

DOI: 10.17586/1023-5086-2022-89-07-90-95

УДК 530.145:535.12:681.7:53.082.5

Доказательство стойкости квантового распределения ключей на непрерывных переменных типа «подключил и работай»

Роман Константинович Гончаров¹✉, Даниил Николаевич Кириченко²,
Ирина Олеговна Воронцова³, Илья Максимович Филипов⁴,
Юрий Александрович Адам⁵, Борис Евгеньевич Первушин⁶,
Борис Александрович Наседкин⁷, Эдуард Олегович Самсонов⁸,
Владимир Ильич Егоров⁹

Университет ИТМО, Санкт-Петербург, Россия

⁹ООО «Кванттелеком», Санкт-Петербург, Россия

¹rkgoncharov@itmo.ru <https://orcid.org/0000-0002-9081-8900>

²dnkirichenko@itmo.ru <https://orcid.org/0000-0002-9567-8169>

³jovorontsova@itmo.ru <https://orcid.org/0000-0001-9861-0816>

⁴imfilipov@itmo.ru <https://orcid.org/0000-0003-4564-8284>

⁵jaadam@itmo.ru <https://orcid.org/0000-0002-5040-0040>

⁶borispervushin@itmo.ru <https://orcid.org/0000-0002-0935-2614>

⁷banasedkin@itmo.ru <https://orcid.org/0000-0002-4507-8616>

⁸eosamsonov@itmo.ru <https://orcid.org/0000-0002-4349-6603>

⁹viegorov@itmo.ru <https://orcid.org/0000-0003-0767-0261>

Аннотация

Предмет исследования. Двусторонние схемы квантового распределения ключей на непрерывных переменных. **Целью работы** является доказательство стойкости системы квантового распределений ключей на непрерывных переменных типа «подключил и работай» в контексте модели доверенного шума со стороны легитимных пользователей. **Метод.** На основе аналога известной реализации в формате «подключил и работай» оценивается производительность такой системы, работающей по протоколу GG02. Оценка проводится в присутствии коллективных атак с учетом эффектов конечной размерности ключа. **Основные результаты.** Стойкий ключ, удовлетворяющий критериям компонуемости, может быть распределен при потерях в канале в 5 дБ, что ожидаемо примерно вдвое меньше, чем в однопроходной схеме. **Практическая значимость.** Двухпроходные схемы квантового распределения ключей являются более стабильными по сравнению с однопроходными, поэтому стойкость в их отношении требует детального рассмотрения. Настоящая работа впервые предлагает рассмотрение стойкости двухпроходной реализации квантового распределения ключей на непрерывных переменных с учетом доверенных шумов оборудования.

Ключевые слова: квантовое распределение ключей на непрерывных переменных, критерий компонуемости, «подключил и работай»

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

Ссылка для цитирования: Гончаров Р.К., Кириченко Д.Н., Воронцова И.О., Филипов И.М., Адам Ю.А., Первушин Б.Е., Наседкин Б.А., Самсонов Э.О., Егоров В.И. Доказательство стойкости квантового распределения ключей на непрерывных переменных типа «подключил и работай» // Оптический журнал. 2022. Т. 89. № 7. С. 90–95. DOI: 10.17586/1023-5086-2022-89-07-90-95

Коды OCIS: 270.5565, 270.5568

ВВЕДЕНИЕ

Квантовое распределение ключей (КРК) [1] как, вероятно, наиболее быстро развивающаяся область квантовых коммуникаций предлагает множество реализаций, по которым можно провести очень подробную классификацию. Это связано, во-первых, с тем, что различные системы КРК могут решать разные задачи, например, компактность КРК на непрерывных переменных (КРКНП) позволяет реализовать их в инфраструктуре Интернета вещей, а КРК на дискретных переменных, использующие крупногабаритные однофотонные детекторы, могут обеспечивать большие расстояния. Во-вторых, различные оптические схемы отличаются в контексте устойчивости.

Данная работа посвящена рассмотрению и сравнению однопроходной и двухпроходной систем КРКНП. Сразу важно отметить, что обе вариации могут быть построены на одном и том же протоколе. Так, например, BB84 [2] может быть реализован в двух вариантах — обычном однопроходном [3] и двухпроходном, называемом «подключил и работай» [4, 5]. Основное отличие выражается в том, что если в однопроходной схеме отправитель (Алиса) подготавливает и отправляет квантовые состояния по квантовому каналу с помощью источника света и определенных методов модуляции, после этого состояния детектируются приемником (Бобом), то в двухпроходной схеме источник находится на стороне Боба, который отправляет опорное состояние (не содержащее информации) Алисе, она модулирует (фактически точно так же подготавливает состояние) и возвращает сигнал в канал, затем протокол реализуется, как обычно. Это, естественно, распространяется на КРКНП, которые, по сути, сталкиваются с теми же искажениями в канале.

Необходимость исследования двухпроходных схем диктуется дополнительными поляризационными искажениями, возникающими в однопроходном канале, компенсировать которые достаточно сложно. В то же время в двухпроходном случае часть искажений может быть компенсирована на обратном, втором, проходе по тому же каналу. Таким образом, целью данной работы является доказательство стойкости системы «подключил и работай» КРКНП в контексте модели доверенного шума со стороны легитимных пользователей.

РЕАЛИЗАЦИЯ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ ТИПА «ПОДКЛЮЧИЛ И РАБОТАЙ»

В работе рассматривается реализация системы типа «подключил и работай», которая близка общепринятой [4, 5] в том смысле, что излучение в целом идет в два прохода (см. рис. 1). Боб посылает Алисе мощный импульс, она делит его на две составляющие — плечо локального осциллятора (ЛО) и сигнальное, затем последнее подвергается гауссовской модуляции.

Сигнальный импульс и ЛО разделяются посредством поляризационного и временного мультиплексирования и возвращаются на втором проходе Бобу, который осуществляет гетеродинный когерентный прием. Гетеродинирование мотивировано необходимостью дальнейшей симметризации протокола, которая не обсуждается в настоящей работе, поскольку основное внимание уделяется защите от коллективных атак.

Следует отметить, что подобная схема уже была представлена ранее [6], однако без конкретного деления на доверенные/недоверенные блоки (в результате доверенность шума не определяется) с использованием локального (генерируемого на стороне получателя) ЛО. Авторы настоящей работы мотивируют использование канального (генерируемого на стороне отправителя) ЛО тем, что он снимает

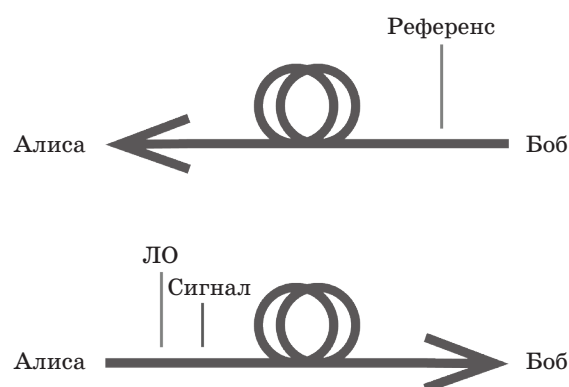


Рис. 1. Упрощенное схематическое изображение двух проходов в рассматриваемой схеме КРКНП типа «подключил и работай». Боб посылает опорные импульсы Алисе, затем она разделяет их на сигнал и ЛО. Рассматривается гауссовская модуляция, однако можно отметить, что возможна и дискретная модуляция

возможные проблемы с синхронизацией и дополнительной подстройкой фазы, однако следует отметить, что конечное расстояние на двух проходах также упадет из-за снижения мощности ЛО. В качестве решения этой проблемы можно использовать усилитель [7]. Кроме того, возможные атаки на ЛО по сторонним каналам утечки можно отслеживать [8].

АНАЛИЗ СТОЙКОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ

Учитывая, что используется модель доверенного аппаратного шума, необходимо разбить схему на блоки, чтобы уточнить, какие шумы они содержат. Разделение проводится следующим образом (независимые шумовые составляющие складываются):

- шум подготовки (или шум первого прохода) ξ_{prep} :
 - относительный шум интенсивности,
 - шумы цифро-аналогового преобразователя,
 - каналный фазовый шум;
- каналный шум (или шум второго прохода) ξ_{ch} :
 - каналный фазовый шум,
 - рэлеевский шум обратного рассеяния, связанный с тем, что мощный сигнал передается одновременно с квантовым на той же длине волны и по оптоволоконному каналу в двух направлениях;
 - шумы получателя ξ_{rec} :
 - шум коэффициента ослабления синфазного сигнала,
 - шум балансного детектора,
 - шум аналого-цифрового преобразователя.

