Evaluation form to "A Formal Approach for Automatic Verication of Imperfect Cryptographic Protocols"

19. november 2007. a.

1 Evaluation gategories

Evaluation criterion	Evaluation
The paper is well readable	Rather Yes than No
Language used in the paper is correct	Yes
The paper is logical and well structured	Yes
The general typeset of the paper is correct	Rather Yes than No
The paper was interesting to read	Rather Yes than No
The paper gives a good overview of the topic	Yes
The material in the paper is mathematically correct	Yes
References to the external sources are presented correctly	Rather Yes than No
All the relevant references are present	Rather Yes than No
The formulas are typed correctly	Rather Yes than No

2 Topic, style ...

1. How to evaluate the selection of the topic? The topic is interesting and very related to the course "Cryptographic Protocols", that I am taking now.

2. How to evaluate general presentation style? The general presentation style is not bad. It is logically structured and the language is very good, but the explanations could be more detailed.

3. How to evaluate the selection of the information given in the paper? The information is selected form ten different sources and it appears to me that everything is important.

4. How to evaluate typesetting of the paper? There were some little mistakes in typesetting of the paper.

5. What was new and interesting to me in the paper? I liked the example of this framework application (Wide Mouthed Frog protocol).

6. What else would I have liked to read? In the paragraph 2.1 there could be some little examples to describe how the semantics is used.

3 Specific shortcomings

1. The paper has the following misprints:

   - There is a bracket missing from the first formula on page 3: $Pr[m \leftarrow A(m_K, G)] \leq p_{dec}(m_K, G)$ for all A and from the algorithm $addKeys$ from the line before the last line: $addKeys(L, p')$.
   - The first line on page 5: "We observe that formal semantics of spi calculus still holds in this extension if we leave out the probability (i.e. 0)".
   - Two sentences further: "Therefore, since we have modified spi-calculus by easing ... "
   - page 6: In the first proof, a comma in the sentence "We have proved that ,in ...

2. The paper has the following mistakes in wording and style:

   - page 4: I would add some verb in this sentence: "The reason we have to approximate is because it is rarely to find blocks with exactly the same probability of decryption.",
   - On the same page, six sentence further there is analogical wording misunderstanding: "The reason we choose to inherit from spi-calculus is because it provides a formal semantics for analyze security protocols."
   - The last formula on page 5 has too much Italic font (equality signs) :).
   - The first line on page 6 and second sentence on page 8 could have "n" in some mathematical style. Also the first "P" in the next sentence could be in Italic.
   - Missing "r" from the next sentece "It also means that proof of correctness ... "
   - page 7: The last theorem has lost a dot and the proofs second sentence has a space before comma. Next sentence don't have a verb, so you could add it for example: "Therefore, in computational model, there are no probabilistic polynomial-time process A that can distinguish P and P_0".
   - page 7: In the spi-calculus notation one *case* has brackets but the others have not. The same style mistake is copied to page 8 also.

3. The paper has the following mathematical mistakes:

   - page 4: probabilistic similarity definition contains expression $|pMax_M - pMax_M|$, which is always zero. I think one of them could be $pMax_N$.

4. The paper has the following mistakes in typesetting:

   - page 10: The figure 1 is empty and its heading could not end with a dot "."
   - There is some serious problem with [MA00] heading in the end of page 5. I think that is caused by this underline, which is not necessary.

5. The paper will be more readable if the author makes the following changes:

   - On page 4 there is used Exp and $pPat$, that are not defined before (though I deduced they are set of expressions and probabilistic patterns).
   - I found some [ref]-s from introduction, that could refer to somewhere.

6. The paper misses the following elements:

   - Conclusion
   - Figure 1

7. The following elements could be removed from the paper: -

8. Other comments: -