УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2019 Том 19 № 6 ISSN 2226-1494 http://ntv.itmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTCS
November–December 2019 Vol. 19 No 6 ISSN 2226-1494 http://ntv.itmo.ru/en/
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

УДК 535.8 doi: 10.17586/2226-1494-2019-19-966-972

ИССЛЕДОВАНИЕ ИНТЕРФЕРЕНЦИИ СЛАБЫХ КОГЕРЕНТНЫХ МНОГОМОДОВЫХ СОСТОЯНИЙ ДЛЯ ЗАДАЧ КВАНТОВОЙ КОММУНИКАЦИИ С НЕДОВЕРЕННЫМ ПРИЕМНЫМ УЗЛОМ

В.В. Чистяков, А.А. Гайдаш, А.В. Козубов, А.В. Глейм

Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: v_chistyakov@itmo.ru

Информация о статье
Поступила в редакцию 01.10.19, принята к печати 30.10.19
Язык статьи — русский

Ссылка для цитирования: Чистяков В.В., Гайдаш А.А., Козубов А.В., Глейм А.В. Исследование интерференции слабых когерентных многомодовых состояний для задач квантовой коммуникации с недоверенным приемным узлом // Научно-технический вестник информационных технологий, механики и оптики. 2019. Т. 19. № 6. С. 966–972. doi: 10.17586/2226-1494-2019-19-6-966-972

Аннотация

Предмет исследования. Представлены результаты аналитического и экспериментального исследования возможности формирования квантовых бит в результате интерференции когерентных многомодовых состояний на приемном узле. Такие состояния образуются на боковых частотах в результате фазовой модуляции несущей частоты из оптического диапазона. Предполагается, что оба абонента распределены в пространстве, однако приемный узел может быть подконтролен злоумышленнику. **Метод.** В работе продемонстрирован метод формирования исходных состояний. Показаны их распространение по оптическому волокну и результат интерференции. Для описания использовано классическое приближение. В эксперименте измеритель мощности подключался на стороне приемного узла. Результат интерференции оптических сигналов наблюдался на четырехпортовом волоконном светоделителе с коэффициентом деления 50:50. Измеряемые величины зависят от разности фаз высокочастотных электрических модулирующих сигналов (4,8 ГГц), используемых при фазовой модуляции в кристалле ниобата лития $LiNbO_3$ интенсивной несущей частоты в оптическом диапазоне (1550 нм). **Основные результаты.** Экспериментально полученные зависимости соотносятся с результатами аналитического исследования. Наблюдается изменение мощности оптического сигнала на боковых частотах фазомодулированного излучения в результате интерференции по гармоническому закону. Видность интерференционной картины при этом достигает 97,4 %. Показано, что предметом дальнейшего исследования является построение модели в рамках терминов квантовой оптики, а также проведение экспериментов в квазиоднофотонном режиме. **Практическая значимость.** Результаты исследования могут найти практическое применение при формировании протоколов для систем квантовой коммуникации и построения новых типов систем. В таких системах повышенное внимание будет уделяться не только к потенциальному воздействию злоумышленника на квантовые состояния в канале, но и на подверженные атакам приемные узлы. Показано, что использование абонентами метода формирования квантовых состояний на боковых частотах позволяет извлекать информацию, а злоумышленник лишен такой возможности из-за неоднозначности результатов срабатывания приемного узла даже при обладании им.

Ключевые слова
квантовые коммуникации, когерентные состояния, интерференция, фазомодулированное излучение

Благодарности
Работа выполнена при государственной поддержке ведущих университетов Российской Федерации (субсидия 08-08).

doi: 10.17586/2226-1494-2019-19-6-966-972

INTERFERENCE OF MULTI-MODE WEAK COHERENT STATES FOR TWIN-FIELD QUANTUM COMMUNICATION APPLICATIONS

V.V. Chistiakov, A.A. Gaidash, A.V. Kozubov, A.V. Gleim

ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: v_chistyakov@itmo.ru

Article info
Received 01.10.19, accepted 30.10.19
Article in Russian

For citation: Chistiakov V.V., Gaidash A.A., Kozubov A.V., Gleim A.V. Interference of multi-mode weak coherent states for twin-field quantum communication applications. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2019, vol. 19, no. 6, pp. 966–972 (in Russian). doi: 10.17586/2226-1494-2019-19-6-966-972

