**MORE RELEVANT PAPERS:**

**TITLE**: A Side-Channel Analysis Resistant Description of the AES S-Box

**TITLE**: Side-Channel Analysis of PUFs and Fuzzy Extractors

**TITLE**: A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks

**TITLE**: Side-Channel Attack Pitfalls

**TITLE**: Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering

**TOP 3 SUGGESTIONS FOR TEAM:**

**TITLE**: Side-Channel Analysis of PUFs and Fuzzy Extractors

**TITLE**: A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks

**TITLE**: Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering

**TITLE**: A Side-Channel Analysis Resistant Description of the AES S-Box

**Abstract:**

So far, efficient algorithmic countermeasures to secure the AES algorithm against (first order) differential side-channel attacks have been very expensive to implement. In this article, we introduce a new masking countermeasure which is not only secure against first-order side-channel attacks, but which also leads to relatively small implementations compared to other masking schemes implemented in dedicated hardware.

Our approach is based on shifting the computation of the finite field inversion in the AES S-box down to GF(4). In this field, the inversion is a linear operation and therefore it is easy to mask.

Summarizing, the new masking scheme combines the concepts of multiplicative and additive masking in such a way that security against first-order side-channel attacks is maintained, and that small implementations in dedicated hardware can be achieved.

**PICK:** In this paper, the publishers came with an approach of a new masking counter measure to secure first order side channel attacks. So, picking this paper would help to explore the new counter measures.

**TITLE**: Low-cost solutions for preventing simple side-channel analysis: side-channel atomicity

**Abstract:**

We introduce simple methods to convert a cryptographic algorithm into an algorithm protected against simple side-channel attacks. Contrary to previously known solutions, the proposed techniques are not at the expense of the execution time. Moreover, they are generic and apply to virtually any algorithm. In particular, we present several novel exponentiation algorithms, namely, a protected square-and-multiply algorithm, its right-to-left counterpart, and several protected sliding-window algorithms. We also illustrate our methodology applied to point multiplication on elliptic curves. All these algorithms share the common feature that the complexity is globally unchanged compared to the corresponding unprotected implementations.

**Drop:** This paper discusses about the solutions to secure the cryptographic algorithms. The paper seemed to have more generic information, so dropping this paper.

**TITLE** : Side-Channel Analysis of PUFs and Fuzzy Extractors

**Abstract:**

Embedded security systems based on Physical Unclonable Functions (PUFs) offer interesting protection properties, such as tamper resistance and unclonability. However, to establish PUFs as a high security primitive in the long run, their vulnerability to side-channel attacks has to be investigated. For this purpose, we analyzed the side-channel leakage of PUF architectures and fuzzy extractor implementations. We identified several attack vectors within common PUF constructions and introduce two side-channel attacks on fuzzy extractors. Our proof-of-concept attack on an FPGA implementation of a fuzzy extractor shows that it is possible to extract the cryptographic key derived from a PUF by side-channel analysis.

**Pick:** This paper discusses the proof of concept about the attacks on an FPGA implementation of fuzzy extractor. This would give the possible side channel attacks information, so picking this paper.

**TITLE**: A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks

**Abstract:**

The fair evaluation and comparison of side-channel attacks and countermeasures has been a long standing open question, limiting further developments in the field. Motivated by this challenge, this work makes a step in this direction and proposes a framework for the analysis of cryptographic implementations that includes a theoretical model and an application methodology. The model is based on commonly accepted hypotheses about side-channels that computations give rise to. It allows quantifying the effect of practically relevant leakage functions with a combination of information theoretic and security metrics, measuring the quality of an implementation and the strength of an adversary, respectively. From a theoretical point of view, we demonstrate formal connections between these metrics and discuss their intuitive meaning. From a practical point of view, the model implies a unified methodology for the analysis of side-channel key recovery attacks. The proposed solution allows getting rid of most of the subjective parameters that were limiting previous specialized and often ad hoc approaches in the evaluation of physically observable devices. It typically determines the extent to which basic (but practically essential) questions such as “How to compare two implementations?” or “How to compare two side-channel adversaries?” can be answered in a sound fashion.

**PICK**: This paper proposes a framework for analysis of cryptographic implementation. Found this paper interesting, so picking this paper.

**TITLE**: Side-Channel Attack Pitfalls

**Abstract:**

While cryptographic algorithms are usually strong against mathematical attacks, their practical implementation, both in software and in hardware, opens the door to side-channel attacks. Without expensive equipment or intrusive monitoring, these attacks bypass the mathematical complexity and find the cryptographic key by observing the power consumption or the execution time variations of the device in normal operation mode. The power traces of 8000 encryptions are for instance sufficient to extract the secret key of an unprotected ASIC AES implementation, which is orders of magnitude smaller than the 2128 tests required to brute force the algorithm. A careful implementation can address these vulnerabilities, yet the solutions conflict with the common design goals to optimize for area, performance and power consumption. This paper introduces the side-channel attack pitfalls, which help create or facilitate the observation of the information leakage, discusses mitigation strategies and identifies opportunities for future research.

