**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»

**Актуальность темы. Соответствие темы современным научным и практическим запросам**

В условиях стремительного развития вычислительных технологий, в частности квантовых вычислений, защита информации становится одной из приоритетных задач в сфере информационной безопасности. Многие традиционные криптографические системы, такие как RSA, DSA, и алгоритмы, основанные на эллиптических кривых, теряют свою актуальность, поскольку квантовые алгоритмы, в первую очередь алгоритм Шора, позволяют эффективно решать лежащие в их основе задачи факторизации и дискретного логарифмирования. Это ставит под угрозу конфиденциальность и целостность информации в большинстве существующих IT-систем.В этой связи тема диссертационного исследования, направленная на разработку устойчивой к квантовым атакам схемы шифрования на основе решеток с использованием принципов Эль-Гамаля, является своевременной и исключительно актуальной. Она отражает современный запрос научного сообщества на разработку криптографических методов, способных эффективно функционировать в условиях появления квантовых компьютеров.Кроме того, работа затрагивает и вопросы защиты данных в облачных средах, где возникает потребность в высокоэффективных и одновременно безопасных схемах обмена ключами и шифрования. Это особенно актуально в условиях глобальной цифровизации и перехода государственных, коммерческих и финансовых систем к облачным и распределенным платформам.Таким образом, рассматриваемая тема отвечает не только академическим интересам, но и практическим потребностям в обеспечении устойчивой к будущим угрозам информационной безопасности.

**Оценка значимости исследуемой проблемы и научной новизны**

Научная значимость проведенного исследования заключается в его вкладе в развитие постквантовой криптографии, особенно в области построения эффективных и

устойчивых схем с открытым ключом. Предложенный подход сочетает две важные идеи: использование задачи поиска короткого целочисленного решения (SIS), являющейся одной из наиболее изученных и надежных решеточных задач, и адаптацию принципов схемы Эль-Гамаля, которая традиционно применялась в контексте других алгебраических структур.Такое сочетание ранее не получило широкого распространения, что свидетельствует о научной новизне работы. Автор не просто объединяет два подхода, но делает это на строго формализованной основе, с учётом специфики решеточных задач и требований безопасности в постквантовой модели угроз.Новизна проявляется также в разработке протокола обмена ключами, адаптированного под решеточную структуру, и в создании эффективного программного прототипа. Показатели производительности, представленные в работе, демонстрируют значительное преимущество предложенной схемы в сравнении с аналогами (в частности, LWE и Ring-LWE), в том числе в скорости генерации ключей.

Таким образом, работа вносит оригинальный вклад как в теоретическое развитие постквантовой криптографии, так и в практическую реализацию безопасных криптографических механизмов.

**Цель и задачи диссертационной работы**

Целью исследования является разработка постквантовой схемы шифрования с открытым ключом, основанной на задаче SIS и принципах Эль-Гамаля, обладающей высокой устойчивостью к квантовым атакам и эффективной с точки зрения вычислительных затрат.

Для достижения данной цели в диссертации были сформулированы и последовательно решены следующие задачи:

1. Проведен анализ существующих криптографических схем и их уязвимостей в условиях постквантовой угрозы.
2. Изучены свойства и применимость решеточных задач, в особенности задачи SIS, для построения криптографических протоколов.
3. Разработана математическая модель схемы обмена ключами на основе решеток, сочетающая преимущества классической схемы Эль-Гамаля и криптостойкости SIS.
4. Реализован программный прототип предложенной схемы, включающий алгоритмы генерации ключей, шифрования и расшифрования.

5. Проведено тестирование устойчивости и эффективности предложенной криптосистемы, включая оценку времени выполнения и устойчивости к атакующему в модели IND-CCA.

Задачи сформулированы четко, логически вытекают из поставленной цели и охватывают как теоретическую, так и практическую стороны криптографической разработки.

**Методология исследования**

Методологическая основа диссертационной работы охватывает как классические, так и современные методы криптоанализа, математического моделирования и экспериментального тестирования. В работе использованы:

- Методы теории решеток, включая анализ задач SIS и их применения в криптографических протоколах;
- Алгоритмические подходы к построению схем с открытым ключом;
- Методы математического моделирования для построения архитектуры схемы;
- Теория вероятностей и криптостойких редукций (включая доказательства в модели QROM);
- Программные средства для реализации и тестирования алгоритмов, включая анализ времени генерации ключей, производительности и устойчивости к атакам.

Особое внимание в работе уделено формализации безопасности схемы: автор опирается на стандартные модели доказательства безопасности, в том числе на IND-CCA-модель, которая отражает реальный уровень устойчивости к адаптивному атакующему.

Такой подход свидетельствует о глубокой методологической проработке и научной зрелости автора.

**Общая оценка работы и деятельности соискателя**

Диссертационная работа представляет собой завершенное научное исследование, выполненное на высоком теоретическом и практическом уровне. Работа логично структурирована, ясно изложена, содержит как подробные математические выкладки, так и результаты программной реализации и тестирования.

Особо следует отметить высокую самостоятельность автора в постановке задачи, выборе методов и анализе полученных результатов. Автор глубоко владеет предметной

областью, демонстрирует критическое мышление, способность к обобщению и аргументированному обсуждению полученных результатов.

Результаты исследования были апробированы в форме публикаций, в том числе в журнале, входящем в базы Scopus и Web of Science, а также в изданиях, рекомендованных КОКСНВО. Это подтверждает как научную ценность работы, так и её соответствие международным стандартам.

Соискатель проявил себя как ответственный, компетентный исследователь, способный к самостоятельному решению сложных научных задач в области криптографии и информационной безопасности.

**Заключение**

Учитывая актуальность темы, высокий уровень научной новизны, логичную структуру, глубину теоретического анализа, качество экспериментальной реализации, а также публикационную активность автора, можно с уверенностью утверждать, что представленная диссертационная работа полностью соответствует требованиям, предъявляемым к научным исследованиям на соискание степени доктора философии (PhD).

Диссертация работа Әмірхановой Д.С является законченным научным исследованием, удовлетворяющим требованиям, предъявляемым к работам на соискание ученой степени доктора философии, по специальности 8D06301 – «Системы информационной безопасности», что явилось основанием для представления работы к защите.

**Зарубежный научный консультант:**

проректор по научным исследованиям и трансферу технологий,

Государственный университет «Киевский авиационный институт»,

доктор технических наук, профессор Сергей ГНАТЮК