Abstract

Subject of Research. We present the results of analytical research and experimental implementation of quantum key distribution protocol based on multi-mode weak coherent states with untrusted detection node. Such states are based on interference of phase-coded sidebands in case, where legitimate users are sending these states to the untrusted detection node that could be controlled by an eavesdropper. **Method.** The method of initial states generation is applied. Their propagation via fiber-optic lines and interference result is shown. A classical approximation is used for description. The experiment is carried out with the power measurement system connected on detection node side. We present the experimental scheme and show that in the classical regime the interference pattern is obtained at the fiber-optic 2x2 beam splitter with 50:50 ratio depending on the phase difference of the radiofrequency modulating signals (4.8 GHz) applied to $LiNbO_3$ phase modulators, which modulate an optical carrier (1550 nm) in the blocks of legitimate users. **Main Results.** Experimental results are in accordance with analytical ones. Harmonical dependence of the optical power at the sidebands is obtained as an interference result. In this case, visibility of interference pattern is up to 97.4% and is good enough. Thus, application of these results in terms of quantum optics and experimentation in quantum single-photon regime might be a subject of future research. **Practical Relevance.** Practical application of research results lies in the development of quantum key distribution protocols and optical schemes with special attention to eavesdropping of quantum states and attacking the detection nodes. Application of the proposed multi-mode coherent states enables the legitimate users to extract information, while an eavesdropper does not obtain any information about encoded bits due to ambiguity of detection events.

Keywords

quantum communications, coherent states, interference, phase modulated radiation

Acknowledgements

This work was financially supported by the Government of the Russian Federation (Grant 08-08).

Введение

Системы квантовой коммуникации позволяют распределять симметричные битовые последовательности, которые могут быть использованы для кодирования информации, требующей высокой степени защищенности, между легитимными пользователями, обычно именуемыми Алиса (отправитель) и Боб (получатель). Благодаря использованию одиночных фотонов и их свойств для формирования этих последовательностей любые попытки злоумышленника, обычно именуемого Евой, незаметно получить ключевую информацию становятся невозможными [1]. Однако отличие практических реализаций таких систем и устройств в их составе от идеальных моделей позволяет разрабатывать методы, способствующие злоумышленнику получить часть, либо полностью весь ключ. Такой подход получил называние квантовый взлом [2]. Одним из таких устройств является детектор одиночных фотонов (ДОФ), который используется для регистрации оптических импульсов, полученных в результате интерференции квантовых состояний. Основные типы применяемых детекторов на базе лавинных фотодиодов и структур, работающих в режиме сверхпроводимости, потенциально уязвимы к атакам с «ослеплением» (выведением из режима счета фотонов) [3–5]. Ввиду этого предложен ряд контрмер, однако в лабораториях, занимающихся квантовым взломом, исследованы не были [6, 7]. Принципиально иным решением данной проблемы является протокол, устойчивый к атакам на измерительном оборудовании MDI (measurement-device independent) [8]. Его реализация представляет собой более сложную инженерную задачу по сравнению с обычными системами квантового распределения ключа (КРК), но эффективно противодействует атакам с навязыванием ключа посредством управления ДОФ [9].

Метод квантовой коммуникации на боковых частотах

Метод квантовой коммуникации, в котором квантовые состояния формируются в результате фазовой модуляции высокоинтенсивной оптической центральной частоты, был предложен [10] и исследовался на возможности по спектральному уплотнению каналов [11, 12], а также на достижение основных параметров, соответствующих мировому уровню [13, 14], и обоснования степени секретности используемого протокола [15, 16]. Исследование устойчивости к возможным атакам злоумышленника проводилось как с теоретической точки зрения [17, 18], так и с практической — исследовался применяемый детектор, функционирующий на основе пробоя в лавинном фотодиоде, и возможные типы атак на систему с таким типом детекторов [19]. Однако возможность построения схемы и реализации протокола, устойчивого к атакам на измерительное оборудование за счет вынесения его в недоверенный узел, исследовано не было. В случае вынесения измерительного оборудования в недоверенный узел требуется формировать сигналы, а также модулировать их независимо Алисой и Бобом. Недоверенный узел включает в себя светоделитель для формирования картины интерференции импульсов, приходящих от легитимных пользователей, выходы которого подключены к детекторам одиночных фотонов. Покажем, как формируются состояния в классическом приближении.

