конференция
РусКрипто

Ежегодная международная научно-практическая конференция
«РусКрипто'2022»

Квантовое распределение ключей на непрерывных переменных

Э.О. Самсонов, Р.К. Гончаров

ООО «СМАРТС-Кванттелеком»
Университет ИТМО

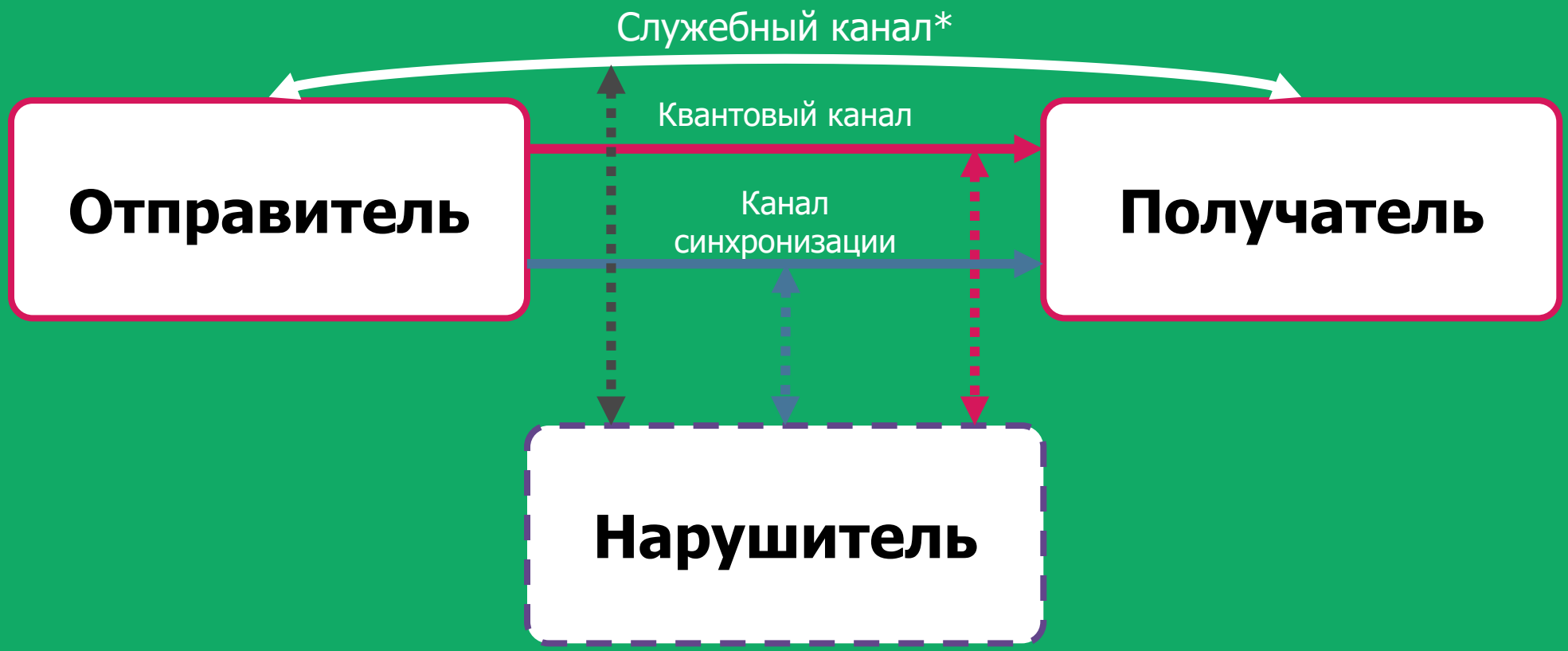
Содержание

- Квантовое распределение ключей. Общий подход
- Квантовое распределение ключей на непрерывных переменных
- Протокол GG02 (гауссовская модуляция)
- Протоколы с дискретной модуляцией
- Прочие реализации КРКНП
- Разработки Университета ИТМО и ООО «СМАРТС-Кванттелеком»

Квантовое распределение ключей

Квантовое распределения ключей (КРК) — это совокупность методов, позволяющих распределить симметричную битовую последовательность посредством кодирования информации внутри квантовых объектов.

