ОТЗЫВ
официального рецензента Жукабаева Тамара Кокеновна на диссертационную работу
Әмірхановой Даны Сайранғажықызы
на тему « Схема постквантового шифрования с открытом ключом на основе решетки
с использованием принципов Эль - Гамаля», предоставленную на соискание степени
доктора философии (PhD) по специальности « 8D06301 – Системы информационной безопасности»

№ п/п	Критерии	Соответствие критериям (подчеркнуть один из вариантов ответа)	Обоснование позиции официального рецензента (замечания выделить курсивом)
1.	Тема диссертации (на дату ее утверждения) соответствует направлениям развития науки и/или государственным программам	1.1 Соответствие приоритетным направлениям развития науки или государственным программам: 1) диссертация выполнена в рамках проекта или целевой программы, финансируемого(ой) из государственного бюджета (указать название и номер проекта или программы); 2) диссертация выполнена в рамках другой государственной программы (указать название программы); 3) диссертация соответствует приоритетному направлению развития науки, утвержденному Высшей научно-технической комиссией при Правительстве Республики Казахстан (указать направление).	Соответствует. Тема диссертации соответствует научно-исследовательским работам, выполняемым в рамках Концепции кибербезопасности «Киберщит Казахстана», утверждённой Постановлением Правительства Республики Казахстан от 30 июня 2017 года № 407 (с изменениями и дополнениями в соответствии с приказом Министра науки и высшего образования Республики Казахстан от 17 марта 2023 года № 236). Концепция разработана в соответствии с Посланием Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная конкурентоспособность» с учётом подходов Стратегии «Казахстан-2050» по вхождению Казахстана в число 30 самых развитых государств мира. Результаты данной работы соответствуют целям и задачам Государственной программы «Информационный Казахстан – 2020».
2.	Важность для науки	Работа вносит/не вносит существенный вклад в науку, а ее важность хорошо раскрыта/не раскрыта.	Результаты диссертационной работы рекомендуются для решения проблемы защиты информации от квантовых атак, обеспечения безопасной передачи конфиденциальных данных, повышения надёжности и эффективности криптографических протоколов, а также для разработки современных систем защиты критически важной инфраструктуры, финансовых

			систем, блокчейн-платформ и IoT-устройств в условиях развития квантовых вычислительных технологий.
3.	Принцип самостоятельности	Уровень самостоятельности: 1) высокий; 2) средний; 3) низкий; 4) самостоятельности нет.	Диссертационная работа Әмірхановой Д.С. – завершённая научная работа, в ней представлены новые научно обоснованные теоретические и экспериментальные результаты, которые являются актуальными для дальнейшего развития систем защиты информации. Все научно – исследовательские работы проведены автором самостоятельно.
	Принцип внутреннего единства	4.1 Обоснование актуальности диссертации: 1) обоснована; 2) частично обоснована; 3) не обоснована.	Интенсивное развитие современных информационных, телекоммуникационных и вычислительных технологий, а также их широкое применение во всех сферах деятельности человека приводит к росту вероятности возникновения киберугроз и увеличению мощности кибератак. В связи с этим обеспечение кибербезопасности становится важнейшим направлением государственной стратегии. Классические криптографические алгоритмы, несмотря на их значительные достижения, не могут гарантировать полной защиты от новых видов атак, в частности квантовых. Использование квантовых алгоритмов (Шора, Гровера и др.) делает традиционные методы защиты потенциально уязвимыми, поскольку они основаны на сложности математических задач для классических вычислительных систем. С появлением квантовых компьютеров, способных эффективно решать эти задачи, значительно снижается надёжность классических криптографических протоколов. Это создаёт острую необходимость в разработке новых криптографических решений, стойких к квантовым атакам. В этой связи особую актуальность приобретает поиск и внедрение постквантовых методов защиты информации, которые обеспечат её безопасность в условиях развития квантовых вычислительных технологий.

