Оптический журнал
Волоконно-оптические линии связи

DOI: 10.17586/1023-5086-2022-89-07-80-89
УДК 535.8, 535.015

Теоретический анализ систем распределения квантовых ключей, не зависящих от измерительных устройств, при их интеграции в волоконно-оптические линии связи с применением технологии плотного мультиплексирования по длине волны

Ирина Олеговна Воронцова[1]✉, Роман Константинович Гончаров[2], Ангелина Дмитриевна Тарабрина[3], Даниил Вадимович Тупяков[4], Егор Алексеевич Болычев[5], Семен Владимирович Смирнов[6], Федор Дмитриевич Киселев[7], Владимир Ильич Егоров[8]

[1, 2, 3, 4, 5, 6, 7, 8]Университет ИТМО, Санкт-Петербург, Россия
[6, 7, 8]ООО «Квантттелеком», Санкт-Петербург, Россия

[1]iovorontsova@itmo.ru https://orcid.org/0000-0001-9861-0816
[2]rkgoncharov@itmo.ru https://orcid.org/0000-0002-9081-8900
[3]adtarabrina@itmo.ru https://orcid.org/0000-0002-7114-8438
[4]tupyakov.daniil@gmail.com https://orcid.org/0000-0002-8804-6569
[5]onixiz56@gmail.com https://orcid.org/ 0000-0001-5394-082X
[6]s.smirnov@itmo.ru https://orcid.org/ 0000-0002-8562-2452
[7]fdkiselev@itmo.ru https://orcid.org/ 0000-0002-3894-511X
[8]viegorov@itmo.ru https://orcid.org/ 0000-0003-0767-0261

Аннотация

Предмет исследования. Влияние шумов, вызванных спонтанным комбинационным рассеянием, четырехволновым смешением и линейными перекрестными помехами в канале, на производительность систем квантового распределения ключей, не зависящих от измерительных устройств, в случае их симметричной и асимметричной реализаций. Приведены математические модели системы квантового распределения ключа, не зависящей от измерительных устройств, а также рассматриваемых канальных шумов. Во всех случаях определена скорость генерации секретного ключа для оценки и последующего анализа производительности систем. По этим результатам выявлены и изложены особенности работы системы квантового распределения ключа, не зависящей от измерительных устройств, при интеграции с существующими системами волоконно-оптических линий связи с применением технологии плотного мультиплексирования с разделением по длине волны. **Целью** данной работы является исследование произвольности не зависящих от измерительных устройств систем квантового распределения ключей при их интеграции в волоконно-оптические линии связи с применением технологии плотного мультиплексирования с разделением по длине волны методами численного моделирования. **Метод.** Для выбора оптимальных конфигураций расположения квантового канала и информационных каналов использован подход, основанный на проведении анализа графика сечения комбинационного рассеяния и отведении для информационных каналов частот, соответствующих областям в стороне от длины волны накачки. Для численного моделирования системы квантового распределения ключей с недоверенным узлом рассмотрена схема однофотонного варианта при симметричной и двух асимметричных реализациях системы. Анализ стойкости проведен

в соответствии с границей Деветака–Винтера, позволяющей оценить в асимптотическом режиме (для симметричных последовательностей бесконечной длины) скорость генерации секретного ключа в присутствии в квантовом канале атак коллективного типа. **Основные результаты.** Подтвержден вывод о том, что оптимальным для не зависящих от измерительных устройств систем квантового распределения ключей является вариант равенства плеч отправителя и получателя (симметричный) с последующим ухудшением результата по мере увеличения параметра асимметричности. В случае расположения квантового канала в С-диапазоне превосходство симметричного варианта минимально, а при увеличении количества информационных каналов до 40 практически неразличимо, в то время как при расположении квантового канала на длине волны 1310 нм (О-диапазон) разница существенна. Кроме того, выделение для квантового канала длины волны 1310 нм позволяет достичь наибольшего расстояния функционирования, которое при этом слабо зависит от количества каналов. **Практическая значимость.** В контексте практической реализации систем квантового распределения ключей особый интерес вызывает возможность их внедрения в существующую телекоммуникационную инфраструктуру посредством совместного распространения квантовых и информационных каналов в волоконно-оптические линии связи, реализованного с применением технологии мультиплексирования, в частности плотного мультиплексирования с разнесением по длине волны. Однако значения мощности, характерные для квантовых сигналов, существенно ниже аналогичных значений информационных сигналов. По этой причине шум от информационных каналов при распространении мощности в одном волокне с квантовыми сильно снижает работоспособность систем квантового распределения ключей. В связи с этим физическое и математическое описание, анализ и численное моделирование шумов и их взаимодействия с различными системами квантового распределения ключей с целью определить наиболее эффективный метод интеграции играют ключевую роль в решении задачи внедрения систем квантового распределения ключей в существующую телекоммуникационную сеть.

Ключевые слова: квантовое распределение ключа, мультиплексирование с разделением по длине волны, скорость генерации секретного ключа, волоконно-оптические линии связи

Благодарность: проект реализуется при финансовой поддержке ОАО «РЖД».

