ABSTRACT

Krutykh M.V. Research on algebraic cryptanalysis of simplified AES algorithm.

The thesis is submitted for the Master Degree in specialism 8.05010201 – Computer Network and Systems – Ternopil Ivan Pul'uj National Technical Univarsity, Ternopil. 2014

Keywords: AES, S-AES, bit, block, byte, cipher text, cipher, decrypt, cryptanalysis, algebraic cryptanalysis, S-box, rijndael, cipher key, linearization, XL-algorithm, NP-complete problem, Finite field.

The work is dedicated to research of AES algorithm to perform its algebraic cryptanalysis.

AES algorithm is resistant to all attacks, which are based on classical methods of cryptanalysis. But in 2002 Nicolas Courtois and Josef Pipdzhyk suggested the possibility of algebraic attacks on ciphers with a similar structure to the AES. Algebraic attacks are aimed at analyzing of vulnerabilities in mathematical parts of algorithm and use its internal algebraic structures.

Raphael Chung-Wei Fan, Sean Simmons, Elizabeth Klyayman and Voronin R. I. researched the possibility of algorithm AES algebraic cryptanalysis. But they performed attack only on a simplified version of the algorithm. The structure and algorithm of symmetric block cipher Rijndael, described in the standard AES, and its simplified version (S-AES) were examined. Software which encrypts text input, decrypts ciphertext, builds a system of equations for the implementation of algebraic cryptanalysis and saves them as a text file, shows step by step demonstration of the formation of these systems was developed. This allows using it in learning purposes and further study opportunities to optimize the process.