Review of "Relationship between higher order attacks and CCZ-equivalence"

Higher order cryptanalysis is a generalization of differential attacks and used against block ciphers which use low degree nonlinear permutations. Two functions which are affinely equivalent have the same immunity against higher order cryptanalysis. Another (and more general) concept of equivalence is the CCZ-equivalence. Since CCZ-equivalence does not keep the degree invariant, the question whether two CCZ-equivalent (but affine-inequivalent) functions have the same resistance against higher order attacks is interesting.

Knudsen explained this attack [12] on a cipher which is invented for the educational purpose of explaining higher order cryptanalysis. Higher order attacks are generally seen as a theoretical attack because they did not lead to many actual cryptanalyses of actual ciphers.

In this thesis it was observed (in Chapter 4) that there exists an attack to this invented cipher, which is independent of the degree of the permutation and therefore 'better' than the original attack proposed in [12]. Two more attacks are presented in Chapter 4 which provides, I believe, a good understanding of higher order attacks. Note that the main aim of Knudsen's paper was educational. What was aimed in this thesis was, of course, not a generic cryptanalysis method, but providing a better understanding and explanation of higher order cryptanalysis. I believe this aim was successfully achieved by giving a higher order attack which actually signifies the importance of the degree of the function.

Moreover, a nice (theoretical) theorem was given for analysis of compositions $F = F_2 \circ F_1^{-1}$ (Theorem 4.2) which relates the degree of F_1 and F_2 to the degree of F. It uses a nice approach which may be helpful to find an algorithm to the question of wheter CCZ-equivalence preserves resistanece against higher order cryptanalysis.

Apart from the mentioned contributions, the author undertakes the task of analysing CCZ-equivalence under some special cases in Chapter 2. The author also implements her algorithms using computers which makes this thesis a combination of very nice theoretical and practical work.

In my opinion, the thesis certainly deserves awarding of a MSc title with the best grade (1.0).