

I. IDENTIFICATION DATA

Thesis name:	Privacy for Secure Distributed Storage Networks
Author's name:	Enio Marku
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Telecommunication Engineering
Thesis reviewer:	Ing. et Ing. Pavel Schlitter, Ph.D.
Reviewer's department:	SITEL, spol. s r.o.

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment	challenging
<i>Evaluation of thesis difficulty of assignment.</i>	
Diploma thesis deals with the problematics of privacy preserving in nowadays very popular technology – cloud services. The theme of the thesis is interesting and also challenging because this problematics is relatively new and not yet been explored too much.	

Satisfaction of assignment	fulfilled
<i>Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.</i>	
Student fully fulfilled the assignment.	

Method of conception	correct
<i>Assess that student has chosen correct approach or solution methods.</i>	
The thesis is logically structured into six chapters. Student starts with motivation and theoretical description of current state of knowledge in this area. Then main cryptographic blocks and protocols for privacy preserving are described. In next chapters author introduces his own PIR protocol based on Shamir Secret algorithm with subsequent optimizations and throughput measurements.	

Technical level	A - excellent.
<i>Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by experience.</i>	
The thesis has a good professional level. Students had to get familiar in detail with very complex cryptographic algorithms and protocols. In the practical part he programmed in Java and addressed the issues associated with deployment his application in real cloud environment.	

Formal and language level, scope of thesis	A - excellent.
<i>Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.</i>	
Formal level of thesis is good. There are some minor typographical and grammar mistakes but without overall impact to the thesis.	

Selection of sources, citation correctness	C - good.
<i>Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are complete and in accordance with citation convention and standards.</i>	
Cited parts are significantly distinguished from his own thoughts. In citation [33] there is only hyperlink without any other information. Also in some cited sources there is no information from which book or magazine the article came from or when it was published (e.g. [21], [25], [48]).	

Additional commentary and evaluation

Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.

All the goals of the thesis were met. Students demonstrated the ability for practical implementation of the proposed theoretical procedures.

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation. Please present apt questions which student should answer during defense.

Proposed thesis is of good quality and all mentioned drawbacks are only minor.

Questions to the student:

- 1) Which part of the protocol or its implementation would be a possible candidate for following optimization to achieve even higher throughput?
- 2) Does throughput depend on number of nodes?

I evaluate handed thesis with classification grade **A - excellent**.

Date: **24.1.2017**

Signature: