Funded by Deutsche Forschungsgemeinschaft German Research Foundation

INDIANA – VERIFYING (RANDOM) PROBING SECURITY THROUGH INDISTINGUISHABILITY ANALYSIS

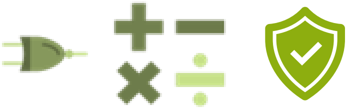
CHRISTOF BEIERLE, JAKOB FELDTKELLER, ANNA GUINET, TIM GÜNEYSU, GREGOR LEANDER,
JAN RICHTER-BROCKMANN, **PASCAL SASDRICH**

EUROCRYPT 2025 | MADRID, SPAIN | MAY 5, 2025

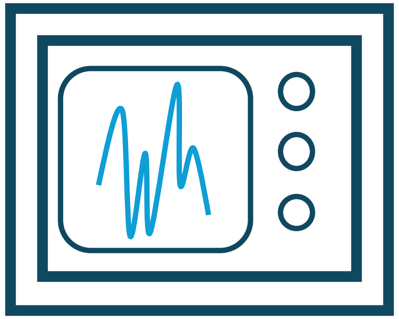
MOTIVATION | PHYSICAL IMPLEMENTATION ATTACKS

CRYPTOGRAPHIC
DEVICE

HARDWARE MASKING SCHEMES



SIDE-CHANNEL ANALYSIS



PASSIVE OBSERVATION OF PHYSICAL CHARACTERISTICS

IMPLEMENTATION OF HARDWARE MASKING SCHEMES IS A COMPLEX, DELICATE, AND ERROR-PRONE PROCESS.

