Szkoła Główna Gospodarstwa Wiejskiego
w Warszawie
Instytut Informatyki Technicznej

Mgr Sylwia Stachowiak

SAT-kryptoanaliza wybranych algorytmów kryptografii symetrycznej

SAT-cryptanalysis of selected symmetric cryptography algorithms

Rozprawa doktorska
Doctoral thesis

Promotor:
dr hab. Mirosław Kurkowski, prof. ucz.
Uniwersytet Kardynała St. Wyszyńskiego
Wyższa Szkoła Policji w Szczytnie
Promotor pomocniczy:
dr hab. Konrad Furmańczyk, prof. ucz.
Szkoła Główna Gospodarstwa Wiejskiego

Warszawa, 2022

Streszczenie

W dzisiejszych sieciach i systemach komputerowych, z oczywistych względów, wymaga się zapewnienia odpowiedniej ochrony przesyłanych lub gromadzonych danych. Do celów tych wykorzystuje się metody i algorytmy kryptograficzne, w tym szyfry symetryczne i asymetryczne.

W rozprawie zawarto wyniki badań dotyczące SAT-kryptoanalizy wybranych szyfrów symetrycznych. Metoda polega na translacji problemu bezpieczeństwa algorytmu kryptograficznego do problemu SAT, z wykorzystaniem bezpośredniego kodowania do formuły boolowskiej. W ramach prowadzonych prac opracowano i opisano formuły kodujące dla trzech różnych szyfrów symetrycznych: Salsa20, AES oraz wybranych modyfikacji DES. Ponadto przeprowadzono serię badań eksperymentalnych łamania brutalnego szyfrów metodą SAT-kryptoanalizy z wybranym tekstem jawnym. Otrzymane wyniki pozwoliły wyznaczyć granice możliwości przeprowadzenia na ww. szyfry ataku brutalnego z wykorzystaniem technik SAT.

Słowa kluczowe: DES, Salsa20, AES, SAT-kryptoanaliza, problem spełnialności formuł logicznych.

Abstract

In today's computer networks and systems, for obvious reasons, it is required to ensure adequate protection of transmitted or collected data. For these purposes, cryptographic methods and algorithms, including symmetric and asymmetric ciphers, are used.

The dissertation contains the results of research on SAT-cryptanalysis of selected symmetric ciphers. The method translates the security problem of a cryptographic algorithm into one of the instances of the SAT problem, using direct encoding into a propositional boolean formula. As part of the work, the encoding formulas for three different symmetric ciphers: Salsa20, AES, and selected DES modifications were developed and described. Moreover, a series of experimental results of ciphers' brutal breaking using the SAT-cryptanalysis method with selected plaintext were carried out. The obtained results allowed us to identify the limits of the possibility of carrying out the above-mentioned brutal attack ciphers using SAT techniques.

Keywords: DES, Salsa20, AES, SAT-cryptoanalysis, Boolean satisfiability problem.