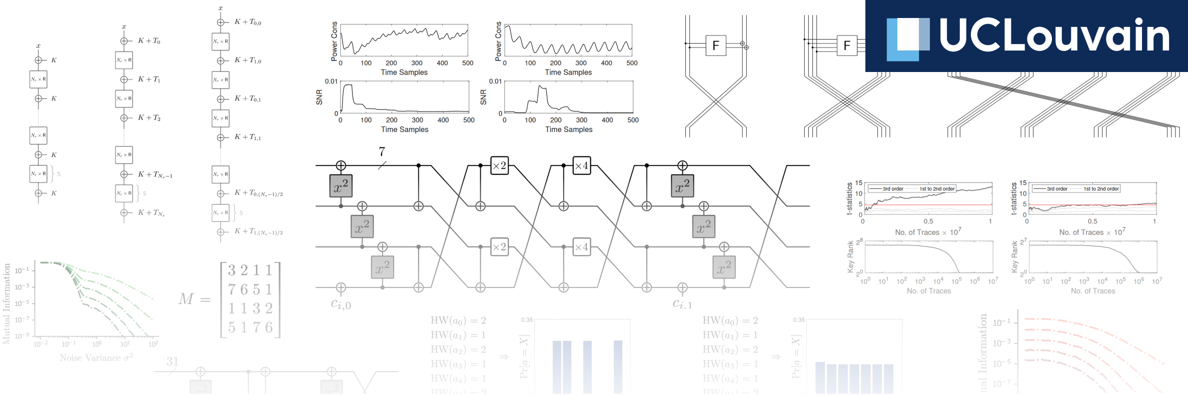


UCLouvain

UCLouvain Institute of Information and Communication Technologies, Electronics and Applied Mathematics (ICTEAM)

Generalized Feistel Ciphers for Efficient Prime Field Masking

Lorenzo Grassi, Loïc Masure, Pierrick Méaux, Thorben Moos, François-Xavier Standaert

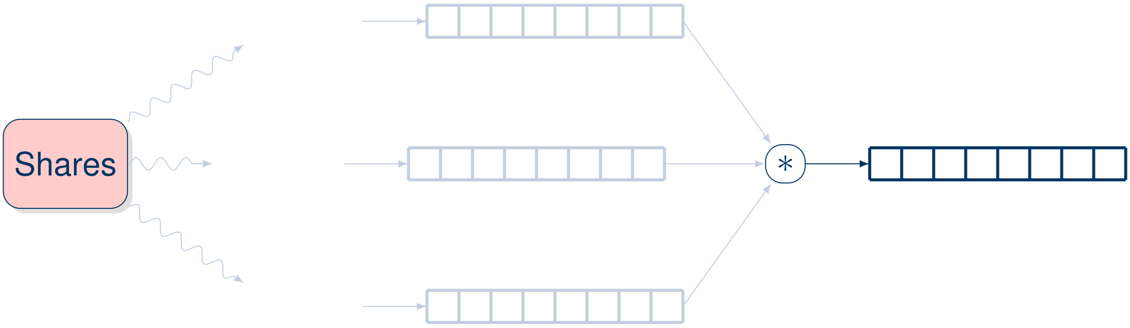
Ruhr University Bochum; University Montpellier, CNRS; Luxembourg University; UCLouvain

May 30th, 2024

European Research Council

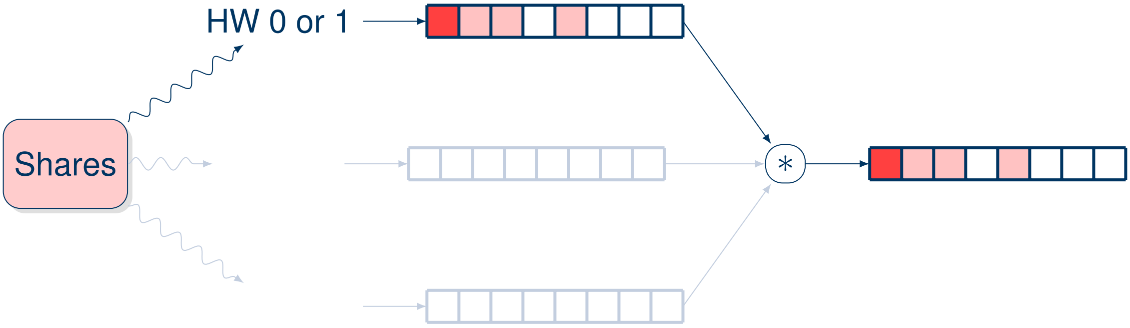
The Power of Masking

Adversaries Make Imprecise Observations, Masking Amplifies Imprecision:



