Report on “Cryptanalytic attacks on the cipher PRINCE”

The task of the thesis was to study, explain and improve various attacks on the lightweight cipher PRINCE. As explained by the author, designers of the PRINCE cipher announced a challenge for cryptanalysts to attack some round-reduced versions of the cipher. The task of the thesis was to explain (a selected set of) these attacks. The selected attacks were of type a) integral and b) MITM. The requirements of a successful thesis included

1. provide explanations of the basics of the above attacks,
2. carefully survey the actual attacks (from the sources mentioned in the thesis, [4] and [5] to be precise),
3. to provide details when necessary,
4. improve the attacks whenever possible.

The last item (4.) in the above list was a requirement for top grade.

Cryptanalysts do not usually require proofs for the weaknesses/distinguishers they find. If *heuristically* an attack works with good probability, then for them, it is safe to claim that a weakness exists for the cipher. I think to explain mathematically why these attacks work (if not mentioned in the original sources) should be considered as an improvement.

I think the author succesfully accomplishes all the necesssary tasks (1., 2. and 3.). Explanations are quite good. There are some small problems like the omission of definition of *half round* as Opponent mentions as well. The author spotted several inaccuracies (for instance on p. 18) in the original sources and evaluated the effects of them on the result. This counts as “providing details” and “carefully survey” part of the requirements.

The author also provides argumentation for the 3.5 round distinguisher (Theorem 3) to explain why it works.

For the 4.5 round distinguisher, the original paper [3] did not supply any information why the distinguisher must work (again, it was probably a “heuristic” distinguisher, that works quite well in practice, but there is no rigorous proof). The author was able to prove several steps. As stated in Observation 5, he was able to find the proof of every transition except one S-box transition. He was able to conjecture the required property (see p .23, last paragraph of Section 3.2.1). The rigorous proof of this conjecture seems to be difficult. The author (experimentating diligently with computer) was able to find a similar scheme that requires $16 \cdot 16 \cdot 2 \cdot 2$ instead of $16 \cdot 16 \cdot 16 \cdot 1$ plaintexts in the *structure*, thus improving efficiency.

He also extends an attack to 7 rounds. Although the extension itself cannot be considered as a real improvement, the author does it in a way that shows good command on the subject matter.

He was also able to find intriguing relations (on the 4.5 round attack) by using $2 \cdot 2 \cdot 2 \cdot 2$ structures. Although this observation does not seem to be usable in an attack, it can be helpful in the rigorous explanation of the distinguisher. (Does not appear in the thesis.)

I think the author shows a good understanding of the subject matter, accomplishes all the required tasks for a good grade. I also think his contributions

- spotting an inaccuracy and correcting it,
- proving why a distinguisher works (whose explanation was not given in the original source),
- finding a related distinguisher that leads to a faster attack,

are good enough to earn him the best grade, even though he was not able to fully prove rigorously why the attack works. A proof of this observation might be difficult.

Suggested grade: 1.0.