MOTIVATION | FORMAL SECURITY REASONING

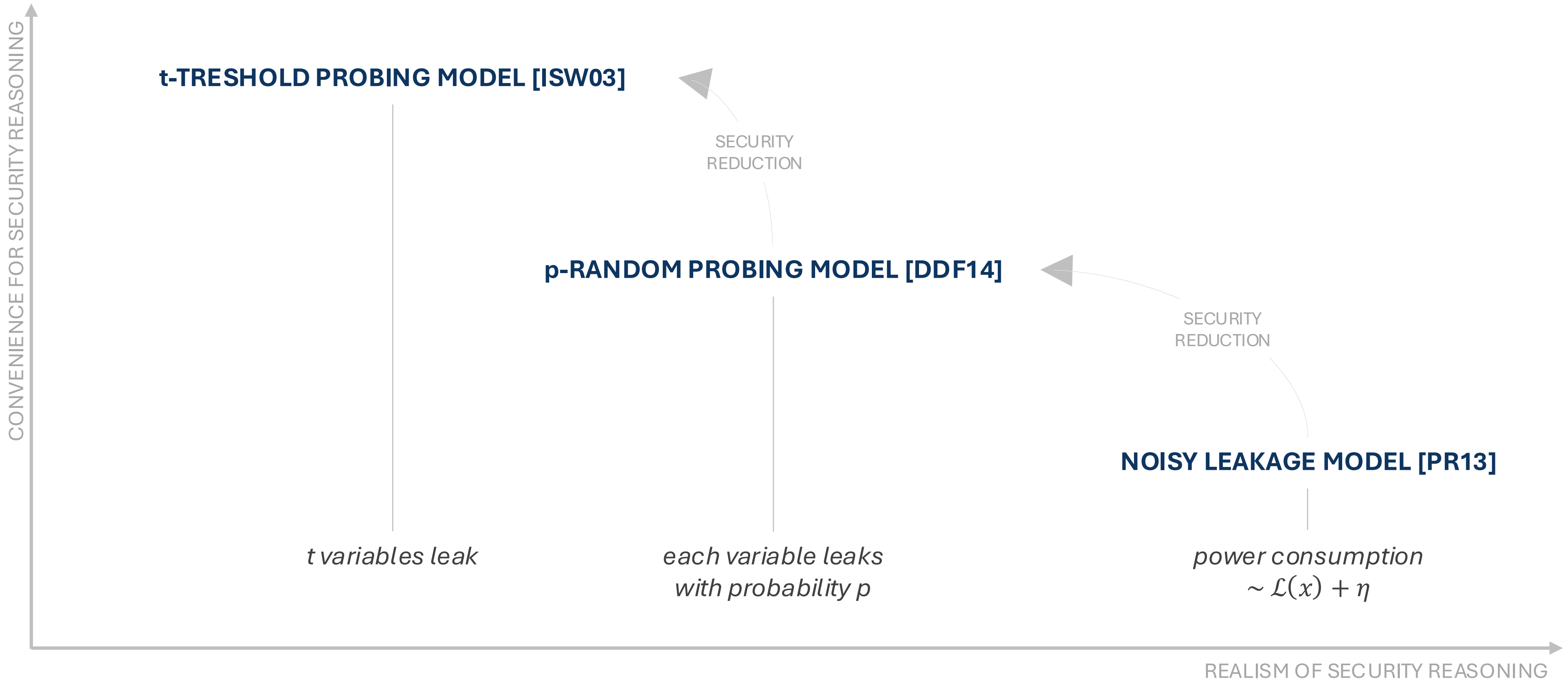
ADVERSARY MODELS

SECURITY PROPERTIES

ARCHITECTURAL & ENVIRONMENTAL CONDITIONS

AUTOMATED SECURITY REASONING TOOLS ALLOW PRE-MANUFACTURING VULNERABILITY DETECTION.

PRELIMINARIES | LEAKAGE MODELS



STATE-OF-THE-ART REASONING TOOLS ARE RESTRICTED (FOR STRUCTURES AND/OR MODELS) OR INCOMPLETE.

CONTRIBUTION | RESEARCH MISSION

DEVELOP

SOUND, ACCURATE AND EFFICIENT TOOLS

FOR VERIFYING THE SECURITY OF

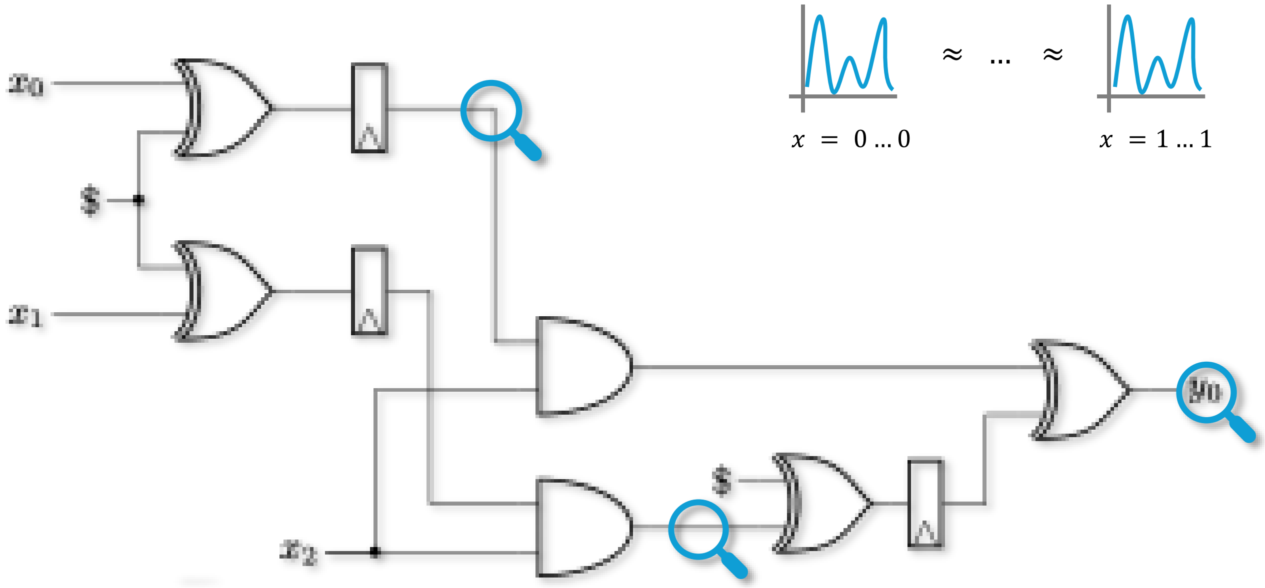
ARBITRARY AND COMPLEX MASKED HARDWARE CIRCUITS