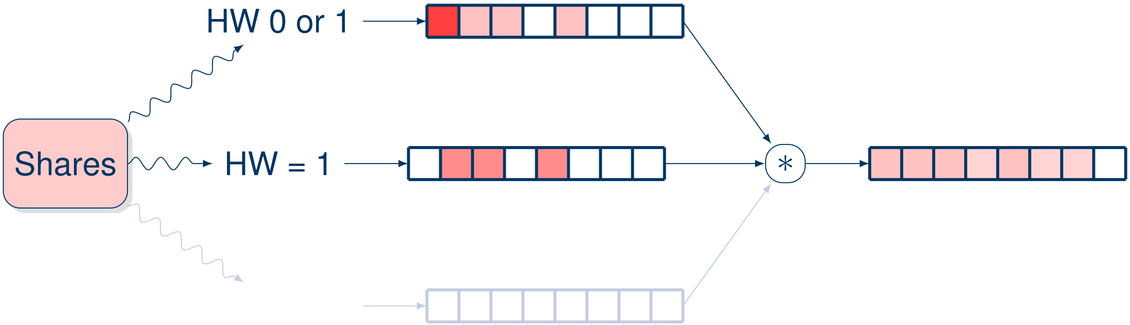
The Power of Masking

Adversaries Make Imprecise Observations, Masking Amplifies Imprecision:



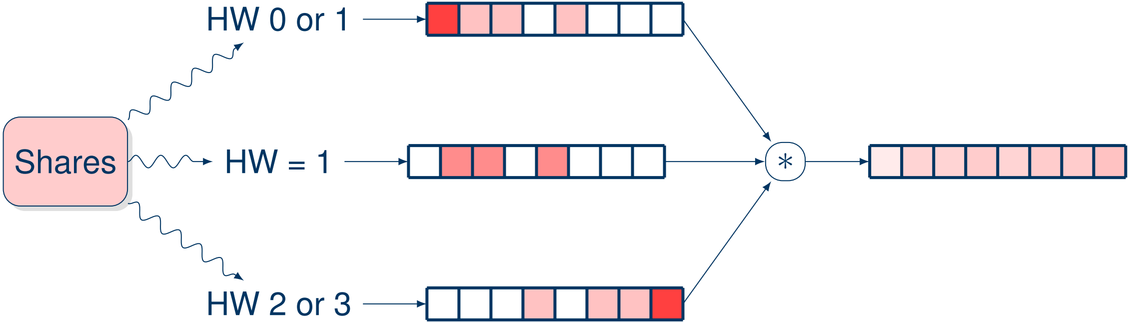
The Power of Masking

Adversaries Make Imprecise Observations, Masking Amplifies Imprecision:

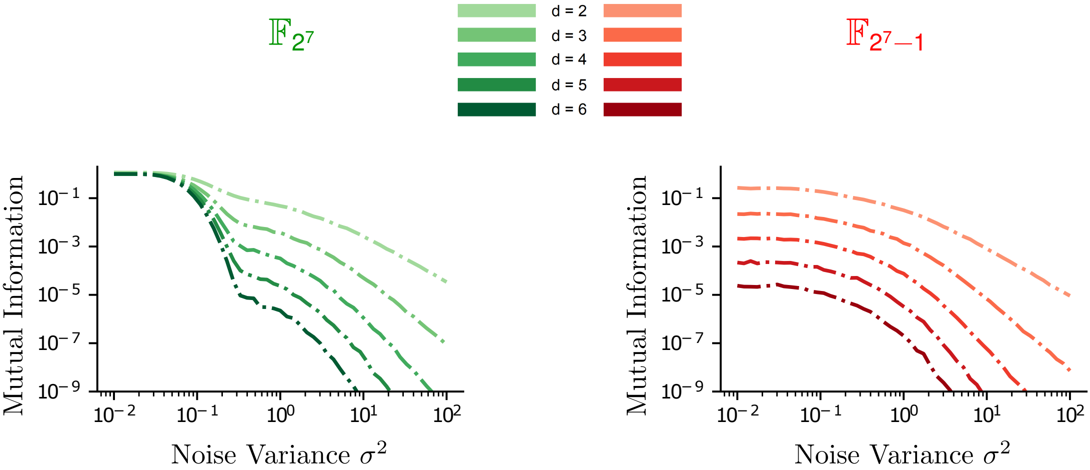


The Power of Masking

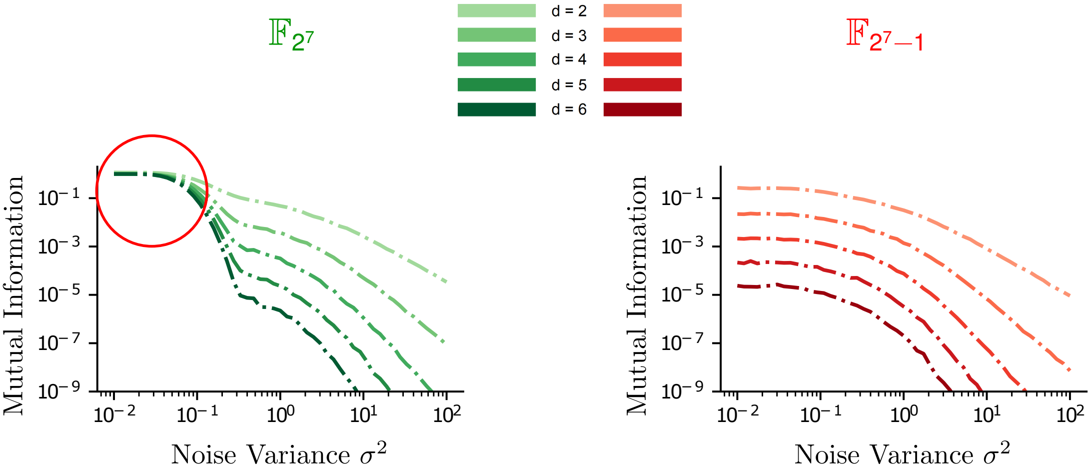
Adversaries Make Imprecise Observations, Masking Amplifies Imprecision:



Always Reliable? Boolean vs. Prime-Field Masking



Always Reliable? Boolean vs. Prime-Field Masking



What Went Wrong?

Noise-Free Hamming Weight Leakage:

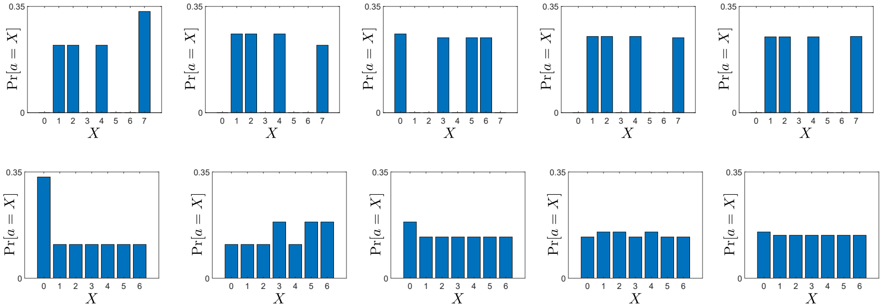
$\mathrm{HW}(a_0) = 2$ $\mathrm{HW}(a_1) = 1$	$\mathrm{HW}(a_0) = 2$ $\mathrm{HW}(a_1) = 1$ $\mathrm{HW}(a_2) = 2$	$\mathrm{HW}(a_0) = 2$ $\mathrm{HW}(a_1) = 1$ $\mathrm{HW}(a_2) = 2$ $\mathrm{HW}(a_3) = 1$	$\mathrm{HW}(a_0) = 2$ $\mathrm{HW}(a_1) = 1$ $\mathrm{HW}(a_2) = 2$ $\mathrm{HW}(a_3) = 1$ $\mathrm{HW}(a_4) = 1$	$\mathrm{HW}(a_0) = 2$ $\mathrm{HW}(a_1) = 1$ $\mathrm{HW}(a_2) = 2$ $\mathrm{HW}(a_3) = 1$ $\mathrm{HW}(a_4) = 1$ $\mathrm{HW}(a_5) = 2$

