МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Криптосистема, основанная на графах

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Романова Романа Александровича

Научный руководитель
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Заведующий кафедрой
д. ф.-м. н., профессор _____ М. Б. Абросимов
19.01.2026 г.

Саратов 2026

ВВЕДЕНИЕ

В последние десятилетия информационные технологии стали неотъемлемой частью практически всех сфер человеческой деятельности. Передача, хранение и обработка данных осуществляются в цифровой форме, что неизбежно приводит к росту требований к их защите. В условиях глобализации, развития распределённых систем и увеличения объёмов передаваемой информации вопросы информационной безопасности приобретают особую актуальность. Криптография как наука о методах защиты информации играет ключевую роль в обеспечении конфиденциальности, целостности и подлинности данных.

Современные криптографические алгоритмы в основном опираются на сложные математические задачи, такие как факторизация больших чисел, вычисление дискретного логарифма или задачи на эллиптических кривых. Несмотря на широкое распространение и доказанную на практике стойкость таких подходов, развитие вычислительных мощностей, а также перспективы появления квантовых компьютеров ставят под сомнение долговременную надёжность традиционных криптосистем. В связи с этим активно ведутся исследования альтернативных криптографических примитивов, основанных на иных математических структурах.

Одним из перспективных направлений в данной области является использование теории графов в криптографии. Графы представляют собой универсальный и наглядный математический аппарат, применяемый для моделирования сложных систем и взаимосвязей. Их свойства активно используются в информатике, теории алгоритмов, сетевых технологиях и анализе данных. В контексте криптографии графы интересны прежде всего наличием большого количества вычислительно сложных задач, для которых на данный момент не существует эффективных алгоритмов решения за полиномиальное время.

Криптосистемы, основанные на графах, используют такие задачи, как поиск изоморфизма графов, нахождение гамильтоновых циклов, кликов максимального размера, раскраска графов и другие комбинаторные проблемы. Сложность этих задач делает их привлекательными с точки зрения построения криптографических алгоритмов, устойчивых к различным видам атак. Кроме того, графовые структуры позволяют гибко настраивать параметры криптосистемы и адаптировать её под конкретные требования безопасности и производительности.

Актуальность разработки и исследования криптосистем, основанных на графах, обусловлена также необходимостью диверсификации криптографических подходов. Использование альтернативных математических основ снижает риски, связанные с возможными прорывами в криптоанализе или появлением новых вычислительных технологий. Графовые криптосистемы рассматриваются как потенциальные кандидаты для постквантовой криптографии, что делает данное направление особенно перспективным в долгосрочной перспективе.

Несмотря на очевидные преимущества, криптосистемы на основе графов пока не получили широкого практического распространения. Это связано как с относительной сложностью их реализации, так и с недостаточной изученностью некоторых аспектов их криптостойкости. Тем не менее, активное развитие теории графов и рост интереса к нестандартным криптографическим решениям создают благоприятные условия для дальнейших исследований в этой области. Анализ существующих подходов и разработка новых схем позволяют оценить реальный потенциал графовых криптосистем и определить области их практического применения.

Целью данной работы является изучение принципов построения криптосистем, основанных на графах, а также анализ их основных характеристик и свойств. В рамках работы рассматриваются теоретические основы графовой криптографии, описываются ключевые математические задачи, лежащие в основе соответствующих алгоритмов, и анализируются возможные сценарии их

использования. Особое внимание уделяется вопросам криптостойкости и эффективности предлагаемых решений.

Для достижения поставленной цели в работе предполагается решение следующих задач: изучение основных понятий теории графов, применяемых в криптографии; анализ существующих графовых криптосистем и протоколов; рассмотрение методов генерации ключей и шифрования на основе графовых структур; а также оценка преимуществ и ограничений данного подхода по сравнению с традиционными криптографическими алгоритмами. Решение указанных задач позволит сформировать целостное представление о возможностях и перспективах графовой криптографии.

Объектом исследования в данной работе являются криптографические системы защиты информации, а предметом исследования – методы и алгоритмы шифрования, основанные на использовании графов и их свойств. В качестве методов исследования применяются анализ научных публикаций, теоретическое обобщение существующих подходов, а также сравнение различных криптографических схем по заданным критериям.

Практическая значимость данной работы заключается в возможности использования полученных результатов при дальнейшем изучении современных и перспективных методов криптографической защиты информации. Материалы работы могут быть полезны студентам и специалистам в области информационной безопасности, а также разработчикам программного обеспечения, интересующимся альтернативными криптографическими решениями. Кроме того, рассмотренные в работе подходы могут служить основой для дальнейших исследований и разработок в области постквантовой криптографии.

Структура данной работы включает введение, три раздела, заключение, список использованных источников и два приложения.

В первом разделе рассматриваются теоретические основы графовой криптографии, основные понятия теории графов и их применение в криптографических алгоритмах.

Во втором разделе приводятся теоретические математические описания графовых криптосистем, рассматривается их математический базис, формулируются ключевые вычислительные задачи и анализируются свойства, обеспечивающие криптостойкость соответствующих алгоритмов.

Третий раздел посвящён практической реализации криптосистем, основанных на графах, включая описание алгоритмов генерации ключей и шифрования.

В заключении подводятся итоги работы и формулируются выводы о перспективах дальнейшего развития графовой криптографии.