Квантовое распределение ключей



*Служебный канал КРК должен быть аутентифицирован и имитозащищён

Квантовое распределение ключей

Квантовое распределение ключей

- стойкое симметричное шифрование;
- быстрый обмен ключами

Квантовая цифровая подпись

- повышение стойкости протоколов цифровой подписи

Квантовое обязательство

- абсолютно стойкая фиксация заданного сообщения

Индустриальная интеграция

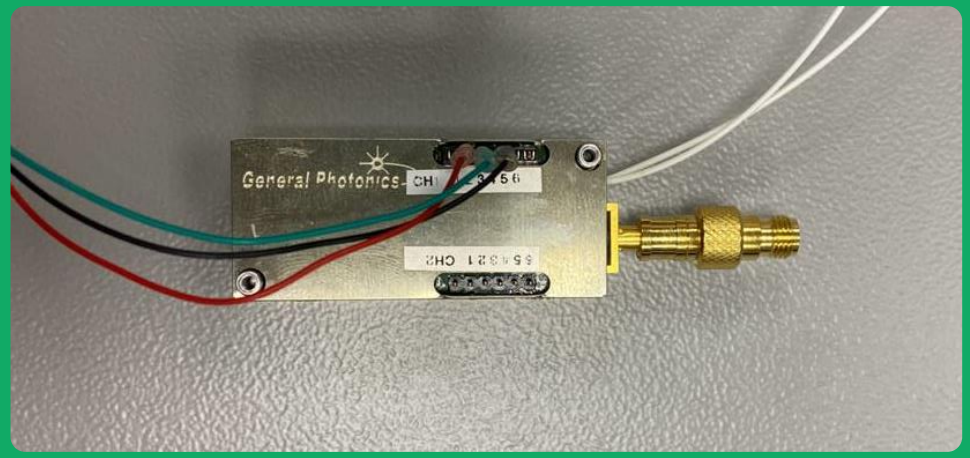
- волоконные системы;
- в свободном пространстве

Лабораторная разработка и демонстрация

- решение проблем стойкости;
- дополнительные этапы в ходе реализации протоколов по сравнению с классическими;
- часто необходима квантовая память

Квантовое распределение ключей

дискретные переменные (ДП)
→
непрерывные переменные (НП)



Малые размеры приёмного модуля

Низкая стоимость

Стандартные телекоммуникационные компоненты

Лучшая производительность на малых расстояниях

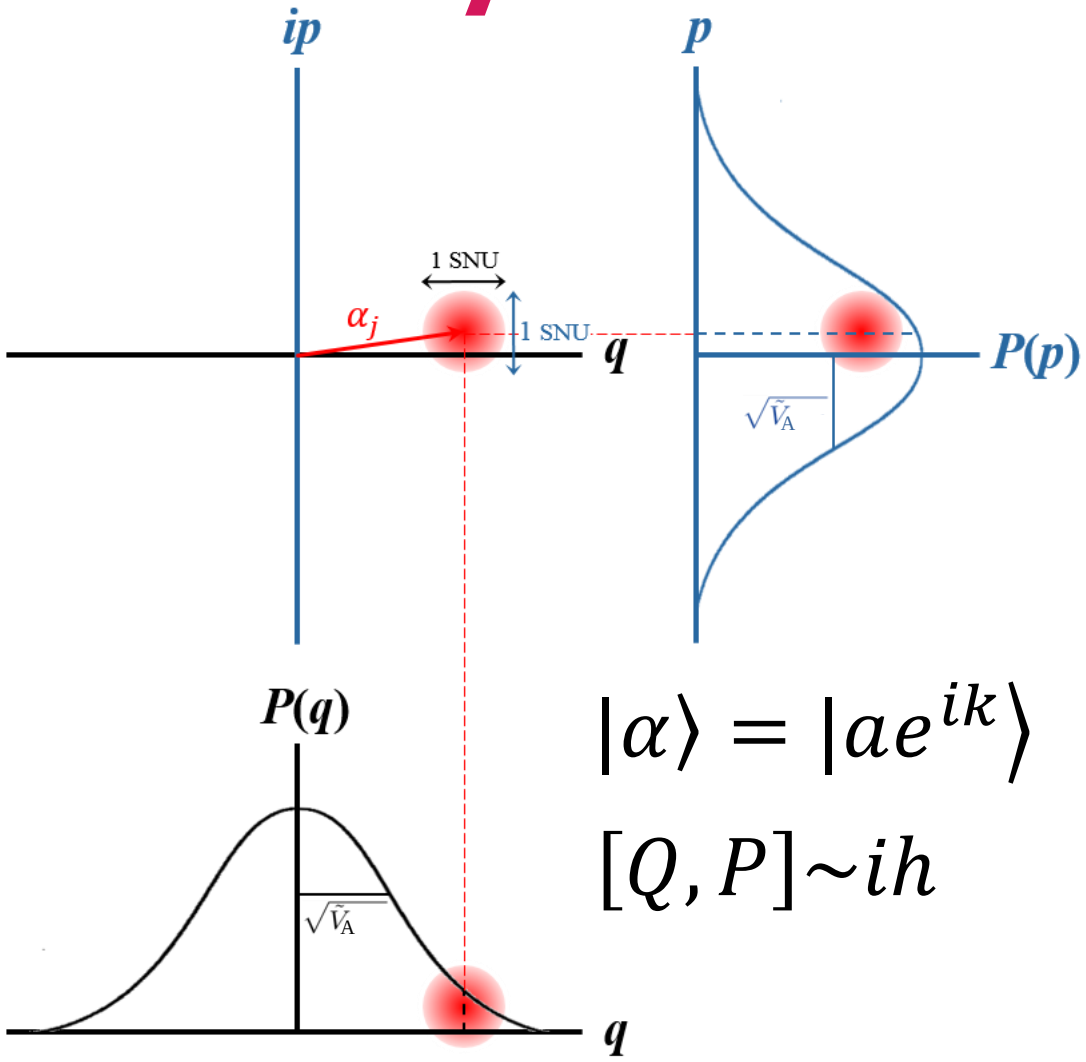
Протоколы КРКДП и КРКНП

Характеристики	КРКДП	КРКНП
Метод кодирования	поляризационное, фазовое, по времени	по квадратурам
Детектирование	детекторы одиночных фотонов	когерентное
Постпроцессинг	генерируется двоичная последовательность	комплексная постобработка в общем случае
Анализ стойкости протоколов	когерентные атаки, конечные ключи, атаки на каналы утечки	когерентные атаки, конечные ключи, атаки на каналы утечки
Протоколы	BB84 (в т.ч. decoy state), COW, DPS, MDI, TF	с дискретной модуляцией, с гауссовской модуляцией (GG02), MDI-КРКНП, TF-КРКНП

