Bachelor's Thesis Opponent's Report

Title: Slide Attacks
Author: Karolína Zenknerová

Thesis content

Author first touches original algorithm of slide attack on self-similar block ciphers. Main part of the thesis describes two of the new slide attack versions for almost self-similar ciphers. These attacks are exceptional in their independence of the number of cipher rounds. The new attacks show that, in case of weak key schedule, modification of cipher's last round need not help.

Published new attacks using slid sets and hypercubes of slid pairs are described. Attack algorithms are explained for ciphers of KSA type, namely full and truncated AES versions with secret S-boxes and identical round keys. Estimates of time and data complexity of both attack algorithms are derived.

Thesis evaluation

Topic. Described attacks are definitely important for the design of block ciphers. The advanced new versions of slide attack are technically more demanding and require elaborated presentation. In the thesis, some of the steps are explained in more detail than sometimes brief published results. On the other hand, for certain algorithm parts author tries to give the idea behind instead of presenting necessary definitions. Also, prior to the description of new attacks the original slide attack should be explained more carefully.

Author's contribution. In some cases, author explains algorithm steps and related complexity estimates in more detail than published papers. Still, some important definitions are omitted from algorithms description.

Mathematical standard. Author formulates the related theory correctly. Formulation of some algorithm steps could be more rigorous.

Use of sources. Author adopted published results, in few cases found own formulations and filled in some details.

Form. Thesis is written in a consistent form. There are some formal errors but their amount is tolerable.

Comments

1. Description of the original slide attack is missing the part of indentifying slid pairs.
2. Definition of KSA in section 1.1.1 is introduced with "A specific case of SPN is KSA ...". The other way around is correct.
3. Sections of 3.1.3 should be named 1K-AESfs and 1K-AESts.
4. Sequences of multiplicities mentioned in section 3.2.2 should be defined explicitly.

Verdict

The work meets the required criteria. I recommend to accept the work as bachelor's thesis.

Opponent will notify chairman of the examination committee of the proposed classification.

Robert El Bashir
7. 6. 2022