НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
сентябрь–октябрь 2026 Том 26 № 5 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
September–October 2026 Vol. 26 No 5 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2026-26-5-900-908
УДК 535.3

Исследование влияния подходов к измерению спектральных характеристик волоконно-оптических элементов систем квантовой коммуникации на скорость генерации ключа

Олег Андреевич Соломатин[1]✉, Полина Алексеевна Морозова[2], Владимир Викторович Чистяков[3], Борис Александрович Наседкин[4]

[1,2,3,4] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] olegun.solom.2016@gmail.com✉, https://orcid.org/0009-0002-8676-5735
[2] Pamorozova@itmo.ru, https://orcid.org/0000-0003-3741-3506
[3] v_chistyakov@itmo.ru, https://orcid.org/0000-0002-2414-3490,
[4] banasedkin@itmo.ru, https://orcid.org/0000-0002-4507-8616

Аннотация

Введение. Предложен метод оценки вносимых спектрально-селективными элементами потерь, позволяющий повысить динамический диапазон измерений и дальнейший расчет характеристик работы системы квантового распределения ключей на непрерывных переменных. В отличие от распространенных методов, использующих источники суперконтинуума, предложенный метод дает возможность точнее оценить защищенность системы к атаке «Троянский конь». **Метод.** Сущность метода состоит в использовании перестраиваемого лазерного источника с добавлением дополнительной фильтрации в оптическую схему для измерения вносимых потерь. Выполнено сравнение результатов измерения потерь, полученных с помощью источника суперконтинуума и перестраиваемого лазерного источника. В случае использования перестраиваемого источника предлагается добавление дополнительной фильтрации в оптическую схему. **Основные результаты.** Показано, что максимальные потери, полученные с перестраиваемым источником, на 20 дБ больше максимальных потерь при работе с источником суперконтинуума. Эксперименты позволили установить, что применение перестраиваемого источника вместе с дополнительной фильтрацией позволяет повысить динамический диапазон измерения вносимых фильтром Coarse Wavelength Division Multiplexing потерь. **Обсуждение.** На примере атаки «Троянский конь» продемонстрировано, что дополнительная фильтрация в схеме с перестраиваемым источником позволяет получить более точные значения пропускания. Это, в свою очередь, влияет на формирование требований к установке мер противодействия, для достижения скорости генерации квантового ключа, максимально близкой к случаю в отсутствии атаки.

Ключевые слова

квантовое распределение ключей на непрерывных переменных, атака «Троянский конь», вносимые потери, перестраиваемый лазерный источник, источник суперконтинуума

Благодарности

Исследование выполнено за счет гранта Российского научного фонда № 24-11-00398.

Ссылка для цитирования: Соломатин О.А., Морозова П.А., Чистяков В.В., Наседкин Б.А. Исследование влияния подходов к измерению спектральных характеристик волоконно-оптических элементов систем квантовой коммуникации на скорость генерации ключа // Научно-технический вестник информационных технологий, механики и оптики. 2026. Т. 26, № 5. С. 900–908. doi: 10.17586/2226-1494-2026-26-5-900-908

© Соломатин О.А., Морозова П.А., Чистяков В.В., Наседкин Б.А., 2026

The influence of approaches for measuring the spectral characteristics of fiber-optic elements of quantum communication systems on the key generation rate

Oleg A. Solomatin[1]✉, Polina A. Morozova[2], Vladimir V. Chistyakov[3], Boris A. Nasedkin[4]

[1,2,3,4] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] olegun.solom.2016@gmail.com✉, https://orcid.org/0009-0002-8676-5735
[2] Pamorozova@itmo.ru, https://orcid.org/0000-0003-3741-3506
[3] v_chistyakov@itmo.ru, https://orcid.org/0000-0002-2414-3490,
[4] banasedkin@itmo.ru, https://orcid.org/0000-0002-4507-8616

Abstract

A method for estimating insertion losses introduced by spectrally selective elements is proposed, which enables an increase in the dynamic range of measurements and subsequent calculations of the performance characteristics for a Continuous Variable Quantum Key Distribution system. In contrast to common approaches that employ supercontinuum sources, the proposed method provides more accurate assessment of the system's resilience against the Trojanhorse attack. The essence of the method consists in using a tunable laser source with additional filtering incorporated into the optical setup for insertionloss measurements. The paper presents a comparative analysis of loss measurement results obtained with a supercontinuum source and a tunable laser source. For the tunable source, the addition of extra filtering in the optical scheme is proposed. It is demonstrated that the maximum loss values measured with the tunable source exceed those obtained with the supercontinuum source by 20 dB. The experiments reveal that employing the tunable source together with additional filtering enhances the dynamic range of insertionloss measurements for Coarse Wavelength Division Multiplexing filters. Using the Trojanhorse attack as a case study, it is shown that additional filtering in the tunablesource configuration yields more accurate transmittance values. This, in turn, affects the formulation of requirements for the implementation of countermeasures, aiming to maintain the quantum key generation rate as close as possible to the case without the attack.

Keywords

quantum key distribution on continuous variables, Trojan horse attack, insertion losses, tunable laser source, supercontinuum source

Acknowledgements

The research was supported by RSF (project No. 24-11-00398).

For citation: Solomatin O.A., Morozova P.A., Chistyakov V.V., Nasedkin B.A. The influence of approaches for measuring the spectral characteristics of fiber-optic elements of quantum communication systems on the key generation rate. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2026, vol. 26, no. 5, pp. 900–908 (in Russian). doi: 10.17586/2226-1494-2026-26-5-900-908

Введение

В настоящее время все большее развитие получают системы квантового распределения ключей (КРК) [1, 2]. КРК — технология, позволяющая двум удаленным пользователям обмениваться зашифрованными данными с высокой степенью защищенности, и, которая обусловлена принципами квантовой механики. В данном контексте важными являются также исследования способов воздействия на системы КРК со стороны потенциального нарушителя, которого принято называть «Евой» [3] или атакой. Целью таких атак является извлечение передаваемой информации за счет недостатков защиты, в том числе в техническом исполнении исследуемых систем. Отметим, что важной задачей для нарушителя является остаться незаметным для легитимных пользователей. В результате исследование таких уязвимостей и поиск мер противодействия позволяет ограничить возможности нарушителя и тем самым повысить защищенность исследуемых систем.

