

Algebraic cryptanalysis is a standard set of techniques for analyzing and attacking practical symmetric cryptographic primitives. It involves representing the relationship between a pair of plaintext, ciphertext and the key as a system of polynomial equations and then solving the system using Gröbner bases. When the equations depend only on the key, we can generate multiple systems of equations.

This thesis examines preprocessing techniques in algebraic cryptanalysis, reducing large systems of equations to improve the performance of practical solving algorithms. Concentrating on a technique that aims to increase the sparsity of the polynomials, we lay the theoretical foundations for two methods. The first method of exhaustively going over all pairs and the second method of finding candidates for similar pairs using Locality-Sensitive Hashing. Finally, we improve on the latter method by targeting the leading monomials.