

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ
БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И
ИНФОРМАТИКИ
Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

Анализ и оценивание параметров генераторов на основе
регистров сдвига

Долгая
Александра Валерьевна

Научный руководитель - доцент кафедры ММАД, кандидат физико-
математических наук

В.Ю. Палуха

Минск, 2025

РЕФЕРАТ

Дипломная работа включает 49 страниц, 10 рисунков, 2 таблицы, 12 источников, 5 приложений.

Ключевые слова: ПРОРЕЖИВАЮЩИЙ ГЕНЕРАТОР, САМОСЖИМАЮЩИЙ ГЕНЕРАТОР, РЕГИСТР СДВИГА, ПЕРИОД ПОСЛЕДОВАТЕЛЬНОСТИ, ЗАВИСИМОСТЬ РАНГА ОТ ПОРЯДКА МАТРИЦЫ, $GF(2)$.

Объект исследования: выходные последовательности генераторов.

Цель работы: нахождение зависимостей рангов матриц от их порядка путем формирования матриц над полем $GF(2)$ из выходных последовательностей прореживающего и самосжимающего генераторов.

Методы исследования: математическое моделирование, линейная алгебра над полем $GF(2)$, статистический анализ, алгоритмическая реализация генераторов и расчетов, графическая интерпретация результатов.

Полученные результаты и их новизна: разработаны и протестированы алгоритмы генерации выходных последовательностей для прореживающего и самосжимающего генераторов на основе LFSR, вычислены зависимости рангов матриц от их порядка, построенных из выходных битов генераторов, что дает представление об их структуре и нелинейных свойствах, новизна заключается в комбинированном применении криптографического анализа и линейной алгебры на $GF(2)$ для оценки качества генераторов, что является полезным при проектировании стойких криптографических систем.

Достоверность материалов и результатов дипломной работы: все полученные данные основаны на строго формализованных математических моделях, примеры реализации последовательностей подтверждают работу генераторов согласно теории, результаты прошли верификацию через статистические тесты, применение различных примитивных порождающих полиномов усиливает обоснованность вывод.

Область применения: информационная безопасность, инженерия, научно-исследовательские институты.

РЭФЕРАТ

Дыпломная праца ўключае 49 старонак, 10 малюнкаў, 2 табліцы, 12 крыніц, 5 прыкладанняў.

Ключавыя словы: ПРАРЭДЖВАЛЬНЫ ГЕНЕРАТАР, САМАСЦІСКАЛЬНЫ ГЕНЕРАТАР, РЭГІСТР ЗРУХУ, ПЕРЫЯД ПАСЛЯДОЎНАСЦІ, ЗАЛЕЖНАСЦЬ РАНГУ АД ПАРАДКУ МАТРЫЦЫ, $GF(2)$.

Аб'ект даследавання: выхадныя паслядоўнасці генератараў.

Мэта працы: знаходжанне залежнасцяў рангаў матрыц ад іх парадку шляхам фарміравання матрыц над полем $GF(2)$ з выходных паслядоўнасцяў прореживающего і самосжимающего генератараў.

Метады даследавання: матэматычнае мадэляванне, Лінейная алгебра над полем $GF(2)$, статыстычны аналіз, алгарытмічная рэалізацыя генератараў і разлікаў, графічная інтэрпрэтацыя вынікаў.

Атрыманыя вынікі і іх навізна: распрацаваны і пратэставаны алгарытмы генерацыі выходных паслядоўнасцяў для прореживающего і самосжимающего генератараў на аснове LFSR, вылічаныя залежнасці рангаў матрыц ад іх парадку, пабудаваных з выходных бітаў генератараў, што дае ўяўленне аб іх структуры і нелінейных уласцівасцях, навізна заключаецца ў камбінаваным ўжыванні крыптаграфічнага аналізу і лінейнай алгебры на $GF(2)$ для ацэнкі якасці генератараў, што з'яўляецца карысным пры праектаванні стойкіх крыптаграфічных сістэм.

Дакладнасць матэрыялаў і вынікаў дыпломнай працы: усе атрыманыя дадзеныя заснаваныя на строга фармалізаваных матэматычных мадэлях, прыклады рэалізацыі паслядоўнасцяў пацвярджаюць працу генератараў паводле тэорыі, вынікі прайшлі верыфікацыю праз статыстычныя тэсты, прымяненне розных прымітыўных спараджаюць поліномов ўзмацняе абгрунтаванасць выснову.

Вобласць ужывання: інфармацыйная бяспека, інжынерыя, навукова-даследчыя інстытуты.

ABSTRACT

Graduate work: 49 pages, 10 pictures, 2 tables, 12 sources, 5 applications.

Key words: PROGRAMMING GENERATOR, SELF-CONNECTING GENERATOR, ADVANCE REGISTER, LETTER PERIOD, RANGE RANGE LOCALITY OF MATRIX, GF(2).

Object of study: output sequences of oscillators.

Objective: finding the dependence of matrix ranks on their order by forming matrices over the field GF(2) from output sequences of thinning and self-compressing generators.

Methods of research: mathematical modelling, linear algebra over the field GF(2), statistical analysis, algorithmic implementation of generators and calculations, graphical interpretation of the results.

Results: the first and second moments were found using the recurrent formula and the derivative of the generating function, the results were compared based on graphs obtained by modeling, and the probabilities of occurrence and non-occurrence of a series of events were found.

Reliability of materials: all obtained data are based on strictly formalised mathematical models, examples of sequences implementation confirm the work of generators according to the theory, the results have been verified through statistical tests, application of various primitive generating polynomials strengthens the validity of the conclusion.

The field of application: information security, engineering, research institutes.