МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра веб-технологий и компьютерного моделирования

Аннотация к дипломной работе

РЕШЕНИЕ НЕКОТОРЫХ СИСТЕМ БУЛЕВЫХ УРАВНЕНИЙ МЕТОДАМИ ЛИНЕАРИЗАЦИИ

БОНДАРЕНКО Александр Юрьевич

Научный руководитель:
кандидат физ.-мат. наук, доцент
Ю.А. Кремень

Минск, 2024

АННОТАЦИЯ

Дипломная работа содержит: 62 страницы, 1 рисунок, 5 таблиц, список использованных источников из 16 наименований.

Ключевые слова: СИСТЕМА БУЛЕВЫХ УРАВНЕНИЙ, ЛИНЕАРИЗАЦИЯ, XL МЕТОД, АЛГОРИТМ ШИФРОВАНИЯ, КРИПТОАНАЛИЗ.

Объект исследования – системы булевых уравнений и их решения.

Предмет исследования – методы линеаризации нелинейных систем булевых уравнений, включая расширение линеаризации и решение линейных систем булевых уравнений, а также их применение для алгебраического криптоанализа на примере алгоритма шифрования A-5-GMR-1.

Цель работы: исследование и реализация эффективных методов для решения систем булевых уравнений. Применение данных методов для алгебраического криптоанализа и анализ их эффективности и точности.

Методы исследования: методы анализа, синтеза, моделирования, а также анализ научной литературы и экспериментальные исследования.

Результаты работы: исследованы и реализованы эффективные и точные методы решения систем нелинейных булевых уравнений, а также применены для алгебраического криптоанализа алгоритма шифрования A-5-GMR-1 с внедрением разработанных приемов их оптимизации.

Области практического применения: криптография и криптографические протоколы, информационные технологии, информационная безопасность, образование. Рекомендуется использовать при анализе стойкости алгоритмов шифрования и оценке рисков при выборе применяемых алгоритмов.

Обоснованность и достоверность полученных результатов подтверждаются проведением анализа влияния применения методов линеаризации для алгебраического криптоанализа алгоритма шифрования A-5-GMR-1 путем экспериментов, которые включали оценку количества известных знаков гаммы, необходимых для успешного нахождения ключа шифрования при различных подходах к линеаризации.

Дипломная работа выполнена автором *самостоятельно*.

АНАТАЦЫЯ

Дыпломная работа змяшчае: 62 старонкі, 1 малюнак, 5 табліц, спіс выкарыстаных крыніц з 16 найменняў.

Ключавыя словы: СІСТЭМА БУЛЕВЫХ УРАЎНЕННЯЎ, ЛІНЕАРЫЗАЦЫЯ, XL МЕТАД, АЛГАРЫТМ ШЫФРАВАННЯ, КРЫПТААНАЛІЗ.

Аб'ект даследавання – сістэмы булевых ураўненняў і іх рашэнні.

Прадмет даследавання – метады лінеарызацыі нелінейных сістэм булевых ураўненняў, уключаючы пашырэнне лінеарызацыі і рашэнне лінейных сістэм булевых ураўненняў, а таксама іх ужыванне для алгебраічнага крыптааналізу на прыкладзе алгарытму шыфравання A-5-GMR1.

Мэта работы: даследаванне і рэалізацыя эфектыўных метадаў для вырашэння сістэм булевых ураўненняў. Ужыванне дадзеных метадаў для алгебраічнага крыптааналізу і аналіз іх эфектыўнасці і дакладнасці.

Метады даследавання: метады аналізу, сінтэзу, мадэлявання, а таксама аналіз навуковай літаратуры і эксперыментальныя даследаванні.

Вынікі работы: даследаваны і рэалізаваны эфектыўныя і дакладныя метады рашэння сістэм нелінейных булевых ураўненняў, а таксама ужытыя для алгебраічнага крыптааналізу алгарытму шыфравання A-5-GMR-1 з укараненнем распрацаваных прыёмаў іх аптымізацыі.

Вобласці практычнага ўжывання: крыптаграфія і крыптаграфічныя пратаколы, інфармацыйныя тэхналогіі, інфармацыйная бяспека, адукацыя. Рэкамендуецца выкарыстоўваць пры аналізе стойкасці алгарытмаў шыфравання і ацэнцы рызык пры выбары ўжывальных алгарытмаў.

Абгрунтаванасць і дакладнасць атрыманых вынікаў пацвярджаюцца правядзеннем аналізу ўплыву ўжывання метадаў лінеарызацыі для алгебраічнага крыптоаналіза алгарытму шыфравання A-5-GMR-1 шляхам эксперыментаў, якія ўключалі ацэнку колькасці вядомых знакаў гамы, неабходных для паспяховага знаходжання ключа шыфравання пры розных падыходах да лінеарызацыі.

Дыпломная работа выканана аўтарам самастойна.

ANNOTATION

The thesis contains: 62 pages, 1 drawing, 5 tables, a list of used sources of 16 titles.

Keywords: SYSTEM OF BOOLEAN EQUATIONS, LINEARIZATION, XL, METHOD, ENCRYPTION ALGORITHM, CRYPTANALYSIS.

The object of research is systems of Boolean equations and their solutions.

The subject of the research is the methods of linearization of nonlinear systems of Boolean equations, including the extension of linearization and the solution of linear systems of Boolean equations, as well as their application for algebraic cryptanalysis using the example of the A-5-GMR-1 encryption algorithm.

Purpose of the work: research and implementation of effective methods for solving systems of Boolean equations. Application of these methods for algebraic cryptanalysis and analysis of their effectiveness and accuracy.

Research methods: methods of analysis, synthesis, modeling, as well as analysisof scientific literature and experimental research.

Results of the work: effective and accurate methods for solving systems of nonlinear Boolean equations have been investigated and implemented, as well as applied to algebraic cryptanalysis of the A-5-GMR-1 encryption algorithm with the introduction of developed optimization techniques.

Areas of practical application: cryptography and cryptographic protocols, information technology, information security, education. It is recommended to use it when analyzing the strength of encryption algorithms and assessing risks when choosing the algorithms used.

The validity and reliability of the results obtained are confirmed by analyzing the impact of using linearization methods for algebraic cryptanalysis of the encryption algorithm A-5-GMR-1 through experiments that included estimating the number of known gamma characters needed to successfully find the encryption key with various linearization approaches.

The thesis was done by the author independently.