Report on "Security of Trapdoor Permutations under Preimage Leakage"

The thesis is on the security of trapdoor permutations under preimage leakage. The thesis defines/introduces a new notion: preimage leakage-resilient trapdoor permutations (PLR-TDPs). The student claims and substantiates that this new definition leads to reduced complexity in design and analysis. Using these ideas, the student proves certain security results (Theorems 3.8 and 3.12).

Topic of the thesis: The topic is suitable for a Master thesis.

Mathematical content: The mathematical content of the thesis is certainly adequate. The student uses cryptographic proof techniques adequately, mostly adopted from [GGKT05] and [GLW20].

Citations/References: Many sources are used effectively and carefully cited overall the thesis. This includes foundational works like [Gol01], recent research articles in leading conferences [GLW20] and well-known research journal articles like [GGKT05].

Student's contribution: Student adopts the proof technique of [GGKT05] to get his main results Theorem 3.8 and Lemma 3.9. In his proof of Theorem 3.8, the student needs a stronger result than a lemma used in [GGKT05] (Lemma 3.10 in the thesis). This stronger Lemma appears in Lemma 3.11, however this seems rather straightforward. Proof of Lemma 3.8 and Lemma 3.9 seem to follow the ideas of [GGKT05], but the students explain them in good detail. An important contribution is the Definition 2.2 itself (Section 2).

My criticism on the formal issues is that the thesis looks more like an extended research article. It is certainly suitable for an expert on the subject, however a more detailed introduction is deservable in a thesis. It is true that an introduction is given, but a few more pages of introduction could be used to explain some of the subject matter. For instance, the student could explain the notions like "hybrid", "digest" , "random oracle", or the function $negl$, although they might be known to experts on the subject.

Comments on formal issues:

- Figure 2.1 of Chapter 2 is above the chapter title. This is quite unusual. It should be placed
- Algorithm parts like .Leak and .Invert should be printed with a different font (Sans Serif or Small Caps) to distinguish them from normal text.
- p.8 dicussed $\Longrightarrow$ discussed.

The use of English is very good overall the thesis.

Question 1 *How would you substantiate your Conjecture 1?*

Conclusion: I think this is a good thesis where the student defines an interesting notion and adopts proof techniques from the literature to prove relevant theorems. I suggest that it should be recognized as a successful thesis. I will notify the committee of my suggested grade.