UNDER

MORE REALISTIC LEAKAGE MODELS

OUR CONTRIBUTIONS

THEORY | SECURITY DEFINITION



INDISTINGUISHABILITY – PROBING SECURITY

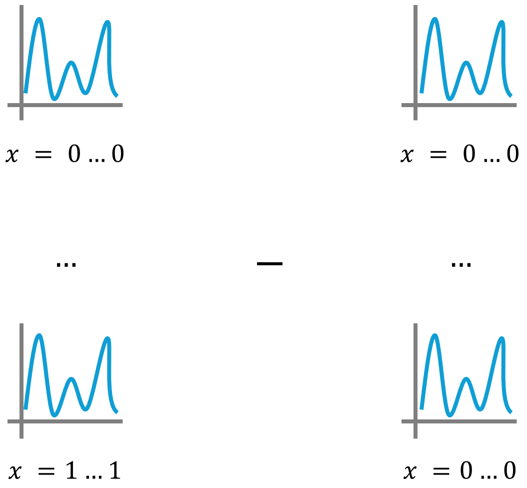
For a fixed set of t probes, an ADVERSARY cannot distinguish between different input values $\mathrm{x} \in \mathbb{F}_2^{\mathrm{n_i}}$.

NEW

$\boxed{\mathcal{L}_{(Enc,A_C,Ex)}(\mathcal{P}) = 0 \textit{ for all sets } \mathcal{P} \subseteq \mathcal{W} \textit{ of up to } t \textit{ probes}}$

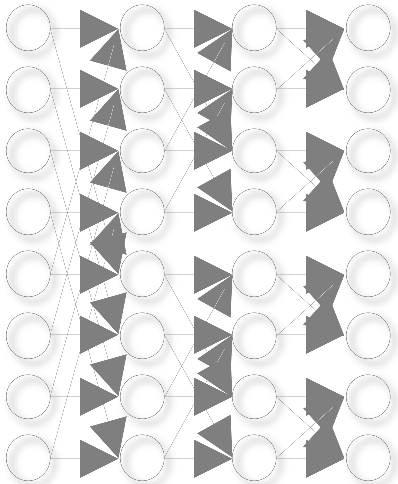
THEORY | DERIVING LEAKAGE FUNCTIONS

ADVERSARIAL OBSERVATIONS



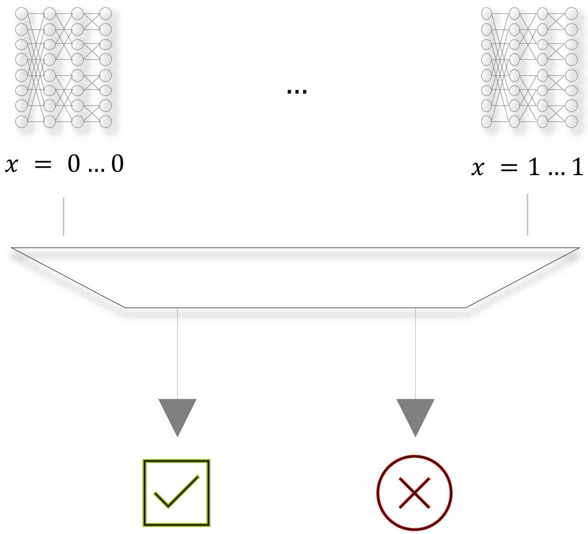
$$D_{H,x}(y) := |H_x^{-1}(y)| - |H_0^{-1}(y)|$$

FOURIER-HADAMARD TRANSFORM



$$\hat{f} : \mathbb{F}_2^m \to \mathbb{R}, \beta \mapsto \sum_{y \in \mathbb{F}_2^m} (-1)^{\langle \beta, y \rangle} f(y)$$

