БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

«Алгебраическая и корреляционная иммунность при анализе криптографических генераторов»

Птушко Григорий Сергеевич

Научный руководитель - кандидат физ.-мат. наук, доцент Вечерко Е. В.

Минск, 2018

Реферат

Дипломная работа, 33 с., 10 рис., 10 табл., 13 источников.

КОРРЕЛЯЦИОННАЯ АТАКА, БЫСТРАЯ КОРРЕЛЯЦИОННАЯ АТАКА, КОРРЕЛЯЦИОННАЯ ИММУННОСТЬ, АЛГЕБРАИЧЕСКАЯ ИММУННОСТЬ, РЕГИСТР СДВИГА С ЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ, КОМБИНИРУЮЩИЙ ГЕНЕРАТОР.

Объект исследования - корреляционная и алгебраическая иммунность булевых функций при анализе криптографических генераторов.

Цель работы - сравнить различные типы атак на криптографические генераторы, провести классификацию булевых функций в зависимости от их корреляционной и алгебраической иммунности.

Методы исследования – изучение предметной области, ознакомление с документациями, моделирование, эксперимент.

Результатом является классификация булевых функций в зависимости от их корреляционной и алгебраической иммунности, получение данных о применимости корреляционных атак в определенных условиях.

Областью применения является сфера создания криптографических генераторов.

Abstract

Diploma work, 33 p., 10 fig., 10 tables, 13 sources.

CORRELATION ATTACK, FAST CORRELATION ATTACK, CORRELATION IMMUNITY, ALGEBRAIC IMMUNITY, LINEAR FEEDBACK SHIFT REGISTER, COMBINING GENERATOR.

The object of research is the correlation and algebraic immunity of boolean functions in the analysis of cryptographic generators.

The purpose of the work is to compare different types of attacks on cryptographic generators, to classify Boolean functions depending on their correlation and algebraic immunity.

Methods of research - study of the subject area, familiarization with the documentation, modeling, experiment.

The result is the classification of Boolean functions depending on their correlation and algebraic immunity, obtaining data on the applicability of correlation attacks under certain conditions.

The scope of application is the creation of cryptographic generators.