Ссылка для цитирования: Воронцова И.О., Гончаров Р.К., Тарабрина А.Д., Тупяков Д.В., Болычев Е.А., Смирнов С.В., Киселев Ф.Д., Егоров В.И. Теоретический анализ систем распределения квантовых ключей, не зависящих от измерительных устройств, при их интеграции в волоконно-оптические линии связи с применением технологии плотного мультиплексирования по длине волны // Оптический журнал. 2022. Т. 89. № 7. С. 80–89. DOI: 10.17586/1023-5086-2022-89-07-80-89

Коды OCIS: 270.5565, 270.5568, 270.558

ВВЕДЕНИЕ

В течение последних десятилетий направление квантовых коммуникаций, а в частности квантовое распределение ключей (КРК), показало и зарекомендовало себя как одну из наиболее активно и динамично развивающихся областей квантовых технологий [1, 2]. Технологии КРК делают возможным рассылать криптографически стойкий ключ между двумя и бóльшим количеством аутентифицированных пользователей, которые соединены между собой квантовым и информационными каналами. Таким образом, теоретически стойкость КРК к атакам со стороны злоумышленника продиктована принципами квантовой механики [3]. Законы квантовой механики в таком случае обеспечивают защиту передаваемых данных от всевозможных существующих технологических разработок, например, в области квантовых вычислений [4].

Одним из способов практической реализации квантового канала для осуществления сеанса КРК является его интеграция в существующие волоконно-оптические линии связи (ВОЛС) [4]. Значения мощности квантового и информационных сигналов отличаются на порядки, что долгое время порождало необходимость выделения так называемого темного волокна специально для квантовых каналов связи. Однако такой подход нельзя считать оптимальным как с практической, так и с экономической точки зрения. Возможным

решением проблемы является применение технологий мультиплексирования каналов, главным образом, плотного мультиплексирования со строгим разделением по длине волны (*dense wavelength division multiplexing* — DWDM). В то же время использование квантового и информационного каналов в одном оптическом волокне с применением технологий DWDM неизбежно приводит к ухудшению квантового сигнала из-за потерь, вызванных канальными шумами. К основным видам канальных шумов в контексте КРК следует отнести спонтанное комбинационное рассеяние (СКР), четырехволновое смешение (ЧВС) и линейные перекрестные помехи (ЛПП) классических информационных каналов [5–7].

Перспективным решением для обеспечения высокой стойкости систем КРК являются протоколы КРК, не зависящие от измерительных устройств (*measurement-device-independent*) — MDI КРК [8]. В данной работе ведется обсуждение одной из возможных реализаций последнего, а именно, рассматривается однофотонный протокол MDI КРК, представляющий интерес в контексте работы с однофотонными источниками. Теоретическое исследование и численное моделирование влияния шумов, вызванных СКР, ЧВС и ЛПП, на производительность системы MDI КРК проводится для симметричной и асимметричной реализаций данного протокола. В работе приводятся математические модели названных шумов, а также описание принципов работы MDI КРК. Скорость генерации секретного ключа для данной системы рассчитывается в случае различных схем расположения каналов (в работе называемых конфигурациями), приводится обоснование их выбора. Все численные расчеты выполнены для равномерной сетки DWDM в вариантах расположения квантового канала в C- и O-диапазонах (на длине волны 1310 нм) телекоммуникационных длин волн. Производительность системы MDI КРК определяется в контексте максимально достижимой дистанции, на которой еще возможна передача секретного ключа. По итогам сравнительного анализа полученных результатов выявляются и формулируются особенности работы системы MDI КРК при интеграции с системой DWDM. Таким образом, целью данной работы является исследование произвольности систем MDI КРК при их интеграции в ВОЛС с применением технологии DWDM методами численного моделирования.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ДЛЯ ОЦЕНКИ СКОРОСТИ ГЕНЕРАЦИИ СЕКРЕТНОГО КЛЮЧА ПРОТОКОЛА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА, НЕ ЗАВИСЯЩЕГО ОТ ИЗМЕРИТЕЛЬНЫХ УСТРОЙСТВ

В основе работы протокола MDI КРК [5–7] лежит предположение о том, что все детекторы, входящие в состав системы, могут находиться под контролем нарушителя. В стандартной схеме MDI КРК отправитель и получатель осуществляют отправку своих квантовых сигналов на недоверенное центральное «реле», называемое Чарли (рис. 1). После этого оба сигнала интерферируют на светоделителе 50:50 и затем следуют на поляризационный светоделитель, где осуществляется проекция либо в горизонтальное, либо в вертикальное состояние поляризации. Измерение считается успешным, если «щелкают» два из четырех задействованных детекторов.

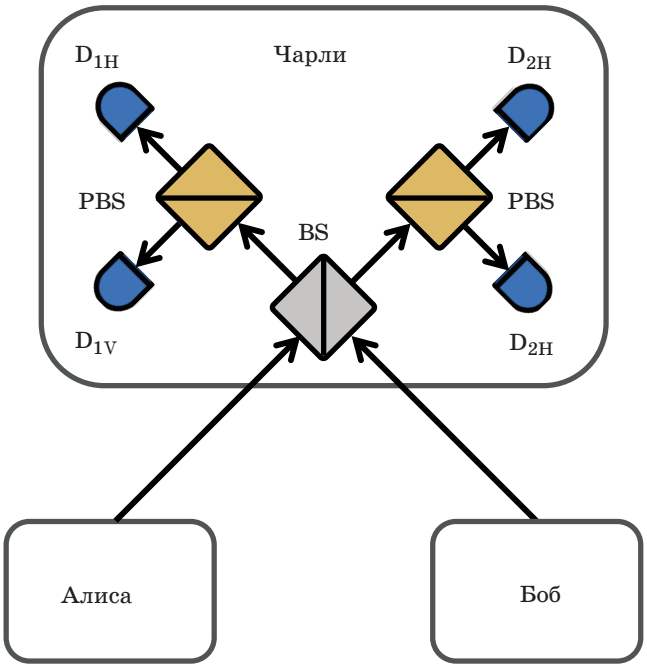

Рис. 1. Упрощенная схема работы протокола MDI. BS — светоделитель 50:50, PBS — поляризационный светоделитель, H — горизонтальное состояние поляризации, V — вертикальное состояние поляризации, D — детекторы

При рассмотрении прямолинейного базиса скорость генерации секретного ключа для однофотонного протокола MDI КРК можно получить следующим образом [9]:

$$R \geq Q_{11}\left[1-H\left(e_{11}\right)\right]-Q_{\mathrm{rect}} f\left(E_{\mathrm{rect}}\right) H\left(E_{\mathrm{rect}}\right), \quad (1)$$

$$Q_{11}=\mu_a \mu_b \exp(-\mu_a-\mu_b) Y_{11}. \quad (2)$$

В приведенном выше уравнении Q_{11} и e_{11} обозначают коэффициент усиления и коэффициент квантовых ошибок, когда отправитель и получатель осуществляют генерацию однофотонного состояния соответственно, μ_a и μ_b — среднее число фотонов, а Y_{11} — вероятность успешного детектирования при условии, что отправитель и получатель посылают одиночные фотоны. Последняя подчиняется выражению

$$e_{11}Y_{11}=$$

$$(1-p_d)^2\left[e_d\frac{\eta_a\eta_b}{2}+e_0\left(2\eta_a+2\eta_b-2\eta_a\eta_b\right)p_d+\right.$$

$$\left.+4e_0\left(1-\eta_a\right)\left(1-\eta_b\right)p_d^2\right]=$$

$$=e_0Y_{11}-\left(e_0-e_d\right)(1-p_d)^2\frac{\eta_a\eta_b}{2}, \quad (3)$$

где $\eta_{a(b)}$ — коэффициент пропускания канала отправителя (получателя), $e_0 = 0{,}5$ — коэффициент ошибок фонового шума, e_d описывает ошибку рассогласования между отправителем и получателем, а p_d — это коэффициент темновых отсчетов детектора.

В свою очередь Q_{rect} описывает коэффициент усиления в прямолинейном базисе, который может быть получен как сумма вероятностей обнаружения в двух сценариях (для выбора разных и одинаковых мод)

$$Q_{\mathrm{rect}}=Q_{\mathrm{rect}}^C+Q_{\mathrm{rect}}^E, \quad (4)$$

где

$$Q_{\mathrm{rect}}^C=2(1-p_d)^2\exp(-\mu'/2)\times$$
$$\times\left[1-(1-p_d)\exp(-\eta_a\mu_a/2)\right]\times \quad (5)$$
$$\times\left[1-(1-p_d)\exp(-\eta_b\mu_b/2)\right],$$

$$Q_{\mathrm{rect}}^E=2p_d(1-p_d)^2\exp(-\mu'/2)\times$$
$$\times\left[I_0(2x)-(1-p_d)\exp(-\mu'/2)\right]. \quad (6)$$

Параметры μ' и x в выражениях (5), (6) определяются как

$$\mu'=\eta_a\mu_a+\eta_b\mu_b, \quad (7)$$

$$x=\sqrt{\eta_a\mu_a\eta_b\mu_b}\,/2. \quad (8)$$

Таким образом, учитывая ошибку рассогласования, получаем

$$E_{\mathrm{rect}}Q_{\mathrm{rect}}=e_dQ_{\mathrm{rect}}^C+(1-e_d)Q_{\mathrm{rect}}^E, \quad (9)$$

где E_{rect} — коэффициент квантовых ошибок в прямолинейном базисе.

КАНАЛЬНЫЕ ШУМЫ

При распространении по ВОЛС квантовый сигнал неизбежно претерпевает потери. В данной статье рассматриваются три эффекта, вносящих основной вклад в общий шум, а именно СПР, ЧВС и ЛПП. Затем проводится анализ влияния этих шумов на квантовый канал и, следовательно, на производительность системы MDI КРК.

Спонтанное комбинационное рассеяние

Эффект СКР приводит к появлению в ВОЛС широкополосного шума. Данный вид шума принято считать незначительным для классических ВОЛС, однако его влияние на системы КРК является существенным [10, 11]. Его эффект на квантовые каналы зависит от относительного сдвига спектра между квантовыми и классическими каналами, а минимизировать его воздействие можно посредством подбора конфигураций расположения информационных и квантового каналов. В данной работе рассматривается ситуация, когда сигналы в квантовом и классическом каналах распространяются в оптическом волокне в одном направлении как в плече «получатель–реле», так и «отправитель–реле». Данная конфигурация соответствует случаю, когда информация должна быть передана третьей стороне, находящейся на реле. Рассмотрение конфигурации прямой посылки «отправитель–получатель» с регенерацией интенсивности на реле и учетом эффекта обратного СКР в плече «реле–получатель» в данной работе не приводится, однако оно представляет интерес для анализа

и будет выполнено в последующих работах. В этом случае шум прямого СКР, вызванный присутствием классических каналов, определяется как [5, 12]

$$P_{\mathrm{ram},f} = P_{\mathrm{out}} l \sum_{c=1}^{N_{\mathrm{ch}}} \rho\left(\lambda_{\mathrm{c}}, \lambda_{\mathrm{q}}\right) \Delta\lambda, \qquad (10)$$

где P_{out} — выходная мощность одного классического канала, l — длина оптического волокна, N_{ch} — количество информационных каналов в системе DWDM, $\rho(\lambda_{\mathrm{c}}, \lambda_{\mathrm{q}})$ — нормированное сечение рассеяния для длин волн информационных (λ_{c}) и квантового (λ_{q}) каналов, $\Delta\lambda$ — полоса пропускания системы фильтрации квантовых каналов.

Чтобы напрямую удовлетворить требования по коэффициенту ошибок для систем DWDM, вместо входных используются значения выходной мощности P_{out}. Выходная мощность может быть определена через чувствительность приемника R_x (дБм) и вносимые потери IL (дБм) системы как

$$P_{\mathrm{out}} = R_x + \mathrm{IL}. \qquad (11)$$

Четырехволновое смешение

Еще одним нелинейным эффектом, важным в контексте рассмотрения ВОЛС с DWDM, является ЧВС — нелинейный эффект третьего порядка, который заключается в генерации гармоник (в данном случае — паразитных) на суммарных или разностных частотах относительно основных частот системы при выполнении законов сохранения энергии и импульса [13].

Бывают ситуации, когда фотоны генерируются на частотах квантового канала [14] вследствие стимулированного ЧВС. При работе с такими конфигурациями важно правильно учитывать шум ЧВС.

Для трех сигналов накачки с частотами f_i, f_j и f_k значение пиковой мощности P_{ijk} сигнала, сгенерированного на новой частоте $f_i + f_j - f_k$, определяется следующим образом [5]:

$$P_{ijk} = \eta\gamma^2 D^2 p^2 \exp(-\xi L) \times \times \left(\frac{\left(1-\exp(-\xi L)\right)^2}{9\xi^2}\right) P_s P_l P_h, \qquad (12)$$

где эффективность фазового синхронизма для ЧВС η и параметр $\Delta\beta$ задаются уравнениями

$$\eta = \xi^2 / \left(\xi^2 + \Delta\beta^2\right) \times \times \left[1 + 4\exp(-\xi L) \frac{\sin^2\left(\frac{\Delta\beta L}{2}\right)}{\left(1-\exp(-\xi L)\right)^2}\right], \qquad (13)$$

$$\Delta\beta = \frac{2\pi\lambda^2}{c} \left|f_i - f_k\right| \left|f_j - f_k\right| \times \times \left[D_c + \frac{dD_c}{d\lambda}\left(\frac{\lambda^2}{c}\right)\left(\left|f_i - f_k\right| + \left|f_j - f_k\right|\right)\right] \qquad (14)$$

соответственно. В уравнениях (13), (14) L — дистанция взаимодействия распространяемых по волокну сигналов, D — параметр вырождения ($D = 6$, $D = 3$), $P_{i(j,k)}$ и $f_{i(j,k)}$ — входные значения мощности и оптических частот взаимодействующих полей соответственно, γ — нелинейный коэффициент третьего порядка, ξ — коэффициент потерь, D_c и $dD_c/d\lambda$ — параметры дисперсии оптического волокна, λ — длина волны результирующего сигнала ЧВС.

Таким образом, результирующая мощность шума, возникающего в оптическом волокне вследствие эффекта ЧВС[1], может быть получена как сумма всех произведений результирующих сигналов ЧВС с частотами, совпадающими с частотой квантового канала f_q

$$P_{\mathrm{FWM}} = \sum P_{ijk},\ f_i + f_j - f_k = f_q. \qquad (15)$$

Линейные перекрестные помехи

Линейные перекрестные помехи в канале вносят вклад в общий шум в любой системе DWDM. Происхождение ЛПП в основном связано с несовершенством демультиплексоров [15].

Соответствующий шум может существенно повлиять на слабый квантовый сигнал, если изоляции более мощных классических информационных каналов недостаточно. Утечка

[1] FWM — *four-wave mixing*.

мощности из фильтра в квантовый канал может быть получена следующим образом:

$$P_{\mathrm{LCXT}} = P_{\mathrm{out}} - \mathrm{ISOL}, \qquad (16)$$

где LCXT[2] — ЛПП, P_{out} (дБм) — выходная мощность волокна для одного классического канала, ISOL (дБ) — неэффективность фильтра, отделяющего квантовый канал от классического.

Мощность шума всех описанных типов затем может быть преобразована в вероятность обнаружения фотона для использования в дальнейших расчетах как

$$p_{\mathrm{ram},f/\mathrm{FWM/LCXT}} = \\ = \frac{P_{\mathrm{ram},f/\mathrm{FWM/LCXT}}}{hc/\lambda_q}\Delta t\eta_{\mathrm{D}}\eta_{\mathrm{B}}, \qquad (17)$$

где η_{D} — эффективность детектора одиночных фотонов, $\eta_{\mathrm{B}} = 10^{-0{,}1\mathrm{IL}}$ — коэффициент пропускания, связанный с вносимыми потерями, h — постоянная Планка и c — скорость света.

ЧИСЛЕННОЕ МОДЕЛИРОВАНИЕ И РЕЗУЛЬТАТЫ

Чтобы выбрать оптимальную конфигурацию для расположения квантового канала, был выбран подход, предложенный в работе [16]. Его суть заключается в том, что комбинационное рассеяние света показывает минимальные значения на удалении от длины волны излучения накачки, стало быть, размещать каналы надо в этих областях. Подход, предложенный в статье, был адаптирован под условия, соответствующие нашему случаю, и использован для выбора конфигураций. Таким образом, были использованы области с наименьшими значениями комбинационного рассеяния, присваивались квантовому каналу дли́ны волн, соответствующие длинам волн сетки, а затем рассчитывалась максимальная дистанция передачи ключа в каждом случае.

Окончательный перечень конфигураций, предложенных для дальнейших расчетов, приведен в таблице.

[2] LCXT — *linear channel crosstalk*.

Описание оптимальной конфигурации, выбранной для численных расчетов

Конфигурация	Число каналов	Длина волны квантового канала, нм
№ 1	10	1536,61
№ 2	10	1310
№ 3	40	1537,40
№ 4	40	1310

С помощью численного моделирования для каждой из конфигураций были получены зависимости скорости генерации секретного ключа от длины квантового канала с использованием математической модели для протокола MDI QKD и трех источников шума (СКР, ЧВС и ЛПП), рассмотренных в предыдущих разделах данной работы.

Параметры системы DWDM: $\xi = 0{,}18$ дБ/км, $\Delta\lambda = 15$ ГГц, $N_{\mathrm{ch}} = 10$ или 40, $R_x = -32$ дБм и $\mathrm{IL} = 8$ дБ.

Система MDI КРК была рассмотрена для симметричной и двух асимметричных реализаций (понимая под асимметричностью соотношение между путями L_a и L_b отправителя и получателя соответственно). Таким образом, в работе рассматриваются три варианта: симметричная ($L_a/L_b = 1$) и две асимметричные реализации ($L_a/L_b = 3/2$ и $L_a/L_b = 2/1$). Результаты моделирования приведены на рис. 2.

В ряде работ уже было показано, что оптимальным вариантом работы систем MDI КРК являются его симметричные реализации, при этом скорость генерации секретного ключа будет быстро снижаться при увеличении уровня асимметрии между путями отправителя и получателя. В связи с этим для успешной практической реализации протоколов MDI КРК применяются симметричные каналы [17, 18], а также преднамеренное добавление потерь в одном (меньшем) канале, чтобы сбалансировать общие потери в двух плечах [19]. Данная тенденция подтверждается результатами проведенного численного моделирования, приведенными на рис. 2. Для всех четырех рассмотренных конфигурациий наибольшая дистанция распространения достигается в случае симметричной реализации MDI КРК (кривая *1* на графиках), которая уменьшается по мере увеличения асимметричности плеч отправителя и получателя. Далее следует сформулировать

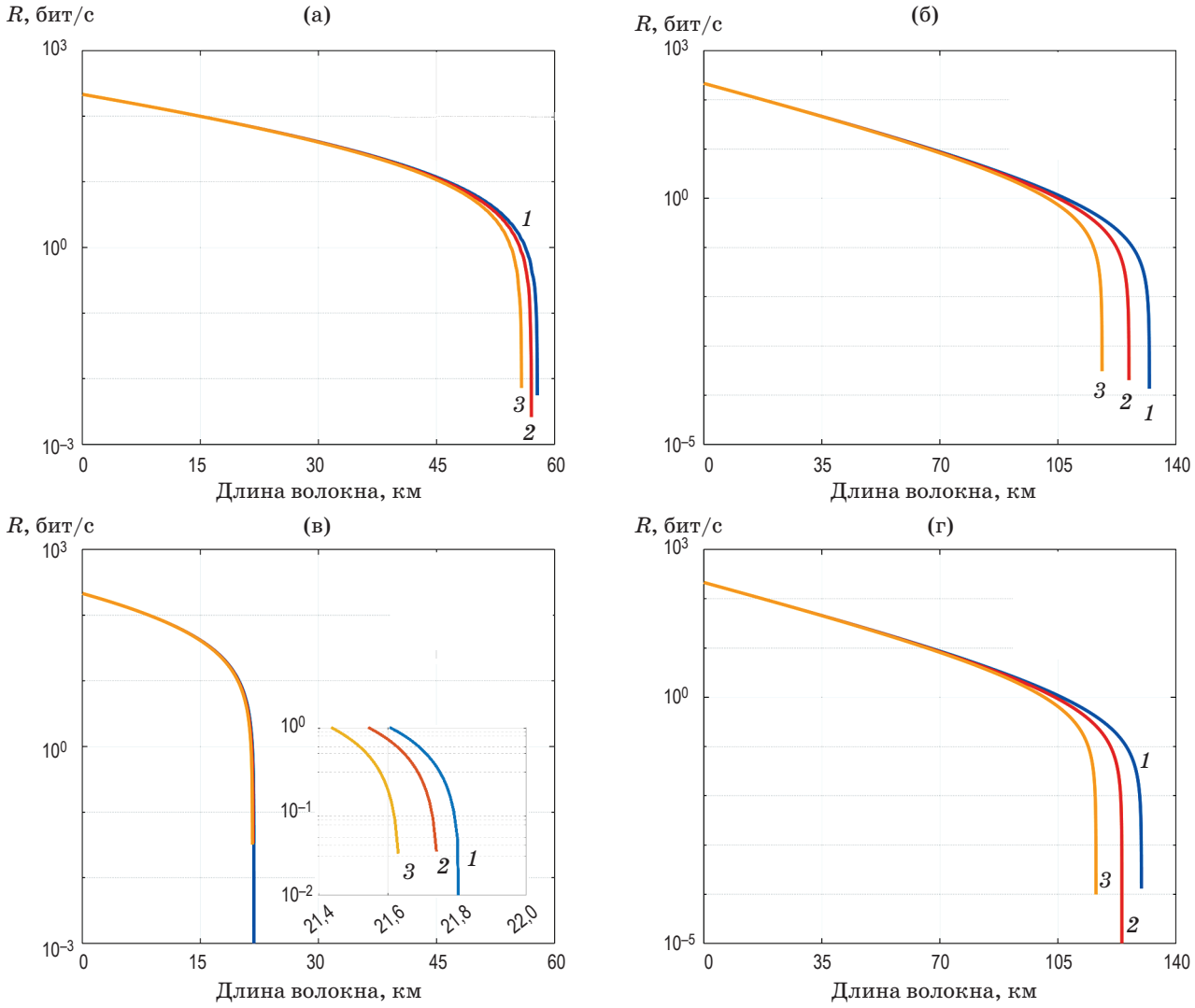

Рис. 2. Зависимости скорости генерации секретного ключа систем MDI КРК в случаях 10 каналов и квантового канала в С-диапазоне (Конфиг. № 1) — (а), 10 каналов и квантового канала на длине волны 1310 нм (Конфиг. № 2) — (б), 40 каналов и квантового канала в С-диапазоне (Конфиг. № 3) — (в) и 40 каналов и квантового канала на длине волны 1310 нм (Конфиг. № 4) — (г). $L_a/L_b = 1$ — *1*, $L_a/L_b = 3/2$ — *2*, $L_a/L_b = 2/1$ — *3*

ряд особенностей, отличающих поведение MDI КРК в рассмотренных случаях.

При расположении квантового канала на длине волны 1310 нм (рис. 2б, г), значения максимальной дистанции распространения значительно больше, чем при расположении квантового канала в С-диапазоне (рис. 2а, б). При этом расположение квантового канала на длине волны 1310 нм при увеличении количества каналов с 10 до 40 не приводит к значительному уменьшению максимальной дистанции функционирования. Противоположная ситуация наблюдается при расположении квантового канала в С-диапазоне: значение максимальной дистанции при этом более чем в 2 раза меньше соответствующих результатов в О-диапазоне даже в случае 10 каналов, а при увеличении их количества до 40 наблюдается критическое снижение дистанции до 21 км. При этом асимметричность не оказывает значительного влияния: для конфигурации с 40 каналами (рис. 2б) разница находится в диапазоне сотни метров, что не столь существенно.

ЗАКЛЮЧЕНИЕ

Методами численного моделирования проведено теоретическое исследование производи-

тельности системы MDI КРК при интеграции с ВОЛС DWDM в присутствии шумов СКР, ЧВС и ЛПП для симметричной и двух асимметричных реализаций системы. В работе были рассмотрены оптимальные конфигурации — схемы расположения квантового и информационных каналов на сетке DWDM. Критерием оценки производительности служило значение максимально достижимого расстояния системы КРК, на котором еще может быть осуществлена генерация секретного ключа. В результате был подтвержден вывод о том, что оптимальным для систем MDI КРК является вариант равенства плеч отправителя и получателя (симметричный) с последующим ухудшением результата по мере увеличения параметра асимметричности. При расположении квантового канала в С-диапазоне превосходство симметричного случая минимально, а при увеличении количества информационных каналов до 40 практически неразличимо, в то время как при расположении квантового канала на длине волны 1310 нм (О-диапазон) разница существенна. Кроме того, выделение для квантового канала длины волны 1310 нм позволяет достичь наибольшего расстояния функционирования, которое при этом слабо зависит от количества каналов. Полученные результаты позволяют сделать выводы о реализации систем MDI КРК на практике с целью получения оптимальных результатов. Рассмотрение модификации протокола MDI КРК с использованием состояний-ловушек и соответствующее усложнение математической модели для данной модификации протокола открывают потенциал для дальнейших исследований.

СПИСОК ИСТОЧНИКОВ

1. Scarani V., Bechmann-Pasquinucci H., Cerf N., et al. The security of practical quantum key distribution // Rev. Modern Phys. 2009. V. 81. № 3. P. 1301–1350. https://doi.org/10.1103/RevModPhys.81.1301
2. Pirandola S., Andersen U.L., Banchiet L., et al. Advances in quantum cryptography // Advances Opt. and Photon. 2020. V. 12. № 4. P. 1012–1236. https://doi.org/10.1364/AOP.361502
3. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Rev. Modern Phys. 2002. V. 74. № 1. P. 145. https://doi.org/10.1103/RevModPhys.74.145
4. Shor P.W. Algorithms for quantum computation: Discrete logarithms and factoring // Proc. 35th Annual Symp. Foundations of Computer Sci. 1994. P. 124–134. DOI: 10.1109/SFCS.1994.365700
5. Mlejnek M., Kaliteevskiy N., Nolan D. Reducing spontaneous Raman scattering noise in high quantum bit rate QKD systems over optical fiber // arXiv preprint. 2017. arXiv:1712.05891. https://doi.org/10.48550/arXiv.1712.05891
6. Niu J.N., Sun Y.M., Cai C., Ji Y.F. Optimized channel allocation scheme for jointly reducing four-wave mixing and Raman scattering in the DWDM-QKD system // Appl. Opt. 2018. V. 57. № 27. P. 7987–7996. https://doi.org/10.1364/AO.57.007987
7. Kumar R., Qin H., Alléaume R. Coexistence of continuous variable QKD with intense DWDM classical channels // New J. Phys. 2015. V. 17. № 4. P. 043027. https://doi.org/10.1088/1367-2630/17/4/043027
8. Lo H.K., Curty M., Qi B. Measurement-device-independent quantum key distribution // Phys. Rev. Lett. 2012. V. 108. № 13. P. 130503. https://doi.org/10.1103/PhysRevLett.108.130503
9. Ma X., Razavi M. Alternative schemes for measurement-device-independent quantum key distribution // Phys. Rev. A – Atomic, Molecular, and Opt. Phys. 2012. V. 86. № 6. P. 062319. https://doi.org/10.1103/PhysRevA.86.062319
10. Lin R., Chen J. Minimizing spontaneous Raman scattering noise for quantum key distribution in WDM networks // 2021 Optical Fiber Commun. Conf. and Exhib. (OFC). San Francisco, CA, USA. June 6–10 2021. P. 1–3.
11. Cai C., Sun Y., Ji Y. Intercore spontaneous Raman scattering impact on quantum key distribution in multicore fiber // New J. Phys. 2020. V. 22. № 8. P. 083020. https://doi.org/10.1088/1367-2630/aba023
12. Eraerds P., Walenta N., Legré M., et al. Quantum key distribution and 1 Gbps data encryption over a single fibre // New J. Phys. 2010. V. 12. № 6. P. 063027. https://doi.org/10.1088/1367-2630/12/6/063027
13. Boyd R.W. Nonlinear optics. 4th ed. San Diego, CA: Academic Press, 2020. 634 p.
14. Lin Q., Yaman F., Agrawal G.P. Photon-pair generation in optical fibers through four-wave mixing: Role of Raman scattering and pump polarization // Phys. Rev. A – Atomic, Molecular, and Opt. Phys. 2007. V. 75. № 2. P. 023803. https://doi.org/10.1103/PhysRevA.75.023803

