

Leakage Analysis with Information Theoretic Metrics

Hassan TRIQUI <hassan.triqui@Secure-IC.com>



Introduction

Implementation-level security evaluations is a scientific field that has recently known fundamental advances, notably through the introduction of a practice-oriented unified framework for the analysis of side-channel attacks [SMY09].

This work suggests that the resistance of a given implementation against attacks (*e.g.* CPA [BCO04]) is **too specific a criterion** to fairly assess the actual security level of a system.

Instead, some hints for the use of **attack-agnostic evaluation schemes** are promoted.

In this poster, we first survey the existing implementation-level weaknesses assessments. We show that they are both not scientific at all and definitely too *ad hoc*.

Then, we investigate serious methodologies such as:

- stochastic methods [SLP05, Sch08], adapted to the context of leakage estimation,
- mutual information metric [VCS09].

The first method **trades some characterization accuracy** for profiling feasibility in practical amounts of times [GLRP06]. The second method seems optimal, but for the **length of the preprocessing**.

We therefore suggest to both:

- speed-up the computations and
- characterize each single bit of the implementation.

Bitwise Mutual Information Analysis (*aka* MIA [GBTP08]) is shown to be a tool of choice. Results on “intentionally leaking” power-constant netlists are illustrated.

References

- [BCO04] Éric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In *CHES*, volume 3156 of *LNCS*, pages 16–29. Springer, August 11–13 2004. Cambridge, MA, USA.
- [GBTP08] Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual information analysis. In *CHES, 10th International Workshop*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer, August 10–13 2008. Washington, D.C., USA.
- [GLRP06] Benedikt Gierlichs, Kerstin Lemke-Rust, and Christof Paar. Templates vs. Stochastic Methods. In *CHES*, volume 4249 of *LNCS*, pages 15–29. Springer, October 10–13 2006. Yokohama, Japan.
- [Sch08] Werner Schindler. Advanced stochastic methods in side channel analysis on block ciphers in the presence of masking. *Journal of Mathematical Cryptology*, 2(3):291–310, October 2008. ISSN (Online) 1862-2984, ISSN (Print) 1862-2976, DOI: 10.1515/JMC.2008.013.
- [SLP05] Werner Schindler, Kerstin Lemke, and Christof Paar. A Stochastic Model for Differential Side Channel Cryptanalysis. In *LNCS*, editor, *CHES*, volume 3659 of *LNCS*, pages 30–46. Springer, Sept 2005. Edinburgh, Scotland, UK.
- [SMY09] François-Xavier Standaert, Tal Malkin, and Moti Yung. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 443–461. Springer, April 26–30 2009. Cologne, Germany.
- [VCS09] Nicolas Veyrat-Charvillon and François-Xavier Standaert. Mutual Information Analysis: How, When and Why? In *CHES*, volume 5747 of *LNCS*, pages 429–443. Springer, September 6–9 2009. Lausanne, Switzerland.

Traditional Attack-Based Methodology does not Help Pinpoint the Leakage

Context:

- Hardware AES accelerator, susceptible to be attacked by side-channel attacks;
- Dual-rail with precharge logic (DPL) used for the protection;
- Prototyping evaluation in an FPGA (Secure-IC’s corporate prototyping board).

CPA results on SBOX 0 for two DPL variants of AES – each slightly leaking.