**PICK** :the paper discusses about the side channel attack pitfalls, this is a useful paper as per my knowledge.

**TITLE:**

On Insecurity of the Side Channel Attack Countermeasure Using Addition-Subtraction Chains under Distinguishability between Addition and Doubling

<https://link.springer.com/chapter/10.1007/3-540-45450-0_32>

**Abstract:**

We show that a randomized addition-subtraction chains countermeasure against side channel attacks is vulnerable to SPA attack, a kind of side channel attack, under distinguishability between addition and doubling. A side channel attack is an attack that takes advantage of information leaked during execution of a cryptographic procedure. The randomized addition-subtraction chains countermeasure has been proposed by Oswald-Aigner, and is a random decision inserted into computations. However, its immunity to side channel attacks is still controversial. As for timing attack, a kind of side channel attack, the randomized addition-subtraction chains countermeasure is also vulnerable. Moreover, compared with other countermeasures against side channel attacks, the randomized addition-subtraction chains countermeasure, after being improved to prevent side channel attacks, is much slower.

**DROP:** This paper more speaks about the arithmetic counter measures, which seemed more generic.

**TITLE:** An overview of side channel analysis attacks

**Abstract:**

During the last ten years, power analysis attacks have been widely developed under many forms. They analyze the relation between the power consumption or electromagnetic radiation of a cryptographic device and the handled data during cryptographic operations. The goal of this paper is to give a global view of statistical attacks based on side channel analysis. These techniques are classified into two classes: attacks without reference device (e.g. Differential Power Analysis, Correlation Power Analysis) and attacks using a reference device (e.g. Template Attack, Stochastic Model Attack). In this paper, we present the attacks with an easy comprehensible way and focus on their implementation aspect. The pros and cons of each attack is highlighted in details with concrete electromagnetic signals. At least, our paper proposes also some solutions to enhance the existing attacks.

Drop: the paper discusses about the different classes of attacks and their proposed solution. But I was looking more stuff regarding the encryption.

**TITLE**: Trojan Side-Channels: Lightweight Hardware Trojans through Side-Channel Engineering

**Abstract:**

The general trend in semiconductor industry to separate design from fabrication leads to potential threats from untrusted integrated circuit foundries. In particular, malicious hardware components can be covertly inserted at the foundry to implement hidden backdoors for unauthorized exposure of secret information. This paper proposes a new class of hardware Trojans which intentionally induce physical side-channels to convey secret information. We demonstrate power side-channels engineered to leak information below the effective noise power level of the device. Two concepts of very small implementations of Trojan side-channels (TSC) are introduced and evaluated with respect to their feasibility on Xilinx FPGAs. Their lightweight implementations indicate a high resistance to detection by conventional test and inspection methods. Furthermore, the proposed TSCs come with a physical encryption property, so that even a successful detection of the artificially introduced side-channel will not allow unhindered access to the secret information.

PICK: This paper more discusses about the TSC evaluation and feasibility on Xilinx FPGA. The paper more related to the project.

**TITLE**: Algebraic Side-Channel Analysis in the Presence of Errors

<https://link.springer.com/content/pdf/10.1007%2F978-3-642-15031-9_29.pdf>

**Abstract:**

Measurement errors make power analysis attacks difficult to mount when only a single power trace is available: the statistical methods that make DPA attacks so successful are not applicable since they require many (typically thousands) of traces. Recently it was suggested to use algebraic methods for the single-trace scenario, converting the key recovery problem into a Boolean satisfiability (SAT) problem, then using a SAT solver. However, this approach is extremely sensitive to noise (allowing an error rate of well under 1% at most), and the question of its practicality remained open. In this work we show how a single-trace side-channel analysis problem can be transformed into a pseudo-Boolean optimization (PBOPT) problem, which takes errors into consideration. The PBOPT instance can then be solved using a suitable optimization problem solver. The PBOPT syntax provides for a more expressive input specification which allows a very natural representation of measurement errors. Most importantly, we show that using our approach we are able to mount successful and efficient single-trace attacks even in the presence of realistic error rates of 10%–20%. We call our new attack methodology Tolerant Algebraic Side-Channel Analysis (TASCA). We show practical attacks on two real ciphers: Keeloq and AES.

Drop:

The paper more discusses about the arithmetic approaches to the SCA attacks.

**TITLE:** On the Exact Success Rate of Side Channel Analysis in the Gaussian

<https://link.springer.com/content/pdf/10.1007%2F978-3-642-04159-4_11.pdf>

**Abstract:**

Nowadays, Side Channel Analysis is one of the most powerful cryptanalytic technique against cryptosystems embedded in portable devices such as smart cards. Faced with this threat, it is of crucial importance to precisely determine what is achievable by a given side channel adversary against a cryptosystem producing a given side channel leak- age. This can be answered by evaluating the success rate of an attack according to the adversary capacities and to the leakage properties.

In this paper, we investigate the issue of evaluating the success rate of side channel analysis in the widely admitted Gaussian leakage model. We introduce a new approach that allows us to efficiently compute the success rate of an attack in this model and we apply it to the two main families of side channel analysis: differential side channel analysis and profiling side channel analysis.

**Drop:** This paper discusses about the evaluation of the success rate of the attack which at this point is irrelevant for the project.