ОТЗЫВ НАУЧНОГО КОНСУЛЬТАНТА

на диссертационную работу докторанта PhD Юбузовой Халичи Ибрагимовны на тему: «Методы безопасного распределения ключей на базе протоколов квантовой криптографии», представленной на соискание степени доктора философии (PhD) по специальности 6D070400 – «Вычислительная техника и программное обеспечение»

Диссертационная работа Юбузовой Халичи Ибрагимовны является итогом многолетних исследований в области квантовой криптографии, выполненных в период с 2012 по 2018 гг. на основе материалов, собранных и обработанных лично автором, трехлетнего обучения в докторантуре КазНИТУ им. К.И. Сатпаева, научных стажировок в Национальном авиационном университете (г. Киев, Украина) и Белорусской государственной академии связи (г. Минск, Беларусь).

Диссертационная работа посвящена разработке и исследованию современных методов повышения эффективности распределения ключей шифрования на базе протоколов квантовой криптографии, что является актуальным направлением исследований, которое имеет теоретическое и практическое значение.

Цель, задачи и защищаемые положения диссертации сформулированы четко, текст написан грамотно с использованием специализированной терминологии в области квантовой криптографии, каждый пункт выводов обоснован и подтвержден качественными эффектами и количественными показателями.

Диссертант проанализировала текущее состояние в области квантовой криптографии, в частности вопросы, связанные с распределением ключей шифрования с помощью кодирования классической информации в состояния фотонов, которые являются носителем кубитов или кутритов; выявила, что наиболее эффективными являются квантово-криптографические протоколы с использованием кутритов (с точки зрения информационной емкости); определила, что большинство современных результатов в области квантовой криптографии связаны с повышением стойкости и скорости передачи данных, а также то, что повышение уровня стойкости непременно приводит к понижению скорости обработки и передачи данных. Это понижает эффективность распределения ключей шифрования в режиме реального времени. Полученные автором результаты в совокупности ориентированы на повышение эффективности распределения ключей за счет использования предложенных в работе методов и моделей на базе протоколов квантовой криптографии.

Научная новизна полученных результатов заключается в следующем:

1. Получила дальнейшее развитие классификация квантово-криптографических методов, которая позволяет расширить возможности по выбору необходимых квантово-криптографических методов для построения безопасных систем распределения ключей шифрования.

2. Разработана модель квантового детерминистического протокола в режиме контроля подслушивания, которая позволяет обеспечить безопасное и быстрое распределение ключей (в контексте реализации некогерентной атаки), а также сформулировать практические рекомендации по разработке квантово-криптографических систем в условиях использования деполяризационного квантового канала и присутствия нарушителя.

3. Разработана модель квантового детерминистического протокола в режиме передачи сообщений, которая дает возможность повысить уровень доступности квантового канала при передаче ключа детерминистическим протоколом при небольшом уровне природных шумов.

4. Предложен новый метод усиления секретности, который позволяет повысить скорость передачи без потерь стойкости детерминистических протоколов квантовой криптографии с использованием пар кутритов к некогерентной атаке.

5. Впервые реализован синтез комбинированной модели на основе разработанных модели режима контроля подслушивания и модели режима передачи сообщений квантового детерминистического протокола с парами перепутанных кутритов с использованием предложенного метода усиления секретности. Усовершенствован метод безопасного распределения ключей, что позволило повысить скорость и обеспечить помехоустойчивость деполяризационного квантового канала.

Полученные в диссертационной работе результаты могут быть использованы для решения актуальной и важной проблемы распределения ключей криптографических систем, а также для повышения эффективности систем криптографической защиты информации.

Изложенные научные положения, выводы и рекомендации являются полностью обоснованными, а достоверность предложенных диссертантом теоретических положений, гипотез и математических моделей подтверждается соответствующими экспериментальными данными и результатами верификации предложенных методов и протоколов. Полученные во время экспериментов, данные соответствуют теоретическим выводам работы и полностью подтверждают их. Корректно применены методы теории защиты информации, теории криптографии и криптоанализа, квантовой теории информации, квантовой механики, объектно-ориентированного программирования и имитационного моделирования.

В процессе написания диссертационной работы Юбузова Х.И. проявила себя квалифицированным специалистом, способным анализировать потоки информации, генерировать идеи и решать поставленные научные задачи.

Полученные результаты обсуждались и были апробированы на международных и республиканских научных конференциях, семинарах и симпозиумах, а также в отчетах научно-исследовательского проекта «Квантово-криптографические методы защиты критической информационной инфраструктуры государства», в котором диссертант выступала в качестве исполнителя.

По теме диссертационного исследования соискателем опубликовано 36 работ, в том числе 3 опубликованы в изданиях, рекомендованных Комитетом по обеспечению качества в сфере образования и науки МОН Республики Казахстан; 6 статей, индексируемых в базе данных Scopus и Web of Sciences; 3 статьи в зарубежных журналах и 21 материал на международных научных конференциях, 1 раздел в коллективной монографии на английском языке.

Диссертационная работа Юбузовой Халичи Ибрагимовны «Методы безопасного распределения ключей на базе протоколов квантовой криптографии» отвечает всем требованиям, предъявляемым к докторским диссертациям и рекомендуется к защите для присвоения ей степени доктора философии (PhD) по специальности 6D070400 «Вычислительная техника и программное обеспечение».

Научный консультант
д.т.н., профессор Б.С. Ахметов

«___» _____ 2022 г.

РАСТАЙМЫН: Абай атындағы ҚазҰПУ
ПЕРСОНАЛДЫ БАСҚАРУ БӨЛІМІНІҢ БАСТЫҒЫ
ЗАВЕРЯЮ: НАЧАЛЬНИК ОТДЕЛА ПО УПРАВЛЕНИЮ ПЕРСОНАЛОМ КазНПУ имени Абая
ҚОЛЫ ПОДПИСЬ _____