КРКНП. Классификация

Классификация	Предмет
по основному сценарию протокола	«приготовление-детектирование»; «основанный на запутанности»
по реализации квантового канала	оптоволокно; свободное пространство
по проходности	однопроходные; двупроходные
по типу модуляции	гауссовская; негауссовская
по сигнальным состояниям	одномодовые сжатые; одномодовые когерентные; многомодовые когерентные; двумодовые сжатые; тепловые
по типу когерентного детектирования	гомодинное; гетеродинное (двойное гомодинное); гетеродинное с переносом частоты
по реализации ЛО	на стороне отправителя; на стороне получателя
по типу согласования ключа	прямое; обратное

GG02. Гауссовская модуляция



$$|\alpha\rangle = |ae^{ik}\rangle$$

$$[Q, P] \sim ih$$

Генерация посылок:

$$Q \sim \mathcal{P} \sim \mathcal{N}(0, V_A),$$
$$a|\alpha_j\rangle = \alpha_j|\alpha_j\rangle,$$
$$\frac{1}{2}(q + ip)|\alpha_j\rangle = (q_j + ip_j)|\alpha_j\rangle,$$
$$q_j \in Q, p_j \in \mathcal{P}.$$

Итоговое двумерное гауссовское распределение — это распределение по ансамблю всех посылок

Дисперсия распределения объявляется публично.

Неизбежен вакуумный шум

Laudenbach F. et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations // Advanced Quantum Technologies. – 2018. – Т. 1. – №. 1. – С. 1800011.

GG02. Оптическая схема

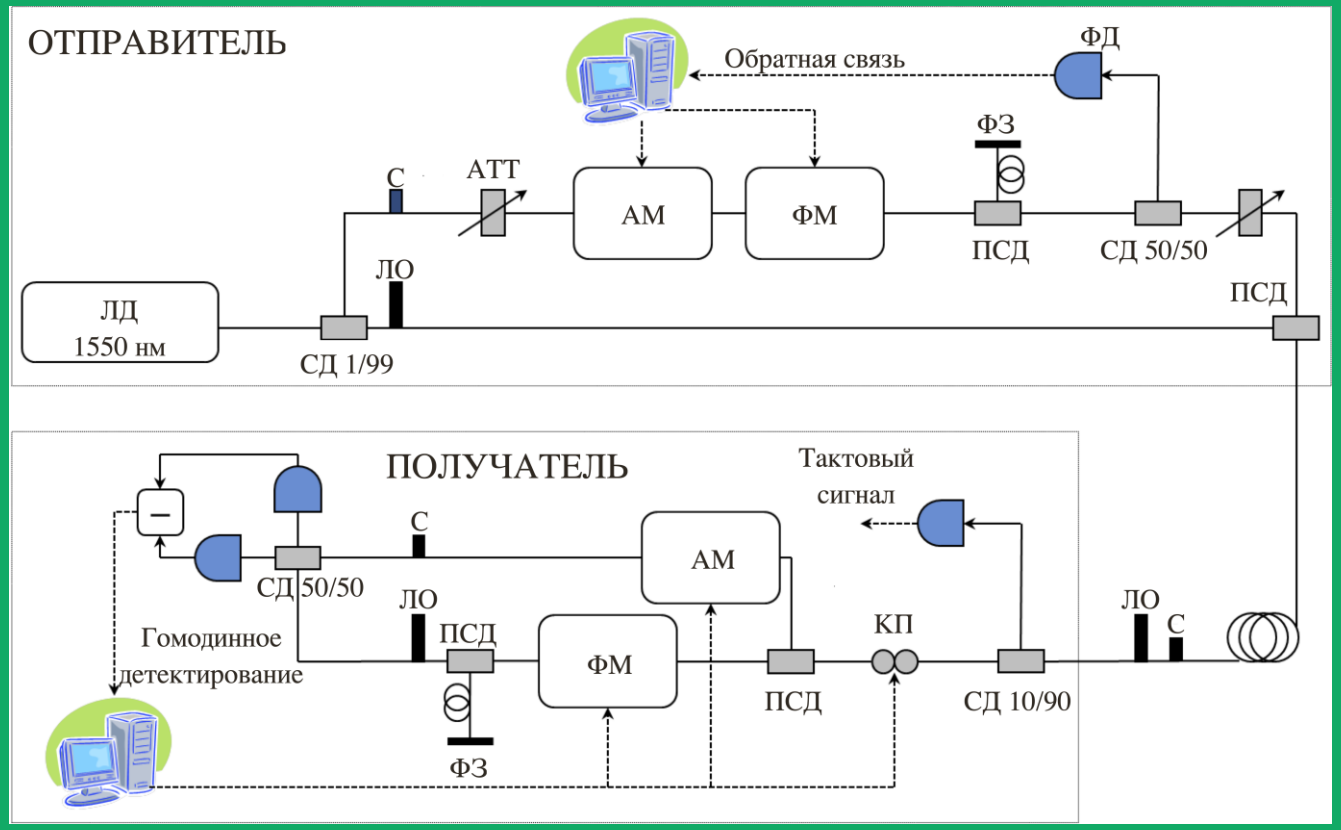


Схема установки КРКНП (GG02) с гомодинным детектированием

ЛД — лазерный диод;
(П)СД — (поляризационный) светоделитель;
С — сигнал;
ЛО — локальный осциллятор;
АТТ — аттенюатор;
АМ — амплитудный модулятор;
ФМ — фазовый модулятор;
ФЗ — фарадеевское зеркало;
ФД — фотодиод;
КП — контроллер поляризации

Jouguet P., Kunz-Jacques S., Leverrier A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation // Physical Review A. – 2011. – Т. 84. – №. 6. – С. 062317.

