FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Reviewer:	Ing. Jan Bělohoubek, Ph.D.
Student:	Adam Verner
Thesis title:	Power side channel attack with a controllable power supply
Branch / specialization:	Computer Security and Information technology
Created on:	12 June 2023

Evaluation criteria

1. Fulfillment of the assignment

- ▸ [1] **assignment fulfilled**
  [2] assignment fulfilled with minor objections
  [3] assignment fulfilled with major objections
  [4] assignment not fulfilled

2. Main written part

90 / 100 (A)

The work is well-written, and it contains no unnecessary parts. Typos are infrequent even some typos and duplicate words occur. "Private communication" should not be a part of the bibliography! I appreciate the "future work" chapter is a part of the thesis, but it seems to be vague: the author here resigned on important questions arising from the thesis itself and enumerates related topics only.

3. Non-written part, attachments

100 / 100 (A)

The assignment is fulfilled. I appreciate that student extended an open framework and his work was approved and merged into the upsteam.

4. Evaluation of results, publication outputs and awards

85 / 100 (B)

Student contributed to an open-source project.

The topic covered by the thesis has publication potential because it aims the practical experimentation, however, the results are not satisfactory yet. It might be necessary to perform additional experiments or extract more from existing data. There is for sure some work ahead to be publication-ready if intended.

The overall evaluation

95 /100 (A)

The assignment is fulfilled. Real issues are minor, the student did a considerable amount of work. The results are in question and probably should be classified as work-in-progress now, but the topic is hard: the dependency of DPA strength on supply voltage could be really negligible on the used target.

Questions for the defense

1) Please clarify: have you used the same input data for all measurements? In other words: did you compare random or equal datasets for different voltages (from the perspective of the power model)?

2) More comment than a question: did you consider using the distinguisher (correlation coefficient or difference of means) for voltage dependency directly? E.g. a difference in the "difference of means" for exactly the same data and different voltages could disclose the trend compared to the number o traces only (here you compare responses to different stimuli!).

Instructions

Fulfillment of the assignment

Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Main written part

Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies?

Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 52/2021, Art. 3.

Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Non-written part, attachments

Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Evaluation of results, publication outputs and awards

Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

The overall evaluation

Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.