В сценарии доверенного шума [9, 10] предполагается, что оборудование остается недоступным для Евы, т.е. шум первого прохода и шум приемника не поддаются манипуляциям Евы, но продолжают влиять на границу Холево (не в пользу Евы) χ . Здесь также можно отметить, что несмотря на то, что наличие даже доверенных потерь (и доверенного отправителя T_{send} и доверенного получателя T_{rec}) влияет и на взаимную информацию I_{AB} , которая уменьшается медленнее. Также уточняем, что рассматриваем схему обратного согласования.

Выражения для избыточного шума приведены в публикациях [11, 12], количественные

оценки далее даны приблизительно. Для двухпроходных схем вводится выражение для шума обратного рэлеевского рассеяния [6, 13, 14]

$$\xi_{\text{RB}} = \frac{\beta_R [1 - T_{\text{ch}}^2] V_A f_{\text{sym}} \delta t}{T_{\text{send}} T_{\text{ch}}^2}, \quad (1)$$

где β_R — коэффициент обратного рассеяния Рэля, f_{sym} — частота отправки сигналов, δt — время интегрирования детектора, $T_{\text{ch}} = 10^{-\zeta L/10}$ — коэффициент потерь в канале с L как длиной квантового канала и ζ как удельным затуханием в единицах дБ/км.

Скорость генерации секретного ключа конечной длины оценивается с учетом критериев компонуемости в соответствии с границей Деветака–Винтера [15] против коллективных атак [1, 16–18]

$$K = f_{\text{sym}} r_{\text{coll}}^{\text{finite}}, \quad (2)$$

$$r_{\text{coll}}^{\text{finite}} \geq \frac{n(1 - \text{FER})}{n_{\text{states}}} \times \left(\beta I_{AB}(w) - \chi(w) - \frac{\Delta_{\text{AEP}}}{\sqrt{n}} + \frac{\Theta}{n} \right), \quad (3)$$

$$\Delta_{\text{AEP}} = 4 \log_2 (2\sqrt{d} + 1) \sqrt{\log_2 \left(\frac{18}{(1 - \text{FER})^2 \epsilon_s^4} \right)}, \quad (4)$$

$$\Theta = \log_2 \left[(1 - \text{FER}) \left(1 - \epsilon_s^2 / 3 \right) \right] + 2 \log_2 \sqrt{2} \epsilon_h, \quad (5)$$

$$\epsilon = 2(1 - \text{FER}) \epsilon_{\text{pe}} + \epsilon_{\text{cor}} + \epsilon_s + \epsilon_h, \quad (6)$$

где n символов переходят к конечному ключу из изначально n_{states} символов, Δ_{AEP} — количество информации, потерянной из-за сглаживания [19], FER — частота ошибок в кадре, β — эффективность согласования, Θ соответствует процедуре хеширования и несовершенству исправления ошибок [1, 16], d — размер эффективного алфавита, а ϵ_j — параметр стойкости.

Граница Холево оценивается через энтропию фон Неймана S и симплектические собственные значения v_j как

$$\chi_E = S_E - S_{E|B}, \quad (7)$$

$$v_{E;1,2} = \frac{1}{2} \left(\sqrt{(V + T_{ch}(V-1) + 1 + \xi_{ch})^2 - 4T_{ch}(V^2 - 1)} \pm \right. \quad (8)$$

$$\left. \pm (T_{ch}(V-1) + 1 + \xi_{ch} - V) \right),$$

$$v_{E|B;3,4} = \frac{\sqrt{(e_1 + e_3)^2 - 4e_2^2} \pm (e_3 - e_1)}{2(T_{ch}T_{rec}V_A/\mu + 1 + \xi/\mu + 1)}, \quad (9)$$

$$e_1 = V((1 - T_{det})W_{rec} + T_{det}W_{ch} + 1) + T_{ch}(W_{ch} - V)(1 + (1 - T_{rec})W_{rec}), \quad (10)$$

$$e_2 = \sqrt{T_{ch}(W_{ch}^2 - 1)}(T_{det}V + (1 - T_{det})W_{rec} + 1), \quad (11)$$

$$e_3 = (1 - T_{det})W_{ch}W_{rec} + T_{det}T_{ch}(VW_{ch} - 1) + T_{det} + W_{ch}, \quad (12)$$

$$W_{ch} = \xi_{ch} / (1 - T_{ch}) + 1, \quad (13)$$

$$W_{rec} = \xi_{rec} / (1 - T_{det}) + 1. \quad (14)$$

В выражениях выше $V = V_A + 1$. Полученные выражения для шума и коэффициента пропускания были заключены в доверительные интервалы, которые естественным образом вытекают из следующей процедуры оценки параметров [1, 12]:

$$T_{det} \rightarrow T_{det} + 2w\xi / V_A \sqrt{T_{ch}T_{det} / (\mu n_{pe})}, \quad (15)$$

$$T_{ch} \rightarrow T_{ch} - 2w\xi / V_A \sqrt{T_{ch} / (\mu n_{pe})}, \quad (16)$$

$$\xi_{ch} \rightarrow \xi_{ch} + w \frac{\xi_{ch} + \mu}{\sqrt{2\mu n_{pe}}}. \quad (17)$$

Для расчетов использованы следующие параметры: $\mu = 2$, $V_A = 6$, $\xi_{ch, common} = 0,003T_{ch}$, $\xi_{rec} = 0,1$, $T_{det} = 10^{-0,725}$, $FER = 0,03$, $\beta = 0,95$, $n = 2 \times 10^8$, $n_{states} = 6 \times 10^8$, $n_{pe} = 6 \times 10^7$, $d = 2^4$, $\varepsilon_s = \varepsilon_h = 10^{-10}$, $\varepsilon = 5,6 \times 10^{-9}$, $w = 6,34$, $\beta_R = 10^{-0,8}$, $f_{sym} = 50$ МГц, $T_{send} = 10^{-1,225}$, $\delta t = 5 \times 10^{-9}$ с.

Следует уточнить, что в варианте «подключил и работай» необходимо учитывать падение мощности ЛО на первом проходе, однако с учетом и без того больших потерь на

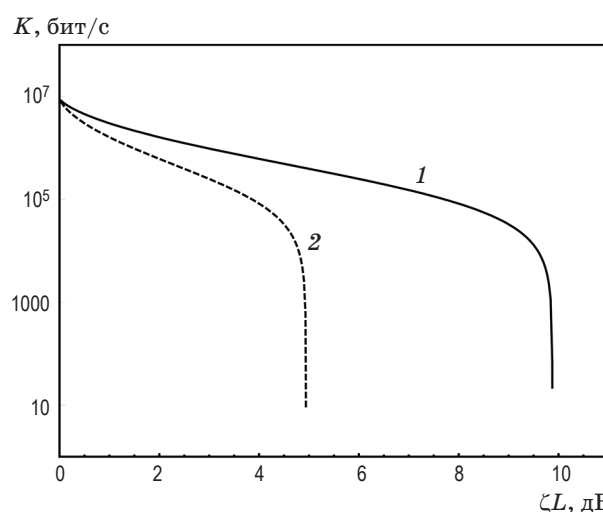


Рис. 2. Зависимости скоростей генерации секретного ключа от потерь в канале в двух реализациях — обычная однопроходная схема (1) и схема «подключил и работай» (2). Все условия и параметры предполагаются одинаковыми, за исключением перестроенного двустороннего канала и дополнительного шума в реализации «подключил и работай»

оборудовании Боба это мало влияет на обнаружение избыточного шума.

Можно сравнить характеристики описанной системы типа «подключил и работай» КРКНП с общепринятой в приближении тех же потерь в оборудовании и совпадающих шумов (значения, отличающиеся для «подключил и работай», отмечены штрихом) в единицах дробового шума: $\xi_{prep} \approx \xi'_{prep} \approx 3,37 \times 10^{-5}$, $\xi_{ch}(\zeta L = 5 \text{ дБ}) \approx 10^{-5}$, $\xi'_{ch}(\zeta L = 5 \text{ дБ}) \approx 3,59 \times 10^{-6}$, $\xi_{rec}(\zeta L = 5 \text{ дБ}) \approx \xi'_{rec}(\zeta L = 5 \text{ дБ}) \approx 0,08$ [12]. Вариант «подключил и работай» учитывает наличие дополнительного шума на первом проходе и шума от обратного рэлеевского рассеяния.

Рисунок 2 показывает, что производительность системы «подключил и работай» значительно снижается. Это, естественно, связано с удвоенными потерями в канале. Увеличенный шум передатчика и дополнительный шум канала со стороны обратного рэлеевского рассеяния имеют влияние, но оно незначительно по сравнению с уровнем шума, обнаруживаемым в типичной установке.

ЗАКЛЮЧЕНИЕ

В работе представлена модификация типа «подключил и работай» для типичной системы

КРКНП с гауссовской модуляцией и канальным ЛО. Теоретическая производительность такой системы сильно снижена, однако при этом повышены стабильность и устойчивость, например, к поляризационным искажениям,

которые автокомпенсируются за два прохода. Детальная оценка таких искажений и более очевидных преимуществ описанного подхода оставлена для последующей работы, как и экспериментальная реализация.

СПИСОК ИСТОЧНИКОВ

1. Pirandola S. Limits and security of free-space quantum communications // *Phys. Rev. Research*. 2021. V. 3. № 1. P. 013279. DOI: 10.1103/PhysRevResearch.3.013279
2. Bennett C.H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // *Theoretical Computer Sci.* 2014. V. 560. P. 7–11. DOI: j.tcs.2014.05.025
3. Marand C., Townsend P.D. Quantum key distribution over distances as long as 30 km // *Opt. Lett.* 1995. V. 20. № 16. P. 1695–1697. DOI: 10.1364/OL.20.001695
4. Stucki D., Gisin N., Guinnard O., et al. Quantum key distribution over 67 km with a plug&play system // *New J. Phys.* 2002. V. 4. № 1. P. 41. DOI: 10.1088/1367-2630/4/1/341
5. Kawamoto Y., Hirano T., Namiki R., et al. "Plug and play" systems for quantum cryptography with continuous variables // *Internat. Quantum Electron. Conf., 2005. IEEE, 2005*. P. 1612–1614. DOI: 10.1109/IQEC.2005.1561132
6. Valivarthi R., Etcheverry S., Aldama J., et al. Plug-and-play continuous-variable quantum key distribution for metropolitan networks // *Opt. Exp.* 2020. V. 28. № 10. P. 14547–14559. DOI: 10.1364/OE.391491
7. Zhang Y., Chen Z., Pirandola S., et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber // *Phys. Rev. Lett.* 2020. V. 125. № 1. P. 010502. DOI: 10.1103/PhysRevLett.125.010502
8. Jouguet P., Kunz-Jacques S., Diamanti E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution // *Phys. Rev. A*. 2013. V. 87. № 6. P. 062313. DOI: 10.1103/PhysRevA.87.062313
9. Usenko V.C., Filip R. Trusted noise in continuous-variable quantum key distribution: A threat and a defense // *Entropy*. 2016. V. 18. № 1. P. 20. DOI: 10.3390/e18010020
10. Laudenbach F., Pacher C. Analysis of the trusted-device scenario in continuous-variable quantum key distribution // *Advanced Quantum Technol.* 2019. V. 2. № 11. P. 1900055. DOI: 10.1002/qute.201900055
11. Laudenbach F., Pacher C., Fung C.H.F., et al. Continuous-variable quantum key distribution with Gaussian modulation — the theory of practical implementations // *Advanced Quantum Technol.* 2018. V. 1. № 1. P. 1800011. DOI: 10.1002/qute.201800011
12. Goncharov R., Kiselev A.D., Samsonov E., Egorov V. Security proof for continuous-variable quantum key distribution with trusted hardware noise against general attacks // *arXiv preprint arXiv:2205.05299*. 2022.
13. Subacius D., Zavriyev A., Trifonov A. Backscattering limitation for fiber-optic quantum key distribution systems // *Appl. Phys. Lett.* 2005. V. 86. № 1. P. 011103. DOI: 10.1063/1.1842862
14. Huang D., Huang P., Wang T., et al. Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol // *Phys. Rev. A*. 2016. V. 94. № 3. P. 032305. DOI: 10.1103/PhysRevA.94.032305
15. Devetak I., Winter A. Distillation of secret key and entanglement from quantum states // *Proc. Royal Soc. A: Mathematical, Physical and Eng. Sci.* 2005. V. 461. № 2053. P. 207–235. DOI: 10.1098/rspa.2004.1372
16. Pirandola S. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks // *Phys. Rev. Research*. 2021. V. 3. № 4. P. 043014. DOI: 10.1103/PhysRevResearch.3.043014
17. Leverrier A. Composable security proof for continuous-variable quantum key distribution with coherent states // *Phys. Rev. Lett.* 2015. V. 114. № 7. P. 070501. DOI: 10.1103/PhysRevLett.114.070501
18. Leverrier A., Grosshans F., Grangier P. Finite-size analysis of a continuous-variable quantum key distribution // *Phys. Rev. A*. 2010. V. 81. № 6. P. 062343. DOI: 10.1103/PhysRevA.81.062343
19. Tomamichel M., Colbeck R., Renner R. A fully quantum asymptotic equipartition property // *IEEE Trans. Inform. Theory*. 2009. V. 55. № 12. P. 5840–5847. DOI: 10.1109/TIT.2009.2032797