Существует большое число различных атак на техническую реализацию систем КРК. Одним из типов атак на системы КРК являются атаки, при которых осуществляется воздействие лазерным излучением [4, 5]. В этом случае целью злоумышленника может быть повреждение элементов оптической схемы, например, повреждение аттенюаторов [6] или получение закодированной информации [7]. Одним из способов, с помощью которого можно осуществлять получение передаваемой информации, является зондирование элементов, осуществляющих кодирование квантовых состояний. Примером подобной атаки, при которой происходит попытка перехвата данных путем зондирования, является атака «Троянский конь» [8]. Реализация этой атаки подразумевает прохождение зондирующих импульсов, отправленных нарушителем, через элементы оптической схемы отправителя или получателя до кодирующего устройства с целью перехвата ключа через побочный канал утечки. При этом излучение проходит через набор оптических компонентов, каждый из которых вносит свои потери, вследствие чего мощность излучения уменьшается. В области спектрально-зависимых атак на системы КРК наибольшую проработку получила атака «Троянский конь»: для нее созданы детальные методики измерения потерь, модели утечки информации и расчета влияния на скорость генерации ключа, что позволяет обоснованно формировать требования к защитным мерам. В отличие от этого, для других типов спектральных атак (например, на Wavelength Division Multiplexing (WDM) фильтры, изоляторы или детекторы) подход, как правило, ограничивается использованием фиксированных пороговых

значений затухания, взятых из паспортных данных или консервативных допущений, без оценки количества информации, доступной нарушителю.

Важным параметром в контексте проведения атаки «Троянский конь» для эффективной реализации является используемая длина волны, которая выбирается нарушителем, на основании характеристик оптической схемы, поскольку принято исходить из предположения, что нарушителю известны характеристики схемы.

Так, в работах, посвященных исследованию данной атаки, рассматривается использование нарушителем лазерных импульсов на длинах волн, находящихся как в телекоммуникационном диапазоне (1250–1650 нм) [9–11], так и за его пределами [10, 12–15]. Для противодействия данной атаке в блоки отправителя и получателя устанавливаются дополнительные оптические элементы с целью ослабления мощности зондирующих импульсов нарушителя при прямом и обратном проходах. К таким элементам относятся изоляторы, циркуляторы, аттенюаторы, обладающие коэффициентом пропускания, значение которого может зависеть от величины длины волны излучения. Величину, на которую уменьшилась мощность излучения после прохождения через элемент, будем называть вносимыми этим элементом потерями. Помимо перечисленных компонентов, в качестве меры противодействия атакам, которая отсекает неиспользуемые легитимными пользователями длины волн, также могут применяться спектрально-селективные элементы на основе тонких пленок [16, 17], которые также называются мультиплексорами или фильтрами Coarse Wavelength Division Multiplexing (CWDM). Такие мультиплексоры могут использоваться в системах КРК для объединения квантового канала и канала синхронизации в одну линию [18, 19].

Предмет исследования

При исследовании атаки «Троянский конь», исходя из рассчитываемого минимального уровня мощности сигнала, который может зарегистрировать нарушитель, выдвигаются требования к уровню вносимых оптическими элементами потерь. Для этого принято считать суммарные потери на этих элементах при прямом и обратном распространении зондирующего излучения. Определение потерь требует высокого уровня точности измерений для избежания возможности утечки данных. В последних работах, затрагивающих расчет потерь в системах КРК, наблюдается тренд на увеличение точности измерений и отход от консервативных методов, подразумевающих суммирование потерь, вносимых компонентами оптической схемы [18, 19], к методам измерения фактических потерь. В вариантах схем блоков КРК, где присутствуют спектральные мультиплексоры, при подсчете потерь важным является выбор источника: источника суперконтинуума или перестраиваемого лазерного источника. В том числе, важной задачей является повышение динамического диапазона измерений пропускания элементов схемы для более точной оценки степени защищенности системы от атак зондирующим излучением.

В настоящей работе исследуется величина вносимых CWDM-фильтрами потерь в зависимости от используемых источников и наличия дополнительной фильтрации, а также влияние используемого подхода оценки вносимых потерь при расчете скорости генерации квантового ключа в системе КРК на непрерывных переменных [20, 21] с учетом атаки «Троянский конь».

Экспериментальная схема

Для проведения измерений с целью измерения вносимых CWDM-фильтром потерь с помощью перестраиваемого лазерного источника была собрана схема, показанная на рис. 1, *a*.

Непрерывное излучение, генерируемое источником излучения (ИИ) HP 8168F, с шириной спектральной линии порядка 100 кГц и диапазоном перестройки 1450–1590 нм, направлялось на амплитудный модулятор (АМ) Covega Mach-10056. К модулятору подключались источник напряжения (ИН) и генератор импульсов (ГИ) с частотой модуляции 1 МГц и скважностью 2 %. В результате на выходе из модулятора получались оптические импульсы с частотой следования 1 МГц и длительностью порядка 20 нс. Далее в схеме устанавливалась система из пары светоделителей (СД), необходимых для мониторинга и дополнительного ослабления сигнала. После первого светоделителя 90/10 большая часть излучения направлялась на фотодиод (ФД) Avesta OD-007BFC, подключенный к осциллографу (ОСЦ) Rohde&Schwarz RTM3004, для контроля импульсной формы оптического сигнала. После второго светоделителя 50/50 половина оставшейся мощности регистрировалась измерителем мощности (ИМ) Grandway FHP 2A04 для дальнейшей оценки среднего числа фотонов в импульсах. Другая часть излучения проходила через блок ослабления сигнала, состоящий из двух аттенюаторов: фиксированного (АТТ) и перестраиваемого (ПАТТ) (Grandway FHA2S02). Сигнал с уменьшенной до необходимого уровня мощностью поступал на тестируемый элемент (ТЭ), после чего регистрировался на детекторе одиночных фотонов (ДОФ) Scontel TCOSPS-CCR-14, который подключался к усилителю сигнала (АМР). Усилитель сигнала в свою очередь присоединялся к частотомеру (ЧМ) Rohde&Schwarz HM8123.

В случае измерения вносимых потерь с помощью широкополосного излучения использовалась схема (рис. 1, *b*). В ней задействован подключенный к блоку управления (БУ) источник суперконтинуума (СК) EFOA-UB Avesta с рабочим диапазоном 1100–2000 нм и интегральной мощностью около 150 мВт. Излучение проходило через изолятор (ИЗО) и тестируемый элемент (ТЭ), после чего регистрировалось на оптическом спектроанализаторе (СА) VIAVI OSA-500 (JDSU) с рабочим диапазоном 1250–1650 нм.

Пропускание тонкопленочного CWDM-фильтра

В качестве исследуемого образца был рассмотрен волоконный CWDM-фильтр с центральной длиной волны пропускания (λ) 1550 нм и шириной на полувысоте

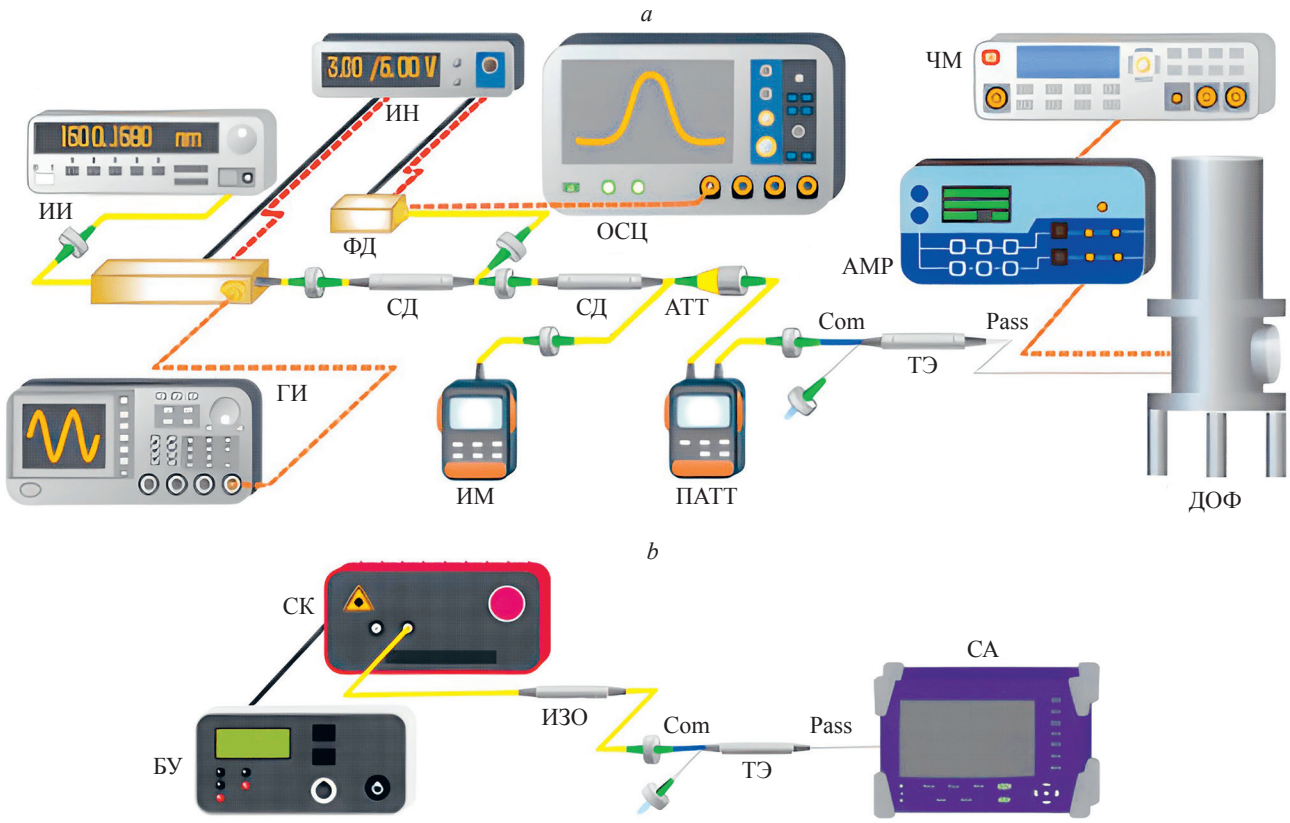

Рис. 1. Схемы экспериментальных установок измерения потерь исследуемых элементов с помощью: перестраиваемого источника (*a*) и источника суперконтинуума (*b*).

Соединения постоянного тока (черные и красные пунктирные линии); оптоволоконные соединения (желтые сплошные линии); волоконные порты тестируемого элемента (голубые и серые линии); соединения при помощи коаксиальных кабелей (оранжевые пунктирные линии)

Fig. 1. Schematic diagram of the experimental setup for measuring the losses of the elements under study using: a tunable source (*a*); a supercontinuum source (*b*).

DC connections (black and red dashed lines); fiber-optic connections (solid yellow lines); fiber ports of the device under test (light blue and gray lines); coaxial cable connections (orange dashed lines)

20 нм. Были измерены значения отсчетов ДОФ после прохождения исследуемого CWDM-фильтра в зависимости от длины волны. Измерения были проведены при помощи установки (рис. 1, *a*), в диапазоне 1500–1590 нм с шагом в 1 нм. Для рассматриваемого компонента были исследованы потери при прохождении излучения в прямом навправлении через порты «Com» и «Pass» и обратном направлении через порты «Pass» и «Com», согласно наименованиям портов из паспорта оптического компонента. Полученные результаты свидетельствуют о том, что потери при прохождении излучения в прямом и обратном направлениях практически равны. Основные различия связаны в первую очередь с потерями на оптических соединениях.

Для выбранного CWDM-фильтра было также исследовано пропускание с помощью источника суперконтинуума. В этом случае излучение, прошедшее через исследуемый элемент, регистрировалось на оптическом анализаторе спектра. Измеренные с помощью схемы (рис. 1, *b*) с источником суперконтинуума и оптическим спектроанализатором потери A приведены на графике (рис. 2, кривая *2*) вместе с полученным ранее спектром CWDM-фильтра (кривая *1*).

Полученный с помощью схемы (рис. 1, *b*) с источником суперконтинуума и оптическим спектроанализатором результат приведен на графике (рис. 2, кривая *2*) вместе с полученным ранее спектром CWDM-фильтра (кривая *1*). При сравнении видно, что на некоторых участках спектра потери фильтра, полученные с помощью источника суперконтинуума превышают потери, полученные с помощью перестраиваемого источника, на величину, достигающую 20 дБ, за пределами окна пропускания фильтра. Такие результаты могут быть обусловлены выбранным подходом к измерениям. В случае с перестраиваемым лазером использование детектора одиночных фотонов для регистрации сигнала позволяет проводить измерения в более широком динамическом диапазоне [22]. Однако, в отличие от подобного «идеального» случая, в экспериментально полученных данных заметно влияние фотонов используемого лазерного источника, значительно отстоящих от центральной частоты. Для проверки данного предположения в настоящей работе предлагается использование дополнительной фильтрации как способа для повышения динамического диапазона измерения вносимых потерь оптических элементов для случая использова-

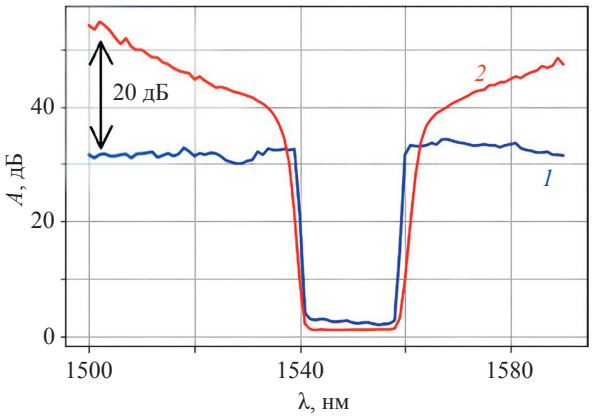

Рис. 2. Измеренные вносимые потери исследуемого CWDM-фильтра при помощи перестраиваемого лазерного источника (кривая *1*) и источника суперконтинуума (кривая *2*).

Интервал 20 дБ показывает примерную разницу, которая достигается между результатами, полученными с разными источниками

Fig. 2. Comparison of CWDM filter insertion losses: *1* is measured with tunable source; *2* is measured with supercontinuum source.

The 20 dB interval indicates the approximate difference achieved between results obtained with different sources

ния перестраиваемого лазерного источника. Для этого в оптическую схему был добавлен многоканальный CWDM-фильтр. Измеренные потери этого фильтра приведены на рис. 3.

Далее были проведены измерения с дополнительной фильтрацией. На рис. 4 представлено сравнение спектров пропускания исследуемого фильтра без фильтрации и при наличии дополнительной фильтрации.

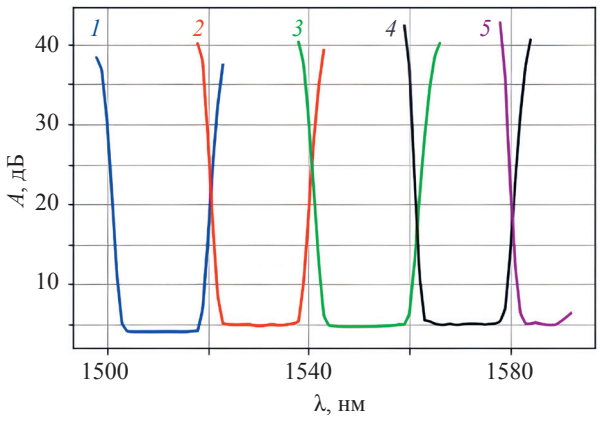

Рис. 3. Оптические потери, вносимые многоканальным CWDM-фильтром, использующимся для дополнительной фильтрации.

Спектры пропускания канала для длин волн: 1510 нм (кривая *1*); 1530 нм (кривая *2*); 1550 нм (кривая *3*); 1570 нм (кривая *4*); 1590 нм (кривая *5*)

Fig. 3. Insertion losses of multichannel CWDM filter used as an additional filtration.

1 is losses of 1510 nm channel; *2* is losses of 1530 nm channel; *3* is losses of 1550 nm channel; *4* is losses of 1570 nm channel; *5* is losses of 1590 nm channel

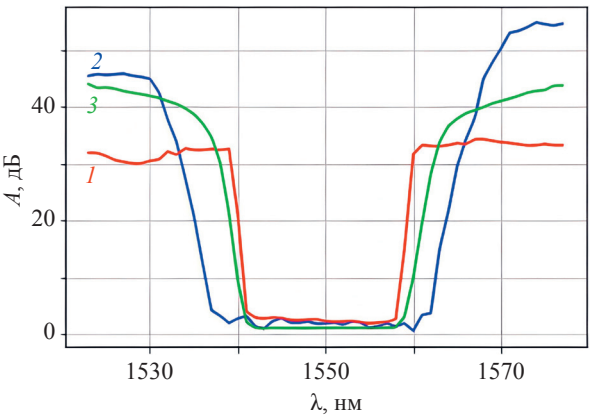

Рис. 4. Измеренные вносимые потери CWDM-фильтра: без (кривая *1*) и с (кривая *2*) дополнительной фильтрацией; с использованием источника суперконтинуума (кривая *3*)

Fig. 4. CWDM filter insertion losses: *1* is measured with no additional filtering; *2* is measured with additional filtering; *3* is measured with supercontinuum source

Полученные результаты демонстрируют что, дополнительная фильтрация приводит к уточнению результатов измерений и позволяет достичь более высокого динамического диапазона по сравнению со случаем с использованием источника суперконтинуума и спектроанализатора. Отметим, что теоретически, используемая для измерений схема позволяет проводить исследования в динамическом диапазоне порядка 100 дБ, но фактически наблюдается ограничение на уровне 30 дБ. Это связано с тем, что пропускание исследуемого фильтра быстро убывает с изменением длины волны. В результате основной вклад в измеренные данные вносят фотоны источника излучения, значительно отстоящие от центральной длины волны. Внесение дополнительных потерь для таких фотонов снижает их вклад, таким образом увеличивая соотношение сигнал-шум для используемого источника. Наиболее значимым соотношение сигнал-шум становится при существенном изменении вносимых потерь с длиной волны, когда в пределах пропускания используемого дополнительного фильтра изменение достигает величины большей, по сравнению с соотношением сигнал-шум используемого источника, что фиксируется в виде выхода на «плато» (рис. 4) измеряемого сигнала.

Сделаем вывод на основании полученных результатов, что использование измерений в отсутствии фильтрации может приводить к более консервативным оценкам вносимых потерь, что, в свою очередь, потребует увеличения числа оптических компонентов используемых в схеме КРК в качестве исправления результата.

Оценка скорости генерации ключа для системы КРК на непрерывных переменных

Пропускание элементов, используемых в системах КРК, при учете возможности реализации атаки «Троянский конь», учитывается как для систем на дискретных переменных [15], так и для систем КРК на непрерывных переменных [23–25]. Рассмотрим в качестве примера влияние пропускания элементов на

скорость генерации для реализации системы КРК на непрерывных переменных.

