FACULTY OF INFORMATION TECHNOLOGY CTU IN PRAGUE

Supervisor's statement of a final thesis

Supervisor:	Ing. Josef Kokeš, Ph.D.
Student:	Arnold Stanovský
Thesis title:	Evaluation of Percy++, A Private Information Retrieval Library
Branch / specialization:	Computer Security and Information technology
Created on:	9 December 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

I consider the assignment mostly fulfilled. The part I feel is not sufficiently described in the thesis is the "Analyze the security properties" from instruction #4 - while the student does explain the security properties in general, my intention was to show how these properties hold in practice (i.e. what kind of data could the server deduce from the queries).

2. Main written part

85 /100 (B)

The majority of the text is clear and to the point. I particularly appreciate Chapter 2 (Use Cases) which I consider very well thought-out and presented. Chapter 1 is well researched and generally fine, but in places fails to explain all the symbols used (e.g. the Omega in section 1.2). Chapter 3 presents the performance differences between different algorithms well but is missing their practical privacy evaluation.
As far as the technical quality is concerned, I noticed a few minor problems (such as missing words or an occasional discrepancy in tenses) but nothing that would hinder understanding. The most disruptive issue is the color shift for the "trivial transfer" between figures 3.2 and 3.3.

3. Non-written part, attachments

90 /100 (A)

The non-written parts are adequate for the task. It might have been more user-friendly to also include the compiled binaries, but that isn't really an issue.

4. Evaluation of results, publication outputs and awards 80 /100 (B)

The thesis focuses on the practical evaluation of existing elements (the PIR algorithms and their implementations) rather than building new ones. I consider that approach valid as the practical usage can be quite distant from the theoretical descriptions. Certainly the benchmark results from the thesis demonstrate what a user should expect if they wanted to enhance their privacy.

5. Activity of the student

[1] excellent activity
[2] very good activity
[3] average activity
▸ **[4] weaker, but still sufficient activity**
[5] insufficient activity

The student tended to work on their own, consultations were fairly limited.

6. Self-reliance of the student

[1] excellent self-reliance
▸ **[2] very good self-reliance**
[3] average self-reliance
[4] weaker, but still sufficient self-reliance
[5] insufficient self-reliance

The overall evaluation 85 /100 (B)

The thesis provides a nice introduction to the problem of private information retrieval as well as a sample code and benchmarks. While I am missing the practical evaluation of the privacy aspects, I appreciate the well written Use Cases chapter. Overall, I recommend the thesis for defense and grade it B-very good.

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.

Activity of the student

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.

Self-reliance of the student

From your experience with the course of the work on the thesis and its outcome, assess the student's ability to develop independent creative work.

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.