A TALE OF RESILIENCE

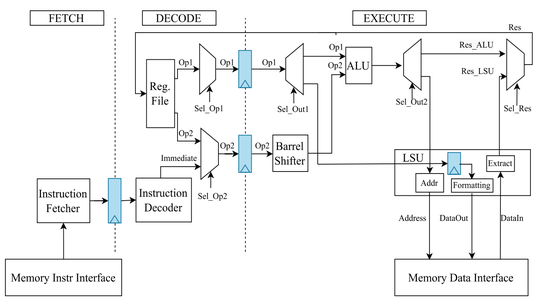
On the Practical Security of Masked Software Implementations

SCAN & READ

L.CASALINO [1], N. BELLEVILLE [1], D. COUROUSSÉ [1], K. HEYDEMANN [2,3]

1 Univ. Grenoble Alpes, CEA, List, F-38000 Grenoble, France
2 Thales DIS, France
3 Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

1. MICRO-ARCHITECTURE-INDUCED LEAKAGE



- Micro-architecture designs rely on memory elements, invisible from the ISA.
- Memory transitions potentially recombine share values, jeopardizing the proven security of masking [1, 2]
- Parallel manipulation of shares might induce exploitable leakage.
- No work considered its impact on masking.

PARALLEL PROCESSING OF SHARES (PPS)

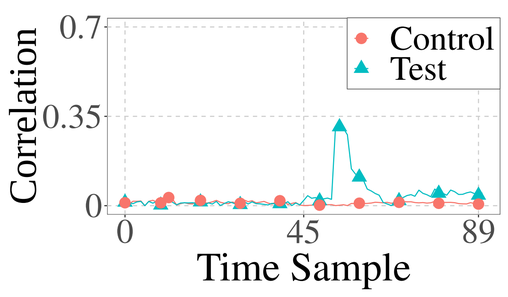
Pipelined micro-architectures might process several shares in parallel.

Cycle	LOAD [X0]	XOR Y, X1
# K	FETCH	
# K + 1	DECODE	FETCH
# K + 2	STALL	STALL
# K + 3	EXECUTE	DECODE
# K + 4		EXECUTE

- At cycle # K + 3, the micro-architecture reads X0 from the memory.
- In the meanwhile, the XOR's inputs are read from the Register File.
- The micro-architecture handles X0 and X1 at the same time (red square).
- One observation gets both X0 and X1.

PPS leakage model: $SHW(X0, X1) = HW(X0) + HW(X1)$

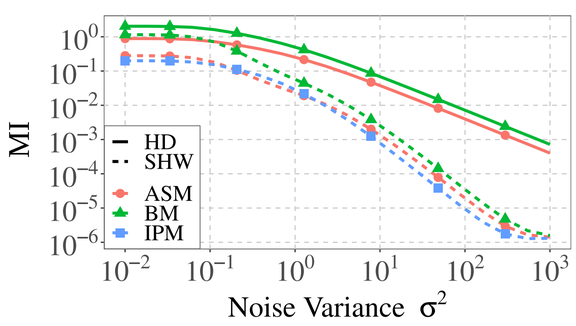
We designed several software benchmarks to characterize the impact of PPS.
We observe a correlation between the PPS leakage model and the side-channel measurements.



- Left plot: correlation analysis on above instruction sequence.
- *Test*: inputs are the shares X0 and X1.
- *Control*: inputs are random variables.

2. DIFFERENT TYPES OF MASKING

The practical security of masking relies on the chosen masking scheme.



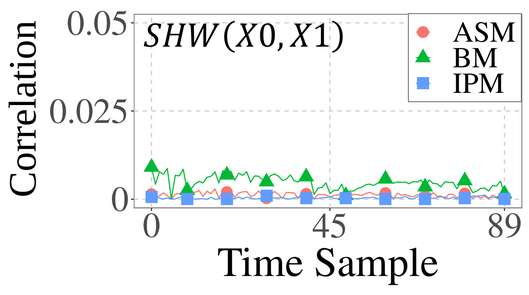
- Left picture: *Mutual Information* of 1st order encodings
  - Transitions: $HD(X0, X1) = HW(X0 \oplus X1)$
  - PPS: $SHW(X0, X1) = HW(X0) + HW(X1)$
- For IPM, transitions (HD) do not leak information (MI = 0).

Boolean (BM)	Arithmetic-Sum (ASM)	Inner-Product (IPM)
$X = X_0 \oplus X_1$	$X = X_0 \boxplus X_1$	$X = X_0 \oplus (L_1 * X_1)$

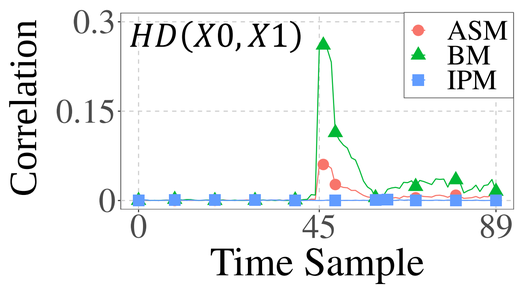
3. THE PRACTICAL SECURITY OF ENCODINGS

Memory transitions and PPS can leak information on multiple shares. But in practice, what security provide the different masking encodings?

SIMPLE 1st ORDER CORRELATION ANALYSIS

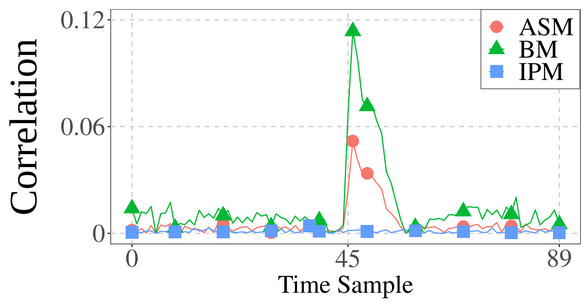


According to the theoretical results, a 1st order analysis can't exploit PPS leakage.



