KTH Computer Science and Communication

Kerstin Frenckner, tel 08–790 9754, e-mail:. kfrenck@csc.kth.se2 February 12, 2009

OPPONENT RECORD

Thesis compiled by Joakim Uddholm Hjalmarsson

Title of thesis: Voting Mix-Net

Opponent: Chjun-chi Chiu

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

The underlying purpose of the project was easy to understand. It was made clear what the purpose of the report were from the abstract. The overall report reflected the purpose as well.

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

The title of the report completely reflect the content of the report because the title is the word that describes the system that is being implemented and tested.

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

The introduction was relevant to the project. The author clearly described the real world problems related to the project but the introduction was short and did not have a general survey of the area.

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

The author did not justify his/hers choice of method. The method was directly chosen with no further explanation.

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

The author did not discuss the extent of the prerequisites for the application.

Is the method adequately described?

The method to implement the Mix-Net protocol was adequately described for a technical person but would be hard for a non technical person to understand. The report lacked a section for different Abbreviations, definitions and acronyms.

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

The results could have been illustrated better with diagrams and pictures for a clearer and easier overview of the result.

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

The author's conclusion can be considered credible because of the limited way he implemented and tested the application.

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

The author used a mix of articles, documents and websites. They are all relevant to the project. but some of the references are only used briefly.

Which sections of the report were difficult to understand?

The implementation part of the report was the hardest to understand because it was all about how the application was going to be implemented, a few pictures and flow charts might have made it easier to understand.

Other comments on the report and its structure.

The report was well structured which made it easy to read and follow.

What are the stronger features of the work/report?

The stronger features of the report is that it keep itself relevant throughout the whole report and managed to get a result from the application that was implemented.

What are the weaker features of the work/report?

The weaker features of the report is that it lacks a section for different Abbreviations, definitions and acronyms. Many of the words that was used in the report is not known to the average person.

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

Because the work was an implementation of an already existing work, the work does not bring a lot of news value.

Summarize the work in a few lines.

A voting application was partially implemented from a Mix-Net protocol made by Wikström, Moran and Khazaei. Then the performance speed was tested of the implemented voting application.

Questions to author:

1. What was the purpose of this report?

2. How much more time would it take you to fully implement the Mix-Net protocol?

3. Would you recommend the Swedish government to start using the fully implemented Mix-Net protocol for Swedish elections?

4. What are the biggest flaws with a computer based voting system?