Report on "Preprocessing Techniques in Algebraic Cryptanalysis"

The thesis is on certain aspects of algebraic cryptanalysis, which is an important attack on various types of ciphers. Specifically, the thesis is a work on methods for manipulating the set of polynomials that are fed into F4 algorithm (which is a Gröbner basis algorithm) in a way to optimize the time complexity of the attack. The thesis gives a theoretical explanation of why heuristic methods of previous works on the subject worked and also the explanation of their behaviour. Supporting experiments are given as well.

The thesis starts with a very good introduction that explains the necessary backgroud material using a standard text [CLO15] that includes ideals, Gröbner bases, and algebraic cryptanalysis.

The second chapter is very short but it gives a concise argument why *preprocessing* works theoretically. Preprocessing is basically modifying the polynomial system that is supposed to give the attacker the key. One must be sure that after these modifications the attacker should be able to get the key from the modified system.

The third chapter is the main part of the thesis and explains the methods used. After giving the introduction to the method that involves LSH (Locality Sensitive Hashing), Jaccard similarity/distance and careful computations of probabilities the author comes up with Corollary 3.7 which gives a nice algorithm for feeding F4 a presumably better system. The rest of the thesis is on experiments that support the veracity of the claims.

Topic of the thesis: The topic is extremely suitable for a thesis.

Mathematical content: The mathematical content is perfectly suitable.

Citations/References: Citations are done carefully and adequately.

Student's contribution: The student gives theoretical reasoning and supporting experiments of heuristic arguments in the literature. This is certainly a valid contribution.

The use of English is good overall the thesis. Some comments:

- overall: dots should follow the height of the operand, e.g., $x_1 + \cdots + x_n$ but $x_1, \ldots, x_n$.
- p. 5: dimention
- overall: 'Em dash' $---$ should be used instead of hyphen $-$ for clauses that explain the sentence.
- Defn 1.17: Shouldn't it be $n-1$ instead of n?
- p. 14: Polynomials modelling (delete s)
- p. 16: Newtx
- Lemma 3.4: Than should be then.
- p. 23: By 3.4 (Lemma 3.4)
- p. 24: In 3.3
- p. 24: In the Section (delete the)

- p. 29: fasten [decrease]
- Conclusion: Both of works [Both works]

Question 1 *Could you explain the error resulting from an error in Magma? Was that a Magma intrinsic?*

Conclusion: I think the thesis certainly deserves to be graded as very successful. It is a well-written thesis with a good contribution to the literature on algebraic cryptanalysis.