			Решением данной проблемы могут стать методы постквантовой криптографии, на разработку которых и направлена работа соискателя.
		4.2 Содержание диссертации отражает тему диссертации: 1) отражает; 2) частично отражает; 3) не отражает.	Содержание диссертации в полном объёме отражает тему, цель и задачи исследования. Поставленные задачи в диссертационной работе полностью выполнены; во всех разделах диссертации подробно представлены результаты проведённого исследования. Общий объём диссертации : 96 страниц машинописного текста, содержащих 39 рисунков, одну таблицу и список использованных источников, состоящий из 85 наименований.
		4.3. Цель и задачи соответствуют теме диссертации: 1) соответствуют; 2) частично соответствуют; 3) не соответствуют.	Цели и задачи исследования соответствуют теме диссертации. Цель исследований - разработка метода создания улучшенной схемы постквантовой криптографии с открытым ключом на основе решеток, использующей принципов шифрования Эль-Гамаля. В соответствии с этой целью были выполнены взаимосвязанные задачи: 1) выполнен анализ существующих методов и алгоритмов классической криптографии, результаты которого подтвердили их уязвимость перед квантовыми атаками, поскольку квантовые алгоритмы способны эффективно взламывать такие системы;; 2) проведен обзор и анализ решёточных схем распределения ключей, выявивший их высокую устойчивость к квантовым атакам за счёт вычислительной сложности базовых математических задач; 3) разработана математическая модель надёжной и производительной постквантовой схемы обмена ключами, основанной на решётках и принципах схемы Эль-Гамаля, что обеспечивает её практическую применимость в современных криптографических протоколах, а также в системах аутентификации, финансовых приложениях, блокчейн-средах и IoT-технологиях; 4) реализован алгоритм и создан прототип постквантовой криптосистемы с открытым ключом, построенной на основе задачи SIS и использующей принципы

			Эль-Гамаля, что позволило существенно повысить скорость генерации ключей (в 240–583 раза по сравнению с решениями на базе LWE и Ring-LWE), а также улучшить устойчивость к ошибкам и стойкость к квантовым атакам по сравнению с классическим вариантом схемы Эль-Гамаля); 5) безопасность предложенной постквантовой криптосистемы проанализирована в модели IND-CCA с редукцией к задаче SIS. Проведённое тестирование прототипа подтвердило корректность реализации, а также её высокие показатели вычислительной эффективности.
		4.4 Все разделы и положения диссертации логически взаимосвязаны: 1) полностью взаимосвязаны; 2) взаимосвязь частичная; 3) взаимосвязь отсутствует.	Введение посвящено обоснованию актуальности, цели и теме диссертационной работы, описанию объекта и предмета научно – исследовательской работы. Обоснована научная новизна и практическая значимость работы. Приведены сведения об апробации и публикации полученных результатов. Первый раздел посвящен подробному анализу 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 втором разделе выполнен обзор и анализ существующих схем распределения ключей на основе решёток, продемонстрировавший их высокую устойчивость к квантовым атакам за счёт вычислительной сложности используемых математических задач. На основе проведённого анализа автором разработана модель эффективной и безопасной схемы обмена ключами, сочетающая решёточные подходы с принципами схемы Эль-Гамаля. Данная комбинация позволяет достичь высокого уровня криптографической стойкости при сохранении высокой производительности, что

			делает предложенное решение практически значимым для использования в современных системах защиты информации. В третьем разделе представлены аспекты программной реализации предложенной схемы. Разработан алгоритм и создан прототип постквантовой криптосистемы с открытым ключом, основанной на решётках и использующей принципы схемы Эль-Гамаля. Проведены исследования и тестирование эффективности разработанной криптосистемы. Теоретическая модель её безопасности обоснована в соответствии с моделью IND-CCA с приведением (редукцией) к задаче SIS в условиях квантово-доступного случайного оракула (QROM), что подтверждает её формальную устойчивость к квантовым атакам. Кроме того, система продемонстрировала высокие показатели скорости работы, что свидетельствует о её перспективности для практического внедрения в современные средства защиты информации.
		4.5 Предложенные автором новые решения (принципы, методы) аргументированы и оценены по сравнению с известными решениями:	В работе проведён всесторонний анализ существующих квантово-устойчивых криптографических систем и методов защиты информации. В рамках критического обзора рассмотрены подходы, основанные на LWE и Ring-LWE, и аргументированы преимущества предложенной схемы на основе задачи SIS в аспектах скорости генерации ключей и криптостойкости. Достоверность полученных научных результатов, а также корректность сделанных выводов подтверждены экспериментальными исследованиями, включая тестирование разработанного прототипа криптосистемы.
		1) критический анализ есть;	
		2) анализ частичный;	
		3) анализ представляет собой не собственные мнения, а цитаты других авторов;	
		4) анализ отсутствует.	
5.	Принцип научной новизны	5.1 Научные результаты и положения являются новыми?	Научные результаты и принципы диссертации являются полностью новыми. Подтверждением является публикация результатов работы в рейтинговых научных изданиях, в том числе в тех что включены в науко-метрическую базу Scopus и Web of Science.
		1) полностью новые;	
		2) частично новые (новыми являются 25-75%);	
		3) не новые (новыми являются менее 25%).	