Аналитически работа модуляторов описывается следующим образом. Пусть высокоинтенсивная оптическая центральная частота задана выражением $Ae^{i\omega t}$ (A — амплитуда, ω — частота несущей). После модуляции в блоке Алисы при малой амплитуде модулирующего сигнала m, используя разложение Якоби–Ангера, получаем сигнал:

$$E = Ae^{i\omega t}e^{ia\sin(\Omega t+\varphi_a)} = Ae^{i\omega t}\sum_{n=-\infty}^{\infty} J_n(m)e^{i(\Omega t+\varphi_a)n}, \quad (1)$$

где Ω — частота модулирующего сигнала, m — индекс модуляции, φ_a — фаза модулирующего сигнала, вводимая на стороне отправителя, $J_n(m)$ — функция Бесселя первого рода, n — номер моды. Из выражения (1) видно, что в результате модуляции вдобавок к основной частоте ω в спектре появляются сигналы на боковых частотах $\omega + n\Omega$ и $\omega - n\Omega$ по обе стороны от центральной частоты.

Исследование зависимости результата интерференции многомодовых когерентных состояний от разности фаз модулирующих сигналов

В случае вынесения измерительного оборудования в недоверенный узел требуется формировать сигналы, а также модулировать их независимо Алисой (a) и Бобом (b). Соответствующие сигналы имеют следующий вид:

$$E_a = Ae^{i\omega t}\sum_n J_n(m)e^{i(\Omega t+\varphi_a)n}, \quad (2)$$

$$E_b = Ae^{i\omega t}\sum_n J_n(m)e^{i(\Omega t+\varphi_b)n}. \quad (3)$$

Для удобства приведем (2) и (3) к виду, где явно вынесена компонента, зависящая от фазы модулирующего сигнала φ_a и φ_b:

$$E_a = \sum_n AJ_n(m)e^{i(\omega+\Omega n)t}e^{i\varphi_a n}, \quad (4)$$

$$E_b = \sum_n AJ_n(m)e^{i(\omega+\Omega n)t}e^{i\varphi_b n}. \quad (5)$$

Для формирования картины интерференции импульсов, приходящих от легитимных пользователей, недоверенный узел включает в себя светоделитель, выходы которого подключены к измерителям оптической мощности. Очевидно, что между несущими частотами будет также наблюдаться разность фаз φ_0, влияющая на картину интерференции. Амплитуда сигналов (4) и (5), поступающих на измерители, приобретает следующий вид в результате интерференции:

$$E_{ab} = \sum_n \frac{AJ_n(m)e^{i(\omega+\Omega n)t}}{\sqrt{2}}(e^{i\varphi_a n} \pm e^{i\varphi_b n}e^{i\varphi_0}). \quad (6)$$

Видно, что члены ряда зависят от фаз, которые вносились Алисой и Бобом. Измерительные приборы фиксируют модуль квадрата амплитуды входящего сигнала на боковых частотах после вырезания спектральным фильтром центральной несущей частоты, так что в зависимости от разности фаз $\Delta\varphi = \varphi_b - \varphi_a$ и, с учетом потерь в квантовом канале и квантовой эффективности (η_c) измерителей оптического сигнала мы получим:

$$P(\Delta\varphi) = \eta_c|A|^2\left(1 - \left(1 \mp \cos(\varphi_0)\right)J_0(m)^2 \pm \cos(\varphi_0)J_0(m\sqrt{2(1+\cos(\Delta\varphi))})\right). \quad (7)$$

