Заключение по содержанию диссертации

Звездина Анатолия Константиновича
(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:

   Квантовое распределение криптографических ключей является одним из основных направлений современных квантовых технологий, а также наиболее развитым с практической точки зрения разделом квантовой информатики. Ключевым элементом экспериментальных реализаций протоколов квантового распределения ключей является оптическая схема, позволяющая осуществлять генерацию и модуляцию квантовых состояний на стороне передатчика, а также производить измерения на стороне приёмника. Существует ряд различных параметров, использующийся для кодирования бит в рамках протоколов распределения ключа. Использование поляризации света для кодирования состояний является одним из наиболее распространённых подходов. Вышеперечисленные факты определяют несомненную актуальность тематики диссертации.

2. Научная новизна выносимых на защиту результатов:

   Все результаты, выносимые на защиту, являются новыми. Так, разработанная оптическая схема по ряду параметров превосходит существующие аналоги, в частности для ее работы требуются только один лазерный источник и только два однофотонных детектора, что позволяет упростить и миниатюризировать систему, избавиться от ряда уязвимостей и увеличить скорость генерации ключа. Использованные для достижения данного результата решения, такие как взаимная компенсация дисперсии поляризационных мод двух модуляторов и ввод излучения в кристалл под углом без необходимости изменения схемы крепления поддерживающего поляризацию волокна к кристаллу, также не были опубликованы ранее. Подробно описана разработанная автором процедура калибровки схемы на основании математической модели преобразования поляризации. Теоретически предложенный метод оценки пассивной утечки информации о ключе впервые позволяет интегрально оценить степень несовпадения оптических мод излучения для различных кубитов, генерируемых в рамках протокола квантового распределения ключа.

3. Теоретическая и практическая значимость диссертационной работы:

Диссертация представляет несомненную практическую значимость, так как разработанная в рамках работы оптическая схема совместно с системами калибровки и стабилизации легла в основу устройства квантового распределения ключей на телекоммуникационных линиях связи. Само устройство тестировалось в том числе в городских оптоволоконных сетях, связывающих узлы операторов связи и отделения банков. В то же время, теоретические результаты, полученные в работе, могут быть полезны в контексте создания будущих стандартов сертификации, а также при разработке оптических схем, реализующих поляризационное кодирование оптических кубитов.

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

Основные результаты работы опубликованы в 9 печатных изданиях, 4 из которых являются рецензируемыми научными журналами, индексируемыми Web of Science и Scopus, 4 – труды конференций, 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. Для разработанного устройства стоит оговорить характерные величины скоростей генерации ключа и предельного расстояния между передатчиком и приемником. Это позволило бы провести сравнение устройства с существующими аналогами систем квантового распределения ключей как в России, так и мире.
2. В контексте описания оптической схемы следует дополнительно обратить внимание на защиту от практических атак. Так, например, для оптической схемы передатчика (Алисы) атаки вида «Троянский конь» могут представлять существенную угрозу безопасности системы.
3. В тексте работы присутствуют ряд опечаток и неточностей. На странице 57 явно неверно указан период импульсов, изображенных на рисунке – 0,5 мкс и 1 мкс вместо 0,4 и 0,8 мкс, соответствующих указанной частоте повторения 10 МГц.

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

Указанные замечания не несут принципиального характера и не умаляют результатов проделанной работы. Диссертация Дуплинского А.В. «Квантовое распределение ключа с высокочастотным поляризационным кодированием» представляет собой квалифицированное, цельное и практически значимое научное исследование.

Автореферат корректно и полно отражает основные положения диссертации. Диссертационная работа полностью соответствует требованиям Положения о присуждении ученых степеней кандидата наук, доктора наук в МФТИ.

Дата 4

Подпись 04.12.2019 / Звездин Анатолий Константинович / расшифровка (полностью)

ПОДПИСЬ Звездина А.К.

ЗАВЕРЯЮ

ВРИО УЧЁНОГО СЕКРЕТАРЯ ИОФ РАН

Подпись Глушков В.В.

«04» декабря 2019 г.