Master's Thesis Review	
Title:	Relationship between higher order attacks and CCZ-equivalence
Author:	Bc. Lucie Deptová
Reviewer:	RNDr. Michal Hojsík, Ph.D.

The thesis deals with CCZ-equivalence of vectorial Boolean functions, higher order differential cryptanalysis and the applications of the former theory to the later.

Chapters 1 is an introduction to the subject of (vectorial) Boolean functions and provides necessary definitions related to iterative block ciphers. Chapter 2 deals with CCZ-equivalence and contains novel results on CCZ-equivalence related matrices. Chapter 3 describes theory related to higher order differential cryptanalysis and two basic attacks. The student also presents two new attacks on five round Feistel cipher with (potentially) better complexity than the original ones. The end of the chapter contains results of experiments with the described attacks. The final chapter presents a straight-forward generalization of the higher-order differential attacks and describes an attempt to use the CCZ-equivalence to get better attack complexity.

The thesis very well written. All sources are clearly stated, proofs (often formulated by the student also for well-known or adopted results) are easy to follow and the included examples illustrate the theory.

Some comments and questions to the student:

- The stated definition of Feistel cipher is a restricted one. In the more general one, the round key is an independent input to the round function. How will the general definition affect stated results?
- Why can't an attacker use directly the equation (4.4) by requesting encryption of plaintexts $v \in F_1(D)$? (Instead of requesting encryption of $z + v,\ v \in F_1(D)$.)
- In section 4.1.2, we know that $|F_1(D)| = |D|$ as F_1 is a permutation by assumption. Hence you do not need to estimate the size of $F_1(D)$ by $deg(F_1(D))$. How this affect the results in the rest of the section?

The student has shown that she has a good understanding of the subject and can come up with novel results. Hence I recommend that it is accepted as Master Thesis and I suggest to grade it *excellent*.

Michal Hojsík
2. 9. 2016