Определим величину сигнала на боковых частотах Алисы и Боба следующим образом:

$$\mu = |A|^2(1 - J_0(m)^2). \quad (8)$$

Так как значение нулевой моды функции Бесселя равно:

$$J_0(m)^2 = 1 - \frac{m^2}{2}, \quad (9)$$

то при индексе модуляции $m < 1$ выражение (6) принимает вид:

$$\mu = |A|^2\frac{m^2}{2}. \quad (10)$$

Используя (8), (9) и (10), выражение (7) для мощностей, наблюдаемых на выходах светоделителя в результате интерференции многомодовых состояний, приходим к следующему выражению:

$$P(\Delta\varphi) = \mu\eta_c(1 \pm \cos(\Delta\varphi)\cos(\varphi_0)). \quad (11)$$

Видно, что мощность в результате интерференции зависит от разности фаз модулирующих сигналов и от фазы оптического сигнала несущей частоты Алисы относительно несущей частоты Боба.

Экспериментальное исследование

Для проведения экспериментальной проверки была собрана оптическая схема (рис. 1). В ходе эксперимента измерения проводились в классическом режиме с помощью измерителей оптической мощности. В качестве источника оптической несущей использовался лазер Л1 с распределенной обратной связью (DFB) с брэгговской решеткой, отличительной особенностью которого является достаточно узкая спектральная полоса излучения (меньше 100 кГц) и возможность перестройки с шагом в 100 МГц в С-диапазоне оптического спектра (191–196 ТГц). Это требуется для подстройки под полосу отражения оптических фильтров на измерительном узле. Для снижения обратных отражений от оптических компонент после Л1 устанавливался оптический изолятор И на основе эффекта Фарадея с величиной изоляции 50 дБ. Так как в рамках иссле-

дования для упрощения подстройки несущих частот Алисы и Боба используется один лазерный источник, то его излучения делятся пополам на 50:50 светоделителе СД1. Далее в результате фазовой модуляции на стороне Алисы и на стороне Боба в спектре на выходе с ФМ1 и ФМ2 соответственно формируются боковые частоты. Частота модулирующего синусоидального сигнала $\Omega = 4{,}8$ ГГц, а амплитуда и фазовый сдвиг формировался при помощи двух цифро-аналоговых преобразователей (ЦАП1 и ЦАП2 соответственно). На входы ЦАПов подавались в цифровом шестнадцатеричном виде сигналы пары квадратурных компонент I и Q в виде таблиц, сформированных в памяти модуля программируемой логической интегральной схемы (ПЛИС). При этом параметры подбирались таким образом, чтобы соотношение боковых к центральной составляло порядка 5 %. Данные оптические сигналы поступали в волоконно-оптическую линию связи и отправлялись на измерительный узел, где сбивались друг с другом на четырехпортовом 50:50 светоделителе СД2, в результате чего наблюдалась их интерференция на измерителях оптической мощности Д1 и Д3. При этом один из измерителей мощности Д2 служил для сигнала обратной связи на ГЕН1 в целях подстройки оптической фазы несущей частоты между двумя плечами с помощью ФМ3 и ФМ4 (рис. 2). Когда разность оптических фаз была скомпенсирована, и центральная мода постоянно наблюдалась в одном из выходных плеч на измерителе оптической мощности Д2, в ручном режиме последовательно производилась смена фазовых состояний радиочастотных модулирующих сигналов посредством изменения значений фазового сдвига при неизменной амплитуде в IQ-таблице ЦАПов с шагом 10°.