GG02. Постобработка

Оценка параметров

после накопления посылок отправитель и получатель оценивают параметры канала

Согласование

- многоуровневое кодирование;
- многомерное согласование

Исправление ошибок

- полярные коды;
- LDPC коды (MET, Raptor)

Усиление стойкости

2-универсальное хеширование с заданной моделью выходной длиной

GG02. Постобработка

Статус: обоснована стойкость против когерентных (общих) атак

Энтропийные соотношения неопределённости

дискретизация квадратур сжатых состояний $\rightarrow Q_\delta, P_\delta$

$$H^\varepsilon_{min}(Q_\delta|E)_{\rho^n} + H^\varepsilon_{min}(P_\delta|B)_{\rho^n} \geq -\log \frac{\delta}{2\pi} S_0^{(1)}\left(1, \frac{\delta^2}{4}\right)^2$$

Гауссовская теорема де Финетти

1. симметризация $\rho^n \rightarrow \rho_{\mathrm{G}}^{\otimes n}$
2. равнораспределённость $H^\varepsilon_{min}(Q_\delta|E)_{\rho_{\mathrm{G}}^{\otimes n}} \approx nH(Q_\delta|E)_{\rho^n}$
3. информация $H^\varepsilon_{min}(Q_\delta|E)_{\rho_{\mathrm{G}}} = H(Q_\delta) - \chi(Q_\delta; E)_{\rho_{\mathrm{G}}}$
4. оценка ковариационной матрицы $\rightarrow$ граница для $\chi(Q_\delta; E)_{\rho_{\mathrm{G}}}$

Furrer F. et al. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks // Physical Review Letters. – 2012. – Т. 109. – №. 10. – С. 100502.
Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction // Physical Review Letters. – 2017. – Т. 118. – №. 20. – С. 200501.

GG02. Постобработка

Статус: обоснована стойкость против когерентных (общих) атак

Энтропийные соотношения неопределённости

- пессимистичная оценка производительности;
- только для сжатых сигнальных состояний

Гауссовская теорема де Финетти

- необходимость симметризации (только гетеродинирование);
- требуется большое число посылок;
- жёсткие критерии стойкости

Furrer F. et al. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks // Physical Review Letters. – 2012. – Т. 109. – №. 10. – С. 100502.
Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction // Physical Review Letters. – 2017. – Т. 118. – №. 20. – С. 200501.

