LABORATOIRE
HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Doctoral Thesis Review

Differential Power Analysis Countermeasures in Programmable Hardware

Submitted by Stanislav Jeřábek

The thesis has been submitted to the Faculty of Information Technology, Czech Technical University in Prague in the Ph.D. study program Informatics.

1. Up-to-dateness of the dissertation.

Since the last 90's, side-channel attacks have been a threat to cryptographic implementations. While several solutions have been presented and evaluated there is still room for efficient and resistant protection. The candidate contributed to the field of practical security of side-channel resistant implementations.

Protection against side-channel attacks is often proposed for lightweight ciphers to fit the constraints of embedded systems. While, this first step allows us to evaluate the sustainability of the approach. Scaling up the solution for standard cipher may present some unexpected issues.

Standard and well-studied ciphers are of particular interest for the industry, with efficiency and effectiveness of side-channel protections. It is thus important to implement and evaluate ad-hoc solutions to offer a good trade-off between security and efficiency.

One important contribution of this thesis is the demonstration that the implementation of dummy rounds can be applied to standard block cipher and that the security does not scale down when implemented with particular attention.

2. Formal structure and organization of the dissertation.

The structure of the thesis is classical.

The introduction briefly motivates the research problem for specialists in the side-channel area. It could be nice to have an introduction to a broader audience to demonstrate the capability of the candidate to explain with simplicity its work. Some unusual terms (e.g. "complex cryptographic algorithm") are not defined and the number of chapters is missing, still dots.

The background is also expert-oriented, this could be a sign of a lack of knowledge. However, this doubt is erased in the next chapters.

Laboratoire Hubert Curien
18 rue du Professeur
Benoit Lauras
42000 Saint-Etienne

Tél. +33 (0)4 77 91 57 80
http://laboratoirehubertcurien.fr

The next chapters present the main contributions of the candidate. The use of the same cryptographic algorithms in different parts could have helped the comparison between both main protections.

The contribution sections are based on different publications of the candidate. These articles have been published in peer-review conferences, and have already been cited by other scientists.

Then the conclusion presents open problems left by the thesis demonstrating the clear vision of the candidate on its work.

The 109 citations used in the thesis demonstrate the knowledge of the candidate on the literature on his subject and also with connected areas. One minor point is the lack of recent citations, which can be explained by the specific topics covered in this thesis.

3. Completion of the dissertation objectives.

The objectives of the thesis are clearly identified in the introduction. They are repeated hereafter.

1. Application of existing countermeasures to conventional cryptographic algorithms.
2. New countermeasures, with competitive performance for hardware implementations.
3. Evaluation of countermeasures in hardware implementations, in terms of efficiency and effectiveness.

Hardware implementations of efficient and effective countermeasures for cryptographic standards are of prime importance for various applications. The counter-measures studied in this thesis have been applied to the AES, Present, and Serpent. The implementations target recent FPGA.

4. Assessment of the methods used in the dissertation.

Scientific methods, tools, and techniques are consistent with state-of-the-art. For the algorithms studied, the platform used for the evaluation and the evaluation tool used.

The algorithms targeted in the thesis are standards of symmetric cryptography. The AES is widely used for baseline comparison since its acceptance as a standard in 2002. However, due to the high over-cost of its implementation and associated countermeasures, it is also of prime interest to look at lightweight cipher. Especially, the small number of rounds made the AES a bad candidate for the dummy round countermeasure.

The designs are implemented for the SAKURA-G board with Xilinx Spartan 6 FPGA. SAKURA boards are widely used for side-channel evaluations. They are built to ease side-channel analysis, they allow to use efficiently external oscilloscopes that are of prime importance for the evaluation of high-frequency implementations. SAKURA boards are widely used in security labs, thus they allow reproducible results.

The evaluation of the side-channel leakages is done with classical leakage assessments introduced by RAMBUS. The use of the non-specific fixed vs. random Welch's t-test is classical in the literature and can be considered as the worst case for the evaluator. Indeed, the non-specific may raise false positive leakages, i.e. leakage that are different according to the values but independent of all the sensitive values.

5. Evaluation of the results and contributions of the dissertation.

The contributions of this thesis are original and valuable in the field of side-channel resistant implementation. The combination of masking with random decomposition and the use of dummy rounds propose efficient side-channel protection. The authors demonstrate the effectiveness of the countermeasure by performing leakage assessments.

6. Remarks, objections, notes, and questions for the defense.

After reading the thesis, I still have some unanswered questions.

Section 3.1.3.1, is there any advantage to decompose the S-box using a larger field or other structure?

Section 3.1.3.2, from my understanding the outputs of R2 are not stored in any register. Thus I wonder how the glitches from this computation are managed to prevent leakages.

In Figure 3.2 (h), while the 4.5 threshold is not reached, it is very close. Maybe more traces are needed to detect a leakage? In particular, since Figure (f) shows first-order leakages, I do not see why combining it with S-box decomposition (that adds noise but should not impact security order) removes the leakages.

To counter S-box decomposition can we imagine combining classical side-channel attacks with an exhaustive search on the S-box decomposition?

For the dummy rounds, can we use a big mac-like attack to detect rounds with similar/identical input and thus perform pre-processing to use classical side-channel attacks?

I have also some remarks that may require a discussion to explain more precisely the view of the candidate.

Can you develop what you mean by "complex cryptographic algorithms"?

Section 2.2 "Threshold implementation is provably secured to an arbitrary d-th order" can you tell me in with model?

The security of the implementation is asserted with T-test. However, the T-test is more of a rule of thumb. Have you tested other methods?

7. The overall evaluation of the dissertation.

Despite the critical remarks listed in the previous sections, I consider this dissertation successful. The main reasons lie in the importance of the results presented and the in-depth evaluation of the countermeasures. The dissertation is original and does not contain any significant formal or factual deficiencies.

8. Recommendation Statement :

The author of the dissertation proved the ability to conduct research and achieve scientific results. In accordance with par. 47, letter (4) of the Law Nr. 111/1998 (The Higher Education Act) I do recommend the thesis for the presentation and defense with the aim of receiving the Ph.D. degree.

In Saint-Étienne, date 10/02/2024

Signature of the reviewer
Dr. Vincent Grosso, Ph.D.

Laboratoire Hubert Curien
18 rue du Professeur
Benoit Lauras
42000 Saint-Etienne

Tél. +33 (0)4 77 91 57 80
http://laboratoirehubertcurien.fr