ОТЗЫВ

официального рецензента Георгий Иашвили 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:	Соответствует.
		1) диссертация выполнена в рамках проекта или целевой программы, финансируемого(ой) из государственного бюджета (указать название и номер проекта или программы);	Настоящая диссертация выполнена в рамках исследовательской работы «8D06301 – Системы информационной безопасности и соответствует содержанию образовательной программы 8D06301 – «Системы информационной безопасности». Тема диссертации связана с научно-исследовательскими работами, выполняемыми в рамках 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).
		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).	
2.	Важность для науки	Работа **вносит** /не вносит существенный вклад в науку, а ее важность **хорошо раскрыта** / не раскрыта.	Разработана новая математическая модель постквантовой схемы шифрования, реализован прототип схемы, обеспечивающей повышение скорости генерации ключей и устойчивость к квантовым атакам. Работа направлена на актуальную задачу обеспечения

			криптографической стойкости в условиях появления квантовых вычислений.
3.	Принцип самостоятельности	Уровень самостоятельности: **высокий**	Диссертационная работа Әмірхановой Д.С. является самостоятельным завершённым научным трудом. Автором проведены все этапы исследований: от математического моделирования до экспериментальной проверки и внедрения результатов.
4.	Принцип внутреннего единства	4.1 Обоснование актуальности диссертации: 1) **обоснована;** 2) частично обоснована; 3) не обоснована.	В условиях появления квантовых вычислений традиционные криптографические алгоритмы (включая алгоритмы на основе дискретного логарифмирования и факторизации чисел) утрачивают свою стойкость перед квантовыми атаками, такими как алгоритм Шора. В ближайшей перспективе массовое развитие квантовых вычислительных систем может поставить под угрозу защищённость существующих криптографических протоколов, используемых в государственных, финансовых и коммерческих системах. В этой связи решение задачи разработки эффективных постквантовых криптографических схем, устойчивых к квантовым атакам, является приоритетным направлением обеспечения национальной и международной кибербезопасности. Разработка постквантовых решений с возможностью практического внедрения особенно важна для защиты критически важной инфраструктуры, обеспечения конфиденциальности данных и создания безопасных цифровых сервисов в условиях грядущей квантовой эры.
		4.2 Содержание диссертации отражает тему диссертации: 1) **отражает;** 2) частично отражает;	Содержание диссертации в полном объёме отражает тему, цель и задачи исследования. Начиная с введения, трёх разделов и заключения, в диссертации в полном объёме изложены результаты, соответствующие теме

		3) не отражает.	научно-исследовательской работы. Общий объём диссертации - 96 страниц, 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. Для достижения цели были решены следующие логически связанные задачи: 1) проведен анализ популярных методов и алгоритмов традиционной криптографии, который показал, что они не обладают устойчивостью к квантовым атакам, а квантовые алгоритмы способны эффективно взламывать такие системы; 2) выполнен анализ схем распределения ключей на основе решеток, который показал их высокую устойчивость к квантовым атакам благодаря сложности задач, лежащих в их основе; 3) 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; 4) разработан алгоритм и прототип постквантовой схемы с открытым ключом на основе решеток, использующей принципов Эль-Гамаля на основе SIS, что позволила 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); 5) безопасность

			предложенной постквантовой криптосистемы исследована в модели IND-CCA на основе задачи SIS. Проведено тестирование прототипа, подтвердившее её корректность и вычислительную эффективность.
		4.4 Все разделы и положения диссертации логически взаимосвязаны: 1) **полностью взаимосвязаны;** 2) взаимосвязь частичная; 3) взаимосвязь отсутствует.	Структурно диссертация состоит из введения, 3 разделов и заключения. Все разделы и положения диссертации логически связаны. 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.
		4.5 Предложенные автором новые решения (принципы, методы) аргументированы и оценены по сравнению с известными решениями:	В работе проведен многокритериальный анализ квантовых систем и методов защиты. Как следствие приведён критический анализ существующих решений (LWE, Ring-LWE), обоснованы преимущества предложенной схемы на основе SIS по скорости и устойчивости. Достоверность каждого научного результата, решения и вывода, сформулированных в диссертации, подтверждается экспериментальными исследованиями (прототипом модели).
		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

		1) **полностью новые;**	публикация результатов работы в рейтинговых научных изданиях, в том числе в тех что включены в наукометрическую базу Scopus и Web of Science.
		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 исследования докторанта являются полностью обоснованными. Достоверность предложенных докторантом теоретических положений, гипотез и математических моделей подтверждается соответствующими экспериментальными данными и результатами верификации предложенных методов и 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 криптографических протоколов, систем**
		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.	**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
		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.	

			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 криптографических протоколов, систем

		1) **да;**	аутентификации, финансовых систем, блокчейн и IoT-технологий Практические результаты работы, подтверждены соответствующими доказательствами.
		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:	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.
		1) **высокое;**	
		2) среднее;	
		3) ниже среднего;	
		4) низкое.	
11.	Замечания к диссертации	Замечаний, снижающих научную или практическую значимость работы, не имеется. Работа выполнена на высоком уровне.	
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)	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 и заслуживает присуждения степени доктора философии (PhD) по специальности 8D06301 – «Системы информационной безопасности».

Рецензент, PhD, ассоциированный профессор
кафедры «Информационные технологии»
Кавказского университета
(Тбилиси, Грузия)

Георгий Иашвили