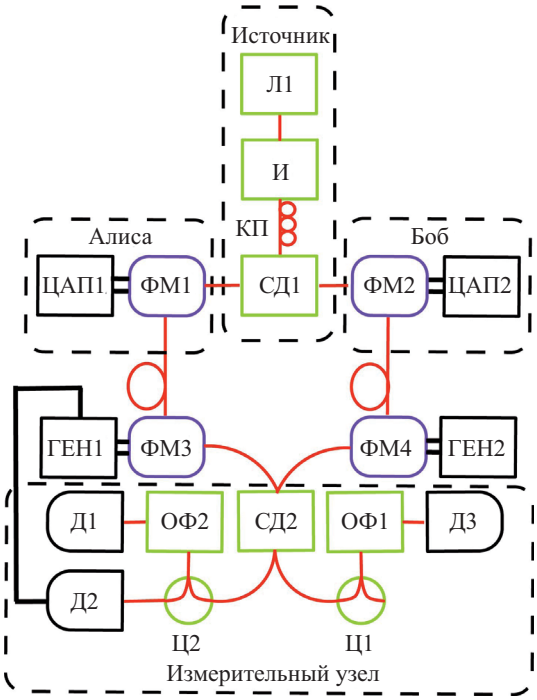

Рис. 1. Схема эксперимента: Л1 — лазерный источник излучения, И — оптический изолятор, КП — контроллер поляризации, СД — оптический светоделитель, ФМ — электрооптический фазовый модулятор, ЦАП — цифро-аналоговый преобразователь, ГЕН — генератор сигналов произвольной формы, Ц — оптический циркулятор, ОФ — оптический фильтр, Д — детектор

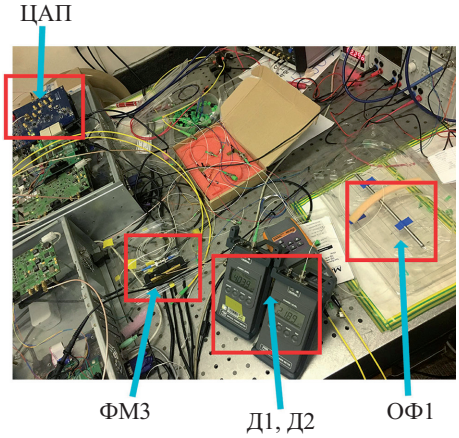

Рис. 2. Фото экспериментального стенда

В результате наблюдалась зависимость, показанная на рис. 3. Значение конструктивной интерференции на первом детекторе составило величину $I_{max} = 6{,}3$, а деструктивной — $I_{min} = 0{,}2$ мкВт, тогда как на втором $I_{max} = 6{,}13$ и $I_{min} = 0{,}08$ мкВт соответственно.

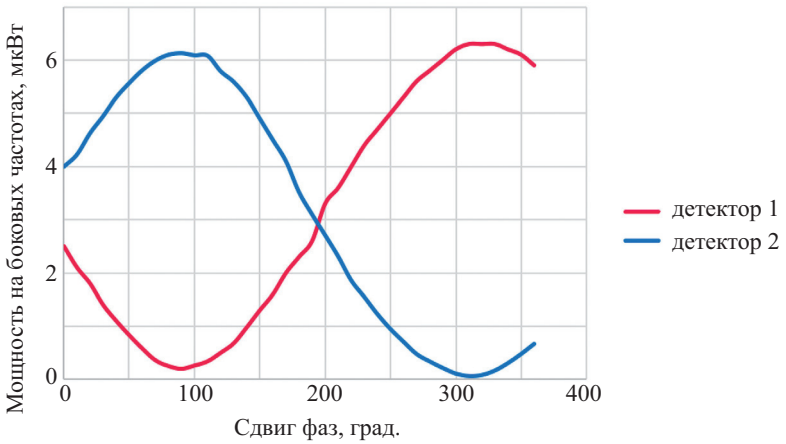

Рис. 3. Зависимость мощности оптического сигнала на боковых частотах в результате интерференции от разности фаз модулирующих сигналов

Если определить отношение I_{max} к I_{min} как контраст, то в первом плече контраст был равен 31,5, а во втором — 76,6. Такое различие связано в первую очередь с трудностью подстройки длины волны Л1 под два независимых спектральных фильтра ОФ1 и ОФ2 и, как следствие, засветкой от центральной несущей. Видность интерференционной картины определяется как:

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}}.$$

В первом случае видность составила $V1 = 93{,}8$ %, а во втором — $V2 = 97{,}4$ %. Значение видности интерференционной картины вносит значительный вклад в квантовый коэффициент ошибок по битам (QBER), который характеризует функционирование системы в целом и является критерием для оценки наличия злоумышленника в канале.

Таким образом, показано, что экспериментально полученные зависимости (рис. 3) соответствуют по форме полученным аналитически зависимостям (11).

