АННОТАЦИЯ

диссертационной работы докторанта PhD по образовательной программе 8D06301 – «Системы информационной безопасности» Әмірхановой Дана Сайранғажықызы на тему «Схема постквантового шифрования с открытом ключом на основе решетки с использованием принципов Эль-Гамаля»

Актуальность темы. В настоящее время традиционная криптография столкнулась с множеством проблем в связи с быстрым развитием современных вычислительных технологий, таких как квантовые вычисления и технологии облачных вычислений. Квантовые вычисления, обладая потенциалом экспоненциального ускорения обработки данных, представляют особую угрозу для алгоритмов RSA, ECC и Эль-Гамаля, поскольку алгоритм Шора позволяет эффективно решать задачи факторизации и дискретного логарифмирования, лежащие в основе их безопасности. По мере развития квантовых компьютеров криптографические алгоритмы, обеспечивающие нашу цифровую безопасность, могут стать уязвимыми для атак, что требует разработки криптографических примитивов, устойчивых к квантовым атакам. Облачные вычисления, с другой стороны, порождают новые проблемы безопасности, связанные с конфиденциальностью, целостностью и приватностью данных. Хотя они предоставляют удобный доступ к огромным вычислительным ресурсам и хранилищам, они также вызывают такие проблемы, как несанкционированный доступ к данным, утечки и внутренние угрозы. Обеспечение безопасности данных в облаке требует надёжных криптографических механизмов, защищённых протоколов связи и строгого контроля доступа. В ответ на вызовы, предъявляемые квантовыми вычислениями и развивающимися вычислительными технологиями, криптография на основе решёток выступила в качестве интересного решения, основанного на трудности решения решёточных задач, таких как задача поиска короткого целочисленного решения (SIS). В данной работе представлена новая схема шифрования с открытым ключом, устойчивая к квантовым атакам, основанная на решётках и использующая принципы Эль-Гамаля. Схема базируется на задаче поиска короткого целочисленного решения (SIS) и включает протокол обмена ключами, основанный на данной задаче, что обеспечивает безопасность как от квантовых, так и от классических атакующих. Конструкция схемы проста и предоставляет решение для безопасной передачи данных в современных криптографических средах. Это достижение подчёркивает продолжающуюся эволюцию криптографии в ответ на вызовы, предъявляемые квантовыми вычислениями и новыми технологиями. Исходя из вышеизложенного, можно прийти к выводу, что в настоящий

момент необходимость в эффективных методах, алгоритмах для улучшения защиты от квантовых атак с использованием метода Эль-Гамаля на основе решёток актуальна.

Цель диссертационной работы. Разработка метода создания улучшенной схемы постквантовой криптографии с открытым ключом на основе решеток, использующей принципов Эль-Гамаля.

Поставленная цель определила основные задачи диссертации.

1) Анализ популярных методов и алгоритмов традиционной криптографии и их устойчивости в условиях постквантовой криптографии.
2) Исследование схем распределения ключей на основе решёток.
3) Разработка модели эффективной и безопасной постквантовой схемы обмена ключами на основе решёток с использованием принципов Эль-Гамаля.
4) Разработка алгоритма и прототипа постквантовой криптосистемы с открытым ключом на основе решёток, использующей принципов Эль-Гамаля.
5) Исследование и тестирование эффективности предложенной постквантовой криптосистемы.

Объектами исследования являются процесс криптогафических защиты данных с использованием схем с открытым ключом от классических и квантовых атак.

Научная новизна диссертационной работы заключается в следующем:

- Разработана математическая модель эффективной и безопасной постквантовой схемы обмена ключами на основе решеток с использованием принципов Эль-Гамаля, что позволяет создать эффективные постквантовые схемы с открытым ключом для криптографических протоколов, систем аутентификации, финансовых систем, блокчейн и IoT-технологий.
- Разработан алгоритм и прототип постквантовой схемы с открытым ключом на основе решеток, использующей принципы Эль – Гамаля, что позволило повысить скорость генерации ключей шифрования в 240-583 раз (по сравнению с аналогами – LWE, Ring-LWE), и обеспечило стойкость к квантовым атакам(по сравнению с классической схемой Эль-Гамаля).

Методы исследования. Классическая криптография, теория решеток, оценки эффективности алгоритмов, экспериментальное тестирование.

Основное положение, выносимое на защиту.

1. Разработана математическая модель эффективной и безопасной постквантовой схемы обмена ключами на основе решеток с использованием принципов Эль-Гамаля, что позволяет создать эффективные постквантовые схемы с открытым ключом для криптографических протоколов, систем аутентификации, финансовых систем, блокчейн и IoT-технологий.

2. Разработан алгоритм и прототип постквантовой схемы с открытым ключом на основе решеток, использующей принципы шифрования Эль - Гамаля, что позволило повысить скорость генерации ключей шифрования в 240-583 раз (по сравнению с аналогами - LWE, Ring-LWE), и обеспечило стойкость к квантовым атакам (по сравнению с классической схемой Эль-Гамаля).

3. Предложена и обоснована теоретическая модель безопасности криптосистемы в соответствии со стандартом IND-CCA, с редукцией к задаче SIS в модели квантово-доступного случайного оракула (QROM), что обеспечивает формальную устойчивость схемы к квантовым атакам.

