A Review on “Cryptographic reductions” by Margus Niitsoo

Referee: Long Ngo

<table>
<thead>
<tr>
<th>Evaluation criterion</th>
<th>No</th>
<th>Rather no than yes</th>
<th>More or less</th>
<th>Rather yes than no</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The paper is well readable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Language used in the paper is correct</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>The paper is logical and well structured</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The general typeset of the paper is correct</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>The paper was interesting to read</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>The paper gives a good overview of the topic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>The material in the paper is mathematically correct</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>References to the external sources are presented correctly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>All the relevant references are present</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>The formulae are typed correctly</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>

Answer the following questions in free text.

1. How to evaluate the selection of the topic?

   The topic is interesting. To me cryptographic reductions play an important role in security analysis. Although it is not a new thing but essential.

2. How to evaluate general presentation style?

   Clear

3. How to evaluate the selection of the information given in the paper

   - I think the introduction should state clearly “what this paper is about” and “the outline of the rest”. It helps a reader to know if this paper is exactly what he is looking for or not and if he wants to continue reading the rest or not
   - The information is “to the point”. We can see several type of reductions

4. How to evaluate typesetting of the paper?

   Good
5. What was new and interesting to me in the paper?

I am interested in security protocol analysis, and this paper gives me a nice overview of an important technique for security analysis. Before I did not have time to read this technique.

6. What else would I have liked to read?

Nothing.

Please refer to specific shortcomings.

1. The paper has the following misprints:

   Perhaps NO

2. The paper has the following mistakes in wording and style
   - In Section 2.1, line 6, I think you should use a different “c”, for avoiding misunderstanding. Also in 4 lines after that, what is “t”.
   - Are there 7 different types of crypto reductions? You said 7 but I counted 4.

3. The paper has the following mathematical mistakes:

   Perhaps NO

4. The paper has the following mistakes in typesetting:

   Perhaps NO

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

6. The paper misses the following elements (topics, references, figures, proof steps, etc.):

   Formally it should have an abstract

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

   Perhaps NO

8. Other comments

   I was a bit surprised that your topic was changed from the original one, “Hash computation”, 😊