LEAKAGE FUNCTION

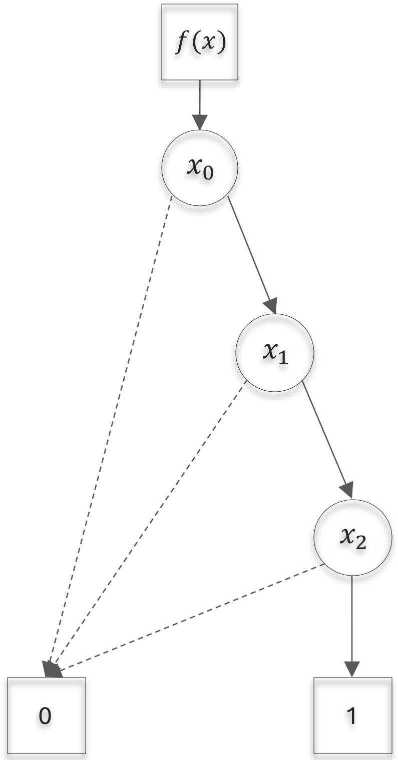


$$\mathcal{L}_{(Enc, A_C, Ex)}(\mathcal{P})$$

NEW

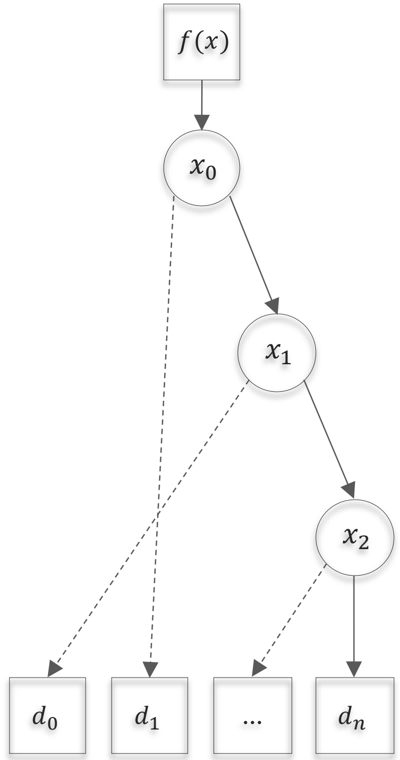
Computing the leakage function (efficiently) allows to detect leakage in the probing and random probing models.

IMPLEMENTATION | GRAPH-BASED DECISION DIAGRAMS



BINARY DECISION DIAGRAMS

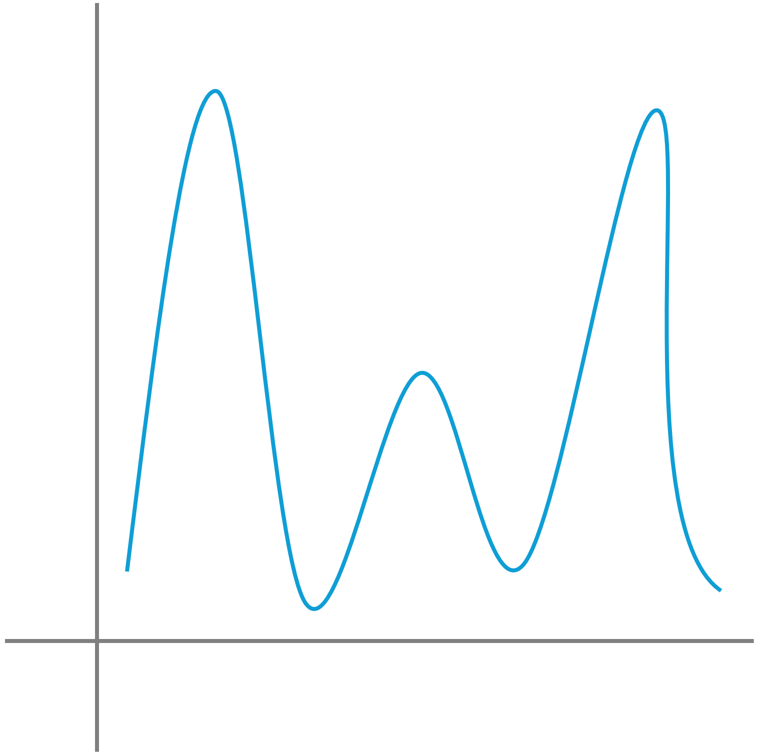
A Reduced Ordered Binary Decision Diagram is a concise and unique (i.e., canonical) graph-based representation of a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$