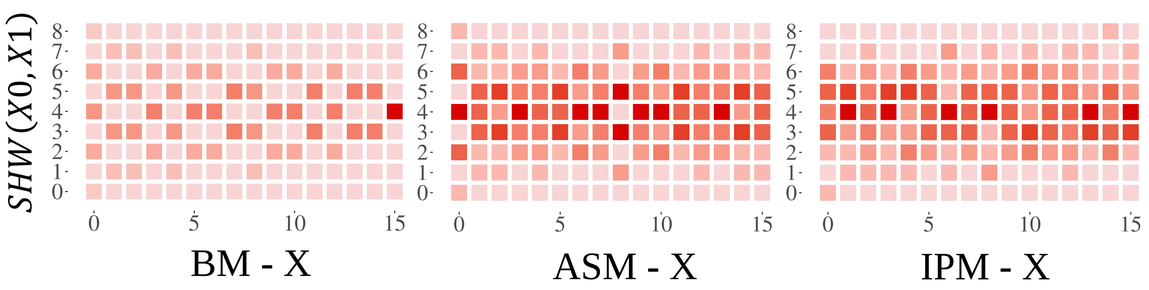
Memory transitions easily leak the BMed value. On the other hand, ASM leaks less whereas IPM does not.

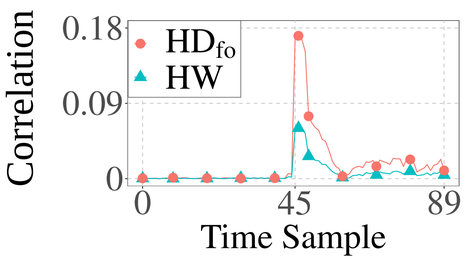
1st ORDER CORRELATION WITH PRE-PROCESSING



- We can pre-process the power trace to detect 1st order leakage when PPS takes place.
- For each sample s, keep the traces for which s' value is under (or above) a given threshold k.
- Hence, we convert higher-order leakages into lower-order ones [4].

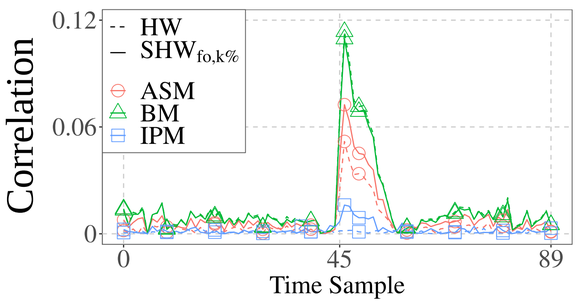
EXPLOITING MOMENT-BASED LEAKAGE MODELS





- Previous analyses relied on the *Hamming Weight* model.
- Such model better suits the structure of BM.
- We can use the first-order moment of ASM and IPM's leakage distribution to build better leakage models.

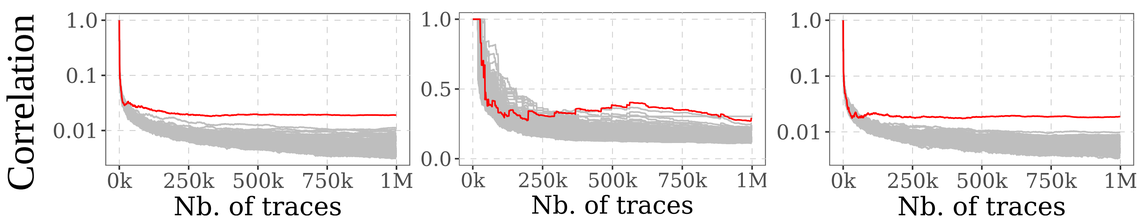
EXPLOITING PPS vs IPM



- We combine trace pre-processing and first-order moment leakage models to exploit PPS-based leakage.
- Left figure: improved correlation with respect to using Hamming Weight model, both for ASM and IPM

4. THE PRACTICAL SECURITY OF MASKED AES-128

The analyses of encodings provided a first understanding of the practical security of the different masking schemes. What about fully-masked implementations?
We studied 4 AES implementations (unprotected, BM, ASM, IPM), each verified to be value-based leakage free, but vulnerable due to some micro-architectural effect.
We report the most relevant CPA results:



ASM – 1st-order HD	IPM – 1st-order SHW + pre-processing	IPM – 1st-order HD of discrete logs
The ASM implementation shows low resilience to transition-based leakages.	IPM can be broken via PPS-based leakage exploitation, although resilient to transition-based leakages by design.	The log/alog-based multiplication applies log function to shares. Transitions of log(share) leaks in IPM implementation.

5. CONTRIBUTIONS SUMMARY

Our work provides new insights concerning the impact of the micro-architecture on the practical security of masked software implementations.

- PPS-based leakage is observable in the software context.
- PPS leakage can be exploited against all the considered masking schemes by slightly adapting [4].
- We exhibit two attacks against IPM: one via PPS leakages, one via the transition-based leakage from the logarithm representation of masking encodings in the finite field multiplication.

REFERENCES

[1] B. Marshall et al., "MIRACLE: micro-architectural leakage evaluation A study of micro-architectural power leakage across many devices," TCHES, 2022.
[2] B. Gigerl et al. "Secure and efficient software masking on superscalar pipelined processors,", ASIACRYPT, 2021.
[3] O. Bronchain et. al, "Leakage certification revisited: Bounding model errors in side-channel security evaluations," in CRYPTO, 2019.
[4] T. Moos and A. Moradi, "On the easiness of turning higher-order leakages into first-order,", COSADE, 2017.