$\mathbb{F}_{2^3}$

$a = a_0 \oplus \ldots \oplus a_{d-1}$

$\mathbb{F}_{2^3-1}$

$a = a_0 + \ldots + a_{d-1} \bmod 7$



State of the Art

- Dziembowski et al., TCC 2016 [1]:
  - Masking in groups of prime order can amplify arbitrarily low noise levels (lack of subgroups)
  - Exponential security in the number of shares in presence of any non-injective leakage function
- Masure et al., Eurocrypt 2023 [2]:
  - Information theoretic evaluation of the properties of prime-field masking under common leakage models such as Hamming weight and bit leakage + first practical results
  - Toy AES-prime cipher based on a small Mersenne-prime and a bijective power map as S-box
- Cassiers et al., TCHES 2023 [3]:
  - Efficient arbitrary-order composable masked gadgets for *squaring*, half as costly as multipl.
- Faust et al., Eurocrypt 2024 [4]:
  - For Hamming-weight-like leakage functions, security of prime-field masking is $\approx \log(p)^d$

[1] Dziembowski, Faust and Skórski, Optimal Amplification of Noisy Leakages, TCC 2016
[2] Masure, Méaux, Moos and Standaert, Effective and Efficient Masking with Low Noise using Small-Mersenne-Prime Ciphers, Eurocrypt 2023
[3] Cassiers, Masure, Momin, Moos and Standaert, Prime-Field Masking in Hardware and its Soundness against Low-Noise SCA Attacks, TCHES 2023
[4] Faust et al, Connecting Leakage-Resilient Secret Sharing to Practice: Scaling Trends and Physical Dependencies of Prime Field Masking, Eurocrypt 2024

This work

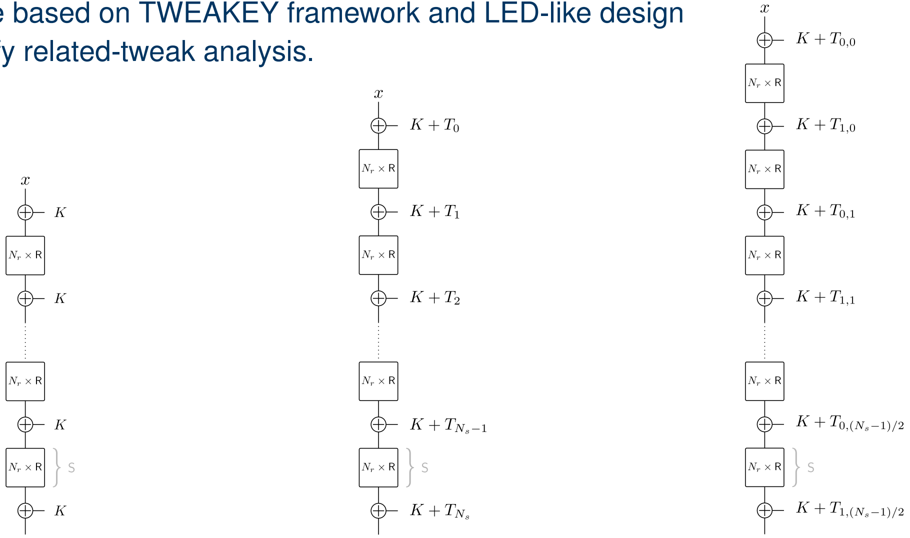
Missing so far? An efficient lightweight cryptographic primitive to demonstrate relevance and further study the potential advantages of prime-field masking.

We address this by

1. introducing the FPM (Feistel for Prime Masking) family of tweakable block ciphers based on a generalized Feistel structure
2. proposing a first instantiation of FPM which we denote as small $-$ pSquare
3. comparing small $-$ pSquare to $\texttt{SKINNY}$ in terms of efficiency vs. security tradeoff

A new Family of Tweakable Block Ciphers: FPM_τ

Structure based on TWEAKEY framework and LED-like design to simplify related-tweak analysis.

