From Algebraic Cryptanalysis to Cipher Design: A Research Journey in Mathematical Cryptography

Abstract

My research explores how mathematical methods can be applied not only to analyze the security of cryptographic algorithms but also to design algorithms that are more resistant to cryptanalytic attacks. This presentation summarizes that journey through two interconnected research projects, from algebraic cryptanalysis to lightweight cipher design.

My undergraduate research investigated Gröbner Basis as a method for solving multivariate polynomial systems generated by algebraic attacks. By studying concepts from polynomial rings and ideal theory, I showed how Gröbner Basis transforms a polynomial system into an equivalent but substantially simpler one while preserving its solution set, making the search for solutions more efficient. The approach was demonstrated through algebraic attacks on simplified stream and block ciphers, where the resulting polynomial systems were successfully reduced, enabling the recovery of the encryption keys.

Building upon this work, my master's research focused on strengthening cryptographic design by modifying the Key Scheduling Algorithm (KSA) of SMALLPRESENT-[2], a simplified version of the internationally standardized lightweight block cipher PRESENT that employs the same KSA. The proposed modification significantly increases the algebraic complexity of the generated round keys while improving randomness and diffusion properties without sacrificing computational efficiency, providing insights into strengthening the KSA of PRESENT itself.

Through this presentation, I hope to demonstrate how mathematical foundations can bridge cryptanalysis and cipher design, illustrating how understanding algebraic attacks can contribute to the development of more secure cryptographic algorithms.