АВТОРЫ

Роман Константинович Гончаров — 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

Даниил Николаевич Кириченко — инженер, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; Scopus ID 8627412800; <https://orcid.org/0000-0002-9567-8169>; dnkirichenko@itmo.ru

Ирина Олеговна Воронцова — 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

Илья Максимович Филипов — инженер, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; Scopus ID 57208314288; <https://orcid.org/0000-0003-4564-8284>; imfilipov@itmo.ru

Юрий Александрович Адам — инженер, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; Scopus ID 57290760500; <https://orcid.org/0000-0002-5040-0040>; iaadam@itmo.ru

Борис Евгеньевич Первущин — инженер, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; Scopus ID 57215883567; <https://orcid.org/0000-0002-0935-2614>; borispervushin@itmo.ru

Борис Александрович Наседкин — научный сотрудник, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; Scopus ID 56543625300; <https://orcid.org/0000-0002-4507-8616>; banasedkin@itmo.ru

Эдуард Олегович Самсонов — кандидат физико-математических наук, ведущий научный сотрудник, Лидирующий исследовательский центр «Национальный центр квантового интернета», Университет ИТМО, Санкт-Петербург, 199034, Россия; Scopus ID 57215883422; <https://orcid.org/0000-0002-4349-6603>; eosamsonov@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 «Кванттелеком», Санкт-Петербург, 199178, Россия; Scopus ID 55429352600; <https://orcid.org/0000-0003-0767-0261>; viigorov@itmo.ru

AUTHORS

Roman K. Goncharov — 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

Daniil N. Kirichenko — engineer, Leading Research Center «National Center for Quantum Internet», ITMO University, Saint-Petersburg, 199034, Russia; Scopus ID 8627412800; <https://orcid.org/0000-0002-9567-8169>; dnkirichenko@itmo.ru

Irina O. Vorontsova — 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

Ilya M. Filipov — engineer, Leading Research Center «National Center for Quantum Internet», ITMO University, Saint-Petersburg, 199034, Russia; Scopus ID 57208314288; <https://orcid.org/0000-0003-4564-8284>; imfilipov@itmo.ru

Yuri A. Adam — engineer, Leading Research Center «National Center for Quantum Internet», ITMO University, Saint-Petersburg, 199034, Russia; Scopus ID 57290760500; <https://orcid.org/0000-0002-5040-0040>; iaadam@itmo.ru

Boris E. Pervushin — engineer, Leading Research Center «National Center for Quantum Internet», ITMO University, Saint-Petersburg, 199034, Russia; Scopus ID 57215883567; <https://orcid.org/0000-0002-0935-2614>; borispervushin@itmo.ru

Boris A. Nasedkin — researcher, Leading Research Center «National Center for Quantum Internet», ITMO University, Saint-Petersburg, 199034, Russia; Scopus ID 56543625300; <https://orcid.org/0000-0002-4507-8616>; banasedkin@itmo.ru

Eduard O. Samsonov — PhD in Physics, leading researcher, Leading Research Center «National Center for Quantum Internet», ITMO University, Saint-Petersburg, 199034, Russia; Scopus ID 57215883422; <https://orcid.org/0000-0002-4349-6603>; eosamsonov@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>; viigorov@itmo.ru