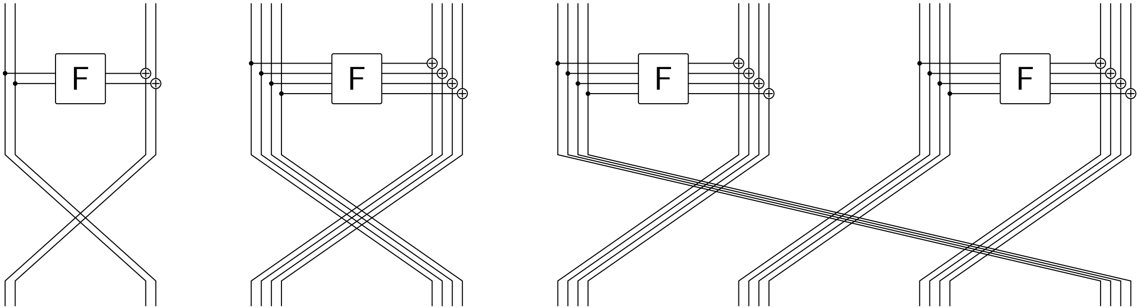


(a) FPM_0 (b) FPM_1 (c) FPM_2

Rounds R of FPM$_\tau$

Type-II generalized Feistel to obtain tweakable block ciphers with cheap/efficient inverses.

Defined by $b \cdot c$ where b is the number of branches and c the field elements per branch.



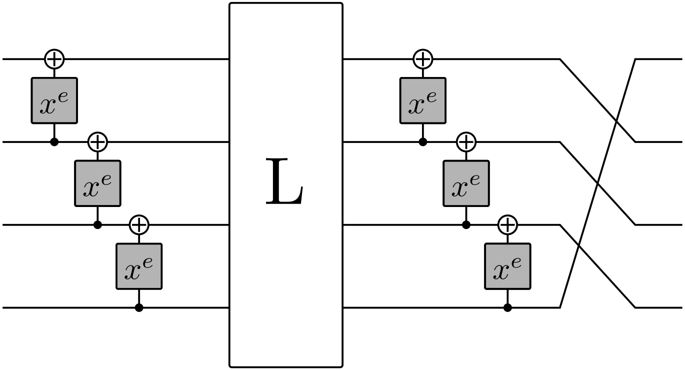
(a) 2×2 (b) 2×4 (c) 4×4

F-function of FPM$_\tau$

F-function with two layers of non-linear power maps via Type-III generalized Feistel.

MDS matrix multiplication as linear layer in the middle.

F shall be bijective (to avoid collisions) and provide full non-linear diffusion.

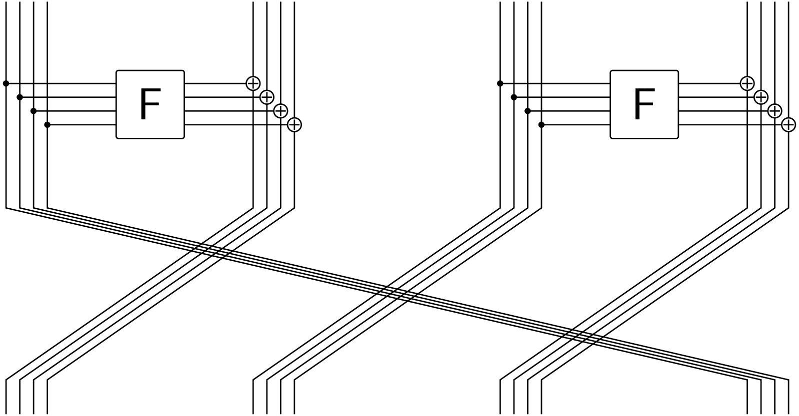


Section 1

First Instance of FPM_τ: $\mathrm{small}-\mathrm{pSquare}$

Instance: small — pSquare **for Hardware**

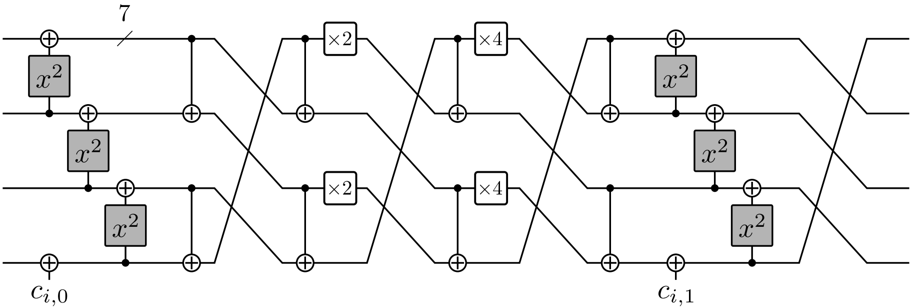
State is defined by 4 branches of 4 $\mathbb{F}_p$ elements each, with $p = 2^7 - 1 = 127$ ("small-p").
State and key size are $4 \cdot 4 \cdot 7 = 112$ bit, tweak size is given by $\tau \cdot 112$ with $\tau \in \{0, 1, 2\}$