		5.2 Выводы диссертации являются новыми?	Выводы диссертации являются полностью новыми.
		1) полностью новые;	
		2) частично новые (новыми являются 25-75%);	
		3) не новые (новыми являются менее 25%).	
		5.3 Технические, технологические, экономические или управленческие решения являются новыми и обоснованными:	Технические и технологические решения диссертационной работы являются новыми и обоснованными.
		1) полностью новые;	
		2) частично новые (новыми являются 25-75%);	
		3) не новые (новыми являются менее 25%).	
6.	Обоснованность основных выводов	Все основные выводы основаны/не основаны на весомых с научной точки зрения доказательствах либо достаточно хорошо обоснованы (для qualitative research (куолитатив ресеч) и направлений подготовки по искусству и гуманитарным наукам).	Результаты, полученные в ходе исследования, являются обоснованными. Корректность сформулированных теоретических положений, гипотез и математических моделей подтверждена результатами экспериментальных исследований и верификацией разработанных методов и применяемых стандартов.
7.	Основные положения, выносимые на защиту	Необходимо ответить на следующие вопросы по каждому положению в отдельности:	На защиту вынесены следующие положения: 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**
		7.1 Доказано ли положение?	
		1) доказано;	
		2) скорее доказано;	
		3) скорее не доказано;	
		4) не доказано;	

		5) в текущей формулировке проверить доказанность положения невозможно. 7.2 Является ли тривиальным? 1) да; 2) нет; 3) в текущей формулировке проверить тривиальность положения невозможно. 7.3 Является ли новым? 1) да; 2) нет; 3) в текущей формулировке проверить новизну положения невозможно. 7.4 Уровень для применения: 1) узкий; 2) средний; 3) широкий; 4) в текущей формулировке проверить уровень применения положения невозможно. 7.5 Доказано ли в статье? 1) да; 2) нет; 3) в текущей формулировке проверить доказанность положения в статье невозможно.	**аутентификации, финансовых систем, блокчейн и IoT-технологий;** 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да, 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". **2) Разработан алгоритм и прототип постквантовой схемы с открытым ключом на основе решеток, использующей принципов Эль-Гамаля на основе SIS, что позволило повысить скорость генерации ключей шифрования в 240-583 раз (по сравнению с аналогами – LWE, Ring-LWE), а также устойчивость к ошибкам и стойкость к квантовым атакам (по сравнению с классической схемой Эль-Гамаля);** 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да, Dana Sairangazhykyzy Amirkhanova, Maksim Iavich and Orken Mamyrbayev.*Cryptography* 2024, *8*(3),31."Lattice- based Post-Quantum Public Key Encryption Scheme Using ElGamal's Principles" (Scopus, процентиль 66%, Web of Science – Q2).

			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; 7.1 доказано; 7.2 нет; 7.3 да; 7.4 широкий; 7.5 да, 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”. Dana Sairangazhykyzy Amirkhanova, Maksim Iavich and Orken Mamyrbayev.*Cryptography* 2024, *8*(3),31.”Lattice- based Post-Quantum Public Key Encryption Scheme Using ElGamal’s Principles” (Scopus, процентиль 66%, Web of Science – Q2).
8.	Принцип достоверности.	8.1 Выбор методологии - обоснован или методология достаточно подробно описана:	Выбранная докторантом методология обоснована и подробно описана. В диссертационной работе использованы критический анализ, современные научные методы анализа и исследований, методы оценки эффективности алгоритмов, а также экспериментальное тестирование.
	Достоверность источников и предоставляемой информации	1) да;	
		2) нет.	
		8.2 Результаты диссертационной работы получены с использованием современных методов научных исследований и методик обработки и интерпретации данных с применением компьютерных технологий:	Результаты диссертации были получены с использованием современных методов научного исследования, обработки и интерпретации данных с использованием компьютерных технологий. В работе использовались программное и аппаратное обеспечения для реализации криптосистемы: Python; Matplotlib; Numpy; Colab google.