КРКНП с дискретной модуляцией

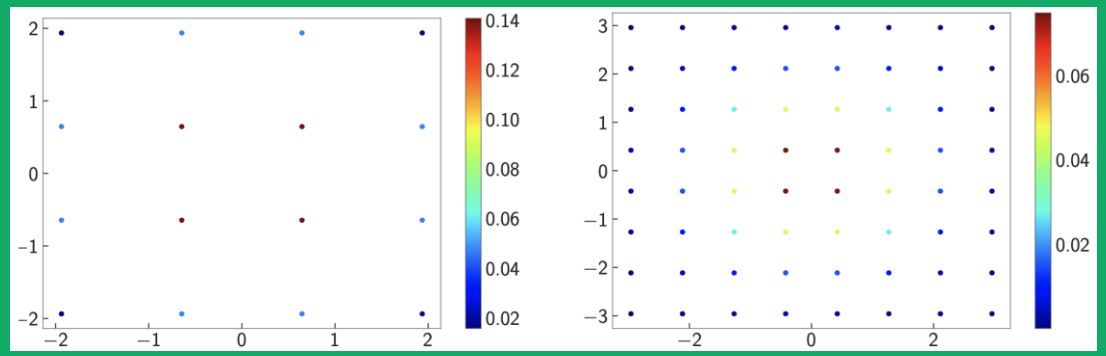
Проще реализация

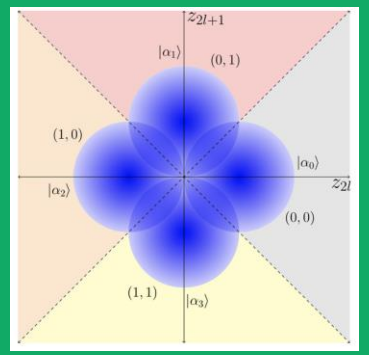
Проще коррекция ошибок

Статус: задача о доказательстве стойкости не решена

Негауссовость не позволяет оценить корреляции аналитически

Методы полуопределённого программирования

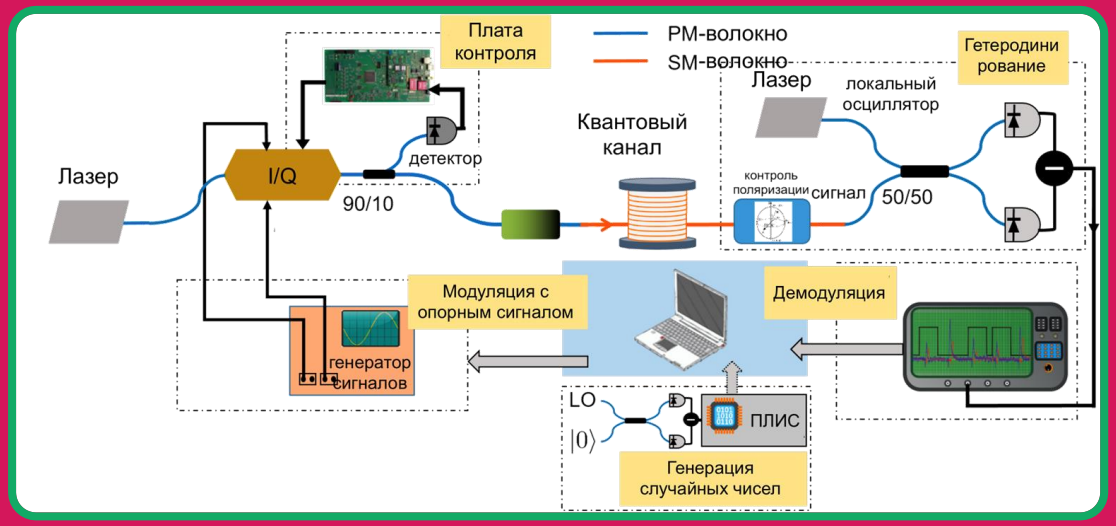




Lin J., Upadhyaya T., Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution // Physical Review X. - 2019. - Т. 9. - №. 4. - С. 041064.

Denys A., Brown P., Leverrier A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation //Quantum. - 2021. - Т. 5. - С. 540.

Прочие реализации КРКНП

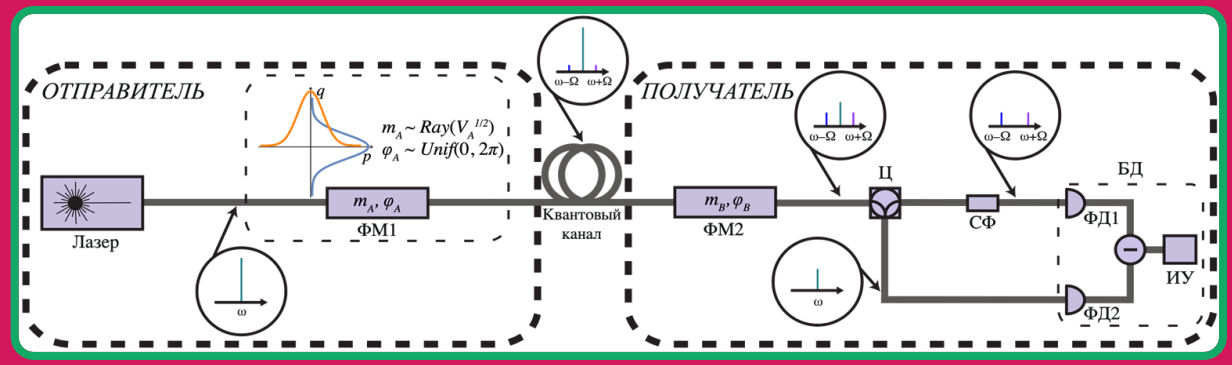


КРКНП с генерацией локального осциллятора на стороне получателя

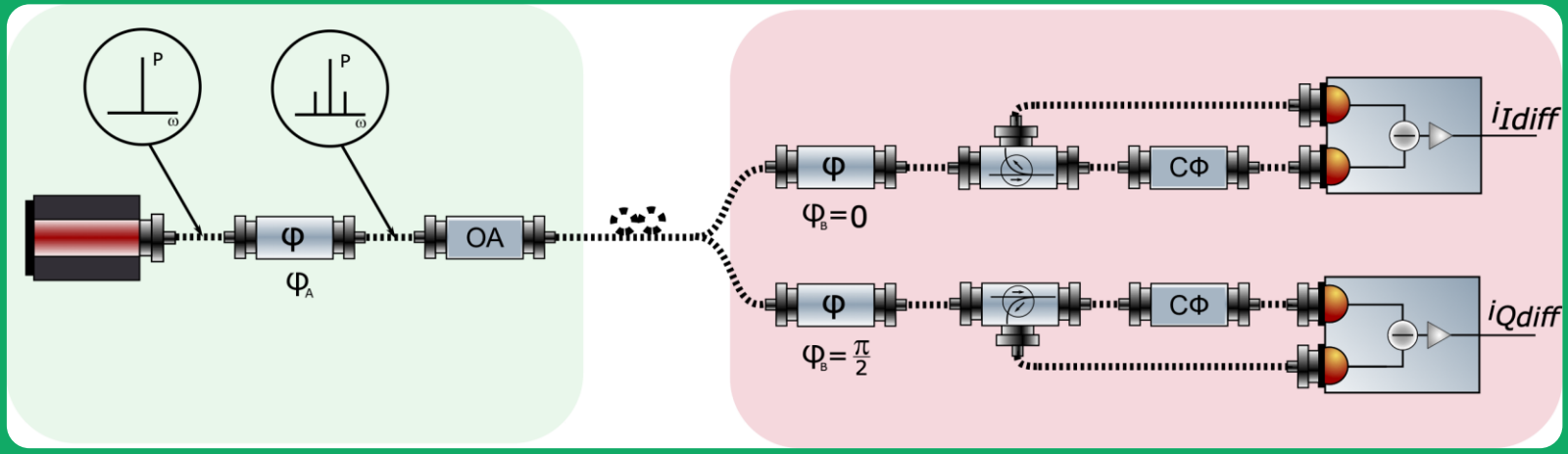
Jain N. et al. Practical continuous-variable quantum key distribution with composable security // arXiv preprint arXiv:2110.09262. – 2021.

