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 диссертационного исследования заключается в том, что развитие квантовых технологий ставит под угрозу безопасность традиционных криптографических систем, применяемых в большинстве современных информационных инфраструктур. В этой связи особенно остро стоит задача разработки криптографических решений, устойчивых к атакам с использованием квантовых компьютеров. Кроме того, стремительное развитие облачных технологий, а также необходимость защиты персональных и корпоративных данных формируют устойчивый научный и прикладной интерес к теме постквантовой криптографии.

Представленная к защите диссертационная работа посвящена разработке схемы постквантового шифрования с открытым ключом, сочетающей решеточные методы и принципы классической схемы Эль-Гамаля. Автор аргументированно обосновывает актуальность использования задачи поиска короткого целочисленного решения (SIS) как базовой криптографической предпосылки, обладающей доказанной стойкостью как к классическим, так и к квантовым атакам.

В своей диссертации Әмірханова Д.С. рассматривает как теоретические основы постквантовой криптографии, так и проектирует прикладное решение — схему шифрования, основанную на современной алгебраической модели. Автор не только формализует структуру схемы, но и разрабатывает эффективный алгоритм, подтверждающий практическую реализуемость предложенного подхода.

Научная новизна диссертации заключается в оригинальной интеграции решеточной криптографии с принципами схемы Эль-Гамаля. Такое сочетание обеспечивает не только устойчивость к атакам в условиях квантовой модели, но и значительное улучшение производительности по сравнению с существующими аналогами (в том числе LWE и Ring-LWE). В работе представлены точные количественные показатели, свидетельствующие о росте скорости генерации ключей в 240–583 раза. Автором выполнен также анализ стойкости схемы в модели IND-CCA, что соответствует международным стандартам оценки безопасности криптографических протоколов. Проведены программная реализация схемы и её экспериментальная верификация, что подтверждает жизнеспособность разработанного решения как в теоретическом, так и в прикладном аспекте.

Особое внимание в диссертации уделено построению модели обмена ключами и её применимости в современных цифровых инфраструктурах, включая финансовые системы, блокчейн, IoT и другие области, где высока потребность в защите данных от потенциальных квантовых угроз. Это придает исследованию практическую ценность и перспективу широкого внедрения.

Объективность и достоверность результатов исследования, полученных в процессе реализации поставленных задач, подтверждаются научными публикациями автора, включая статью в журнале, индексируемом в Scopus и Web of Science (Q2), а также в изданиях, рекомендованных Комитетом по обеспечению качества в сфере науки и высшего образования (КОКСНВО).

Научная новизна исследования выражена в:

- создании модели эффективной схемы шифрования на основе SIS и Эль-Гамаля;
- разработке алгоритма, устойчивого к квантовым атакам;
- формализации методики оценки криптостойкости в постквантовой модели;
- экспериментальной проверке производительности предложенной схемы на программном уровне.

Результаты исследования могут быть использованы в национальных и международных системах цифровой безопасности, особенно в условиях внедрения квантово-устойчивых стандартов. Также они могут быть применены в рамках реализации стратегий кибербезопасности, в том числе концепции «Кибершит Казахстана».

Диссертационная работа продемонстрировала высокий научно-методологический уровень. Әмірханова Д.С. показала зрелость как исследователь, обладающий необходимыми теоретическими знаниями, практическими навыками, умением формулировать задачи и находить эффективные пути их решения. Все позиции диссертации согласованы, логически обоснованы, продуманы и выстроены в логическую научную конструкцию.

Полученные результаты обладают научной новизной, высокой теоретической значимостью и широким практическим потенциалом в контексте перехода к квантово-устойчивым системам защиты информации.

В соответствии с вышеизложенным, считаю, что диссертационное исследование Әмірхановой Д.С на тему «Схема постквантового шифрования с открытым ключом на основе решеток с использованием принципов Эль-Гамаля» на соискание степени доктора философии (PhD) по специальности 8D06301 – «Системы информационной безопасности» соответствует предъявляемым требованиям, является самостоятельным и завершённым научным трудом и может быть допущено к защите.

Зарубежный научный консультант,
директор Научной ассоциации по
кибербезопасности (SCSA),
профессор и начальник направления
по кибербезопасности Кавказского университета (Грузия) **М.Явич**