FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

June 3, 2024

Supervisor's evaluation of MSc thesis "Preprocessing Techniques in Algebraic Cryptanalysis" by Bc. Kristýna Mašková

The MSc thesis of Kristýna Mašková investigates recent heuristics in the domain of algebraic cryptanalysis proposed by the research group led by Martin Jureček at the Czech Technical University (CTU). The author aims to provide a formal foundation for these works, explaining their efficacy and suggesting potential improvements for these attacks. The thesis outlines the necessary theoretical background on algebraic cryptanalysis and details the techniques proposed by Bielik et al. (SECRYPT 2022) and in the MSc thesis of Berušková (CTU 2023). The author then constructs a theoretical framework for these attacks, proposes an improved attack, and validates both the model and the proposed improvement experimentally.

In algebraic cryptanalysis, the attacker constructs a system of polynomial equations from available pairs of plaintexts and ciphertexts created using the same key. The goal is to solve the polynomial system and recover the key. As observed by Bielik et al., while a growing number of plaintext/ciphertext pairs initially help the performance of practical solvers (e.g., the Groebner bases-based solver implemented in Magma), the practical performance eventually degrades. Thus, a natural overarching question is whether one can take such an overdetermined polynomial system and reduce the number of polynomial equations while improving the practical performance of the employed solver. The heuristic evaluated in Berušková's thesis is to eliminate monomials by pairwise addition of polynomials, i.e., equivalently, XORing the characteristic vectors of the polynomials mod 2, and running the solver on the sparsest polynomials. Additionally, Berušková employed Locality Sensitive Hashing (LSH) to avoid the quadratic overhead induced by considering all pairs of polynomials when attempting to sparsify the system.

To explain the observed efficacy of such preprocessing, the author studies the sparsification process via pairwise XORing in the context of uniform polynomial systems. This is motivated by the intuition that robust symmetric ciphers should behave pseudorandomly, i.e., the systems of polynomial equations arising in their cryptanalysis should be computationally indistinguishable from a uniformly random polynomial system of the same dimensions. As a new contribution, the author provides quantitative bounds on such sparsification of uniform polynomial systems and evaluates the theoretical model's predictions experimentally on polynomial systems derived from small-scale variants of the block cipher AES. Subsequently, the author presents the theory behind

Computer Science Institute of Charles University
Malostranské nám. 2/25, 118 00 Praha 1
Czech Republic
phone: 951554230, fax: 257531014
e-mail: sekretariat@iuuk.mff.cuni.cz

optimization based on Locality Sensitive Hashing. Additionally, she proposes a more fine-grained variant of the LSH-based attack and estimates the optimal parameters for the attack experimentally.

To summarize, the thesis addresses a timely problem in algebraic cryptanalysis rigorously, with appropriate citations of sources. Moreover, the author presents new results in this area that can serve as a basis for future research. I believe that, after some minor editing, the results can be submitted for publication in a relevant conference on cryptography.

The student has clearly fulfilled the goals of the thesis, and I strongly recommend accepting it as an MSc thesis.

Mgr. Pavel Hubáček, Ph.D.