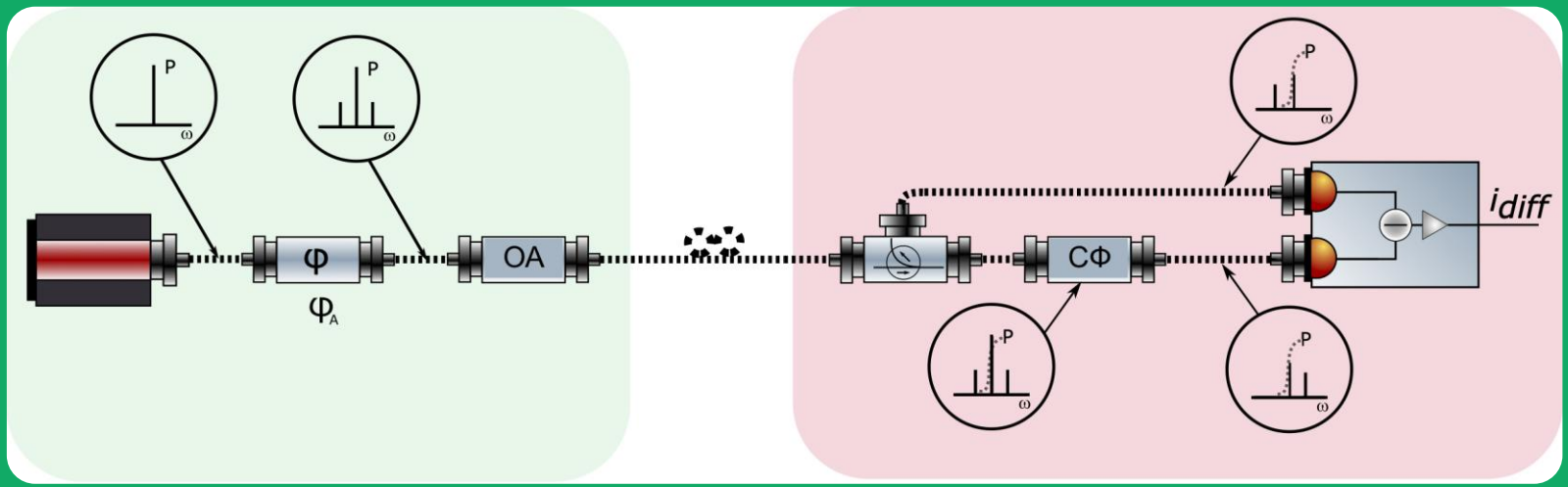
КРКНП на боковых частотах с реализацией протокола GG02

Goncharov R., Samsonov E., Kiselev A. D. Subcarrier wave quantum key distribution system with gaussian modulation // Journal of Physics: Conference Series. - IOP Publishing, 2021. - Т. 2103. - №. 1. - С. 012169.



Деятельность





Схемы КРК на боковых частотах с когерентным детектированием двух квадратур

Результаты работы в области КРКНП

- получено 6 РИД;
- опубликовано 7 статей;
- апробация на 6 конференциях;
- закрыт 1-й этап проекта по разработке комплекса КРКНП

Деятельность. РИД

1. Программа для исследования системы квантовых коммуникаций на боковых частотах с фазовой манипуляцией;
2. Программа для исследования системы квантовых коммуникаций на боковых частотах с гауссовской модуляцией;
3. Программа для исследования системы квантовых коммуникаций на боковых частотах с когерентным методом приёма;
4. Устройство квантовой рассылки симметричной битовой последовательности на поднесущей частоте модулированного излучения с гетеродинным методом приема;
5. Устройство квантовой рассылки симметричной битовой последовательности на поднесущей частоте модулированного излучения с гомодинным методом приема;
6. Устройство квантовой рассылки симметричной битовой последовательности на поднесущей частоте модулированного излучения с двойным гомодинным методом приема.

