FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Student:	Abdullah Bhatti
Supervisor:	Ing. Jiří Buček, Ph.D.
Thesis title:	Masked AES cipher on a microcontroller and Second-order DPA
Branch of the study:	Design and Programming of Embedded Systems

Date: 29. 1. 2019

Evaluation criterion:	*The evaluation scale: 1 to 4.*
1. Fulfilment of the assignment	***1 = assignment fulfilled,*** *2 = assignment fulfilled with minor objections,* *3 = assignment fulfilled with major objections,* *4 = assignment not fulfilled*

Criteria description:
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.

Comments:
The assignment was fulfilled.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
2. Main written part	*50 (E)*

Criteria description:
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. 26/2017, 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.

Comments:
The includes presents all necessary parts relevant to the thesis assignment, although sometimes in insufficient detail. The description of Differential Power Analysis (DPA) and Second-Order DPA is too terse. It would benefit from better explanation how the key hypotheses are formed, and how they are evaluated using the measurements. The student includes sections on hardware countermeasures against DPA, which could be reduced in favor of better explanation of DPA. The presentation of results seems rushed, probably caused by the student running out of time.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
3. Non-written part, attachments	*60 (D)*

Criteria description:
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.

Comments:
The student adopted code for a masked AES implementation from a previous thesis of Sochůrková (2016), which used a single mask. Then he implemented his own version using multiple masks. The student performed First and Second-Order DPA on several variants of the code, first with masking disabled (mask set to zero), and later with masking enabled. The student was successful in breaking the single mask implemenation using Second-Order DPA. The multiple mask implementation was not broken, but this was probably caused by variable execution time of the rand() function in the standard library, therefore including an inadvertent hiding-in-time countermeasure.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Evaluation of results, publication outputs and awards	*70 (C)*

Criteria description:
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.

Comments:

The results of the thesis will be used in teaching hardware security courses (MI-HWB and MIE-HWB).

Evaluation criterion:	*The evaluation scale: 1 to 5.*
5. Activity and self-reliance of the student	*5a:* *1 = excellent activity,* *2 = very good activity,* *3 = average activity,* ***4 = weaker, but still sufficient activity,*** *5 = insufficient activity* *5b:* *1 = excellent self-reliance,* *2 = very good self-reliance,* *3 = average self-reliance,* ***4 = weaker, but still sufficient self-reliance,*** *5 = insufficient self-reliance.*

Criteria description:

From your experience with the course of the work on the thesis and its outcome, review the student's activity while working on the thesis, his/her punctuality when meeting the deadlines and whether he/she consulted you as he/she went along and also, whether he/she was well prepared for these consultations (5a). Assess the student's ability to develop independent creative work (5b).

Comments:

The student required detailed instructions on the progress of his thesis. He was active enough to successfully perform the necessary work.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*60 (D)*

Criteria description:

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.

Comments:

The student proved his ability to perform independent creative work in his field of study. Despite the aforementioned shortcomings, I hereby recommend the thesis for defense.

Signature of the supervisor: