Supervisor's statement of a final thesis

Czech Technical University in Prague **Faculty of Information Technology**

Student: Bc. Peter Poljak
Supervisor: Ing. Josef Kokeš
Thesis title: The Impossible Differential Cryptanalysis
Branch of the study: Computer Security

Date: 26. 1. 2017

Evaluation criterion: *The evaluation scale: 1 to 5.*

1. Difficulty and other comments on the assignment

1 = extremely challenging assignment,
2 = rather difficult assignment,
3 = assignment of average difficulty,
4 = easier, but still sufficient assignment,
5 = insufficient assignment

Criteria description:
Characterize this final thesis in detail and its relationships to previous or current projects. Comment what is difficult about this thesis (in case of a more difficult thesis, you may overlook some shortcomings that you would not in case of an easy assignment, and on the contrary, with an easy assignment those shortcomings should be evaluated more strictly.)

Comments:
I rate the assignment as unusually difficult due to its highly mathematical nature and the lack of suitable explanatory materials. The student had to understand a novel technique in detail sufficient not only to perform an attack against a cipher, but also to explain its principles and behavior to other people.

Evaluation criterion: *The evaluation scale: 1 to 4.*

2. 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 thesis meets the assignment statement. In Comments indicate parts of the assignment that have not been fulfilled, completely or partially, or extensions of the thesis beyond the original assignment. If the assignment was not completely fulfilled, try to assess the importance, impact, and possibly also the reason of the insufficiencies.

Comments:
The assignment was completed successfully.

Evaluation criterion: *The evaluation scale: 1 to 4.*

3. Size of the main written part

1 = meets the criteria,
2 = meets the criteria with minor objections,
3 = meets the criteria with major objections,
4 = does not meet the criteria

Criteria description:
Evaluate the adequacy of the extent of the final thesis, considering its content and the size of the written part, i.e. that all parts of the thesis are rich on information and the text does not contain unnecessary parts.

Comments:
Formally, the length of the report satisfies the requirements for a master's thesis. Unfortunately, this has been partially achieved through tricks such as an extensive use of paragraphs, or through text sections which duplicate more formal expressions used before them. If the density of the text were matching the expected levels of master theses, the text length would fall well below the requirements.

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

4. Factual and logical level of the thesis

70 (C)

Criteria description:
Assess whether the thesis is correct as to the facts or if there are factual errors and inaccuracies. Evaluate further the logical structure of the thesis, links among the chapters, and the comprehensibility of the text for a reader.

Comments:
The report makes it easy (caveats follow) to understand the technique of impossible differentials cryptanalysis. The frequent use of specific examples gives the reader an easy-to-follow guide where she can easily verify her own results against the results she should get according to the technique. In this aspect, the report serves its purpose very well.

The last part of the explanation of the impossible differentials (page 24, 25) fails to provide a clear understanding to the reader due to skipping several important explanations: It is easy to forget why we can work with the input difference, and it is very easy to get confused by the differences between table 3.2 and the list of impossible differentials at the end of page 24. Fortunately, these issues are easy to spot and fix.

Tables 4.1 and 4.2 need an explanation of the meaning of the input and output values. At the moment, the reader needs to be deeply familiar with Heys' Tutorial on Linear and Diffferential Cryptanalysis ([3] in the thesis) to properly understand these values, and even then it is easy to make mistakes (e.g. are these values calculated in MSB or LSB order?).

It would be beneficial if the individual components of the analysis in chapters 4.1 to 4.6 took the theorem-proof form rather that example-conclusion. Examples serve well in providing better understanding, but they should not stand alone in the reasoning. For example, it's not clear where the second paragraph of 4.3 comes from and if it indeed is true; some proof is required here.

The algorithm on page 34 tends to mix the specifics of data structures used in the actual implementation into the general process (variables start, end), and as such needs to be modified before actual use.

It is quite unclear what's the real difference between the 1st and 2nd variant of the attack on 2-round Baby Rijndael (chapters 4.9.1, 4.9.2): The impossible differentials are necessarily the same in both variants (otherwise we couldn't combine SubBytes and MixColumns into a single operation) and since MixColumns is not used in the last round at all, it can't influence the process of the cryptanalysis. As far as I can tell, the difference only influences the speed of pre-calculation of the impossible differentials. The difference could be significant if we performed the decryption for more than one round, then the MixColumns operation would take place and the variants might lead to different results, but unfortunately the time constraints prevented any exploration of this possibility.

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

5. Formal level of the thesis *70 (C)*

Criteria description:
Assess the correctness of formalisms used in the thesis, the typographical and linguistic aspect s, see Dean's Directive No. 12/2014, Article 3.