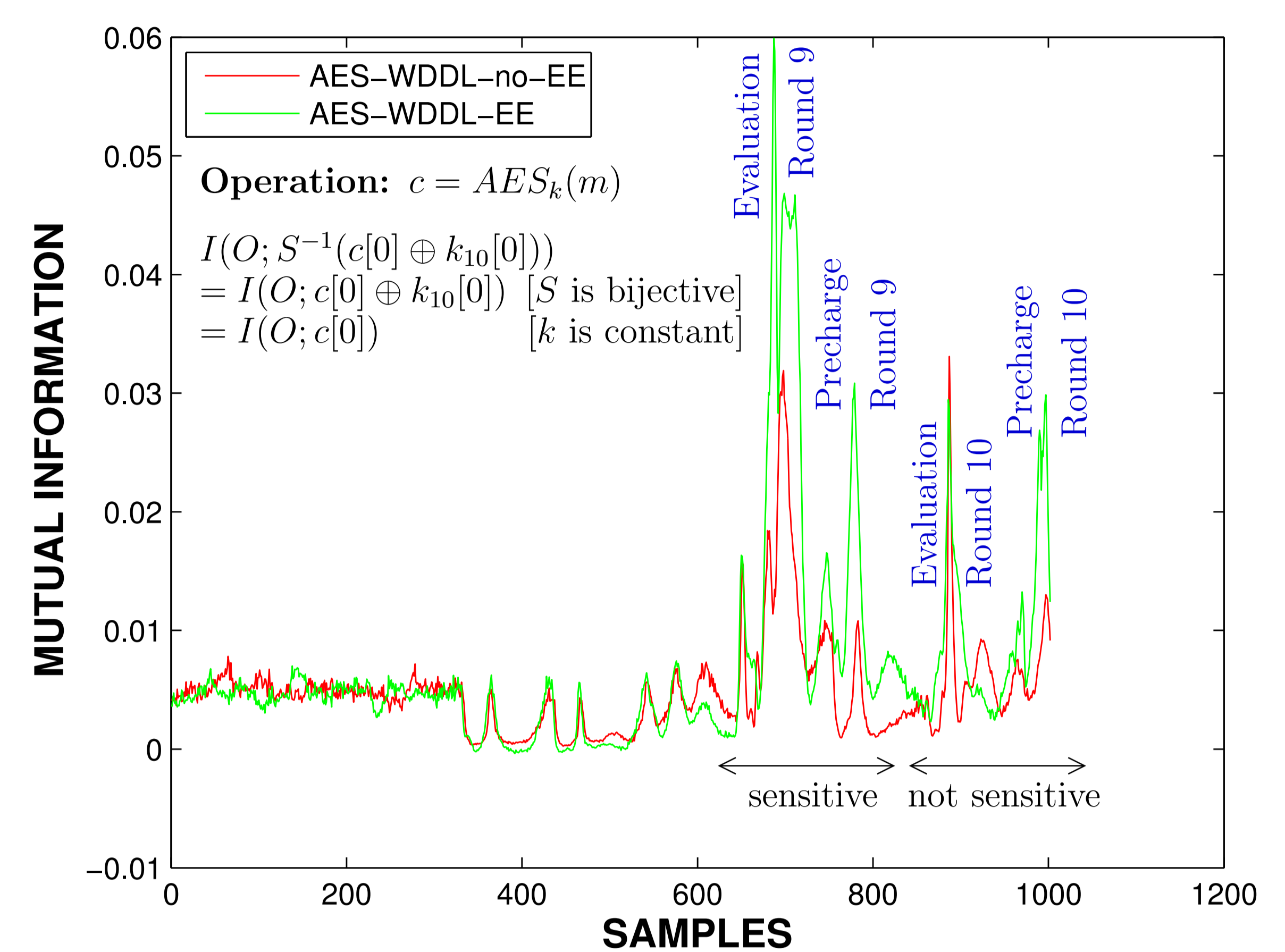
Implementation	No. of Traces to break the implementation								
	SBOX BIT index	0	1	2	3	4	5	6	7
WDDL-EE	8314	X ¹	1340	X	7000	X	12232	X	
WDDL-noEE	X	X	1150	X	X	X	X	X	X

¹ In this table, X signifies failure of the mounted attack with up to 40000 traces.

But how to identify the resources contributing to the leakage?

Information Theoretic Approaches at the Word-Level

Comparison of Mutual Information leaked from an AES protected using DPL-EE and DPL-noEE.

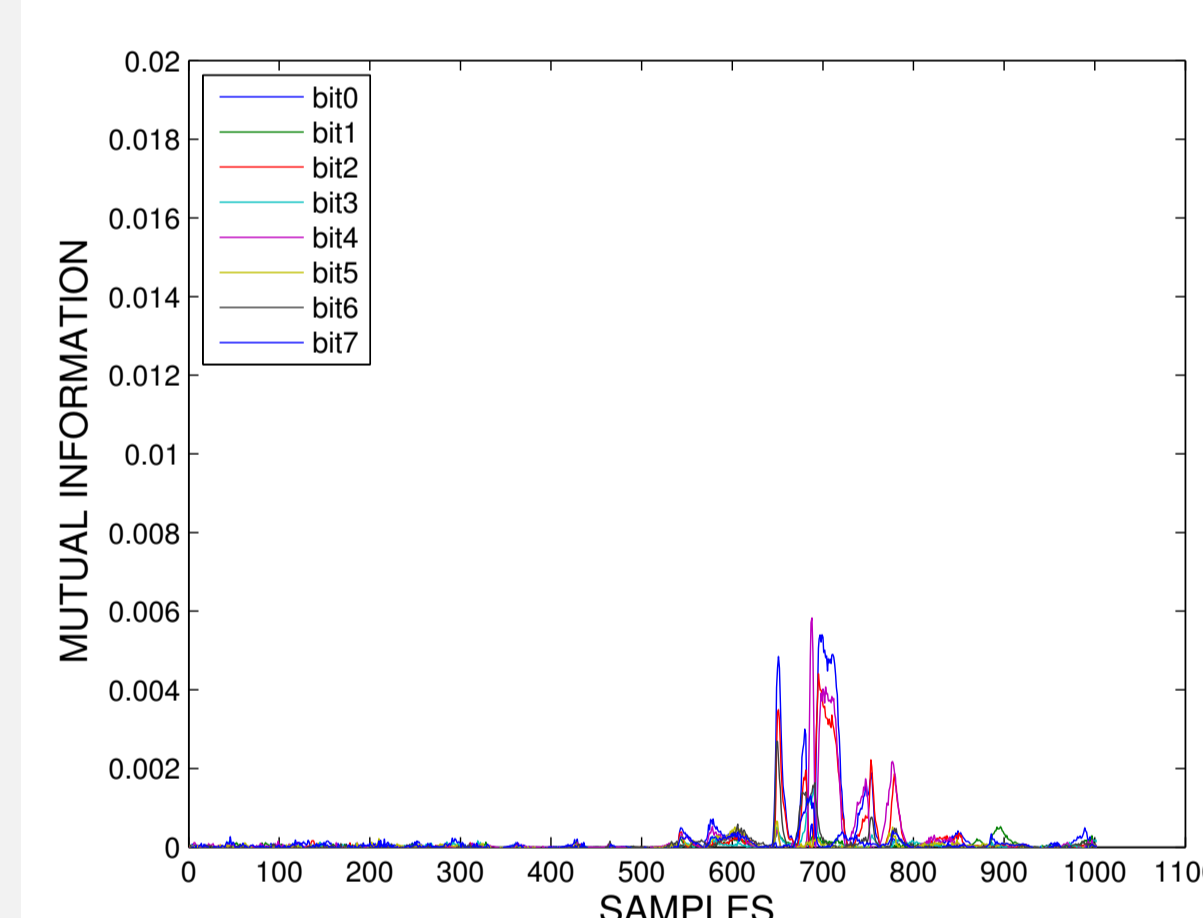


In this case, the **sbox level** is too inaccurate to grasp what’s going on...

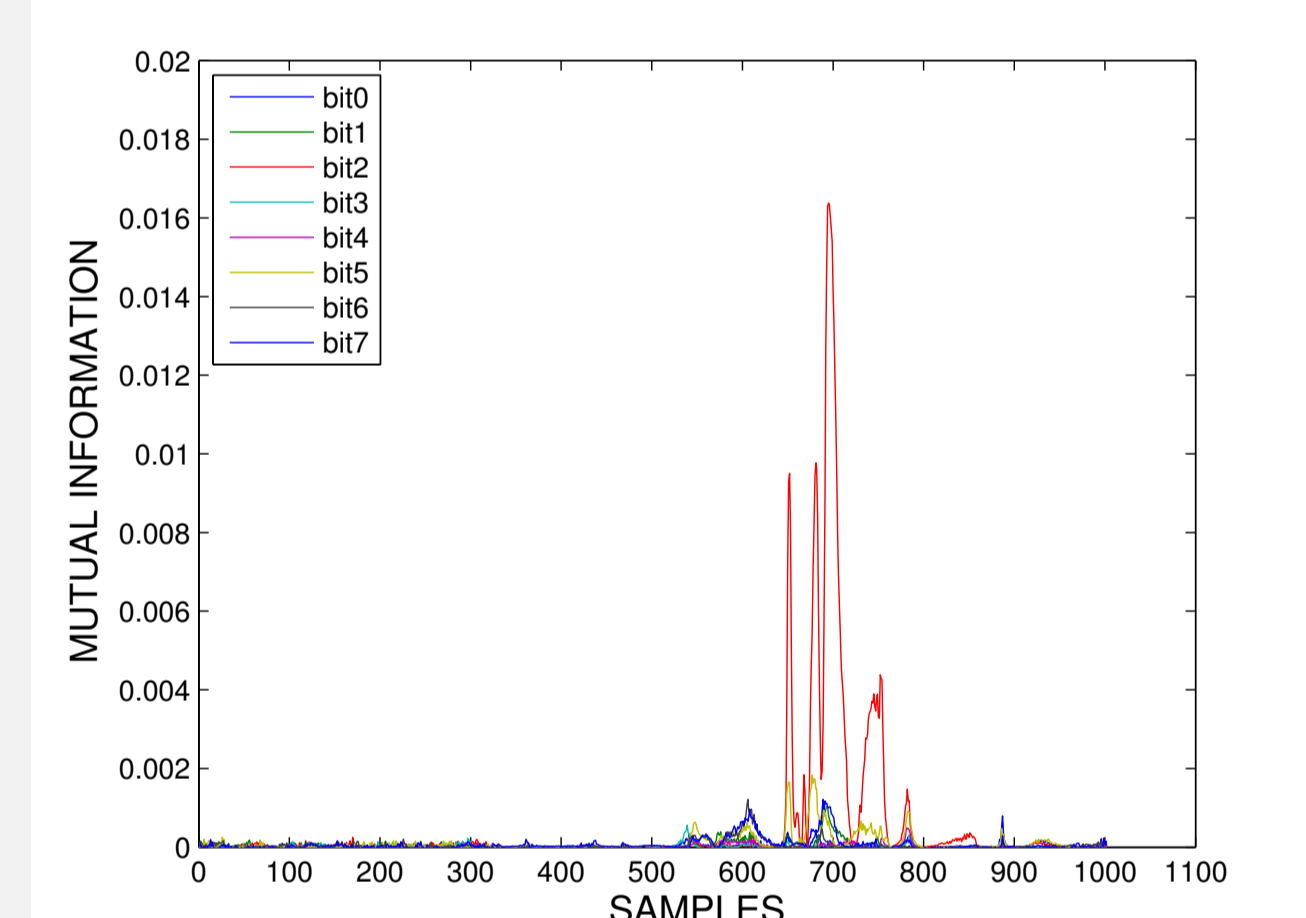
The designer is not really helped to know why this sbox is leaking, more or less.