Заключение

Показана принципиальная возможность осуществления протокола квантовой коммуникации на боковых частотах, устойчивого к воздействию злоумышленника на измерительное оборудование. Приведено теоретическое подтверждение в терминах классической оптики того, что интерференция состояний на боковых частотах фазомодулированного излучения в недоверенном узле позволяет фиксировать коррелирующие фазовые состояния у легитимных пользователей, при том что наличие доступа у злоумышленника к этому узлу не дает возможность получить ключевую информацию. Предложена экспериментальная схема, и в классическом режиме получена картина интерференции в зависимости от разности фаз модулирующих сигналов в блоках легитимных пользователей.

Литература

1. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир, 2006. 824 с.
2. Jain N., Anisimova E., Khan I., Makarov V., Marquardt C., Leuchs G. Trojan-horse attacks threaten the security of practical quantum cryptography // New Journal of Physics. 2014. V. 16. P. 123030. doi: 10.1088/1367-2630/16/12/123030
3. Makarov V., Hjelme D.R. Faked states attack on quantum cryptosystems // Journal of Modern Optics. 2005. V. 52. N 5. P. 691–705. doi: 10.1080/09500340410001730986
4. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination // Nature Photonics. 2010. V. 4. N 10. P. 686–689. doi: 10.1038/nphoton.2010.214

References

1. Nielsen M.A., Chuang I.L. *Quantum computation and quantum information*. Cambridge University Press, 2000, 676 p.
2. Jain N., Anisimova E., Khan I., Makarov V., Marquardt C., Leuchs G. Trojan-horse attacks threaten the security of practical quantum cryptography. *New Journal of Physics*, 2014, vol. 16, pp. 123030. doi: 10.1088/1367-2630/16/12/123030
3. Makarov V., Hjelme D.R. Faked states attack on quantum cryptosystems. *Journal of Modern Optics*, 2005, vol. 52, no. 5, pp. 691–705. doi: 10.1080/09500340410001730986
4. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 2010, vol. 4, no. 10, pp. 686–689. doi: 10.1038/nphoton.2010.214