Comments:
The language used throughout the thesis isn't quite suitable to a technical text where we desire precision and clarity. The current text may be easier to understand by a layman, but the expressions tend to be too vague for use in a master thesis.

Despite multiple editors going over the text, the English used is riddled with errors. The structure of the sentences makes it too clear the writer is not a native speaker, and the frequent incorrect use of the articles doesn't help either. More repetitions of the review-edit process would be desirable.

All instances of the use of quotes symbols are incorrect - a closing quote symbol should be different from the opening one.

The "ff" sequences look particularly ugly in the algorithm on page 34.

The Figures tend to be a part of the text rather than standalone entities referenced from the text (e.g. in chapter 4).

I am rather unhappy with the fact that the time complexity of each attack is first documented in the conclusion. The conclusion should summarize the previously described results, not present new ones.

Generally, I don't understand the distinction between a bold text and an italic text in this thesis. It seems they are used interchangeably throughout the report.

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

6. Bibliography *70 (C)*

Criteria description:
Evaluate the student's activity in acquisition and use of studying materials in his thesis. Characterize the choice of the sources. Discuss whether the student used all relevant sources, or whether he tried to solve problems that were already solved. Verify that all elements taken from other sources are properly differentiated from his own results and contributions. Comment if there was a possible violation of the citation ethics and if the bibliographical references are complete and in compliance with citation standards.

Comments:
The student's choice of materials for the thesis is satisfactory, although I think the original materials (e.g. Matsui: Linear Cryptanalysis Method for DES Cipher) should be used instead of study materials or links to generic encyclopaedia. Some newer sources could surely be found, too.

The citations are handled correctly as per requirements, unfortunately, there are rather few of them - the majority of the sources are only explicitly used in the two pages of Impossible differential cryptanalysis history (section 3.1). It is unclear on which materials the actual explanation of the technique (the rest of section 3) was based. The date of recovery of the online materials is not listed. The use of italics seems to be inconsistent through the Bibliography.

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

7. Evaluation of results, publication outputs and awards

85 (B)

Criteria description:
Comment on the achieved level of major results of the thesis and indicate whether the main results of the thesis extend published state-of-the-art results and/or bring completely new findings. Assess the quality and functionality of hardware or software solutions. Alternatively, evaluate whether the software or source code that was not created by the student himself was used in accordance with the license terms and copyright. Comment on possible publication output or awards related to the thesis.

Comments:
Despite the mistakes mentioned above, the achieved results are in fact quite nice. I am particularly happy about the fact that the student managed to understand the technique well enough to be able to explain it to the reader in a straightforward and easy-to-understand manner. That in itself is very valuable. The analysis of Baby Rijndael is also promising, although it suffers from some errors and from the fact that only a simple last-round-descent was performed due to the time constraints.

Evaluation criterion: *No evaluation scale.*

8. Applicability of the results

Criteria description:
Indicate the potential of using the results of the thesis in practice.

Comments:
The thesis doesn't reveal any brand new discoveries, but it summarizes the known facts about the impossible differential cryptanalysis in a very easy-to-understand manner which will allow future students to make use of this novel and interesting technique. The use of English, even not-so-great English, helps here as well. On the other hand, the benefits of the thesis are somewhat diminished by the lack of precise formulations of theorems and proofs.

Evaluation criterion: *The evaluation scale: 1 to 5.*

9. Activity and self-reliance of the student

9a:
1 = excellent activity,
2 = very good activity,
3 = average activity,
4 = weaker, but still sufficient activity,
5 = insufficient activity

9b:
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:
Review student's activity while working on this final thesis, student's punctuality when meeting the deadlines and consulting continuously and also, student's preparedness for these consultations. Furthermore, review student's independency.

Comments:
The student was very active and above-average self-reliant.

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

10. The overall evaluation

80 (B)

Criteria description:
Summarize the parts of the thesis that had major impact on your evaluation. The overall evaluation **does not** have to be the arithmetic mean or any other formula with the values from the previous evaluation criteria 1 to 9.

Comments:
While the submitted thesis is not perfect and would benefit from more time dedicated to it (both the research and the editing), it achieves the goal of explaining the Impossible Differential Cryptanalysis quite well. I appreciate that the student tried to make his work useful to as many users as possible through the use of English and through the extensive use of examples. Despite some of the shortcomings of the work, which were partially caused by the lack of time to study them more thoroughly, this lack of time caused by the complex nature of the topic matter and the time required to understand it, I think the overall result is quite good and will be a significant help to beginner cryptographers.

Signature of the supervisor: