Opinion on "Security of cryptographic schemes for contact tracing"

The thesis is on a recent important cryptography topic on contact tracing. It concerns security/privacy issues of recent algorithms used in tracing the contacts of Covid-positive patients in the ongoing pandemic. Several methods were published to address the issue [TPH20,Pie20]. Also, a security model was introduced in [DDL20].

First the authors define the schemes of [Pie20] in Section 2. Making use of recent sources on the subject matter [CDN15,KL15], the author describes the schemes carefully. In Section 3, the author uses the security model in [DDL20] to evaluate the scheme DP4T introduced in [Pie20] (which was defined in the beginning of Section 3 of the thesis in review). In [DDL20], the model is used to analyze the security of DP3T. The author carefully extends this to DP4T.

The author introduces new attacks in Section 3.2.3. These are

- Contact Identity Disclosure by a Server Owner, and
- Time of Contact Disclosure.

Then he shows that while DP4T is resistant to these attacks, a few previous attacks found in the literature are not. He also deduces conditions on when a scheme is resistant to such attacks. I think that these new definitions are quite meaningful and the attacks they describe makes sense.

The mathematical content of the thesis is commensurate with the level used in the field. I think the author shows good understanding of the proof methods.

Author's contribution is, as explained above, introducing two new attacks based on two rather meaningful assumptions and writing them in the way done in [DDL20] for previous attacks. I think the contribution is noteworthy. Also, some recent results were explained in some extra detail.

Use of sources: The author makes good use of recent research and sources (such as textbooks on the subject matter). The citations are properly done. One small comment is that in a bibliography, when an Internet resource (such as IACR e-prints) is given, the URL should be present along with access date.

The form of the thesis is quite good. One easily understands what the subject is, what the previous results were, what the contributions are, etc. Succint introduction and conclusion is provided. There is a few typos, which I mention below, that does not diminish the quality of the work.

Overall, I think that this is a good thesis and it deserves the best grade (1.0).

- p.4 asymptotic → asymptomatic
- p.13 "commit if a randomized" → "commit is a randomized"
- p.17 time is united → maybe synchronized instead of united?
- p.17 there are stored all the messages → "all the messages are stored"
- Definitions 14,17,18. What are the respective definitions of strong and weak? In the definitions, you should link it to the Figures 3.3, 3.4 and 3.5.
- p.19: "In other words, If the" → if

Faruk Göloğlu
Prague, 23/6/2021