5. Lydersen L., Akhlaghi M.K., Majedi A.H., Skaar J., Makarov V. Controlling a superconducting nanowire single-photon detector using tailored bright illumination // New Journal of Physics. 2011. V. 13. P. 113042. doi: 10.1088/1367-2630/13/11/113042
6. Honjo T., Fujiwara M., Shimizu K., Tamaki K., Miki S., Yamashita T., Terai H., Wang Z., Sasaki M. Countermeasure against tailored bright illumination attack for DPS-QKD // Optics Express. 2013. V. 21. N 3. P. 2667–2673. doi: 10.1364/OE.21.002667
7. Koehler-Sidki A., Dynes J.F., Lucamarini M., Roberts G.L., Sharpe A.W., Yuan Z.L., Shields A.J. Best-practice criteria for practical security of self-differencing avalanche photodiode detectors in quantum key distribution // Physical Review Applied. 2018. V. 9. N 4. P. 044027. doi: 10.1103/PhysRevApplied.9.044027
8. Lo H.-K., Curty M., Qi B. Measurement-Device-Independent Quantum Key Distribution // Physical Review Letters. 2012. V. 108. N 13. P. 130503. doi: 10.1103/PhysRevLett.108.130503
9. Liu Y., Chen T.-Y., Wang L.-J., Liang H., Shentu G.-L., Wang J., Cui K., Yin H.-L., Liu N.-L., Li L., Ma X., Pelc J.S., Fejer M.M., Peng C.-Z., Zhang Q., Pan J.-W. Experimental measurement-device-independent quantum key distribution // Physical Review Letters. 2013. V. 111. N 13. P. 130502. doi: 10.1103/PhysRevLett.111.130502
10. Мазуренко Ю.Т., Меролла Ж.-М., Годжебюр Ж.-П. Квантовая передача информации с помощью поднесущей частоты. Применение к квантовой криптографии // Оптика и спектроскопия. 1999. Т. 86. № 2. С. 181–183.
11. Capmany J. Photon nonlinear mixing in subcarrier multiplexed quantum key distribution systems // Optics Express. 2009. V. 17. N 8. P. 6457–6464. doi: 10.1364/OE.17.006457
12. Capmany J., Ortigosa-Blanch A., Mora J., Ruiz-Alba A., Amaya W., Martínez A. Analysis of Subcarrier Multiplexed Quantum Key Distribution Systems: Signal, Intermodulation, and Quantum Bit Error Rate // IEEE Journal on Selected Topics in Quantum Electronic. 2009. V. 15. N 6. P. 1607–1621. doi: 10.1109/JSTQE.2009.2031065
13. Gleim A.V., Egorov V.I., Nazarov Y.V., Smirnov S.V., Chistyakov V.V., Bannik O.I., Anisimov A.A., Kynev S.M., Ivanova A.E., Collins R.J., Kozlov S.A., Buller G. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference // Optics express. 2016. V. 24. N 3. P. 2619–2633. doi: 10.1364/OE.24.002619
14. Gleim A.V., Chistyakov V.V., Bannik O.I., Egorov V.I., Buldakov N.V., Vasilev A.B., Gaidash A.A., Kozubov A.V., Smirnov S.V., Kynev S.M., Khoruzhnikov S.E., Kozlov S.A., Vasil'ev V.N. Sideband quantum communication at 1 Mbit/s on a metropolitan area network // Journal of Optical Technology. 2017. V. 84. N 6. P. 362–367. doi: 10.1364/JOT.84.000362
15. Gaidash A.A., Kozubov A.V., Chistyakov V.V., Miroshnichenko G.P., Egorov V.I., Gleim A.V. Security conditions for sub-carrier wave quantum key distribution protocol in errorless channel // Journal of Physics: Conference Series. 2017. V. 917. N 6. P. 062014. doi: 10.1088/1742-6596/917/6/062014
16. Kozubov A., Gaidash A., Miroshnichenko G. Finite-key security for quantum key distribution systems utilizing weak coherent states. arXiv preprint // arXiv:1903.04371. 2019.
17. Miroshnichenko G.P., Kozubov A.V., Gaidash A.A., Gleim A.V., Horoshko D.B. Security of subcarrier wave quantum key distribution against the collective beam-splitting attack // Optics express. 2018. V. 26. N 9. P. 11292–11308. doi: 10.1364/OE.26.011292
18. Gaidash A., Kozubov A., Miroshnichenko G. Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems // Journal of the Optical Society of America B: Optical Physics. 2019. V. 36. N 3. P. B16–B19. doi: 10.1364/JOSAB.36.000B16
19. Chistiakov V., Huang A., Egorov V., Makarov V. Controlling single-photon detector ID210 with bright light // Optics Express (in print).