FPM$_\tau$ F-function (small-pSquare)

- Invertible MDS matrix with low depth and number of additions [1].
- Square as the non-linear power map due to efficient masked gadgets [2].

$$M = \begin{bmatrix} 3 & 2 & 1 & 1 \\ 7 & 6 & 5 & 1 \\ 1 & 1 & 3 & 2 \\ 5 & 1 & 7 & 6 \end{bmatrix}$$



[1] Duval and Leurent, MDS Matrices with Lightweight Circuits, ToSC 2018
[2] Cassiers, Masure, Momin, Moos and Standaert, Prime-Field Masking in Hardware and its Soundness against Low-Noise SCA Attacks, TCHES 2023

Hardware Cost when Masked

Comparison to Automated Tool (Serialized Pipelined) [1]

small-pSquare $\tau = 1$

Freq. *MHz*	d	Area *GE*	Power *mW*	Latency *cyc/enc*	Rand. *bit/enc*
100	2	20735.75	2.8794	256/2	11k
	3	39958.75	5.5274	256/2	27k
	4	59404.75	8.2398	256/2	65k
250	2	26823.25	3.5092	256/2	11k
	3	48147.50	6.5390	256/2	27k
	4	72245.00	9.9639	256/2	65k
500	2	33663.25	4.6977	640/5	11k
	3	57478.75	8.3328	640/5	27k
	4	86320.25	12.1962	640/5	65k
1000	2	46481.75	7.3055	1280/10	11k
	3	79853.25	12.3280	1280/10	27k
	4	117094.00	18.2342	1280/10	65k

SKINNY-128-256

Freq. *MHz*	d	Area *GE*	Power *mW*	Latency *cyc/enc*	Rand. *bit/enc*
100	2	39016.25	9.1220	2160/9	8k
	3	57757.00	13.4186	2160/9	23k
	4	78243.00	17.9452	2160/9	46k
250	2	39016.25	9.1220	2160/9	8k
	3	57757.00	13.4186	2160/9	23k
	4	78243.00	17.9452	2160/9	46k
500	2	39016.25	9.1220	2160/9	8k
	3	57757.00	13.4186	2160/9	23k
	4	78243.00	17.9452	2160/9	46k
1000	2	39256.75	9.1467	2160/9	8k
	3	58274.75	13.5388	2160/9	23k
	4	78972.25	18.1421	2160/9	46k

[1] Knichel, Moradi, Müller and Sasdrich, Automated Generation of Masked Hardware, TCHES 2022

Hardware Cost when Masked

Comparison to Public Implementation (Serialized) [1]

small-pSquare $\tau = 1$

Freq. *MHz*	d	Area *GE*	Power *mW*	Latency *cyc/enc*	Rand. *bit/enc*
100	2	15332.25	1.9296	256/1	11k
	3	27215.75	3.4077	256/1	27k
	4	39237.50	4.9897	256/1	65k
250	2	20471.00	2.4330	256/1	11k
	3	34485.25	4.2527	256/1	27k
	4	48511.25	6.1763	256/1	65k
500	2	21186.50	2.3152	640/1	11k
	3	34677.25	3.9515	640/1	27k
	4	50638.25	5.9314	640/1	65k
1000	2	24377.25	2.6962	1280/1	11k
	3	41025.75	4.7424	1280/1	27k
	4	58694.00	7.1102	1280/1	65k

SKINNY-128-256

Freq. *MHz*	d	Area *GE*	Power *mW*	Latency *cyc/enc*	Rand. *bit/enc*
100	2	18035.75	2.5276	288/1	9k
	3	28740.75	4.1347	288/1	28k
	4	41136.75	5.9918	288/1	55k
250	2	18035.75	2.5276	288/1	9k
	3	28740.75	4.1347	288/1	28k
	4	41136.75	5.9918	288/1	55k
500	2	18035.75	2.5361	288/1	9k
	3	28775.50	4.1321	288/1	28k
	4	41143.75	5.9978	288/1	55k
1000	2	19077.50	2.5824	288/1	9k
	3	29998.25	4.2289	288/1	28k
	4	42781.25	6.1521	288/1	55k