Деятельность. Статьи

1. Samsonov E.O., Goncharov R., Gaidash A., Kozubov A.V., Egorov V.I., Gleim A. Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis // Scientific Reports - 2020, Vol. 10, No. 1, pp. 10034;
2. Samsonov E., Goncharov R., Fadeev M., Zinoviev A., Kirichenko D., Nasedkin B., Kiselev A., Egorov V. Coherent detection schemes for subcarrier wave continuous variable quantum key distribution // Journal of the Optical Society of America B: Optical Physics - 2021, Vol. 38, No. 7, pp. 2215-2222;
3. Goncharov R.K., Zinovev A.V., Kiselev F.D., Samsonov E.O. Heterodyne-based subcarrier wave quantum cryptography under the chromatic dispersion impact // Наносистемы: Физика, химия, математика = Nanosystems: Physics, Chemistry, Mathematics - 2021, Vol. 12, No. 2, pp. 161-166;
4. Pervushin B.E., Fadeev M.A., Zinovev A.V., Goncharov R.K., Santev A.A., Ivanova A.E., Samsonov E.O. Quantum random number generator using vacuum fluctuations // Наносистемы: Физика, химия, математика = Nanosystems: Physics, Chemistry, Mathematics - 2021, Vol. 12, No. 2, pp. 156-160;
5. Goncharov R.K., Samsonov E.O., Kiselev A.D. Subcarrier wave quantum key distribution system with Gaussian modulation // Journal of Physics: Conference Series - 2021, Vol. 2103, No. 1, pp. 012169;
6. Goncharov R., Kiselev A., Veselkova N., Ali R., Kiselev F.D. Discrimination and decoherence of Schrodinger cat states in lossy quantum channels // Наносистемы: Физика, химия, математика = Nanosystems: Physics, Chemistry, Mathematics - 2021, Vol. 12, No. 6, pp. 697-702;
7. Гончаров Р.К., Кириченко Д.Н., Фадеев М.А., Зиновьев А.В., Самсонов Э.О. Исследование методов когерентного приема сигнала на поднесущих частотах модулируемого излучения // Сборник трудов XII Международной конференции «Фундаментальные проблемы оптики–2020» (Санкт-Петербург, 19-23октября 2020г.) - 2020. - С. 67-68

Деятельность. НИР

Разработка и создание системы квантовой коммуникации на непрерывных переменных

Осуществлён выбор оптимального протокола КРКНП:
- гауссовская модуляция;
- гетеродинное детектирование

Проведено доказательство стойкости для системы КРКНП с гауссовской модуляцией

Разработана схема экспериментального образца

Деятельность. НИР

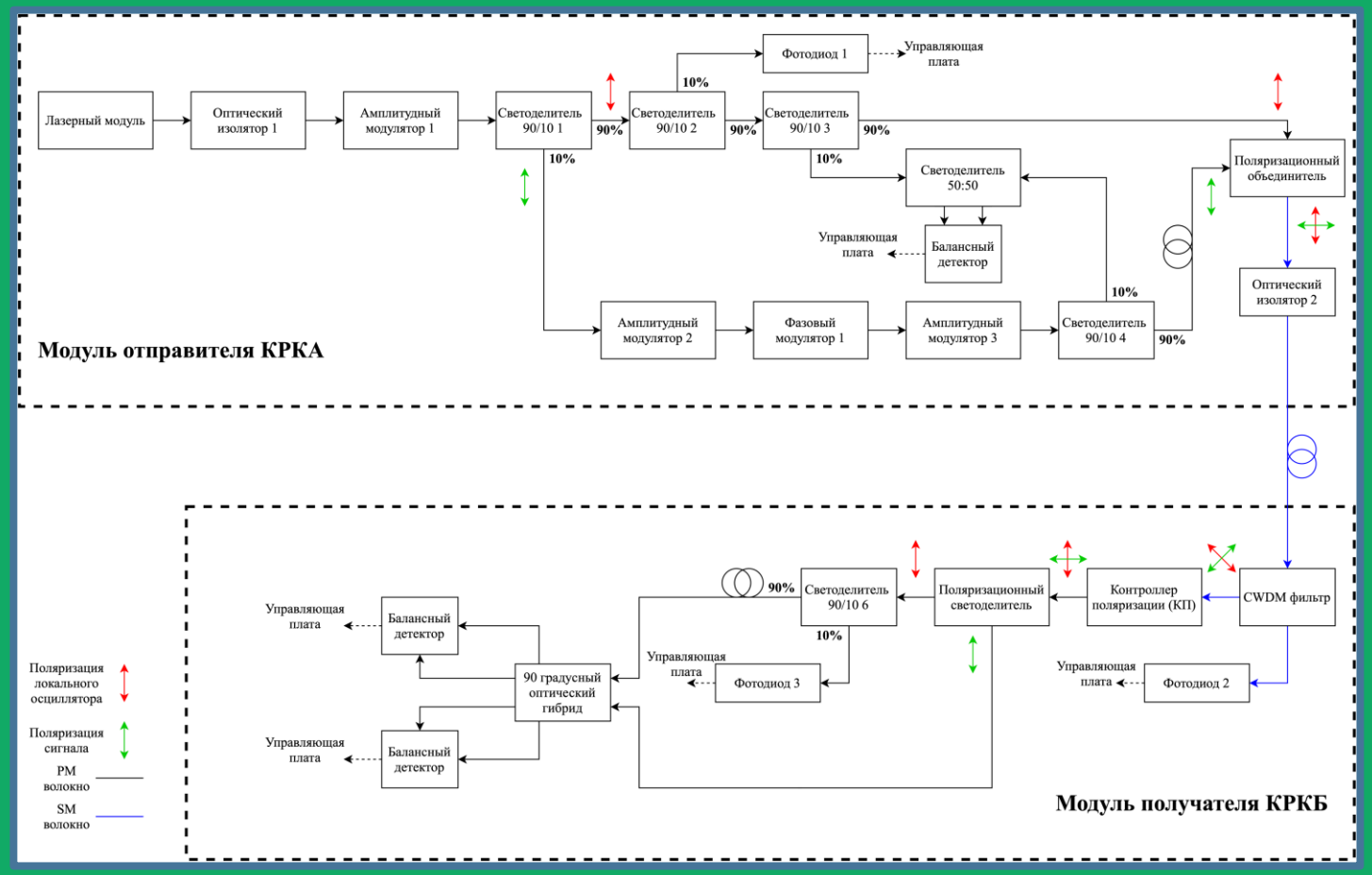


Схема установки КРКНП с гауссовской модуляцией и гетеродинным детектированием

Стойкость против коллективных атак

Контрмеры против атак на оборудование

К публикации по проекту готовятся 6 работ

Вопросы

???

