ОТЗЫВ

научного руководителя, д.ф.-м.н., Молоткова Сергея Николаевича на диссертационную работу Сущева Ивана Сергеевича «Исследование комбинированных атак на волоконные системы квантового распределения ключей», представленную на соискание учёной степени кандидата физико-математических наук по специальности 1.3.19. Лазерная физика

Иван Сергеевич Сущев в 2022 году с отличием окончил магистратуру физического факультета МГУ имени М.В. Ломоносова. В 2022 году он поступил в аспирантуру физического факультета МГУ имени М.В. Ломоносова. За время обучения в аспирантуре И.С. Сущев успешно выполнил учебный и научный план, а также сдал кандидатские экзамены.

И.С. Сущев присоединился к научной группе волоконной квантовой криптографии в Центре Квантовых Технологий МГУ имени М.В. Ломоносова в 2020 году. За время работы в лаборатории с участием И.С. Сущева было выпущено более 20 публикаций, включая 7 работ в международных рецензируемых журналах и 2 патента на изобретение. И.С. Сущев неоднократно проявлял себя во всероссийских конкурсах научных работ. В частности, в 2025 году И.С. Сущев занял первое место во Всероссийском конкурсе для молодых ученых от фонда «Система» и Российской Академии Наук в номинации «Искусственный интеллект и квантовые технологии».

Диссертационная работа И.С. Сущева посвящена вопросам безопасности систем квантового распределения ключей (КРК), или квантово-криптографическим системам. Такие системы призваны обеспечить безопасность обмена данными между пользователями путем передачи квантовых состояний света. Существующие на сегодняшний день протоколы КРК обладают доказанной криптографической стойкостью, однако практическая реализация систем, использующих такие протоколы, оказывается несовершенной. Нарушитель может воспользоваться данными несовершенствами для нарушения конфиденциальности передаваемых данных. В связи с этим остро встает вопрос практической безопасности реальных систем КРК с учетом всех возможных несовершенств технической реализации и сопряженных с ними атак, проводимых нарушителем. В работе И.С. Сущева рассматриваются вопросы практической защищенности волоконных квантово-криптографических систем в условиях проведения нарушителем атак наиболее общего вида – комбинированных атак, эксплуатирующих как технические аспекты реальной системы, так и особенности квантово-криптографического протокола. Результаты настоящей работы представляют значительный интерес как для разработчиков систем КРК, так и для специализированных организаций, проводящих сертификацию криптографических средств.

Первая глава посвящена литературному обзору вопроса безопасности систем КРК. В ней кратко описаны принципы работы систем КРК, сформулировано достаточное условие секретности ключей, выработанных в сеансе КРК, а также рассмотрены теоретические и экспериментальные подходу к учету несовершенств технической реализации при анализе безопасности систем КРК. Выделено несколько классов атак на системы КРК: среди атак

на квантовые состояния выделены унитарная атака и атаки на многофотонную компоненту; среди атак на техническую реализацию выделены атаки по побочным каналам, атаки навязывания и атаки с изменением параметров системы. Дано определение комбинированной атаки, и отмечены подходы, позволяющие проанализировать безопасность системы КРК в условиях проведения комбинированных атак общего вида.

Вторая глава посвящена исследованию безопасности систем КРК при наличии побочных каналов утечки информации. Рассмотрен наиболее общий случай считывания информации нарушителем из побочных каналов при их комбинировании с коллективной унитарной атакой. В работе теоретически доказано, что утечка информации при такой комбинированной атаке при заданной наблюдаемой частоте ошибок на приемной стороне ограничена величиной, зависящей лишь от интенсивности излучения – среднего числа фотонов – в побочном канале. Данное обстоятельство позволяет отказаться от используемых в прошлых работах модельных допущений, ограничивающих тип квантовых состояний, используемых нарушителем. Также в главе представлен экспериментальный способ измерения интенсивности в побочном канале, связанным с активным оптическим зондированием. И.С. Сущевым были разработаны экспериментальные установки для измерения спектров пропускания волоконных компонентов в пределах 1100–1800 нм с динамическим диапазоном до 120 дБ, а также оптический рефлектометр для измерения коэффициента отражения в этом же спектральном диапазоне с сантиметровым пространственным разрешением. С помощью данных установок была исследована реальная квантово-криптографическая система и проведен анализ ее устойчивости к атакам по побочным каналам.

Третья глава посвящена уязвимостям систем КРК, возникающим из-за не строгой «однофотонности» используемого излучения. В работе исследуется вопрос потенциальных рисков безопасности, связанных с несанкционированным увеличением интенсивности легитимного излучения, которое может быть спровоцировано нарушителем путем воздействия мощным лазерным излучением на оптические аттенюаторы, входящие в состав передатчика КРК. До сих пор считалось, что подобное вмешательство приводит к возможности проведения атаки с расщеплением по числу фотонов, которая на сегодняшний день остается умозрительной и недостижимой на практике в связи с необходимостью проведения неразрушающих измерений числа фотонов и использования долгосрочной квантовой памяти. При этом вопрос существования практически реализуемых атак оставался открытым. В работе И.С. Сущева ответ на этот вопрос был получен: как оказалось, система оказывается уязвимой к атакам с безошибочными измерениями при достижении некоторого уровня увеличения интенсивности излучения (10–20 дБ). Для реализации подобных измерений нарушителю требуется лишь экземпляр приемной станции КРК с пассивным выбором базиса. В работе впервые теоретически рассмотрены различные варианты проведения таких атак и получены количественные соотношения, позволяющие сделать вывод о практической безопасности систем КРК с учетом риска увеличения среднего числа фотонов.

Говоря о работе в целом, хочется отметить ее практическую значимость для области квантовой криптографии. Результаты диссертационной работы И.С. Сущева крайне важны для проектирования систем КРК с сохранением надлежащего уровня безопасности. Кроме

того, методы исследования потенциальных уязвимостей систем КРК, разработанные И.С. Сущевым, могут быть использованы при сертификации квантово-криптографических систем выработки и распределения ключей. Стоит отметить, что настоящая работа выполнялась в тесном сотрудничестве с специализированной лабораторией ООО «СФБ Лаб». В данной организации с участием И.С. Сущева проводились исследования системы КРК производства компании АО «ИнфоТеКС», в результате чего в 2022 году был получен первый в России сертификат регулятора для квантово-криптографической системы. Методы исследований систем КРК, предложенные И.С. Сущевым, сегодня используются при проведении сертификационных исследований в «СФБ Лаб».

Хочу также с удовольствием отметить личные качества Ивана Сергеевича, он очень воспитан, тактичен, интеллигентен, с ним приятно обсуждать различные научные сложные вопросы. Он полностью сложившийся научный высококвалифицированный сотрудник, который еще не раз порадует новыми и интересными научными результатами в достаточно сложной области квантовой информатики и квантовой криптографии.

Таким образом, рекомендую диссертационную работу «Исследование комбинированных атак на волоконные системы квантового распределения ключей» Сущева Ивана Сергеевича к защите на соискание ученой степени кандидата наук по специальности 1.3.19. Лазерная физика.

01.06.2026

Доктор физ.-мат. наук,
в.н.с. Центра квантовых технологий
физического факультета
МГУ имени М.В. Ломоносова — С.Н.Молотков

Подпись С.Н. Молоткова заверяю
Ученый секретарь Ученого совета
физического факультета
МГУ имени М.В. Ломоносова, проф — С.Ю. Стремоухов