Для определения зависимости параметров работы системы КРК от вносимых в канал потерь выполним расчет параметра скорости генерации ключа. Оценка влияния подхода к определению пропускания спектрально-селективных элементов на скорость генерации ключа, производилась для оптической схемы КРК непрерывных переменных [25]. Для такой схемы оценка скорости генерации (K) выполнялась следующим способом [16]:

$$K \geq r(1 - FER)(1 - \nu)(\beta I_{AB} - \chi),$$

где r — частота следования импульсов; FER (Frame Error Rate) — частота появления ошибок в информационном кадре; ν — доля импульсов, отбрасываемая для работы алгоритмов компенсации и для оценки параметров; β — эффективность процедуры согласования; I_{AB} — взаимная информация между отправителем (A) и получателем (B); χ — граница Холево.

Параметры моделируемой системы КРК непрерывных переменных следующие: r = 25 МГц; β = 0,97; FER = 0,9; ν = 0,5.

На рис. 5 представлен результат расчета скорости генерации ключа (K) в зависимости от вносимых в канале потерь ζL. Согласно полученной оценке для рассматриваемой схемы без учета влияния атаки «Троянский конь» распределение ключа возможно на расстояние, соответствующее вносимым потерям в канале порядка 10 дБ.

Зависимость от вносимых потерь оптических компонентов, используемых в схеме отправителя для КРК непрерывных переменных, можно учесть при оценке границы Холево [16], поскольку в случае атаки «Троянский конь», среднее число фотонов будет зависеть от пропускания волоконно-оптической схемы при двойном прохождении зондирующих импульсов нарушителя. Среднее число фотонов (μ), которое попадет в квантовый канал, можно оценить следующим образом:

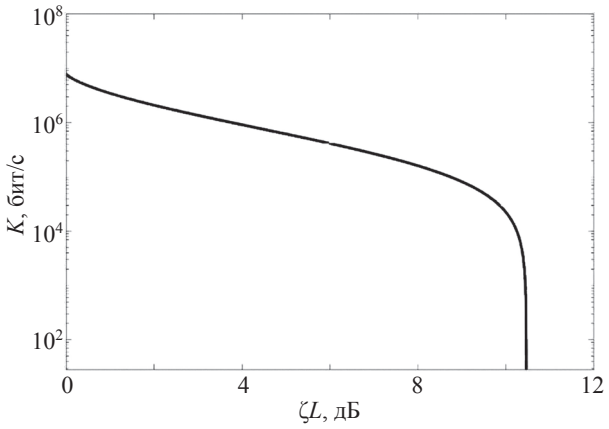

Рис. 5. Зависимость скорости генерации секретного ключа от вносимых в канале потерь

Fig. 5. Dependence of secret key rate generation on the channel losses

$$\mu = \frac{10^{-A/10} cP}{Fh\lambda},$$

где c — скорость света; P — максимально-возможная мощность зондирующего излучения нарушителя на входе в блок получателя; A — оптические потери в блоке получателя при прямом и обратном прохождениях зондирующего излучения нарушителя; F — частота следования импульсов нарушителя; h — постоянная Планка; λ — длина волны зондирующего излучения нарушителя.

Для оценки среднего числа фотонов, доступного нарушителю при реализации атаки «Троянский конь», использовались следующие значения: F = 25 МГц; P = 10 Вт [6]; λ = 1550 нм. Взаимную информацию между отправителем и нарушителем можно оценить при помощи следующей упрощенной формулы:

$$I_{AE} = \log_2(1 - 2\mu).$$

Границу Холево можно оценить согласно формуле, представленной в работе [23]:

$$\hat{\chi} = \chi + 2(1 - \chi)I_{AE}.$$

В результате была проведена оценка (рис. 6) минимального требуемого пропускания исследуемой оптической схемы отправителя для двойного прохождения зондирующих импульсов нарушителя, при котором генерация ключа становится невозможной для различного уровня вносимых потерь в канале.

Из полученной зависимости (рис. 6) видно, что минимальные вносимые потери в блоке отправителя, при которых возможно распределение ключа составляют 121 дБ для величины потерь в канале порядка 1,5 дБ и увеличиваются с ростом потерь в канале, вплоть до 154 дБ для потерь 10 дБ. При этом различие данных требований для диапазона длин волн 1500–1590 нм не превышало десятых долей децибелов. Поскольку при оценке пропускания системы также принято учитывать величину отражения, то требование к пропусканию волоконно-оптических элементов, используемых в схеме, можно оценить меньшей величиной. Для этого воз-

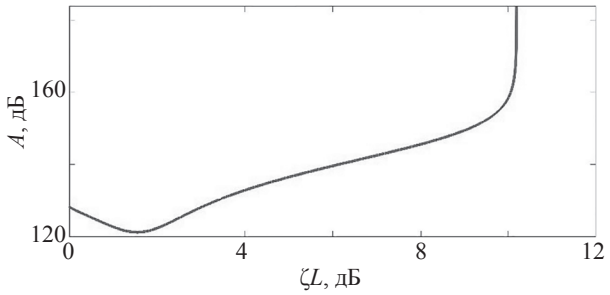

Рис. 6. Зависимость требуемого уровня вносимых потерь схемы получателя при прохождении через нее импульсов нарушителя на выходе из системы квантового распределения ключей от потерь в канале

Fig. 6. Dependence of the required total transmission of the receiver module under propagation of the eavesdropper's probe pulses on the channel loss

можно воспользоваться средним значением отражения для волоконно-оптических элементов из работы [22], которое составило порядка –63 дБ. В таком случае минимальное значение вносимых потерь равно 58 дБ, а максимальное — 91 дБ. Таким образом, в зависимости от выбранного подхода к измерениям может потребоваться различное число CWDM-фильтров, чтобы ослабить излучение вне окна пропускания фильтров. В случае использования перестраиваемого источника без дополнительной фильтрации потребуется не менее двух фильтров. Отметим, что если применить для оценки измерения, полученные с использованием суперконтинуума, или измерения, полученные для перестраиваемого лазерного источника с дополнительной фильтрацией, для выполнения требований, приводящих к наибольшей дальности распределения ключа, потребуется один фильтр.

Обсуждение

В результате проведенных измерений получены спектры пропускания CWDM-фильтра. При исследовании пропускания фильтра в качестве источника излучения использовались перестраиваемый источник и источник суперконтинуума. Согласно данным, представленным на рис. 3 видно, что по краям исследуемого спектрального диапазона наибольшие потери зарегистрированы при использовании источника суперконтинуума. Разница на некоторых участках спектра достигает 20 дБ. Таким образом измерения при помощи суперконтинуума приводят к менее консервативной оценке пропускания исследуемого элемента. Вместе с тем схемы, использующие источники суперконтинуума без дополнительной фильтрации, имеют ограничения, связанные с интегральной мощностью. Высокая интегральная мощность таких источников может приводить к нагреву исследуемого элемента и, как следствие, к изменению его спектральных характеристик. Другое ограничение, связанное с интегральной мощностью источника, накладывается измерительным оборудованием, что вызывает ограничение динамического диапазона измерений, поскольку корректная работа схем в таком случае требует ослабления излучения суперконтинуума до приемлемого уровня мощности. При этом в таких схемах также требуется дополнительная фильтрация, для исключения вклада от кратных гармоник излучения [19].

Более широкий динамический диапазон измерений достигается при использовании перестраиваемых источников, использующих дополнительную фильтрацию [22]. В настоящей работе используемый перестраиваемый лазерный источник можно рассматривать как источник после фильтрации с соотношением сигнал-шум порядка 20 дБ. Использование дополнительной фильтрации приводит к увеличению соотношения до величины порядка 30 дБ. При этом наблюдается расширение динамического диапазона измерений, таким образом получается оценка пропускания рассматриваемого CWDM-фильтра более близкая к реальным характеристикам фильтра. Предполагается, что дальнейшее увеличение соотношения сигнал-шум для используемого источника приведет к более точным измерениям в рассматриваемом динамическом диапазоне.

Заключение

Консервативная оценка пропускания исследуемого фильтра может повлиять на число элементов, используемых в качестве мер противодействия, для достижения скорости генерации квантового ключа, максимально близкой к случаю в отсутствии атаки. В работе рассмотрено влияние вносимых потерь на скорость генерации системы квантового распределения ключей на непрерывных переменных. Установка мер противодействия атаке «Троянский конь» в систему требует достижения минимально-требуемого уровня вносимых потерь атакуемой системы, при прохождении зондирующих импульсов нарушителя в двух направлениях (прямом и обратном). Продемонстрировано, что в таком случае для достижения максимальной дальности распределения ключа, близкой к случаю отсутствия влияния атаки требуется не менее 91 дБ вносимых потерь. В случае использования консервативной оценки потребуется не менее двух CWDM-фильтров, рассмотренных в работе, а в случае оценки пропускания, полученной для источника с дополнительной фильтрацией достаточно одного элемента. Таким образом продемонстрировано, что дополнительная фильтрация для схемы с перестраиваемым источником позволяет получить более точные значения пропускания, что в свою очередь влияет на формирование требований к установке мер противодействия атаке «Троянский конь».

Литература

1. Pan D., Long G.-L., Yin L, Sheng Y.-B., Ruan D., Ng S.X., et al. The evolution of quantum secure direct communication: On the road to the qinternet // IEEE Communications Surveys & Tutorials. 2024. V. 26. N 3. P. 1898–1949. doi: 10.1109/comst.2024.3367535
2. Tian X.-H., Yang R., Liu H.-Y., Fan P., Zhang J.-N., Gu C., et al. Experimental demonstration of drone-based quantum key distribution // Physical Review Letters. 2024. V. 133. N 20. P. 200801. doi: 10.1103/PhysRevLett.133.200801
3. Lee C., Sohn I., Lee W. Eavesdropping detection in BB84 quantum key distribution protocols // IEEE Transactions on Network and Service Management. 2022. V. 19. N 3. P. 2689–2701. doi: 10.1109/tnsm.2022.3165202

References

1. Pan D., Long G.-L., Yin L, Sheng Y.-B., Ruan D., Ng S.X., et al. The evolution of quantum secure direct communication: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 2024, vol. 26, no. 3, pp. 1898–1949. doi: 10.1109/comst.2024.3367535
2. Tian X.-H., Yang R., Liu H.-Y., Fan P., Zhang J.-N., Gu C., et al. Experimental demonstration of drone-based quantum key distribution. *Physical Review Letters*, 2024, vol. 133, no. 20, pp. 200801. doi: 10.1103/PhysRevLett.133.200801
3. Lee C., Sohn I., Lee W. Eavesdropping detection in BB84 quantum key distribution protocols. *IEEE Transactions on Network and Service Management*, 2022, vol. 19, no. 3, pp. 2689–2701. doi: 10.1109/tnsm.2022.3165202