5. Lydersen L., Akhlaghi M.K., Majedi A.H., Skaar J., Makarov V. Controlling a superconducting nanowire single-photon detector using tailored bright illumination. *New Journal of Physics*, 2011, vol. 13, pp. 113042. doi: 10.1088/1367-2630/13/11/113042
6. Honjo T., Fujiwara M., Shimizu K., Tamaki K., Miki S., Yamashita T., Terai H., Wang Z., Sasaki M. Countermeasure against tailored bright illumination attack for DPS-QKD. *Optics Express*, 2013, vol. 21, no. 3, pp. 2667–2673. doi: 10.1364/OE.21.002667
7. Koehler-Sidki A., Dynes J.F., Lucamarini M., Roberts G.L., Sharpe A.W., Yuan Z.L., Shields A.J. Best-practice criteria for practical security of self-differencing avalanche photodiode detectors in quantum key distribution. *Physical Review Applied*, 2018, vol. 9, no. 4, pp. 044027. doi: 10.1103/PhysRevApplied.9.044027
8. Lo H.-K., Curty M., Qi B. Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*, 2012, vol. 108, no. 13, pp. 130503. doi: 10.1103/PhysRevLett.108.130503
9. Liu Y., Chen T.-Y., Wang L.-J., Liang H., Shentu G.-L., Wang J., Cui K., Yin H.-L., Liu N.-L., Li L., Ma X., Pelc J.S., Fejer M.M., Peng C.-Z., Zhang Q., Pan J.-W. Experimental measurement-device-independent quantum key distribution. *Physical Review Letters*, 2013, vol. 111, no. 13, pp. 130502. doi: 10.1103/PhysRevLett.111.130502
10. Mazurenko Yu.T., Merolla J.-M., Godgebur J.-P. Quantum transmission of information with the help of subcarrier frequency. Application to quantum cryptography. *Optics and Spectroscopy*, 1999, vol. 86, no. 2, pp. 145–147.
11. Capmany J. Photon nonlinear mixing in subcarrier multiplexed quantum key distribution systems. *Optics Express*, 2009, vol. 17, no. 8, pp. 6457–6464. doi: 10.1364/OE.17.006457
12. Capmany J., Ortigosa-Blanch A., Mora J., Ruiz-Alba A., Amaya W., Martínez A. Analysis of Subcarrier Multiplexed Quantum Key Distribution Systems: Signal, Intermodulation, and Quantum Bit Error Rate. *IEEE Journal on Selected Topics in Quantum Electronic*, 2009, vol. 15, no. 6, pp. 1607–1621. doi: 10.1109/JSTQE.2009.2031065
13. Gleim A.V., Egorov V.I., Nazarov Y.V., Smirnov S.V., Chistyakov V.V., Bannik O.I., Anisimov A.A., Kynev S.M., Ivanova A.E., Collins R.J., Kozlov S.A., Buller G. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. *Optics express*, 2016, vol. 24, no. 3, pp. 2619–2633. doi: 10.1364/OE.24.002619
14. Gleim A.V., Chistyakov V.V., Bannik O.I., Egorov V.I., Buldakov N.V., Vasilev A.B., Gaidash A.A., Kozubov A.V., Smirnov S.V., Kynev S.M., Khoruzhnikov S.E., Kozlov S.A., Vasil'ev V.N. Sideband quantum communication at 1 Mbit/s on a metropolitan area network. *Journal of Optical Technology*, 2017, vol. 84, no. 6, pp. 362–367. doi: 10.1364/JOT.84.000362
15. Gaidash A.A., Kozubov A.V., Chistyakov V.V., Miroshnichenko G.P., Egorov V.I., Gleim A.V. Security conditions for sub-carrier wave quantum key distribution protocol in errorless channel. *Journal of Physics: Conference Series*, 2017, vol. 917, no. 6, pp. 062014. doi: 10.1088/1742-6596/917/6/062014
16. Kozubov A., Gaidash A., Miroshnichenko G. Finite-key security for quantum key distribution systems utilizing weak coherent states. arXiv preprint. *arXiv:1903.04371*, 2019.
17. Miroshnichenko G.P., Kozubov A.V., Gaidash A.A., Gleim A.V., Horoshko D.B. Security of subcarrier wave quantum key distribution against the collective beam-splitting attack. *Optics express*, 2018, vol. 26, no. 9, pp. 11292–11308. doi: 10.1364/OE.26.011292
18. Gaidash A., Kozubov A., Miroshnichenko G. Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems. *Journal of the Optical Society of America B: Optical Physics*, 2019, vol. 36, no. 3, pp. B16–B19. doi: 10.1364/JOSAB.36.000B16
19. Chistiakov V., Huang A., Egorov V., Makarov V. Controlling single-photon detector ID210 with bright light. *Optics Express* (in print).

Авторы

Чистяков Владимир Викторович — инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56400453700, ORCID ID: 0000-0002-2414-3490, v_chistyakov@itmo.ru

Гайдаш Андрей Алексеевич — инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56400865700, ORCID ID: 0000-0001-9870-9285, andrewdgk@gmail.com

Козубов Антон Владимирович — инженер, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 57035361700, ORCID ID: 0000-0002-4468-5406, kozubov.anton@gmail.com

Глейм Артур Викторович — кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56316444200, ORCID ID: 0000-0003-2307-5454, agleim@itmo.ru

Authors

Vladimir V. Chistiakov — Engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56400453700, ORCID ID: 0000-0002-2414-3490, v_chistyakov@itmo.ru

Andrei A. Gaidash — Engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56400865700, ORCID ID: 0000-0001-9870-9285, andrewdgk@gmail.com

Anton V. Kozubov — Engineer, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 57035361700, ORCID ID: 0000-0002-4468-5406, kozubov.anton@gmail.com

Artur V. Gleim — PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56316444200, ORCID ID: 0000-0003-2307-5454, agleim@itmo.ru