Отзыв
зарубежного научного консультанта
о диссертационной работе Әмірхановой Д.С.,
«Схема постквантового шифрования с открытом ключом на основе решеток с использованием принципов Эль-Гамаля»,
представленной к защите на соискание ученой степени доктора философии (PhD) по специальности 8D06301- «Система информационной безопасности»

1. Актуальность исследования

Переход к квантовым вычислениям представляет фундаментальный вызов существующей инфраструктуре информационной безопасности. Алгоритмы RSA, ECC и даже гибридные протоколы с открытым ключом оказываются уязвимыми перед квантовыми атаками, основанными на алгоритме Шора. В данной ситуации необходимость разработки новых схем шифрования с постквантовой стойкостью приобретает стратегическое значение как в глобальном, так и в национальном контексте, включая реализацию Концепции «Киберщит Казахстана».Предложенная в диссертации Әмірхановой Д.С. схема объединяет в себе математическую строгость решеточной криптографии и концептуальную ясность схемы Эль-Гамаля. Это обеспечивает не только криптографическую устойчивость, но и практическую реализуемость, что особенно важно в контексте цифровой трансформации.

2. Степень разработанности проблемы

Автор демонстрирует глубокое понимание современных криптографических систем и их уязвимостей в условиях появления квантового противника. Обзор литературы включает как классические, так и новейшие разработки, в том числе стандарты NIST по постквантовой криптографии. На их фоне чётко обосновано направление работы, основанное на задаче поиска короткого целочисленного решения (SIS), как на одной из наиболее надёжных и признанных базовых задач постквантовой криптографии.

Также автор анализирует особенности протоколов с открытым ключом, распределения ключей, и даёт оценку существующим решеточным схемам, таким как LWE и Ring-LWE, выявляя их ограничения, которые затем преодолевает в своей собственной разработке.

3. Цель и задачи исследования

Целью диссертации является разработка эффективной и устойчивой к квантовым атакам схемы шифрования с открытым ключом, основанной на задаче SIS и принципах Эль-Гамаля.

Для достижения поставленной цели автор решает комплекс исследовательских задач:

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.

Решение каждой из задач представлено последовательно, логично и методически выверено.

4. Научная новизна

Новизна диссертационного исследования заключается в следующем:

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.

2. Разработан алгоритм и прототип постквантовой схемы с открытым ключом на основе решеток, использующей принципов шифрования Эль - Гамаля, что позволило повысить скорость генерации ключей шифрования.

5. Степень обоснованности результатов и точность выводов

Все выводы обоснованы строгими математическими доказательствами, подтверждены моделированием и экспериментальными результатами. Использованы устойчивые методы оценки сложности задач на решетках, а также криптографические принципы доказательства безопасности схем в адаптивной модели. Автор корректно указывает границы применимости модели и честно формулирует условия, при которых схема сохраняет свои свойства.

Достоверность данных подтверждается публикациями в международных рецензируемых журналах, включая статью в журнале Web of Science (Q2, Scopus percentile 66).

6. Апробация и публикационная активность

Результаты исследования прошли успешную апробацию в рамках семинаров кафедры «Кибербезопасность, обработка и хранение информации» Satbayev University, а также на научных конференциях. По теме диссертации опубликованы:

- статья в международном журнале из базы Web of Science и Scopus;
- 3 статьи в изданиях, рекомендованных КОКСНВО;

что полностью соответствует требованиям Комитета по обеспечению качества в сфере науки и высшего образования.

7. Заключение и рекомендация к присуждению степени

Диссертационная работа Әмірхановой Даны Сайранғажықызы выполнена на высоком научном уровне, сочетает теоретическую строгость и практическую направленность. Автор продемонстрировала высокий уровень профессиональной подготовки, самостоятельность в проведении научного исследования и способность решать актуальные задачи современной криптографии.Представленная диссертация отвечает всем требованиям, предъявляемым к научно-квалификационным работам на соискание степени доктора философии (PhD) по специальности 8D06301 – «Системы информационной безопасности», и может быть рекомендована к защите, а автор заслуживает присуждения соответствующей степени.

Научный консультант,
зам.директор РГП «Института
информационных и вычислительных
технологий» КН МОН РК, PhD
профессор **Мамырбаев О.Ж**