Теоретическое и практическое значение работы. Теоретическая значимость исследовательской работы заключается в том, что она способствует продвижению в разработке криптографических систем, устойчивых к квантовым атакам, и расширяет возможности применения математических методов в области информационной безопасности. Практическая значимость исследовательской работы заключается в применении разработанного алгоритма и программного обеспечения для дальнейшего использования в развитии других технологий, обеспечивающих безопасность как от квантовых, так и от классических угроз.

Разработанная схема проста и эффективно по скорости и обеспечивает решение для безопасной передачи данных в современных криптографических средах. Это достижение подчеркивает продолжающуюся эволюцию криптографии для решения проблем, связанных с квантовыми вычислениями и технологии облачных вычислений.

Апробация работы. Основные положения и результаты диссертационного исследования докладывались и обсуждались на научных семинарах кафедры «Кибербезопасность, обработка и хранение информации» КазНИТУ имени К. И. Сатпаева, в лаборатории ИИВТ, а также в SCSA и Кавказском университете (Caucasus University).

Достоверность результатов. Достоверность и обоснованность результатов диссертационной работы подтверждается наличием публикаций в изданиях, представленных Комитетом по контролю в сфере образования и науки МНВО РК, в журналах, входящих в международные информационные ресурсы Web of Science и Scopus (MDPI, Швейцария) и в международных научных конференциях, и по результатам, полученным другими авторами.

Связь с государственными программами. Тема диссертационной работы напрямую связана с приоритетами, обозначенными в Концепции кибербезопасности «Киберщит Казахстана», утверждённой Постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407(с изменениями и дополнениями соответствии приказа

Министра науки и высшего образования Республики Казахстан от 17 марта 2023 года № 236). Концепция «Киберщит Казахстана» определяет формирование устойчивой и защищённой цифровой среды как ключевое направление государственной политики в области национальной безопасности. Одним из её стратегических ориентиров является развитие информационной безопасности, устойчивой к перспективным угрозам**,** включая угрозы, связанные с развитием квантовых технологий. В этом контексте разработка постквантовых криптографических решений**,** таких как предлагаемая в диссертации схема, соответствует целям и задачам Концепции. Представленная работа направлена на создание отечественной криптографической технологии, устойчивой к квантовым атакам, и может быть применима для защиты информационно-коммуникационной инфраструктуры**,** критических объектов**,** финансовых систем**,** а также в рамках реализации цифровой трансформации и защиты национальных данных**.**

Публикации. Исследования и результаты, относящиеся к теме диссертации, были представлены на основе следующих публикаций:

1) Dana Sairangazhykyzy Amirkhanova, Maksim Iavich and Orken Mamyrbayev.*Cryptography* 2024, *8*(3),31. https://doi.org/10.3390/cryptography8030031 (Scopus, процентиль 66,Web of Science – Q2).”Lattice- based Post-Quantum Public Key Encryption Scheme Using ElGamal’s Principles”.

2) Әмірханова Д.С., Мамырбаев О.Ж., Вестник КазНПУ им Абая. Серия: физико-математические науки Том 83 № 3(2023). “Cryptographic analysis of the scheme of polylinear cryptography”.

3) Әмірханова Д.С., Мамырбаев О.Ж., Вестник НАН РК: Серия: Physico-Mathematical Series ISSN 1991-346X Volume 3. № 351 (2024).“El-Gamal’s Cryptographic Algorithm: Mathematical Foundations, Applications And Analysis”.

4) Әмірханова Д.С., Мамырбаев О.Ж., Вестник ВКТУ: Серия: Информационно - коммуникационные технологии ISSN 1561-4212 № 1(2025))“Research And Development of a Cryptography Algorithm Based on Polylinear Algebra Using Blockchain Methodology”.

Структура и объем диссертации. Диссертационная исследовательская работа состоит из введения, 3 разделов, заключения, списка литературы из 85 наименований и 1 приложения. Работа изложена на 96 страницах и содержит 39 рисунков, 1 таблицу.

Во введении раскрыты актуальность, конкретизированы проблемы, связанные с исследуемой темой. Приведены цель и задачи исследования, научная новизна и практическая ценность работы, методы исследования.

В первой главе диссертации представлены анализ популярных методов и алгоритмов традиционной криптографии, который показал их уязвимость перед квантовыми атаками, поскольку квантовые алгоритмы способны эффективно взламывать такие системы. Также проанализирована

постквантовая криптография и её значимость в современной криптографии, поскольку она предлагает методы и алгоритмы, устойчивые к атакам квантовых компьютеров.

Во второй главе диссертации проведён анализ существующих схем распределения ключей на основе решёток, который подтвердил их высокую устойчивость к квантовым атакам благодаря сложности базовых вычислительных задач. На основе данного анализа разработана модель эффективной и безопасной схемы обмена ключами, использующей решёточные методы и принципов Эль-Гамаля. Такое сочетание обеспечивает высокий уровень криптостойкости и производительности, делая предлагаемое решение практически применимым в современных системах защиты информации.

В третьей главе на основе программной реализации, разработан алгоритм и прототип постквантовой схемы с открытым ключом на основе решёток, использующей принципов Эль-Гамаля. Также проведённое исследование и тестирование эффективности предложенной криптосистемы, обоснована теоретическая модель безопасности криптосистемы в соответствии со стандартом IND-CCA, с редукцией к задаче SIS в модели квантово-доступного случайного оракула (QROM), что обеспечивает формальную устойчивость схемы к квантовым атакам. Кроме того, система продемонстрировала высокую скорость работы, что делает её перспективной для практического применения.

В заключении отражены основные результаты и выводы по диссертационной работе.