FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH ústav
TECHNOLOGIÍ telekomunikací

Review report on the dissertation thesis

Candidate: Ing. Stanislav Jeřábek

Thesis title: Differential Power Analysis Countermeasures in Programmable Hardware

Formal structure and organization of the dissertation

The dissertation thesis submitted for consideration is 61 pages long. The dissertation thesis is organized into 5 chapters, the first introduction describes the main motivation, problem statement and goals. The second chapter explains the necessary theoretical background of the side-channels. The thesis briefly presents the theoretical background of side-channel analysis, side-channel attacks, and countermeasures. Naturally, the thesis focuses on power analysis and countermeasures that are applicable to FPGA (Field Programmable Gate Array) implementations. Chapter 3 describes own FPGA implementations of AES and Serpent protected by countermeasures. Author proved no leakage using first-order non-specific Welch's t-test. In Chapter 4, author presents the second own hardware Dummy Rounds countermeasure scheme that was also evaluated using Welch's t-test. The structure and scope of the thesis corresponds to the requirements for a dissertation thesis. I have no complaints about the structure and organization of the thesis, it is clear that candidate is very erudite and proceeded logically and with knowledge of the matter. Figures are also clear with sufficient resolution.

Up-to-dateness of the dissertation

The author worked on a very up to date topic in the field of security, focused on FPGA countermeasures for block cipher standard (AES) and cipher Serpent. Very important fact is that author realized the experiments based on well known testbed (SAKURA G board) utilizing FPGA Xilinx Spartan-6. Currently, this equipment is widely used by the scientific community and the results are thus suitably reproducible and the future research can follow up without problems. Moreover, the FPGA acceleration of cipher algorithms will play a critical role in the future with regard to the demanding computations in the post-quantum cryptography. People encounter implementation of AES on a daily basis, for example when browsing the internet utilizing the HTTPS protocol, therefore there is no doubt about the timeliness of the work. The references included in the thesis are 109, that cover research domain decently till year 2021. It is clear that this topic is a socially necessary, up-to-date, well elaborated and scientifically.

Completion of the dissertation objectives

I read the whole thesis with interest, the candidate set the following main goals clearly:

- implementation of complex cryptography algorithms secured by known countermeasures used primarily for lightweight algorithms.
- Proposal of new countermeasure implemented in hardware offering better or at least competitive combination of security, overhead and implementation complexity.
- Examine countermeasures used in software implementations and the transferability of their principles to hardware implementations.

I can unequivocally state that all the stated objectives of the dissertation have been met. However, the defined objectives are from my point of view very general, I do not see a direct link to the state of the art.

Evaluation of the results and contributions of the dissertation

The dissertation thesis considers the same research domain of FPGA, as the master thesis, however there is no overlap because the dissertation thesis focuses only on power analysis. The thesis is written primary as an overview text with explanation of basics including the own research and experimental results (chapter 3 and 4). The results presented were either taken from existing research literature or the candidate's own published research. In total, **five** of **eleven** publications selected by candidate are directly relevant to the thesis content. I was able to see from databases and direct search the most important papers (together 6 papers in Scopus database with 6 citations excluding the self citation, h-index 2 - 26.2.2024). As a result, I conclude that core contributions were already published by the candidate. One can criticize the articles published at conferences that are not so competitive (local conference MECO and DDECS). Exception are conference papers A1 and M5 from Euromicro Conference on Digital System Design - the conference is B1 according the `http://www.conferenceranks.com/`, however on the web-page `https://portal.core.edu.au/conf-ranks/` I can not see the conference at all.

Other disadvantage of the thesis results is also the absence of articles in the journal in WoS. Unfortunately, I cannot know the requirements for doctoral students at CTU but compared to our students, it is not usual to defend thesis without journal paper. The scientific and research level of the results of the thesis is rather lower, the scope of the work carried out, both theoretical and practical, is sufficient. Although the number of scientific results is lower, own contribution fulfils the requirements for a dissertation thesis.

Remarks, objections, notes, questions for the defense

Although the topic of the thesis is a highly technical scientific text, the argumentation and the application of mathematical apparatus are clear and natural. There are no parts of the thesis that, from the reader's point of view, appear unclear, incomprehensible or inaccurate. However, there are formal deficiencies in the thesis, which unnecessarily bring down the overall level of the thesis. In the following text, I will give some examples of a typographical error:

- The thesis is organized into . . . chapters (p.2) - number is missing.
- Naive is the more usual spelling than naïve (p.4).
- The sentence "remove the dependency of processed data and sidechannel output from an attacker's point of view" is twice p. 8.
- Abbreviations should not be in the title of the example p. 9.
- Abbreviations are not defined when first used in thesis e.g. FPGA.
- Abbreviations such a FPGA or AES are lowercase in bibliography.
- I would recommend describing the axes of the graph in sec. 3.3.

In the following text I present questions about the candidate's dissertation.

Q1: Considering the topic of the thesis, I do not understand why a benchmark comparing countermeasures and FPGA resource utilization was not done (comparing the number of LUTs, FF etc.). There is only one sentence on page 37 and 42. Why the comparison was not provided in the table ?

Q2: Why the own countermeasure implementation (based on lightweight cipher) was not directly compared with the standard countermeasure (based on standard cipher) ?

Q3: Why was only 1 million power traces used for evaluation ? For FPGA implementation it could be not enough.

Q4: I do not understand why the author do not present raw power trace of AES and Serpent, and do not discuss the noise in measurement setup - it is crucial to understand the results of power analysis. It is important to understand better the leakage, it is associated with samples.

Q5: How many power traces was necessary to carry out standard CPA attacks for FPGA implementation and your setup (first order CPA, AES and Serpent) ? Have you tried the standard CPA attack on your power traces ?

Q6: Generally 1.25 million of power traces are not enough for second order CPA that is targeted to FPGA implementation. Why you did not measure more power traces ?

Q7: Why the own implementations was not compared based on first order attack (e.g CPA based on PGE) for different number of power traces ? Considering the title of the thesis, it would be the most logical approach.

Q8: Do you still plan to publish some results or follow-up research in a journal ?

The overall evaluation of the dissertation

On the basis of the evaluation of the content of the dissertation thesis, its professional level, the quality of the research results, I conclude that the thesis meets all requirements to defense.
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 RECOMEND** the thesis for the presentation and defense with the aim of receiving the Ph.D. degree.

Brno 26.2.2024

....
doc. Ing. Zdeněk Martinásek, Ph.D.
Ústav telekomunikací FEKT VUT v Brně