15. Hill A., Payne D. Linear crosstalk in wavelength-division-multiplexed optical-fiber transmission systems // J. Lightwave Technol. 1985. V. 3. № 3. P. 643–651. DOI: 10.1109/JLT.1985.1074232
16. Bahrani S., Razavi M., Salehi J.A. Wavelength assignment in hybrid quantum-classical networks // Scientific Reports. 2018. V. 8. № 1. P. 1–13. https://doi.org/10.1038/s41598-018-21418-6
17. Da Silva T.F., Vitoreti D., Xavier G.B., et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits // Phys. Rev. A. 2013. V. 88. № 5. P. 052303. https://doi.org/10.1103/PhysRevA.88.052303
18. Comandar L., Lucamarini M., Fröhlich B., et al. Quantum key distribution without detector vulnerabilities using optically seeded lasers // Nature Photon. 2016. V. 10. № 5. P. 312–315. https://doi.org/10.1038/nphoton.2016.50
19. Rubenok A., Slater J.A., Chan P., Lucio-Martinez I., Tittel W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks // Phys. Rev. Lett. 2013. V. 111. № 13. P. 130501. https://doi.org/10.1103/PhysRevLett.111.130501

АВТОРЫ

Ирина Олеговна Воронцова — студент, инженер, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; Scopus ID 57208314288; https://orcid.org/0000-0001-9861-0816; iovorontsova@itmo.ru

Роман Константинович Гончаров — студент, инженер, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; Scopus ID 57208314288; https://orcid.org/0000-0002-9081-8900; rkgoncharov@itmo.ru

Ангелина Дмитриевна Тарабрина — студент, лаборант, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; https://orcid.org/0000-0002-7114-8438; adtarabrina@itmo.ru

Даниил Вадимович Тупяков — студент, лаборант, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; https://orcid.org/0000-0002-8804-6569; tupyakov.daniil@gmail.com

Егор Алексеевич Болычев — студент, лаборант, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; https://orcid.org/0000-0001-5394-082X; onixiz56@gmail.com

Семен Владимирович Смирнов — кандидат физико-математических наук, старший научный сотрудник, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; научный сотрудник, ООО «Кванттелеком», Санкт-Петербург, 199178, Россия; Scopus ID 57209025430; https://orcid.org/ 0000-0002-8562-2452; s.smirnov@itmo.ru

Федор Дмитриевич Киселев — кандидат физико-математических наук, старший научный сотрудник, Лиди-

AUTHORS

Irina O. Vorontsova — student, Engineer, Leading research center «National center for quantum internet», ITMO University, Saint-Petersburg, 199034, Russia; Scopus ID 57208314288; https://orcid.org/0000-0001-9861-0816; iovorontsova@itmo.ru

Roman K. Goncharov — student, Engineer, Leading research center «National center for quantum internet», ITMO University, Saint-Petersburg, 199034, Russia; Scopus ID 57208314288; https://orcid.org/0000-0002-9081-8900; rkgoncharov@itmo.ru

Angelina D. Tarabrina — student, Laboratory assistant, Leading research center «National center for quantum internet», ITMO University, Saint-Petersburg, 199034, Russia; https://orcid.org/0000-0002-7114-8438; adtarabrina@itmo.ru

Daniil V. Tupyakov — student, Laboratory assistant, Leading research center «National center for quantum internet», ITMO University, Saint-Petersburg, 199034, Russia; https://orcid.org/0000-0002-8804-6569; tupyakov.daniil@gmail.com

Egor A. Bolychev — student, Laboratory assistant, Leading research center «National center for quantum internet», ITMO University, Saint-Petersburg, 199034, Russia; https://orcid.org/ 0000-0001-5394-082X; onixiz56@gmail.com

Semyon V. Smirnov — PhD in Physics, Senior Researcher, Leading research center «National center for quantum internet», ITMO University, Saint-Petersburg, 199034, Russia; Researcher, LLC «Quanttelecom», Saint-Petersburg, 199178, Russia; Scopus ID 57209025430; https://orcid.org/ 0000-0002-8562-2452; s.smirnov@itmo.ru

Fedor D. Kiselev — PhD in Physics, Senior Researcher, Leading research center «National center for quantum

рующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; старший научный сотрудник, ООО «Квантелеком», Санкт-Петербург, 199178, Россия; Scopus ID 57214097409; https://orcid.org/ 0000-0002-3894-511X; fdkiselev@itmo.ru

Владимир Ильич Егоров — кандидат физико-математических наук, ведущий научный сотрудник, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; начальник отдела научных исследований, ООО «Квантелеком», Санкт-Петербург, 199178, Россия; Scopus ID 55429352600; https://orcid.org/ 0000-0003-0767-0261; viegorov@itmo.ru

internet», ITMO University, Saint-Petersburg, 199034, Russia; Senior Researcher, LLC «Quanttelecom», Saint-Petersburg, 199178, Russia; Scopus ID 57214097409; https://orcid.org/0000-0002-3894-511X; fdkiselev@itmo.ru

Vladimir I. Egorov — PhD in Physics, Leading Researcher, Leading research center «National center for quantum internet», ITMO University, Saint-Petersburg, 199034, Russia; Head of the Scientific Research Department, LLC «Quanttelecom», Saint-Petersburg, 199178, Russia; Scopus ID 55429352600; https://orcid.org/ 0000-0003-0767-0261; viegorov@itmo.ru

Статья поступила в редакцию 15.04.2022, одобрена после рецензирования 27.04.2022, принята к печати 18.05.2022