Bitwise Mutual Information Methodology do Pinpoint the Leakage —> Positive Feedback to the HW Designer!

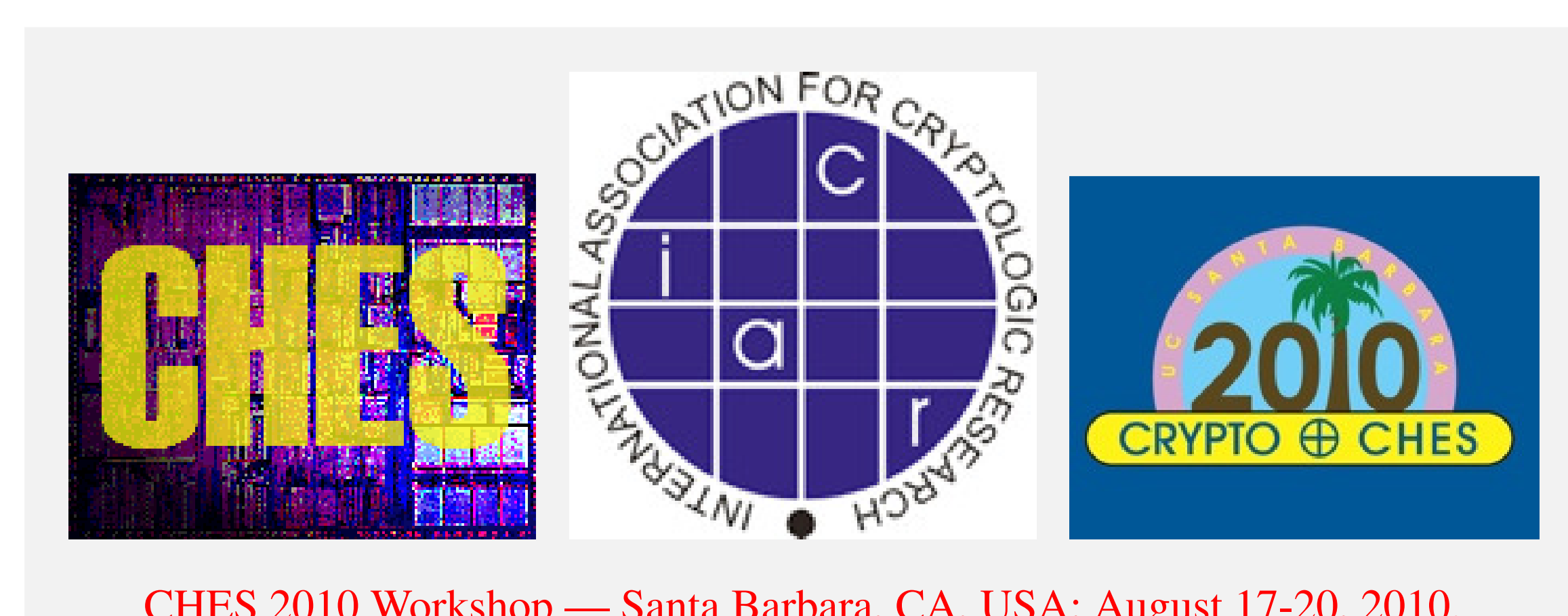
Bitwise leakage of SBOX0 in DPL-EE.