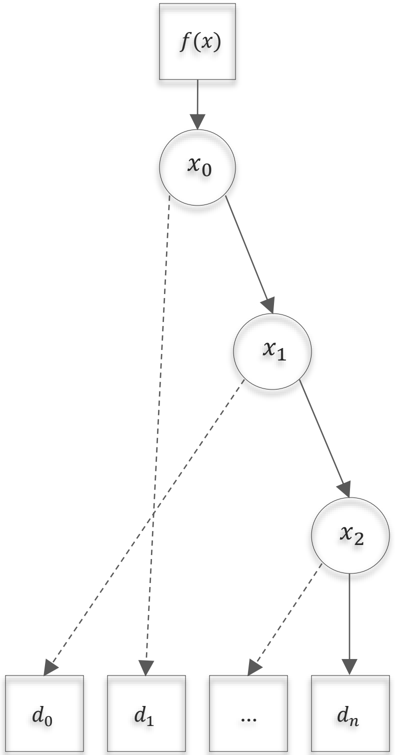
MULTI-TERMINAL BINARY DECISION DIAGRAMS

MTBDDs are an extension to represent functions from a multi-dimensional Boolean domain to an arbitrary value set $f\colon \mathbb{F}_2^n \to \mathbb{D}$.

IMPLEMENTATION | FROM THEORY TO PRACTICE



(DISCRETE) PROBABILITY DISTRIBUTION



VECTOR OF OCCURENCES (FREQUENCIES)

NEW

Computing the Fourier-Hadamard Transform and the leakage function maps to basic BDD and MTBDD operations.