4. Sun S.-H., Xu F., Jiang M.-S., Ma X.-C., Lo H.-K., Liang L.-M. Effect of source tampering in the security of quantum cryptography // Physical Review A. 2015. V. 92. N 2. P. 022304. doi: 10.1103/physreva.92.022304
5. Makarov V., Bourgoin J.-P., Chaiwongkhot P., Gagné M., Jennewein T., Kaiser S., et al. Creation of backdoors in quantum communications via laser damage // Physical Review A. 2016. V. 94. N 3. P. 030302. doi: 10.1103/physreva.94.030302
6. Huang A., Li R., Egorov V., Tchouragoulov S., Kumar K., Makarov V. Laser-damage attack against optical attenuators in quantum key distribution // Physical Review Applied. 2020. V. 13. N 3. P. 034017. doi: 10.1103/physrevapplied.13.034017
7. Koehler-Sidki A., Dynes J.F., Paraïso T.K., Lucamarini M., Sharpe A.W., Yuan Z.L., et al. Backflashes from fast-gated avalanche photodiodes in quantum key distribution // Applied Physics Letters. 2020. V. 116. N 15. P. 154001. doi: 10.1063/1.5140548
8. Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G. Trojan-horse attacks on quantum-key-distribution systems // Physical Review A. 2006. V. 73. P. 022320. doi: 10.1103/physreva.73.022320
9. Jain N., Stiller B., Khan I., Makarov V., Marquardt C., Leuchs G. Risk analysis of trojan-horse attacks on practical quantum key distribution systems // IEEE Journal of Selected Topics in Quantum Electronics. 2015. V. 21. N 3. P. 6600710. doi: 10.1109/jstqe.2014.2365585
10. Sajeed S., Minshull C., Jain N., Makarov V. Invisible trojan-horse attack // Scientific Reports. 2017. V. 7. N 1. P. 8403. doi: 10.1038/s41598-017-08279-1
11. Bondar K.D., Sushchev I.S., Bulavkin D.S., Bugai K.E., Sidelnikova A.S., Melkonian D.M., et al. Broadband optical time-domain reflectometry for security analysis of quantum key distribution // Physical Review Applied. 2025. V. 24. N 1. P. 014010. doi: 10.1103/368v-t34p
12. Tan H., Petrov M., Zhang W., Han L., Liao S.-K., Makarov V., et al. Wide-spectrum security of quantum key distribution // PRX Quantum. 2025. V. 6. N 4. P. 040331. doi: 10.1103/smdh-dcpm
13. Nasedkin B.A., Filipov I.M., Ismagilov A.O., Chistiakov V.V., Kiselev F.D., Tsypkin A.N., et al. Analyzing transmission spectra of fiber-optic elements in the near IR range to improve the security of quantum key distribution systems // Bulletin of the Russian Academy of Sciences: Physics. 2022. V. 86. N 10. P. 1164–1167. doi: 10.3103/s1062873822100148
14. Nasedkin B., Ismagilov A., Chistiakov V., Gaidash A., Shimko A., Kiselev A.D., et al. Vulnerabilities of quantum key distribution systems in the visible range // Journal of the Optical Society of America B. 2026. V. 43. N 3. P. 416–425. doi: 10.1364/josab.585882
15. Nasedkin B., Kiselev F., Filipov I., Tolochko D., Ismagilov A., Chistiakov V., et al. Loopholes in the 1500–2100-nm range for quantum-key-distribution components: Prospects for Trojan-horse attacks // Physical Review Applied. 2023. V. 20. N 1. P. 014038. doi: 10.1103/physrevapplied.20.014038
16. Laudenbach F., Pacher C., Fung C.-H. F., Poppe A., Peev M., Schrenk B., et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations // Advanced Quantum Technologies. 2018. V. 1. N 1. P. 1800011. doi: 10.1002/qute.201800011
17. Wang T., Huang P., Li L., Zhou Y., Zeng G. High key rate continuous-variable quantum key distribution using telecom optical components // New Journal of Physics. 2024. V. 26. N 2. P. 023002. doi: 10.1088/1367-2630/ad1b7e
18. Борисова А.В., Гармаев Б.Д., Бобров И.Б., Негодяев С.С., Синильщиков И.В. Анализ эффективности методов защиты от атак активного оптического зондирования на волоконные системы квантового распределения ключей в спектральном диапазоне 1260−1650 nm // Оптика и спектроскопия. 2020. Т. 128. № 11. С. 1758–1766. doi: 10.21883/OS.2020.11.50182.4-20
19. Makarov V., Abrikosov A., Chaiwongkhot P., Fedorov A.K., Huang A., Kiktenko E., et al. Preparing a commercial quantum key distribution system for certification against implementation loopholes // Physical Review Applied. 2024. V. 22. N 4. P. 044076. doi: 10.1103/PhysRevApplied.22.044076
20. Zhang Y., Bian Y., Li Z., Yu S., Guo H. Continuous-variable quantum key distribution system: Past, present, and future // Applied Physics Reviews. 2024. V. 11. N 1. P. 011318. doi: 10.1063/5.0179566
21. Hajomer A.A.E., Derkach I., Jain N., Chin H.-M., Andersen U.L., Gehring T. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator // Science Advances. 2024. V. 10. N 1. P. eadi9474. doi: 10.1126/sciadv.adi9474

4. Sun S.-H., Xu F., Jiang M.-S., Ma X.-C., Lo H.-K., Liang L.-M. Effect of source tampering in the security of quantum cryptography. *Physical Review A*, 2015, vol. 92, no. 2, pp. 022304. doi: 10.1103/physreva.92.022304
5. Makarov V., Bourgoin J.-P., Chaiwongkhot P., Gagné M., Jennewein T., Kaiser S., et al. Creation of backdoors in quantum communications via laser damage. *Physical Review A*, 2016, vol. 94, no. 3, pp. 030302. doi: 10.1103/physreva.94.030302
6. Huang A., Li R., Egorov V., Tchouragoulov S., Kumar K., Makarov V. Laser-damage attack against optical attenuators in quantum key distribution. *Physical Review Applied*, 2020, vol. 13, no. 3, pp. 034017. doi: 10.1103/physrevapplied.13.034017
7. Koehler-Sidki A., Dynes J.F., Paraïso T.K., Lucamarini M., Sharpe A.W., Yuan Z.L., et al. Backflashes from fast-gated avalanche photodiodes in quantum key distribution. *Applied Physics Letters*, 2020, vol. 116, no. 15, pp. 154001. doi: 10.1063/1.5140548
8. Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 2006, vol. 73, pp. 022320. doi: 10.1103/physreva.73.022320
9. Jain N., Stiller B., Khan I., Makarov V., Marquardt C., Leuchs G. Risk analysis of trojan-horse attacks on practical quantum key distribution systems. *IEEE Journal of Selected Topics in Quantum Electronics*, 2015, vol. 21, no. 3, pp. 6600710. doi: 10.1109/jstqe.2014.2365585
10. Sajeed S., Minshull C., Jain N., Makarov V. Invisible trojan-horse attack. *Scientific Reports*, 2017, vol. 7, no. 1, pp. 8403. doi: 10.1038/s41598-017-08279-1
11. Bondar K.D., Sushchev I.S., Bulavkin D.S., Bugai K.E., Sidelnikova A.S., Melkonian D.M., et al. Broadband optical time-domain reflectometry for security analysis of quantum key distribution. *Physical Review Applied*, 2025, vol. 24, no. 1, pp. 014010. doi: 10.1103/368v-t34p
12. Tan H., Petrov M., Zhang W., Han L., Liao S.-K., Makarov V., et al. Wide-spectrum security of quantum key distribution. *PRX Quantum*, 2025, vol. 6, no. 4, pp. 040331. doi: 10.1103/smdh-dcpm
13. Nasedkin B.A., Filipov I.M., Ismagilov A.O., Chistiakov V.V., Kiselev F.D., Tsypkin A.N., et al. Analyzing transmission spectra of fiber-optic elements in the near IR range to improve the security of quantum key distribution systems. *Bulletin of the Russian Academy of Sciences: Physics*, 2022, vol. 86, no. 10, pp. 1164–1167. doi: 10.3103/s1062873822100148
14. Nasedkin B., Ismagilov A., Chistiakov V., Gaidash A., Shimko A., Kiselev A.D., et al. Vulnerabilities of quantum key distribution systems in the visible range. *Journal of the Optical Society of America B*, 2026, vol. 43, no. 3, pp. 416–425. doi: 10.1364/josab.585882
15. Nasedkin B., Kiselev F., Filipov I., Tolochko D., Ismagilov A., Chistiakov V., et al. Loopholes in the 1500–2100-nm range for quantum-key-distribution components: Prospects for Trojan-horse attacks. *Physical Review Applied*, 2023, vol. 20, no. 1, pp. 014038. doi: 10.1103/physrevapplied.20.014038
16. Laudenbach F., Pacher C., Fung C.-H. F., Poppe A., Peev M., Schrenk B., et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 2018, vol. 1, no. 1, pp. 1800011. doi: 10.1002/qute.201800011
17. Wang T., Huang P., Li L., Zhou Y., Zeng G. High key rate continuous-variable quantum key distribution using telecom optical components. *New Journal of Physics*, 2024, vol. 26, no. 2, pp. 023002. doi: 10.1088/1367-2630/ad1b7e
18. Borisova A.V., Garmaev B.D., Bobrov I.B., Negodyaev S.S., Sinil'shchikov I. Risk analysis of countermeasures against the Trojan-Horse attacks on quantum key distribution systems in 1260–1650 nm spectral range. *Optics and Spectroscopy*, 2020, vol. 128, no. 11, pp. 1892–1900. doi: 10.1134/s0030400x20110077
19. Makarov V., Abrikosov A., Chaiwongkhot P., Fedorov A.K., Huang A., Kiktenko E., et al. Preparing a commercial quantum key distribution system for certification against implementation loopholes. *Physical Review Applied*, 2024, vol. 22, no. 4, pp. 044076. doi: 10.1103/PhysRevApplied.22.044076
20. Zhang Y., Bian Y., Li Z., Yu S., Guo H. Continuous-variable quantum key distribution system: Past, present, and future. *Applied Physics Reviews*, 2024, vol. 11, no. 1, pp. 011318. doi: 10.1063/5.0179566
21. Hajomer A.A.E., Derkach I., Jain N., Chin H.-M., Andersen U.L., Gehring T. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator. *Science Advances*, 2024, vol. 10, no. 1, pp. eadi9474. doi: 10.1126/sciadv.adi9474