Bitwise leakage of SBOX0 in DPL-noEE.



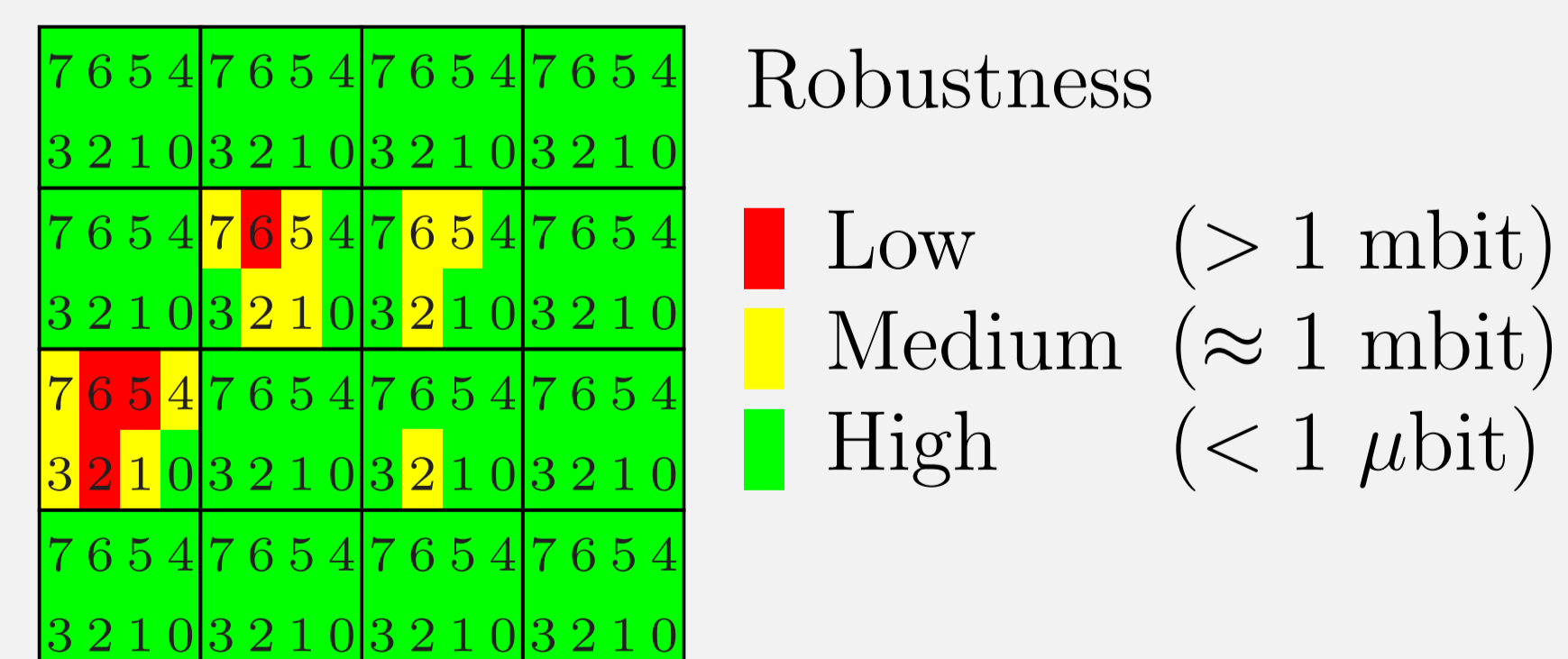
See that the **leaking bits** do correspond exactly to the ones that are **attackable by CPA!**



CHES 2010 Workshop — Santa Barbara, CA, USA; August 17-20, 2010.

Proposal for a Leakage Evaluation Dashboard

AES state leakage analysis:



Analysis configuration.

- *distinguisher*: DoM, DPA, CPA, Spearman, MIA.
- *partitioning*: state bit, distance, switching.
- *round*: 0, 1, ..., 8, 9.

Large amounts of computations. Challenging task! Implemented in the SmartSIC-Analyzer.

Acknowledgments

Experimental characterizations were done by Shivam BHASIN from TELECOM-ParisTech.

The ideas presented in this poster have benefited from fruitful comments and suggestions for improvement during PASTIS’2010 & CryptArchi’2010 workshops (presentations by Dr Philippe NGUYEN, CTO Secure-IC S.A.S.).