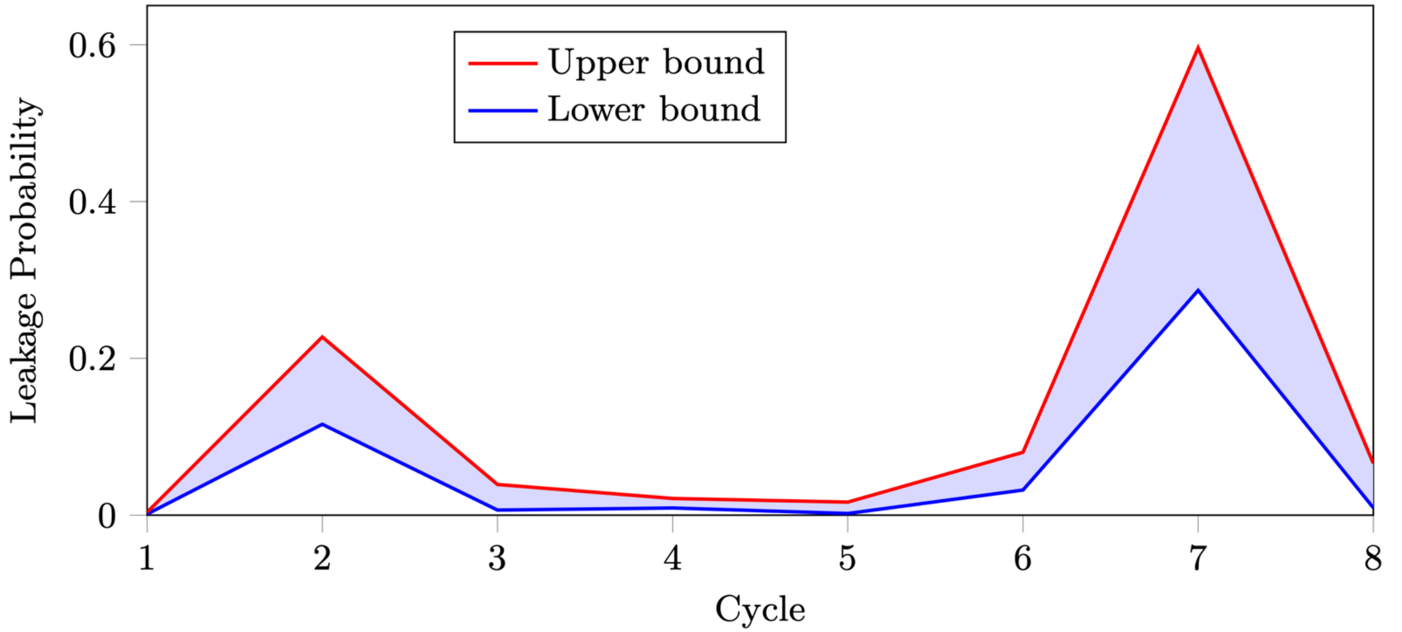
EVALUATION RESULTS

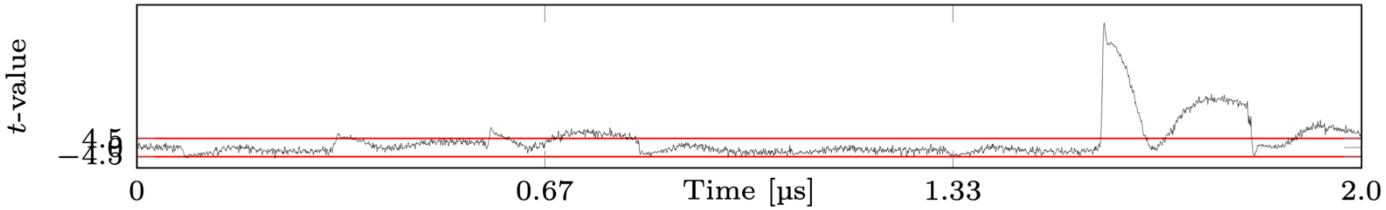
EVALUATION | AES ROUND (RANDOM PROBING)

Cycle	Positions	Probes	Samples	Leakage	Total Elapsed Time
1	16×72	16×2	16×2556	$^{0.056}/_{0.458}$	1.20 min
2	16×138	16×2	16×9453	$^{0.785}/_{0.966}$	6.25 min
3	16×72	16×2	16×2556	$^{0.099}/_{0.472}$	39.33 min
4	16×52	16×2	16×1326	$^{0.145}/_{0.296}$	39.43 min
5	16×52	16×2	16×1326	$^{0.034}/_{0.236}$	39.53 min
6	16×92	16×2	16×4186	$^{0.406}/_{0.738}$	39.79 min
7	16×304	16×2	16×46056	$^{0.992}/_{0.999}$	3.33 h
8	16×102	16×2	16×5151	$^{0.149}/_{0.767}$	3.58 h
9	4×324	16×2	4×52326	$^{0.051}/_{0.981}$	3.76 h

EVALUATION | FROM THEORY TO PRACTICE

VERIFICATION OF A SINGLE AES S-BOX IN THE RANDOM PROBING MODEL





PRACTICAL 2-ND ORDER TVLA RESULTS

CONCLUSION | CONTRIBUTIONS

OUR CONTRIBUTIONS IN A NUTSHELL

1. Formalizing probing security in terms of indistinguishability.

2. Deriving leakage functions using the Fast Fourier-Hadamard Transformation.

3. Implementation of a versatile verification framework: https://github.com/Chair-for-Security-Engineering/INDIANA

TOOL

PAPER

THANK YOU – DO YOU HAVE ANY QUESTIONS?

pascal.sasdrich@rub.de

REFERENCES

[ISW03] *Yuval Ishai, Amit Sahai, David A. Wagner:* ***Private Circuits: Securing Hardware against Probing Attacks.*** *CRYPTO 2003: 463-481*

[PR13] *Emmanuel Prouff, Matthieu Rivain:* ***Masking against Side-Channel Attacks: A Formal Security Proof.*** *EUROCRYPT 2013: 142-159*

[DDF14] *Alexandre Duc, Stefan Dziembowski, Sebastian Faust:* ***Unifying Leakage Models: From Probing Attacks to Noisy Leakage.*** *EUROCRYPT 2014: 423-440*