22. Sushchev I.S., Bulavkin D.S., Bugai K.E., Sidelnikova A.S., Dvoretskiy D.A. Trojan-horse attack on a real-world quantum key distribution system: Theoretical and experimental security analysis // Physical Review Applied. 2024. V. 22. N 3. P. 034032. doi: 10.1103/physrevapplied.22.034032
23. Vorontsova I., Goncharov R., Filipov I., Chistiakov V., Nasedkin B., Trifonov P., et al. Composable security analysis of an experimental continuous-variable quantum key distribution system operating with polar codes // Journal of the Optical Society of America B. 2025. V. 42. N 12. P. 2883–2892. doi: 10.1364/josab.573606
24. Pan Y., Zhang L., Huang D. Practical security bounds against trojan horse attacks in continuous-variable quantum key distribution // Applied Sciences. 2020. V. 10. N 21. P. 7788. doi: 10.3390/app10217788
25. Goncharov R.K., Kiselev A.D., Samsonov E.O., Egorov V.I. Continuous-variable quantum key distribution: security analysis with trusted hardware noise against general attacks // Nanosystems: Physics, Chemistry, Mathematics. 2022. V. 13. N 4. P. 372–391. doi: 10.17586/2220-8054-2022-13-4-372-391

22. Sushchev I.S., Bulavkin D.S., Bugai K.E., Sidelnikova A.S., Dvoretskiy D.A. Trojan-horse attack on a real-world quantum key distribution system: Theoretical and experimental security analysis. *Physical Review Applied*, 2024, vol. 22, no. 3, pp. 034032. doi: 10.1103/physrevapplied.22.034032
23. Vorontsova I., Goncharov R., Filipov I., Chistiakov V., Nasedkin B., Trifonov P., et al. Composable security analysis of an experimental continuous-variable quantum key distribution system operating with polar codes. *Journal of the Optical Society of America B*, 2025, vol. 42, no. 12, pp. 2883–2892. doi: 10.1364/josab.573606
24. Pan Y., Zhang L., Huang D. Practical security bounds against trojan horse attacks in continuous-variable quantum key distribution. *Applied Sciences*, 2020, vol. 10, no. 21, pp. 7788. doi: 10.3390/app10217788
25. Goncharov R.K., Kiselev A.D., Samsonov E.O., Egorov V.I. Continuous-variable quantum key distribution: security analysis with trusted hardware noise against general attacks. *Nanosystems: Physics, Chemistry, Mathematics*, 2022, vol. 13, no. 4, pp. 372–391. doi: 10.17586/2220-8054-2022-13-4-372-391

Авторы

Соломатин Олег Андреевич — аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, https://orcid.org/0009-0002-8676-5735, olegun.solom.2016@gmail.com
Морозова Полина Алексеевна — инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57209072591, https://orcid.org/0000-0003-3741-3506, Pamorozova@itmo.ru
Чистяков Владимир Викторович — кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57211537112, https://orcid.org/0000-0002-2414-3490, v_chistyakov@itmo.ru
Наседкин Борис Александрович — кандидат физико-математических наук, старший научный сотрудник, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 56543625300, https://orcid.org/0000-0002-4507-8616, banasedkin@itmo.ru

Authors

Oleg A. Solomatin — PhD Student, ITMO University, Saint Petersburg, 197101, Russian Federation, https://orcid.org/0009-0002-8676-5735, olegun.solom.2016@gmail.com
Polina A. Morozova — Engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57209072591, https://orcid.org/0000-0003-3741-3506, Pamorozova@itmo.ru
Vladimir V. Chistiakov — PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57211537112, https://orcid.org/0000-0002-2414-3490, v_chistyakov@itmo.ru

Boris A. Nasedkin — PhD (Physics & Mathematics), Senior Researcher, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 56543625300, https://orcid.org/0000-0002-4507-8616, banasedkin@itmo.ru

Статья поступила в редакцию 01.06.2026
Одобрена после рецензирования 16.08.2026
Принята к печати 20.09.2026

Received 01.06.2026
Approved after reviewing 16.08.2026
Accepted 20.09.2026

Работа доступна по лицензии
Creative Commons
«Attribution-NonCommercial»