		1) да;	
		2) нет.	
		8.3 Теоретические выводы, модели, выявленные взаимосвязи и закономерности доказаны и подтверждены экспериментальным исследованием (для направлений подготовки по педагогическим наукам результаты доказаны на основе педагогического эксперимента):	Теоретические выводы и модели были доказаны и подтверждены экспериментальными исследованиями, а также разработанным прототипом.
		1) да;	
		2) нет.	
		8.4 Важные утверждения подтверждены/частично подтверждены/не подтверждены ссылками на актуальную и достоверную научную литературу.	Важные утверждения подтверждаются ссылками на актуальную и достоверную научную литературу.
		8.5 Использованные источники литературы достаточны/не достаточны для литературного обзора.	Список использованной литературы включает 85 ссылок на английском и русском языках.
9	Принцип практической ценности	9.1 Диссертация имеет теоретическое значение:	Диссертация имеет теоретическое значение, достоверность теоретических положений подтверждается корректным применением стандарта , экспериментальными данными и результатами верификации предложенных методов.
		1) да;	
		2) нет.	
		9.2 Диссертация имеет практическое значение и существует высокая вероятность применения полученных результатов на практике:	Результаты, полученные в ходе исследовательских работ, имеют высокую практическую ценность и могут быть использованы для защиты информации.Практические результаты работы, подтверждены соответствующими доказательствами.
		1) да;	
		2) нет.	
		9.3 Предложения для практики являются новыми:	Практические решения являются полностью новыми.

		1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%).	
10.	Качество написания и оформления	Качество академического письма: 1) высокое; 2) среднее; 3) ниже среднего; 4) низкое.	Диссертационная работа Әмірхановой Даны Сайранғажықызы на тему «Схема постквантового шифрования с открытом ключом на основе решетки с использованием принципов Эль - Гамаля», предоставленную на соискание степени доктора философии (PhD) по специальности 8D06301 – «Системы информационной безопасности» подготовлена в соответствии с требованиями. Диссертация написана грамотным научно-техническим языком, формулировки научных положений, выводов четкие и лаконичные, имеют законченный характер.
11.	Замечания к диссертации	Замечания: 1) в работе используется значительное количество аббревиатур и сокращений, что в отдельных случаях может затруднять восприятие текста. 2) в работе присутствуют отдельные рисунки, в которых не всегда уточняются единицы измерения или параметры масштабов, что может затруднять их точную интерпретацию. Указанные замечания не способны повлиять на научную или практическую ценность представленной работы.	
12.	Научный уровень статей докторанта по теме исследования (в случае защиты диссертации в форме серии статей официальные рецензенты комментируют научный уровень каждой статьи докторанта по теме исследования)	Научный уровень статей соответствует требованиям, публикации в рейтинговых журналах Scopus и ККСОН РК подтверждают высокий уровень исследований.	

13.	Решение официального рецензента (согласно пункту 28 настоящего Типового положения)	Указанные замечания не снижают положительной оценки диссертационной работы. Считаю, что рецензируемая диссертационная работа Әмірхановой Даны Сайранғажықызы на тему «Схема постквантового шифрования с открытом ключом на основе решетки с использованием принципов Эль - Гамаля», по своей актуальности, научной новизне, важности для теории и практики, объёму экспериментальных исследований полностью соответствует требованиям, которые предъявляются к диссертациям на соискание степеней PhD Комитетом по обеспечению качества в сфере образования и науки МОН Республики Казахстан, а ее автор Әмірханова Дана Сайранғажықызы заслуживает присуждения степени доктора философии (PhD) по специальности 8D06301 – «Системы информационной безопасности».
й		

Рецензент, PhD, профессор
кафедры «Информационных систем»
Евразийский национальный университет имени Л.Н. Гумилёва
(Астана, Казахстан)

Кукабаева Тамара Кокеновна