# Report on "Cryptographic primitives in odd characteristic"

Most of the symmetric ciphers and therefore attacks on these ciphers are based on binary (characteristic two) primitives. The thesis is a study on a recent paper that extends a popular cryptanalytic idea that requires binary primitives to odd characteristic [Beyne, et al.].

The thesis starts with a good introduction that explains required background where the student uses her lecture notes to succintly describe the preliminaries. This includes functions over vector spaces and polynomials over finite fields, and also basics of cryptographic primitives and attacks. The treatment is very clear and informative. Second chapter is devoted to integral attacks, which is central to the paper and the thesis, and the characteristic two distinguishing property that was introduced in [Lai] and its generalization in [Beyne et al.], The explanations and the proofs are expanded to include more detail. It is clear from the presentation that the student understood the proofs and gave her own version of them. In Chapter 3, the student explains the attack clearly, again expanding to some extent whenever necessary. Chapter 4 is devoted to another cryptanalytic concept called impossible differentials. After explaining the concept the student explains the attack similarly as in the previous chapter.

It is clear to me that the student understood the paper very well and explained it clearly, using her own style expanding several parts. The writing of the thesis is very well. There is a coherent style and the treatment flows nicely. The student uses several resources and citations are done carefully. The mathematical level of the thesis is quite good.

There is a few minor typos:

- distinguishig (p. 8)
- analogically (p. 15)

I think the thesis is a very good one and certainly deserves recognition. I will inform the chairman of the examination committee of the suggested grade.