В приложениях приводится листинг программной реализации рассмотренных криптосистем.

Дипломная работа состоит из введения, 3 разделов, заключения, списка использованных источников и 3 приложений. Общий объем работы – 74 страниц, из них 48 страниц – основное содержание, включая 22 рисунков и 6 таблиц, список использованных источников из 30 наименований.)

КРАТКОЕ СОДЕРЖАНИЕ

Глава 1. Теоретические основы криптосистем, основанных на графах

Рассмотрены основные понятия теории графов и их связь с криптографией. Проанализированы классические и современные проблемы криптографии, сформулированы требования к современным криптографическим системам. Изучены специфические задачи теории графов, такие как изоморфизм графов, поиск гамильтоновских циклов и раскраска графов, которые потенциально могут применяться для повышения устойчивости криптосистем.

Выводы: Определены направления, в которых теория графов может внести значительный вклад в повышение надежности криптографических систем. Показано, что сочетание классических проблем криптографии с современными методами обработки графов открывает перспективы для разработки новых типов криптографических алгоритмов.

Глава 2. Криптосистемы, основанные на графах

Предложены и проанализированы криптосистемы, использующие графы в качестве базовой математической структуры. Описаны принципы их построения, математический базис и алгоритмы шифрования и дешифрования.

2.1 Симметричная криптосистема

Рассматривается симметричная криптосистема, использующая обобщённый граф Петерсена. Данный подход предполагает трехуровневую защиту путем комбинирования симметричных ключей и специальных процедур шифрования. Данная криптосистема оптимальна для небольших объемов данных и демонстрирует высокий уровень криптостойкости благодаря особенностям структуры графа Петерсена.

Выводы: Предложена эффективная симметричная криптосистема, отличающаяся надежностью и быстротой исполнения даже при обработке малых объёмов данных. Однако ограничения по длине обрабатываемых данных делают данную систему неприменимой для крупных массивов информации.

2.2 Асимметричная криптосистема

Описана асимметричная криптосистема, основанная на многомерных квадратичных отображениях над конечным полем. Использование алгебраических графов позволяет обеспечить необходимую гибкость и управляемость структурой нелинейности. Применение аффинных преобразований повышает стойкость системы против известных видов атак.

Выводы: Исследованный подход к созданию асимметричной криптосистемы демонстрирует значительные перспективы для практического применения. Оптимизированная структура центральной функции и случайные аффинные преобразования существенно повышают надежность и универсальность криптосистемы.

2.3 Криптосистема на основе графов Пэли

Анализируется криптосистема, использующая свойства графов Пэли. За счет специфики структуры графов Пэли обеспечивается высокая криптостойкость при относительно простой процедуре шифрования и дешифрования. Важным преимуществом данной системы является возможность эффективного использования небольших ресурсов для шифрования больших объемов данных.

Выводы: Метод шифрования на основе графов Пэли показывает хорошие показатели по соотношению простота реализации и высокий уровень криптостойкости. Дальнейшее развитие данного метода может привести к появлению высокоэффективных систем шифрования для массового применения.

Глава 3. Практическая реализация

Осуществлена практическая реализация предложенных криптосистем. Создана программа на языке Python с использованием графического интерфейса, позволяющего проводить эксперименты с различными видами криптографических систем. Программа предназначена для тестирования и оценки характеристик криптосистем, созданных на основе графов.

Выводы: Программная реализация подтверждает работоспособность предложенных криптографических схем и демонстрирует возможность

практического применения предложенных методов. Создание удобного инструмента для изучения и экспериментирования с графикой способствует дальнейшему развитию криптографических технологий.

ЗАКЛЮЧЕНИЕ

В работе была исследована, разработана и реализована концепция криптографических систем, фундаментально основанных на структурах графов. Теоретическая часть работы включала детальный анализ двух принципиально различных подходов: симметричной криптосистемы на основе обобщённого графа Петерсона и асимметричной гибридной графо-алгебраической схемы. Также была рассмотрена симметричная криптосистема на основе графов Пэли. Для каждой системы были формально описаны математические модели, определены алгоритмы генерации ключей, шифрования и расшифрования, а также проведён анализ криптографических свойств, включая стойкость к известным атакам. Симметричная схема продемонстрировала эффективность использования алгебраических свойств графов для создания компактных и быстрых алгоритмов, в то время как асимметричный прототип показал, как треугольная структура зависимостей, представленная в виде направленного ациклического графа, может быть скрыта за случайными аффинными преобразованиями для формирования стойкого открытого отображения.

Практическая часть работы заключалась в программной реализации описанных алгоритмов на языке Python и создании интерактивного, наглядного и масштабируемого графического пользовательского интерфейса. Интерфейс был спроектирован не только как инструмент управления криптосистемой, но и как образовательная платформа, которая визуализирует ключевые этапы работы алгоритмов и демонстрирует, как именно структуры графов участвуют в криптографических процессах.

Пользователю доступны настройка параметров (размерность, поле, плотность рёбер графа), генерация и загрузка ключей, выполнение операций шифрования, а также визуализация таких компонентов, как матрицы перемешивания и граф зависимостей центрального отображения.

Таким образом, работа вносит вклад как в теоретическую криптографию, предлагая и анализируя новые графовые конструкции, так и в прикладную

область, предоставляя готовый, документированный и расширяемый программный комплекс для дальнейших исследований, тестирования и обучения.