Контактная информация

Электронная почта:
rkgoncharov@itmo.ru

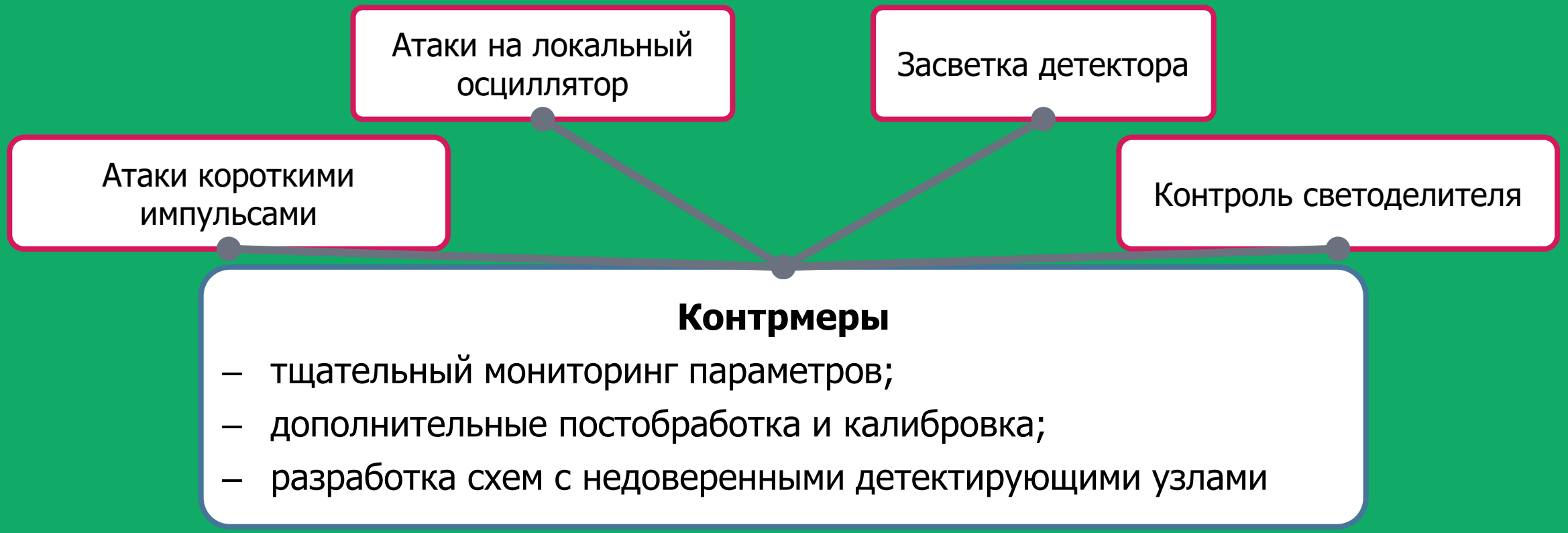
Телефон:
+7 960 191-49-5

Telegram:
t.me/toloro

Сайт:
www.itmo.ru

Дополнительные слайды

Атаки на техническую реализацию



Jouguet P., Kunz-Jacques S., Diamanti E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution // Physical Review A. – 2013. – Т. 87. – №. 6. – С. 062313.
Qin H., Huang A. Q., Makarov V. Short pulse attack on continuous-variable quantum key distribution system. – 2017.
Huang J. Z. et al. Wavelength attack scheme on continuous-variable quantum key distribution system using heterodyne detection protocol // arXiv preprint arXiv:1206.6550. – 2012.
Qin H., Kumar R., Alléaume R. Saturation attack on continuous-variable quantum key distribution system // Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X. – International Society for Optics and Photonics, 2013. – Т. 8899. – С. 88990N.

Гауссовский квантовый канал

Гауссовский квантовый канал характеризуется параметрами:

1) **Избыточный шум**: $\xi = \xi_{\mathrm{ch}} + \xi_{\mathrm{rec}}$,
где ξ_{ch} — компоненты избыточного шума канала;
ξ_{rec} — компоненты избыточного шума получателя;

2) **коэффициент пропускания**: $T = T_{\mathrm{ch}} \cdot T_{\mathrm{rec}}$,
где $T_{\mathrm{ch}} = 10^{-\zeta L/10}$ — коэффициент, отвечающий за потери в канале длины L (при удельных потерях ζ);
$T_{\mathrm{rec}} = \eta_{\mathrm{det}}\eta_{\mathrm{coup}}$ — коэффициент, совмещающий эффективность детектора η_{det} и потери на оборудовании η_{coup}.