МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

СИСТЕМЫ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ И МАТРИЦЫ МАКОЛЕЯ

Заломов Данил Павлович

Научный руководитель:
кандидат физ.-мат. наук,
С.В. Агиевич

Минск, 2022

РЕФЕРАТ

Дипломная работа: 44 с., 6 рис., 1 табл., 9 источников, 2 прил.

МНОГОЧЛЕНЫ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ, МАТРИЦЫ МАКОЛЕЯ, БАЗИС ГРЁБНЕРА, КРИПТОГРАФИЯ НА ОСНОВЕ МНОГОЧЛЕНОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ, АЛГЕБРАИЧЕСКИЙ КРИПТОАНАЛИЗ.

Объект исследования – системы алгебраических уравнений над полем из двух элементов.

Предмет исследования – решение систем алгебраических уравнений над полем из двух элементов с помощью матриц Маколея.

Цель работы: изучить и реализовать методы решения систем алгебраических уравнений с помощью матриц Маколея и, в частности, алгоритм Crossbred.

Методы исследования: аналитическое и программное исследование, сравнение с другими способами решения систем алгебраических уравнений над полем F_2.

Элементы научной новизны: определены особенности алгоритма Crossbred, а также способы его применения для решения систем уравнений.

Область возможного практического применения: результаты, полученные в дипломной работе, могут быть использованы при оценке стойкости криптосистем к алгебраическим атакам.

Автор работы подтверждает, что приведенный в ней расчетно-аналитический материал правильно и объективно отражает состояние исследуемого процесса, а все заимствованные из литературных и других источников методологические и методические положения и концепции сопровождаются ссылками на их авторов.

_____

(подпись студента)

РЭФЕРАТ

Дыпломная праца: 44 с., 6 мал., 1 табл., 9 крыніц, 2 дадаткі.

МНАГАМЕРНЫЯ ПАЛІНАМІЯЛЬНЫЯ СІСТЭМЫ, МАТРЫЦЫ МАКАЛЕЯ, БАЗІС ГРОБНЕРА, КРЫПТАГРАФІЯ НА МНАГАЧЛЕНАХ АД МНОГІХ ПЕРАМЕННЫХ, АЛГЕБРАІЧНЫ КРЫПТААНАЛІЗ.

Аб'ект даследавання – сістэмы алгебраічных ураўненняў над полем з двух элементаў.

Прадмет даследавання – рашэнне сістэм алгебраічных ураўненняў над полем з двух элементаў з дапамогай матрыц Макалея.

Мэта працы: вывучыць і рэалізаваць метады рашэння сістэм алгебраічных ураўненняў з дапамогай матрыц Макалея і, у прыватнасці, алгарытм Crossbred.

Элементы навуковай навізны: вызначаны асаблівасці алгарытму Crossbred, а таксама спосабы яго прымянення для рашэння сістэм ураўненняў.

Вобласць магчымага практычнага прымянення: вынікі, атрыманыя ў дыпломнай рабоце, могуць быць выкарыстаны пры правядзенні алгебраічнага крыптааналіза.

Аўтар працы пацвярджае, што прыведзены ў ёй разлікова-аналітычны матэрыял правільна і аб'ектыўна адлюстроўвае стан доследнага працэсу, а ўсе запазычаныя з літаратурных і іншых крыніц метадалагічныя і метадычныя палажэнні і канцэпцыі суправаджаюцца спасылкамі на іх аўтараў.

_____

(подпіс студэнта)

ABSTRACT

Graduate work: 44 pp., 6 pict., 1 table, 9 sources, 2 appendices.

MULTIDIMENSIONAL POLYNOMIAL SYSTEMS, MACAULAY MATRICES, GRÖBNER BASIS, MULTIVARIATE POLYNOMIAL-BASED CRYPTOGRAPHY, ALGEBRAIC CRYPTOANALYSIS.

The object of research is a system of algebraic equations over a field of two elements.

The subject of research is the solution of systems of algebraic equations over a field of two elements using Macaulay matrices.

Purpose: to study and implement methods for solving systems of algebraic equations using Macaulay matrices and, in particular, the Crossbred algorithm.

The elements of scientific novelty: the features of the Crossbred algorithm, as well as ways of its usage for solving systems of equations have been determined.

The practical application: the results obtained in the graduate work can be used in the conduct of algebraic cryptanalysis.

The author of the work confirms that the calculation and analytical material presented in it correctly and objectively reflects the state of the process under study, and all methodological concepts borrowed from literary and other sources are accompanied by references to their authors.

_____

(student's signature)

ВВЕДЕНИЕ

В настоящее время криптосистемы с открытым ключом, такие как RSA, полагаются на сложность разложения числа на простые множители. Однако, по мере развития технологий, в частности, квантовых компьютеров, нельзя будет полагаться на стойкость существующих алгоритмов. По этой причине, сейчас рассматриваются различные постквантовые криптосистемы на замену существующим.

Исследования постквантовых криптосистем развили идеи, включающие криптографию на основе решеток (Lattice-Based Cryptography, LBC), криптографию на основе хэш-функций (Hash-Based Cryptography, HBC) и криптографию на основе многочленов от нескольких переменных (Multivariate-Based Cryptography, MBC). MBC использует достаточно простой математический аппарат по сравнению с другими постквантовыми системами. Благодаря своей простоте MBC можно использовать на устройствах с низким энергопотреблением, таких как смарт-карты [6].

Задача поиска решения системы уравнений от многих переменных является NP-трудной. Существуют различные подходы к решению системы, например, алгоритмы, основанные на полном переборе или частичном переборе, базисах Грёбнера или представлении систем в виде матриц Маколея, поэтому важно изучать новые алгоритмы, например F5, XL, Booleansolve и др. Одними из перспективных направлений для решения таких систем является подход, основанный на частичном переборе и матрицах Маколея. Комбинирование этих подходов применяются в алгоритме Crossbred [4].

Целью создания алгоритма Crossbred был поиск масштабируемого алгоритма, который решает случайные системы уравнений он нескольких переменных в поле F_2. В частности, учитывая систему многочленов от нескольких перемнnных, этот алгоритм создаст эквивалентную меньшую систему, которую легче решить.

В настоящей работе мы изучаем методы решения систем полиномиальных уравнений с помощью матриц Маколея и, в частности, алгоритм Crossbred. В разделе 1 мы введем базовые понятия для дальнейшей работы с матрицами Маколея. В разделе 2 мы рассмотрим современные подходы алгебраического криптоанализа и определим операции, необходимые для работы с матрицами Маколея. В разделе 3 мы рассмотрим алгоритм, основанный на частичном переборе и матрицах Маколея – алгоритм Crossbred и опишем особенности работы с ним. Предложим способы его ускорения и опишем программную реализацию этого алгоритма. Листинг файлов представлены в приложениях А, Б, В, Г.