Заключение по содержанию диссертации

Маныко Владимир Иванович

(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:

   Квантовая криптография и ее основной раздел – квантовое распределение ключа лежат на стыке двух важнейших современных областей знаний – теории информации и квантовой физики. Развитие этого направления, в первую очередь направлено на создание реальных систем, использующихся для защиты информации. В то же время исследования в данной области способствует развитию квантовой теории информации и квантовой оптики в целом.
   Оптические схемы являются фундаментом экспериментов по квантовому распределению ключей. В силу специфики конечной задачи важно добиться максимально полного соответствия между реальным устройством и теоретической моделью, во избежание снижения уровня секретности генерации. Для решения практических задач также важно демонстрировать высокую скорость распределения ключа. Этот параметр тоже во многом связан с оптической реализацией. Таким образом актуальность работы обуславливается значимостью развития оптических систем, воплощающих в жизнь теоретические протоколы квантовой криптографии.

2. Научная новизна выносимых на защиту результатов:

   В рамках диссертационной работы получен ряд новых результатов:
   1. Создана оригинальная оптическая схема квантового распределения ключей с поляризационным кодированием, обладающая рядом преимуществ по сравнению с аналогами. В частности, схема позволяет использовать только один лазерный источник и изменять частоту приготовления импульсов в широком диапазоне без необходимости внесения изменений со стороны оптики.
   2. Произведено моделирование преобразований поляризации в оптической схеме квантового распределения ключей, что позволило построить систему автоматизированной калибровки схемы с целью обеспечения автономной работы в изменяющихся внешних условиях. В отличие от аналогичных схем, в реализованной системе не требуется наличия дополнительных

измерительных модулей, калибровка производится на основании статистики счёта однофотонных детекторов.

3. Впервые предложена и теоретически обоснована обобщающая методика оценки различимости световых импульсов, базирующаяся на схеме интерференции второго порядка (эффект Хонга-У-Манделя). Данная методика позволяет количественно оценить нежелательную различимость импульсов и тем самым гарантировать секретность квантового распределения ключей в условиях наличия нескольких лазерных источников.

3. Теоретическая и практическая значимость диссертационной работы:

Практическая значимость работы в первую очередь определяется созданием устройства квантового распределения ключа, способного работать в существующих телекоммуникационных сетях. Система прошла ряд полевых испытаний на городских волоконно-оптических линиях связи, в том числе с в сопряжении с шифровальным оборудованием, что, несомненно, свидетельствует о её практической применимости. В свою очередь разработанные теоретические модели могут быть использованы для будущих квантово-оптических экспериментов.

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

Основные результаты диссертации представлены в 4 рецензируемых научных журналах, индексируемых Web of Science и Scopus. Ряд работ опубликован по результатам участия автора в международных конференциях. Оформлен патент на изобретение.

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 работе постулируется использование слабых когерентных импульсов со случайной фазой в качестве альтернативы истинно однофотонным источникам. Однако, рандомизация фазы в данном случае никак не мотивируется. Является ли это требованием протокола или же удобством практической реализации? Возможно ли построение системы квантового распределения ключа с использованием ослабленных когерентных импульсов, но детерминированной фазой?
2. На рисунке 1.6 вблизи нулевой видности значение разбалансировки базисов выходит на постоянное значение 0,5. Однако, из формулы 1.34 это никак не следует. Следует модифицировать формулу на случай малых значений видности, либо отдельно оговорить границы её применимости.
3. В работе многократно используются аббревиатуры КРК и СКИРФ, следовало бы отдельно ввести их перед основной частью работы.

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

Упомянутые вопросы и замечания не умаляют ценности работы. Диссертация Дуплинского А.В. посвящена актуальной тематике и выполнена на высоком научном уровне. Полученные в результате исследования результаты имеют практическую значимость и обладают научной новизной. Таким образом, диссертация соответствует требованиям Положения о присуждении ученых степеней кандидата наук, доктора наук в МФТИ.

Дата 03.12.2019

Подпись Маньков Д.Ч / расшифровка (полностью)

Подпись К.И. Маньков заверяю

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА Савинов С.Ю.