Report on "Slide attacks"

The aim of the thesis was to explain slide attacks and in particular study the recent paper [DKLS, 2020], concentrating on "hypercube of slid pairs", to explain it in a more rigorous way. It is usual in cryptography papers that the explanations are given in a less rigorous way.

The student first explains the cryptographic concepts such as SPN/KSA, Feistel structure, etc. Then a section on probabilistic problems that are usually employed in cryptography (in particular, in the paper that the thesis is based on) is given. The student explains them in detail using external resources. Then the original slide attack is explained in Chapter 2 using [BW, 1999] as the main resource.

Chapter 3 is the main part of the thesis (in particular Section 3.3 ff.). The student describes hypercubes by giving definitions and formulates relevant lemmas. Note that in the original paper these formulations were not provided. Then the student describes the attack in detail expanding the arguments of the original paper. I should note that the original paper contains rather complicated novel arguments. The student's work explaining these complicated ideas satisfies the requirements. She also spots a few simple typos of the original paper (that does not affect the correctness of the original arguments).

On p. 28, the student explains why the probabilistic argument works by referring to the explanations found in the original paper. I know that she has a more detailed explanation of this fact. This was omitted from the thesis because of a small problem in formulation. The student can provide this argument in the presentation and/or in an "Addendum".

I believe that the thesis

- by explaining the mathematical concepts that is integral to the studied paper, and
- by explaining the rather difficult cryptographical contributions of the studied paper by providing more detail,

meets the requirements of a satisfactory thesis. The treatment could be more rigorous as the Opponent suggests.

Some minor errors are listed below.

- A few definitions could have been given in a more succint way.
- Usually sentences should not start with mathematical symbols.
- p. 27 "witch" $\Longrightarrow$ "which"
- p. 27 extra paranthesis before "and compute values"
- p. 28 to structures $\Longrightarrow$ two

We will inform the chairman of the examination committee of the suggested grade.