FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Student: Abdullah Bhatti
Reviewer: Dr.-Ing. Martin Novotný
Thesis title: Masked AES cipher on a microcontroller and Second-order DPA
Branch of the study: Design and Programming of Embedded Systems

Date: 15. 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 goal of the thesis was 1) programming of masked AES implementation on AVR microcontroller and 2) performing first-order and secocd-order DPA (differential power analysis) attack on this implementation. I am not fully assured whether the author had this assignment in his mind all the time, as he does not fully concentrate on these two topics in his thesis, and he deals with some other topics instead. The written report shows many flaws (comments below).

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:
It is not clear whether the author is fully oriented in the area of side-channel analysis and protection against side-channel attacks. Also it is not clear whether the author fully understood the two task he was assigned.
- There are parts of the text that are superfluous as these parts are not related to the topic at all - e.g. subsections 1.6.3-1.6.5 and 1.6.7-1.6.8. Subsection 1.6.6 contains information on randomization of Elliptic Curves, althought the thesis does not deal with EC.
- Subsection 1.6.9 "Fixed memory usage" does not fit into section 1.6 Countermeasures. It tackles the implementation details connected with used SmartCard and therefore should be moved to the proper section.
- The beginning of section 1.7 ATMega163 Smart Card is copy-pasted from the source [9]. Why? Moreover, it is not clear what copy-pasted information is important for the thesis. Again, it looks like padding.
- On the other hand, crucial parts of the thesis are not properly explained and they are hard to read even for experienced reader. For example, the masking scheme in subsubsection 2.2.1.1 Single mask should be illustrated by Figure; the Equation 2.3 is not further simplified and commented, etc. Following subsection 2.2.1.2 and Figure 2.1 are also unclear.
- There are also problems with references. E.g., Dummy cycles in subsection 2.3.3 should be referenced. Atmel Application Note in subsection 2.4.1 should be referenced as well. Moreover, references [7] and [8] (page 53) do not cite relating papers, but proceedings in which the papers were published.
- The structure of the text is problematic, as e.g. implementationm and results are mixed-up together (e.g. in subsection 2.8.2.)
- There are also several typos. E.g., the author several times replaces "first-order"with "single-order" and "second-order" with "double-order". Also, Hamming weight and Hamming distance should always be written with capital H, as they are named after Richard Hamming.
- Also, many mathematical symbols are not properly typesetted - when they appear in common text, they should be put inside mathematical environment, like f, n, etc.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
3. Non-written part, attachments	*50 (E)*

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 CD contains two source codes fo AES - one for single maks, one for multiple mask. However, Mathematica experiments contain just one set of power traces. Which version of the program was analyzed? Moreover, I tried to run Mathematica notebook, but it gets stucked after an assignment to the variable "ho".

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Evaluation of results, publication outputs and awards	*50 (E)*

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:

Results can be reused only partly, due to poor description of the experiment.

Evaluation criterion:	*No evaluation scale.*
5. Questions for the defence	

Criteria description:
Formulate questions that the student should answer during the Presentation and defence of the FT in front of the SFE Committee (use a bullet list).

Questions:

In section 3.2 (page 49) you write: "Finally, we had to apply second-order DPA on our multi-masked masking scheme. Unfortunately, our implementation contained the rand function before the processing of the rounds and we were not able to guess the correct clock cycles for the operations during SubBytes that were leaking information. Our
times were shifted on each iteration of the code due to hiding which was not the case for our single mask masking scheme. When trying to move the rand function to the end of the round, other issues started to present themselves which were not faced due to time constraints and will be touched in the future."

1) Why did you use hiding? This was not part of your assignement. Could you remove hiding from your code? If yes, why did not you do it?

2) Could you run rand() function separately, before the encryption itself? I mean, was it possible to run rand() function first, and after that switch on the synchronization pulse and start the encryption itself? This would eliminate the problem of varying timing of the function rand().

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. The overall evaluation	*50 (E)*

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:

Despite above mentioned flaws I recommend the thesis for a defence and I recommend it to be graded E.

Signature of the reviewer: