OPPONENT RECORD

Thesis compiled by

Josefin Agerblad and Martin Andersen

Title of thesis:

Provably Secure Pseudo-Random Generators

Opponent:

Dmitrij Lioubartsev

Was it easy to understand the underlying purpose of the project? Comments.

Yes. The goal of the project was clear: research and explain the subject of provably secure pseudo-random generators and compare two common algorithms within that subject, and implement one of the algorithms.

Do you consider that the report title justly reflects the contents of the report?

The title is a bit vague. It clearly states the subject of the report, but does not give clues as to what the goals of the project are. For example, a suggestion of an alternative, more descriptive, title is "Comparision of Provably Secure Pseudo-Random Generator Algorithms".

How did the author describe the project background? Was there an introduction and general survey of this area?

The background chapter was very extensive and all relevant material was described in a good order.

To what degree did the author justify his/her choice of method of tackling the problem?

The method was to study background material, and from that, do a small comparison of algorithms according to speed, security and application, and then implement the better one. The two algorithms compared were Blum-Blum-Shub and Blum-Micali. There was no mention of other algorithms. It was simply stated that these two algorithms are the two most famous ones, and it is implied that they are the most commonly used. However, there was no discussion as to why these two are the most used.

Did the author discuss the extent to which the prerequisites for the application of such a method are fulfilled?

Yes, the background chapter clearly stated how the algorithms worked and the math needed to implement them.

Is the method adequately described?

The method description is very brief and seems to rely on the user looking at the source code. An appendix should not be part of the explanation, but should rather be a complement.

Has the author set out his/her results clearly and concisely?

Due to the nature of the project, no strict results were presented. Instead the results consisted of a discussion and a conclusion. It would have been nice to see some output of the implemented algorithm though.

Do you consider the author's conclusions to be credible?

The discussion chapter was very brief and seemed unfinished. One comparison factor was algorithm speed. Naturally, I assumed the "algorithm speed" meant how fast the algorithms could provide output, given input (a similar speed test as to what Kattis does). However, the authors discussed the speed of solving the problem the algorithms were associated with, and I was very confused while reading that section. It was then said that security and speed are basically the same thing. Then why have that as two separate factors? Perhaps a clear definition of how to measure the various factors should be given before the discussion.

What is your opinion of the bibliography? What types of literature are included? Do you feel they are relevant?

The bibliography is very extensive and is utilised well in the background chapter.

Which sections of the report were difficult to understand?

The language overall was fairly simple so it was not very hard to understand. However, the method chapter was very imprecise and hard to get an overview off.

Other comments on the report and its structure.

The structure was well organized and easy to follow. Lots of metatext was also really good for understanding. However, the report contained 12 pages background, and only 2 pages discussion, which seem a bit proportionate.

What are the stronger features of the work/report?

The very extensive and descriptive background.

What are the weaker features of the work/report?

The method and the discussion chapters are very brief. The language in the report is very unscientific.

What is your estimation of the news value of the work?

Because of the briefness of the discussion, and my limited knowledge of the field, I cannot comment on this. A summary of similar work, more than just links in the bibliography, would help.

Summarize the work in a few lines.

The authors did a very good research on the relevant subject and explained it well, but did not utilize that research very well for the discussion. I cannot comment on the algorithm implementation because no analysis was done about it and no results from it were provided. The authors said that the implementation was good simply because it is "an elegant peace of code" and that it is easy to understand, which is not a very convincing argument.

Questions to author:

1. The background chapter is very long (12 pages) compared to the discussion (2 pages). Do you think that structure is good, or what is the motivation to such a disproportionate structure?

2. You simply stated that the Blum-Blum-Shub and Blum-Micali were the two most famous algorithms and that's why you compared them. Are there other algorithms, and why are these two the most common ones?

3. One of the algorithm comparison factors was labelled speed. Naturally, one would assume that algorithm speed was the execution speed, but in this report it is the time it takes to solve the underlying problem. Then it is stated that security is basically the same thing. What is the point of having these two as separate factors? What about also measuring execution speed? What is your opinion on this?