

Заключение по содержанию диссертации

Корнеев Александр Александрович

(Ф.И.О. члена диссертационного совета)

ФИО соискателя: Дуплинский Александр Валерьевич

Название диссертации: «Квантовое распределение ключа с высокочастотным поляризационным кодированием»

Научная специальность: 01.04.21 – Лазерная физика

Ученая степень, на соискание которой представлена диссертация: кандидат физико-математических наук

Дата защиты 23.12.2019

Оценка соответствия диссертации требованиям Положения о присуждении ученых степеней кандидата наук, доктора наук в МФТИ (далее - Положение):

1. Актуальность тематики диссертации:

Актуальность тематики связана с развитием новых квантовых технологий в области передачи и обработки данных, в том числе методов безопасной передачи данных, основанной на методах квантовой криптографии. В настоящее время квантовая криптография переходит от лабораторных прототипов к практическим системам, работающим в банках, коммерческих компаниях и государственных учреждениях. Разработка новых принципов для реализации квантово-криптографических систем, превосходящих существующие аналоги, является важной научной задачей. В диссертационном исследовании представлена новая методика оценки влияния побочных степеней свободы на уязвимость квантово-криптографической системы, реализована новая схема поляризационного кодирования для протокола BB84, продемонстрирована ее работоспособность и определены ее характеристики.

2. Научная новизна выносимых на защиту результатов:

1. Предложена новая методика оценки влияния побочных степеней свободы оптического излучения, т.е. различимости оптических импульсов от различных источников, на защищенность квантового канала.
2. Создана новая схема оптического кодирования для протокола BB84, допускающая масштабирование по частоте вплоть до частоты используемых оптических модуляторов.
3. Впервые выполнено моделирование автономной работы оптической схемы в изменяющихся внешних условиях.
4. Впервые работа предложенной схемы реализации протокола BB84 была продемонстрирована в условиях действующих телекоммуникационных сетей.

3. Теоретическая и практическая значимость диссертационной работы:

Теоретическая значимость работы заключается в предложенной и обоснованной новой методике определения влияния различимости оптических импульсов от различных источников (т.е. побочных степеней свободы оптического излучения) на защищенность квантового канала, дан количественный критерий надежности канала на основании измерения интерференционной картины по схеме Хонга-У-Манделя.

Практическая значимость работы состоит в том, что предложенная схема оптического кодирования была протестирована в реальных оптических сетях, связывающих отделения банков и узлы операторов связи, а также протестировано сопряжение с коммерческим шифровальным оборудованием.

4. Полнота опубликования основных результатов диссертации в рецензируемых научных изданиях в соответствии с требованиями Положения:

Результаты диссертационного исследования опубликованы в международно признанных научных журналах (9 публикаций, из них 4 в рецензируемых журналах, индексируемых Web of Science и Scopus), представлены на 8 международных конференциях, а также имеется патент США на высокоскоростную автокомпенсационную схему распространения квантового ключа.

5. Вопросы и замечания (в соответствии с п. 4.13 Положения соискатель отвечает на сформулированные здесь вопросы и замечания на заседании по защите диссертации):

1. В системе КРК используются однофотонные детекторы с квантовой эффективностью около 10% (стр. 85). Сегодня существуют однофотонные детекторы с более высокой квантовой эффективностью, в том числе и однофотонные лавинные диоды. Чем обусловлен выбор детекторов в работе? Известно ли значение временного разрешения (временной джиттер) используемых детекторов?

2. Там же, на стр. 85, сказано, что частота генерации квантовых состояний составляла 312,5 МГц, а мертвое время детектора устанавливалось на уровне 5 мкс. Не уменьшает ли такой выбор мертвого времени реально доступную частоту генерации квантовых состояний?

6. Общая характеристика диссертации (не включает резолютивную часть):

Представленные замечания несколько не снижают качества диссертационной работы и ее положительной оценки. Диссертация Дуплинского Александра Валерьевича «Квантовое распределение ключа с высокочастотным поляризационным кодированием» представляет собой выполненное на высоком уровне законченное научное исследование, актуальность, новизна и практическая значимость которого не вызывают сомнения. Автореферат объективно и полностью отражает содержание диссертации. Диссертация полностью соответствует требованиям Положения о присуждении ученых степеней кандидата наук в МФТИ.

Дата

Подпись

Цуев
05.12.2019

д.ф.-м.н.

Корнеев А.А.



Подпись

А.А. Корнеев
УДОСТОВЕРЯЮ

начальник

Управления делами

Л.А. Шведова
Л.А. Шведова