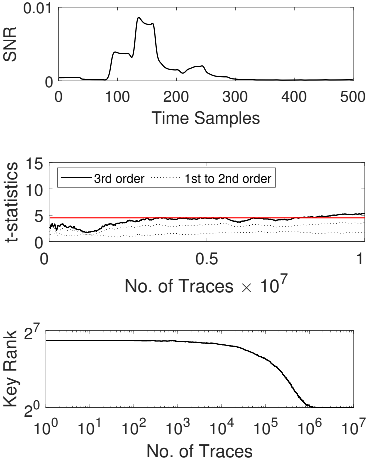
[1] Verhamme, Cassiers and Standaert, Analyzing the Leakage Resistance of the NIST's Lightweight Crypto Competition's Finalists, CARDIS 2022

Cheap Inverse

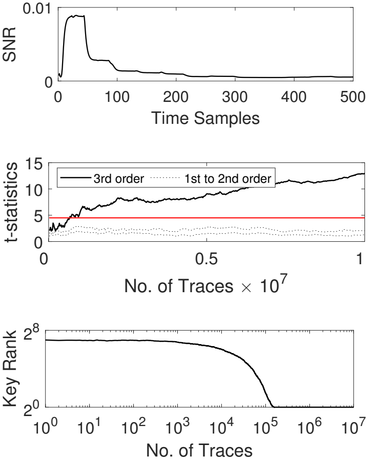
Remember: We get decryption on top almost for free (single-digit percent overhead when masked). For SKINNY the overhead is $\approx$ 100%.

Side-Channel Security Comparison (3 Shares)

small-pSquare $\tau = 1$



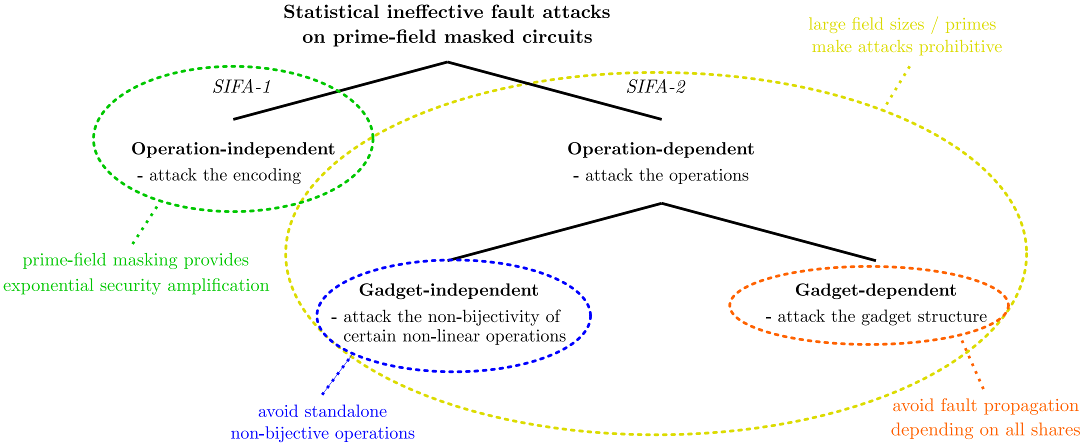
`SKINNY-128-256`



Source Code

- Currently 40 different implementations online (incl. 24 masked HW)
- Reference implementations in C and VHDL
- Optimized hardware implementations in VHDL
- Accepted as Eurocrypt 2024 artifact (Thanks for introducing this!)
- Good news: There is still room for improvement!
- `https://github.com/uclcrypto/small-pSquare`

Teaser: Fault Security



[1] Moos, Saha and Standaert, Prime Masking vs. Faults - Exponential Security Amplification against Selected Classes of Attacks, `https://eprint.iacr.org/2024/147`

Conclusion

- We introduced a general design strategy for tweakable block ciphers optimized for prime-field masking
- We successfully build a lightweight tweakable block cipher for hardware applications, called small-pSquare
- The design is competitive with state of the art binary ciphers, while delivering much better SCA (and potentially FI) security
- Next: FPM_τ instances with larger primes, e.g., for 32-bit platforms?

Prime ciphers optimized for the efficient application of additive masking appear to be promising candidates for physically secure implementations