cryptanalysis results so far (mostly algebraic)
  - Requires parallelism and prime fields

$\Rightarrow$ *Challenge: reduction to standard learning problems*

- Noisy versions: LPL, LWPRN
  - Reductions from LPN and LWE ($\approx$ noise flooding)
  - Tolerates binary fields/rings, serial implem.

$\Rightarrow$ *Challenge: cryptanalysis (& improved reductions)*

- Rich intersection: computational vs. statistical arguments, lattices vs. symmetric cryptanalysis

General conclusions

- The reduced “compatibility” between physical leakages and prime computations is a source of improved security for masking & re-keying
- Leakage in symmetric crypto mostly drove
  - Bitslice primitives with low AND complexity
  - Modes of operation for leveled implementations
- Should also drive new (prime) ciphers & the integration of hard physical learning problems in modes of operation (with the same primes?)
- Both have application in PQ asymmetric crypto!

THANKS!

https://perso.uclouvain.be/fstandae/

Brieuc Balon, Gianluca Brian, Gaëtan Cassiers, Sebastian Faust, Lorenzo Grassi, Clément Hoffmann, Loïc Masure, Pierrick Méaux, Elena Micheli, Thorben Moos, Maximilian Orlt, Emeline Repel, Mélissa Rossi, Adeline Roux-Langlois, …

References (I)

- On prime field masking (encodings, gadgets)
  - Stefan Dziembowski, Sebastian Faust, Maciej Skórski: *Optimal Amplification of Noisy Leakages.* TCC (A2) 2016: 291-318
  - Gaëtan Cassiers, Loïc Masure, Charles Momin, Thorben Moos, François-Xavier Standaert: *Prime-Field Masking in Hardware and its Soundness against Low-Noise SCA Attacks.* IACR Trans. Cryptogr. Hardw. Embed. Syst. 2023(2): 482-518 (2023)
  - Sebastian Faust, Loïc Masure, Elena Micheli, Maximilian Orlt, François-Xavier Standaert: *Connecting Leakage-Resilient Secret Sharing to Practice: Scaling Trends and Physical Dependencies of Prime Field Masking.* EUROCRYPT (4) 2024: 316-344
  - Thorben Moos, Sayandeep Saha, François-Xavier Standaert: *Prime Masking vs. Faults - Exponential Security Amplification against Selected Classes of Attacks.* IACR Trans. Cryptogr. Hardw. Embed. Syst. 2024(4): 690-736 (2024)

References (II)

- On prime ciphers (design and cryptanalysis)
  - Loïc Masure, Pierrick Méaux, Thorben Moos, François-Xavier Standaert: *Effective and Efficient Masking with Low Noise Using Small-Mersenne-Prime Ciphers*. EUROCRYPT (4) 2023: 596-627
  - Lorenzo Grassi, Loïc Masure, Pierrick Méaux, Thorben Moos, François-Xavier Standaert: *Generalized Feistel Ciphers for Efficient Prime Field Masking*. EUROCRYPT (3) 2024: 188-220
  - Brieuc Balon, Lorenzo Grassi, Pierrick Méaux, Thorben Moos, François-Xavier Standaert, Matthias Johann Steiner: *mid-pSquare: Leveraging the Strong Side-Channel Security of Prime-Field Masking in Software*. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2025(4): 486-519 (2025)
  - Tim Beyne, Michiel Verbauwhede: *Integral Cryptanalysis in Characteristic p*. ASIACRYPT (1) 2025: 66-96

References (III)

- On hard physical learning problems
  - Stefan Dziembowski, Sebastian Faust, Gottfried Herold, Anthony Journault, Daniel Masny, François-Xavier Standaert: Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems. CRYPTO (2) 2016: 272-301
  - Sébastien Duval, Pierrick Méaux, Charles Momin, François-Xavier Standaert: *Exploring Crypto-Physical Dark Matter and Learning with Physical Rounding Towards Secure and Efficient Fresh Re-Keying*. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2021(1): 373-401 (2021)
  - Clément Hoffmann, Pierrick Méaux, Charles Momin, Yann Rotella, François-Xavier Standaert, Balazs Udvarhelyi: *Learning with Physical Rounding for Linear and Quadratic Leakage Functions.* CRYPTO (3) 2023: 410-439
  - Clément Hoffmann, Emeline Repel, Adeline Roux-Langlois, François-Xavier Standaert: *Hardness of Learning with Physical Rounding and Noise from Learning With Errors. To appear in* IACR Trans. Cryptogr. Hardw. Embed. Syst. 2026(3)