FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Reviewer:	Ing. David Pokorný
Student:	Bc. František Kovář
Thesis title:	Side-channel Attacks on Supersingular Isogeny Diffie–Hellman Key Exchange
Branch / specialization:	Computer Security
Created on:	22 August 2022

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

The scope of the thesis is optimal and all parts of the assignment have been completed.

2. Main written part

71 /100 (C)

The structure of the text is clear and easy to read. Referencing is extensive, containing 43 citations.

The author could have focused more on the theory of EC, the explanation of the mathematics behind the supersingular EC instead of the foundation of discrete mathematics. The practical part is balanced well.

The diploma thesis contains several mistakes (e.g. the definition of an irreducible polynomial, imprecise non-formal definitions, etc.). In general, I would recommend choosing more scientific formulations instead of "We need two ingredients to define", "This equation looks rather ugly" or "Before we jump into the definition."

The description of the used hardware could be more detailed. Expressions like "it (ChipWhisperer) has most of the needed things" or "we don't have to worry about the noise that much." do not tell us about ChipWhisperer's equipment or signal-to-noise ratio. Sample rate and clock rate information are missing.

The conclusion contains steps taken after the unsuccessful attack that definitely should have been mentioned earlier. The author did not properly distinguish whether this is the first realization of the attack or not.

3. Non-written part, attachments 100 /100 (A)

The author used the relevant implementation of the given cryptosystem. The attack has been implemented in python-jupyter. The code is clear and self-explanatory. The experiment can be replicated. The measured data are attached.

The measuring device is well chosen.

4. Evaluation of results, publication outputs and awards 78 /100 (C)

The attack itself was unsuccessful. The author tried to reveal the reason by checking intermediate results, checking measured data, checking the correlation of hypotheses against processed values, and the oracle was checked. The reason for the failed attack remains unknown.

If the attack was successful, it would be a replica of a previously executed attack on the Double and add algorithm during the isogeny walk, which would be a verification of the attack feasibility.

The most important contribution of this thesis is the code of the attack itself.

The overall evaluation 82 /100 (B)

The thesis contains a well-described SIKE algorithm and a description of the attack's Points of Interest with code examples. It also includes a well-described overview of supersingular EC, existing implementations of the SIKE cryptosystem, and side-channel attacks. The quality of the written text is inadequate for academic writing.

Unfortunately, the attack was unsuccessful.

Questions for the defense

The attacker is in the position of Alice and has access to Bob's power consumption. Since this is a key-exchange protocol, would Alice's data be sufficient to know the shared key? After all, Alice knows the shared key.

What method did you use to decide that the attack was unsuccessful?

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.