Ежегодная международная научно-практическая конференция
«РусКрипто’2020»

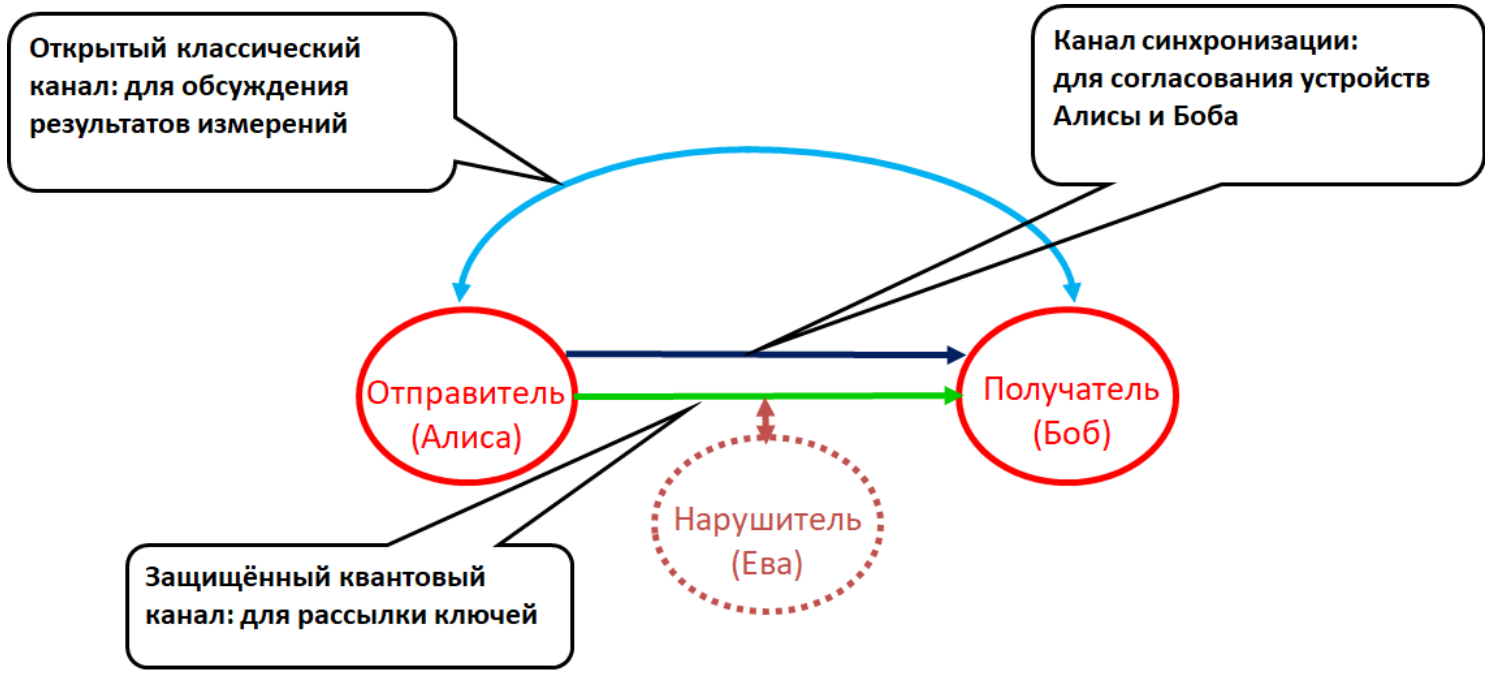
Квантовые системы и сети: задачи и перспективы

Верещагина Елена Валентиновна,
генеральный директор, ООО «Квантттелеком»

План доклада

- Квантовая рассылка ключей (КРК) и интеграция с СКЗИ
- Задачи в области систем КРК:
  - Защита от атак на протокол
  - Алгоритмы обработки квантовых ключей
  - Защита от атак на техническую реализацию
- Задачи в области квантовых сетей:
  - Общие положения по узлам сети
  - Применение доверенных узлов
  - Защита от компрометации отдельных узлов
  - Система управления квантовой сетью

Квантовое распределение ключей



- Стойкость квантовых сетей обусловлена вероятностным характером появления ключей и отсутствием человеческого фактора при их передаче.
- В качестве первоначальных ключей могут быть использованы классические ключи, которые после аутентификации отправителя и получателя могут быть заменены на квантовые

Возможности генерации ключей:

- ФДСЧ
- ПДСЧ
- Ключ на носителе

Одиночный фотон:

- Нельзя незаметно измерить
- Нельзя разделить
- Нельзя скопировать

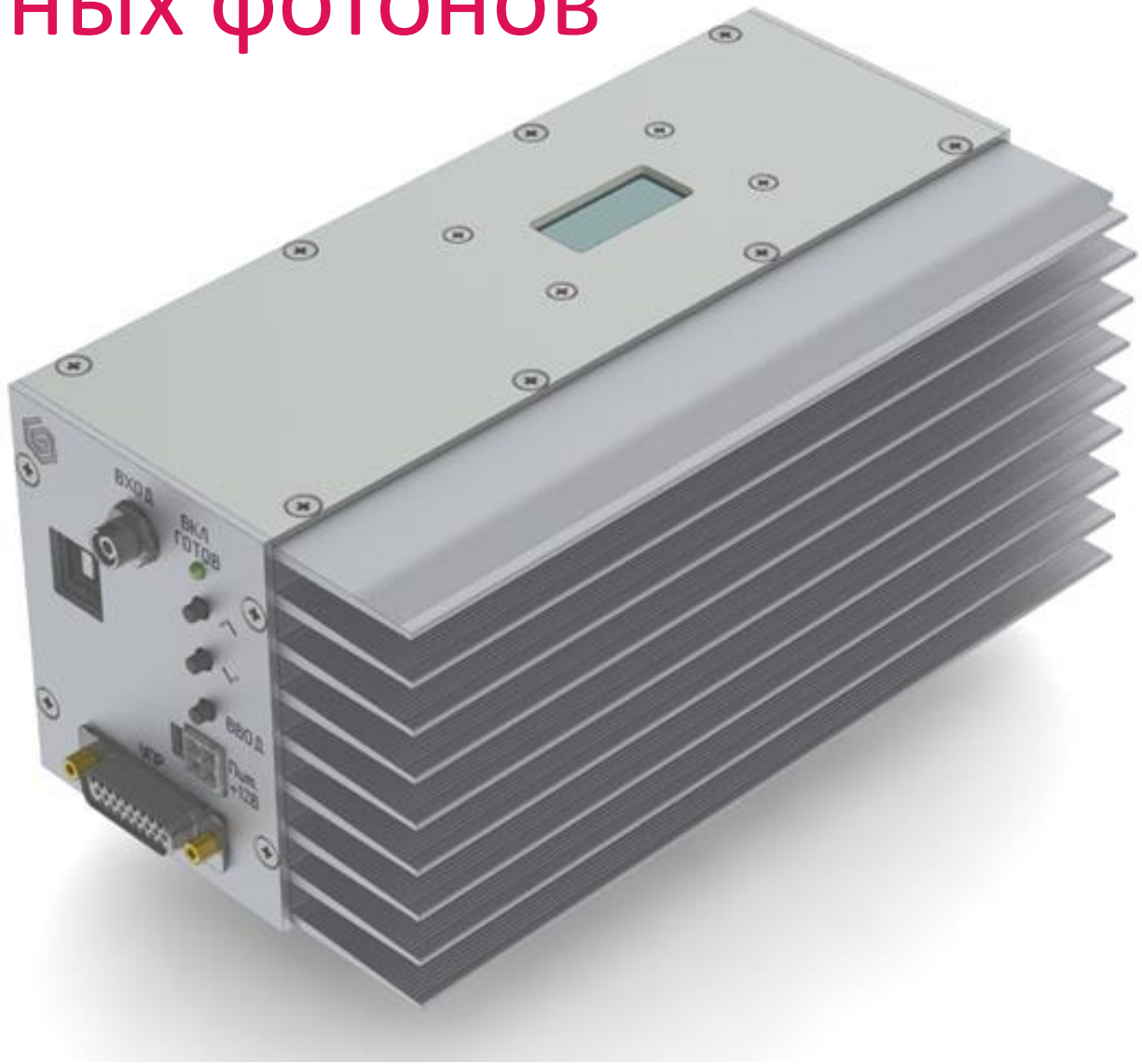
Схема интеграции КРК и СКЗИ (топология «точка-точка»)

Система ККС ВРК «Квантателеком»

Наименование параметра	Разрабатываемая ККС
Клиентские интерфейсы (Клиент)	10 Gbit Ethernet или 8 Gbit FC, модуль SFP+
Линейные интерфейсы (Канал)	2xOTU2e, модуль SFP+
Линейные интерфейсы КРК	КК-1 Gbit Ethernet, тип FC, СК-1 Gbit Ethernet, модуль SFP+
Криптоалгоритм	ГОСТ Р 34.12-2015 (блочный шифр «Magma»)
Режим шифрования	ГОСТ Р 34.13-2015 (режим гаммирования)
Режим выработки имитовставки	ГОСТ Р 34.13-2015
Производительность при передаче	10 Gbit/s Ethernet или 6, 8 Gbit/s FC, производительность не зависит от размера клиентского фрейма
Скорость генерации КвК	не менее 1 кбит/с (для линии связи с потерями 10 дБ (эквивалент 50 км), уточняется по результатам ТИ
Латенсия (Latency), мс	0,044
Резервирование	Автоматическое переключение между линиями за время не более 50 мс
Коррекция ошибок (FEC)	ITU-T G.709/ITU-T G.975.1

Детектор одиночных фотонов

- Собственная разработка «Квантателеком»
- Квантовая эффективность: 10%
- Вероятность темнового срабатывания: 10^{-7}
- Частота стробирования: не менее 100 МГц
- Нестабильность фронта: не более 200пс
- Мертвое время: 1 мкс
- Защита от ослепления



Асимптотическая оценка информации

Скорость генерации стойкого ключа для протоколов подобного класса в асимптотическом приближении бесконечного числа бит при наличии коллективных атак ограничена снизу **границей Деветака-Винтера**:

$$K = \nu_S P_B \left[1 - \mathrm{leak}_{EC}(Q) - \max_E \chi(A:E)\right]$$

где ν_S — частота повторения посылок,
P_B — вероятность успешного декодирования,
Q — квантовый коэффициент ошибок,
$\mathrm{leak}_{EC}(Q)$ — количество информации, раскрытой Алисой по открытому каналу для исправления ошибок

Количество информации ограничено снизу

$$\mathrm{leak}_{EC}(Q) \geq h(Q)$$

$$h(Q) = -Q\log_2 Q - (1-Q)\log_2(1-Q)$$

граница Холево определяется как:

$$\chi(A:E) = S(\rho) - \sum_k p_k S(\rho_k),$$

$$S(\rho) = -Tr\{\rho \log_2 \rho\}$$

В случае многомодовых фазомодулированных состояний

$$\chi(A:E) = h\left(\frac{1}{2}\left(1 - \exp\left[-\mu_0\left(1 - d_{00}^S(2\beta)\right)\right]\right)\right)$$

Исправление ошибок

Оценка (на основе Границы Чернова) вероятности события, при котором при добавлении ΔQ к оцененному по сэмплу k уровню ошибок Q_{est}, суммарное значение уровня ошибок будет все еще меньше действительного значения Q_{real} в битовой последовательности длиной n [1] (предполагая исправление ошибки за один сеанс):

$$Pr(Q_{est} + \Delta Q < Q_{real}) \leq \exp\left(\frac{-2k\Delta Q^2}{1-(k-1)/n}\right)$$

Величина избыточности, необходимое для исправления $Q_{est} + \Delta Q$ ошибки при эффективности алгоритма f_{ec} определяется следующим образом:

$$nf_{ec}h(Q_{est} + \Delta Q)$$

Тогда оптимальное значение размера сэмпла k будет одновременно минимизировать выражение

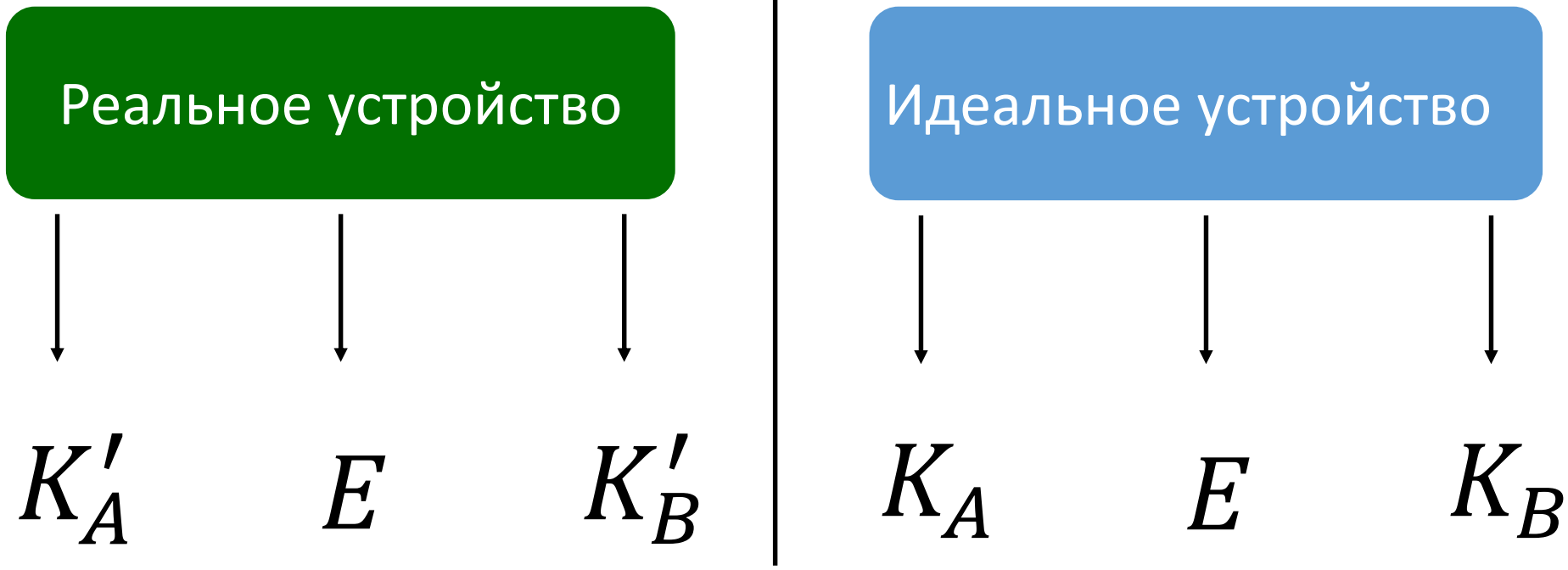
$$\exp\left(\frac{-2k\Delta Q^2}{1-(k-1)/n}\right)$$

и максимизировать скорость генерации ключа, т.е. следующее выражение

$$1 - f_{ec}h(Q_{est} + \Delta Q) - k$$

1. Serfling R. J. Probability inequalities for the sum in sampling without replacement //The Annals of Statistics. – 1974. – С. 39-48.

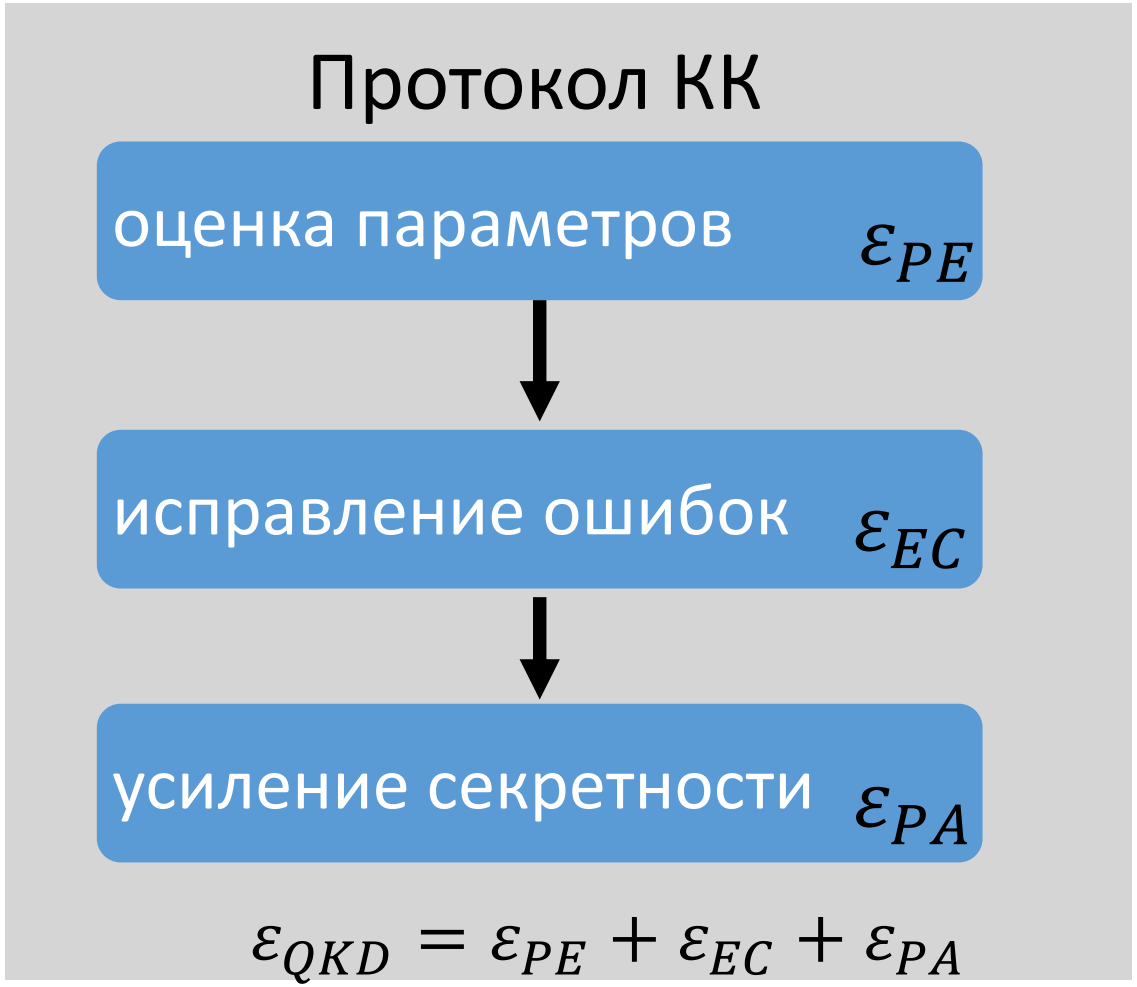
Отличие реального устройства от идеального



$$d = \| \rho_{K'E} - \omega_K \otimes \sigma_E \|_1 \leq \varepsilon$$

Renato Renner, Tutorial: Finite size effect in QKD, QCrypt 2018

Вклад различных параметров



Arnon-Friedman R., Renner R., Vidick T. Simple and tight device-independent security proofs //SIAM Journal on Computing. – 2019. – Т. 48. – №. 1. – С. 181-225.

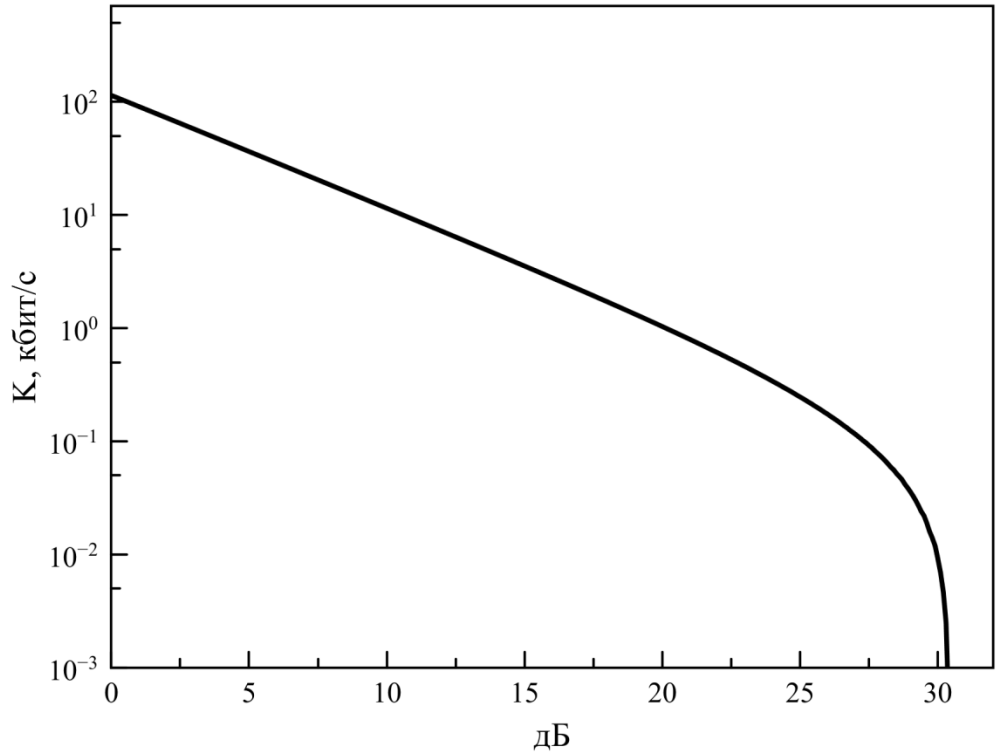
Параметры модели системы КРК «Кванттелеком»

В качестве рабочих параметров системы выбраны следующие значения:

- μ_0 = 4 – среднее число фотонов на центральной моде до модуляции
- μ = 0.2 – среднее число фотонов во всем спектре боковых частот
- Δm = 0.03 – несовпадение индексов модуляции
- $\Delta\varphi$ = 5º – дрожание фазы
- FL = 27 dB – доля пропускания фильтром на центральной моде
- η = 100 Hz – частота темновых срабатываний детектора
- QE = 20% – квантовая эффективность детектора
- η_{Bob} = 8 dB – потери в модуле получателя
- F = 100 MHz – частота смены кодирующей фазы
- n = 107 – необходимое количество бит в сырой битовой последовательности
- $\varepsilon_s = 10^{-10}$ – параметр гладкости мин-энтропии
- $\varepsilon_{PA} = 10^{-10}$ – параметр усиления секретности
- $\varepsilon_{EC} = 10^{-10}$ – вероятность несовпадения битовых последовательностей после
- исправления ошибок
- $\varepsilon_{EC}^{C} = 10^{-10}$ – вероятность неисправления всех ошибок в битовых последовательностях отправителя и получателя

Скорость генерации ε -стойкого ключа

$$K = F \cdot P_{det} \frac{1}{n}(n(1-\chi(\rho)) - 4\sqrt{n}\log(2+\sqrt{2}) \sqrt{\log\left(\frac{2}{\varepsilon_S^2}\right)} - k - code_{EC} - \log\frac{1}{\varepsilon_{EC}} - \log\frac{1}{\varepsilon_{PA}} + 2.)$$

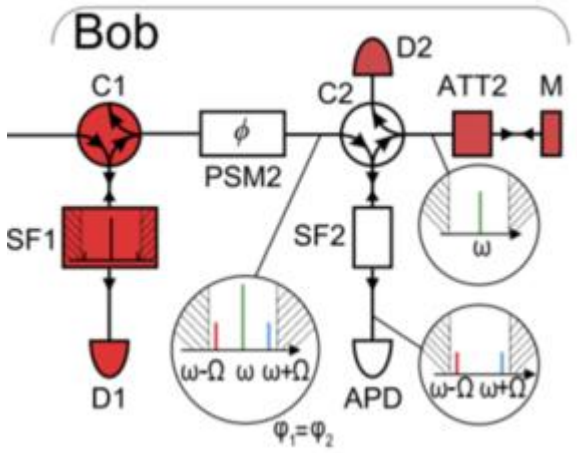


Зависимость скорости генерации стойкого ключа от потерь в канале в системе КРКБЧ с разным количеством задетектированных квантовых битов

Устойчивость реализации к атакам на техническую реализацию

Квантовое распределение ключей на боковых частотах.

Испытания системы КРК на боковых частотах, посвящённые исследованию устойчивости её текущей реализации к атакам на квантовый протокол и техническую реализацию, известным из открытых источников.



Атака	Краткое описание	Возможные контрмеры
Навязывание ключа (ослепление детектора)	Ослепление детектора фотонов сильным излучением (перевод из гейгеровского режима в линейный) и управление срабатываниями с помощью оптических импульсов	• Контроль силы тока в цепи гашения лавины МДФ • Мониторинг излучения засветки • Спектральное ограничение излучения нарушителя
Троянский конь	Отправка нарушителем сильного импульса в блок СКК и измерение фазового сдвига, внесённого модулятором в отражённое излучение	<u>Отправитель:</u> •Добавление оптического изолятора •Установка высоких потерь на аттенюаторах.
		<u>Получатель:</u> •Спектральное ограничение излучения нарушителя •Изоляция отражённого излучения •Регистрация отражённого излучения •Учёт в мат. модели
Переизлучение детектора	Излучение лавинным фотодиодом в блоке получателя СКК вторичного фотона после регистрации сигнального.	Установка циркулятора в СКК получателя, вторичный фотон не возвращается нарушителю в канал.

Этапы развития инфраструктуры квантовых коммуникаций

Квантовая рассылка ключа «точка– точка»

- ►Темное волокно
- ►Переход на стандартное волокно
- ►Интеграция КРК и СКЗИ

Текущий период

Квантовые сетевые технологии

- ► **Интеграция с существующими телекоммуникационными сетями**
- ► **Обеспечение физической безопасности сети**
- ► **Снижение стоимости**

- ►Гибридные сети (мультиплексирование квантовых и информационных каналов)
- ►Квантовые маршрутизаторы
- ►Интеграция с сетями 5G

3-7 лет

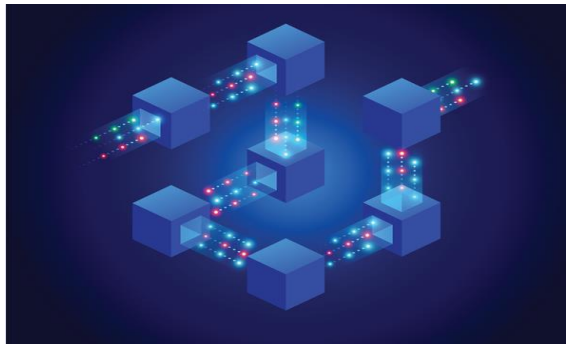
Глобальные квантовые сети

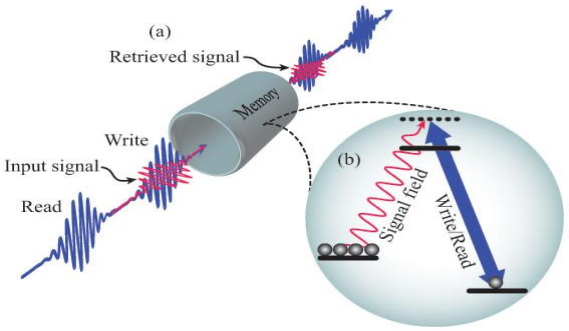
- ► **Не доверенные квантовые сети**
- ► **Распределённые квантовые вычисления**
- ► **Устойчиво работающие крупномасштабные квантовые системы**

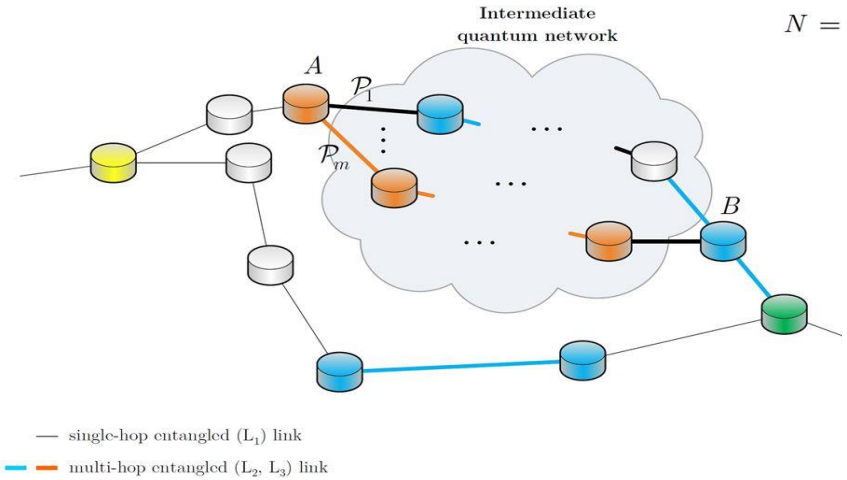
- ►Квантовые повторители
- ►Квантовые вычисления
- ►Мобильные и конечные устройства
- ►Спутниковые квантовые сети

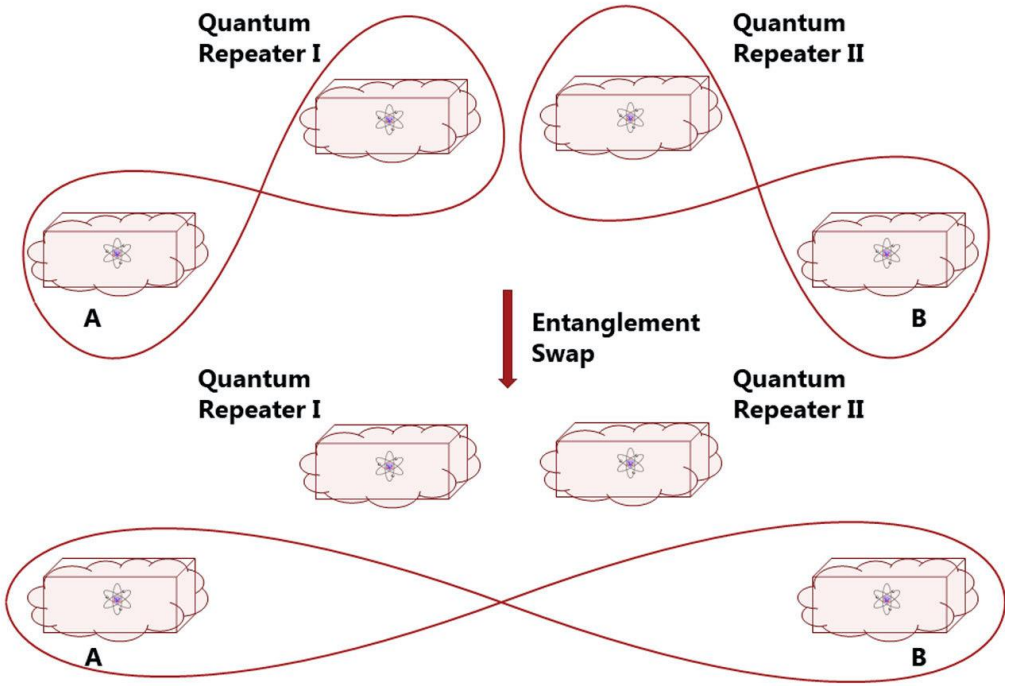
10+ лет

Квантовые повторители и квантовая память









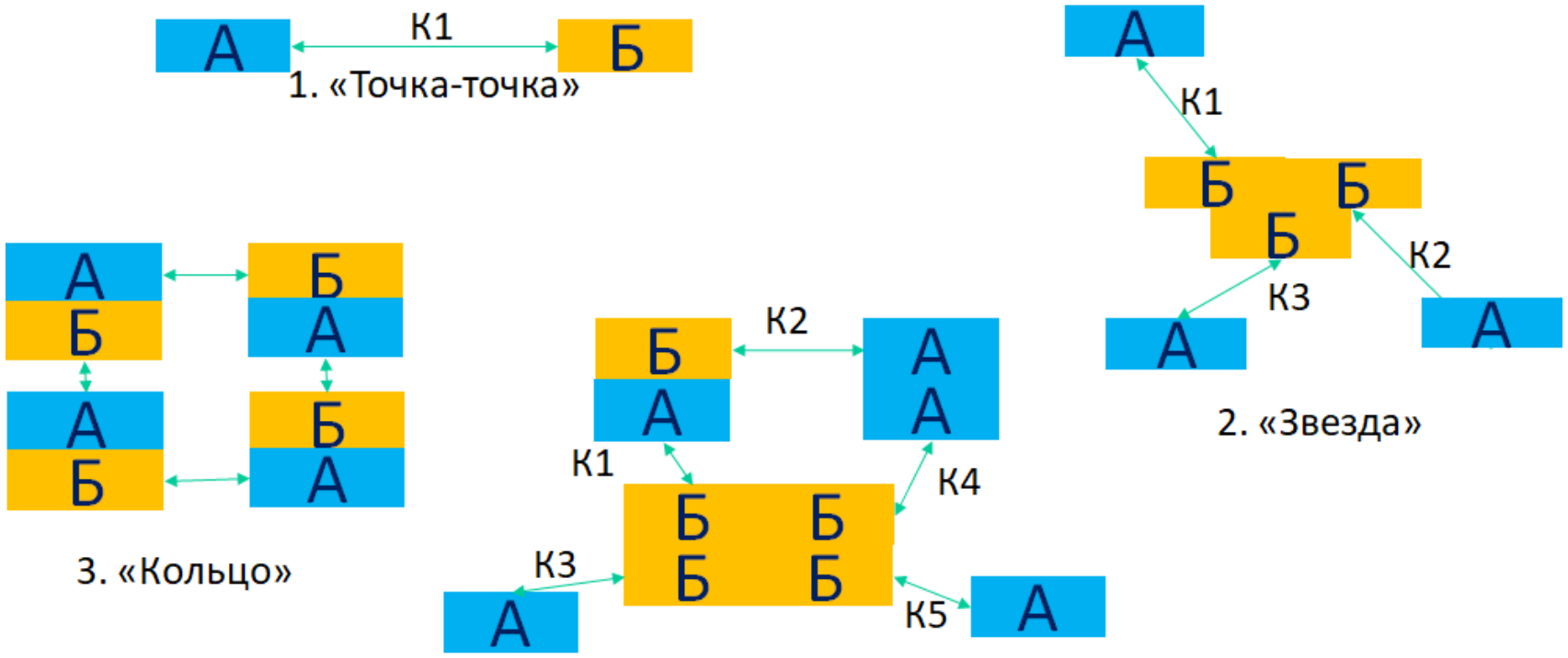
Briegel, H.-J., and R. Raussendorf, Phys. Rev. Lett. 86, 910 (1998)
Gyongyosi, L., Imre, S. Entanglement-Gradient Routing for Quantum Networks. *Sci Rep* **7,** 14255 (2017). https://doi.org/10.1038/s41598-017-14394-w
IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 21, NO. 3, MAY/JUNE 2015
https://phys.org/news/2018-11-important-quantum-network.html
https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/
https://physicsworld.com/a/quantum-memory-works-at-room-temperature/

- **Отсутствие** на сегодняшний день эффективных и надежных реализаций квантовых повторителей с квантовой памятью.

Архитектура квантовых коммуникационных сетей

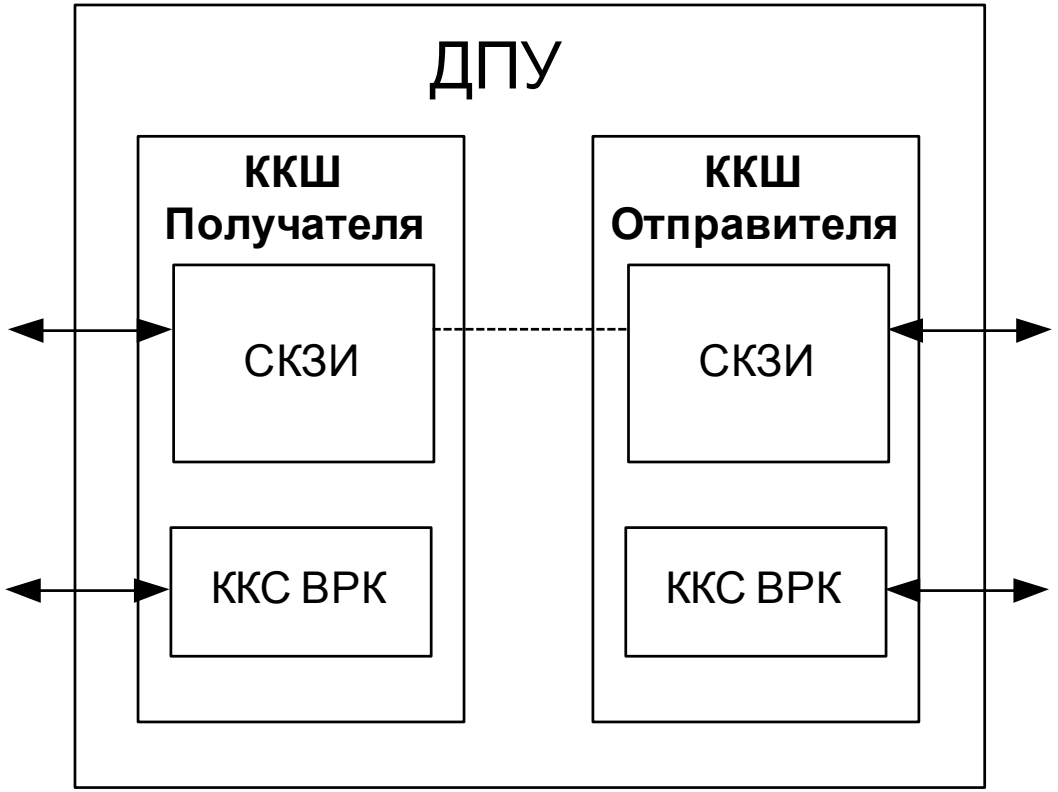
Задача магистральных систем КРК поддерживать одновременную передачу ключевой информации множества пользователей.

Необходимость построения квантовых сетей произвольной топологии: не только «точка-точка», но и «звезда», «кольцо», «смешанная».



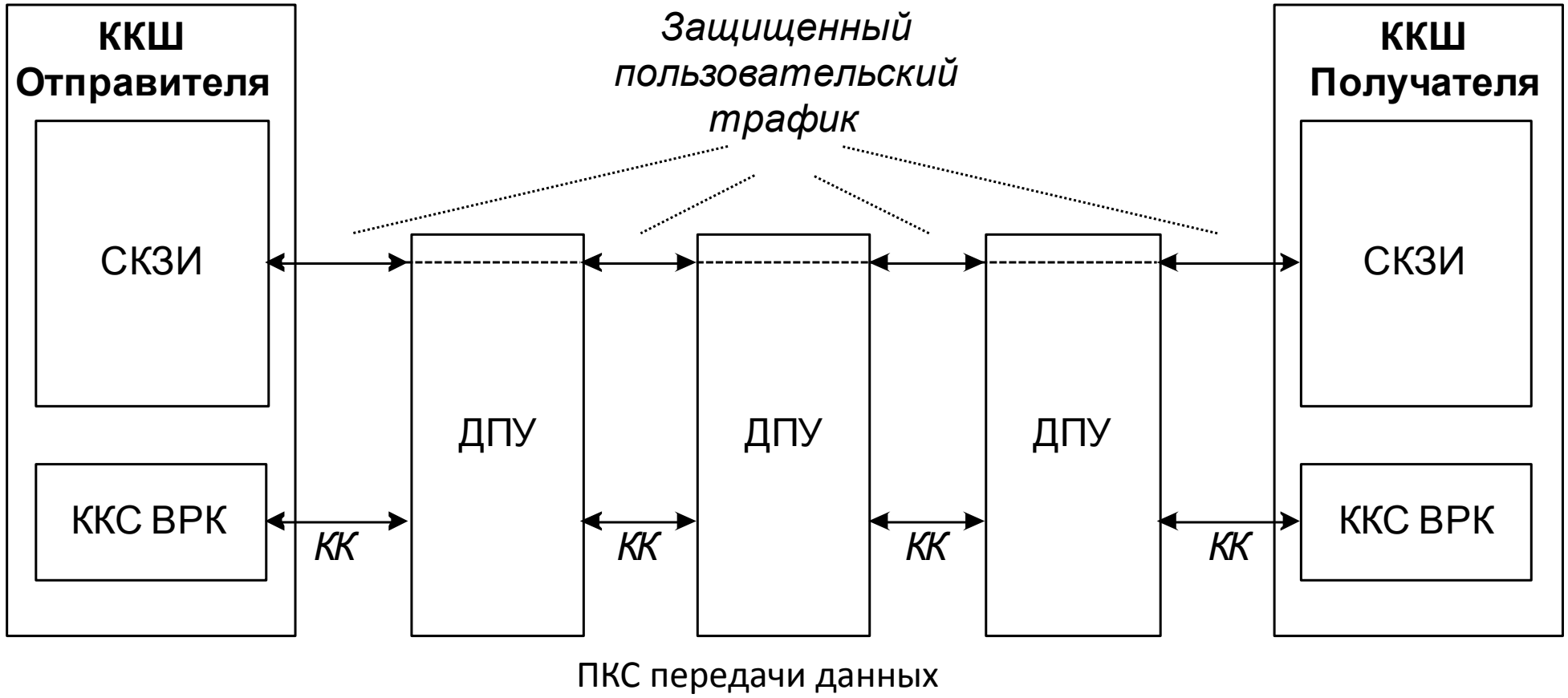
Доверенные узлы в квантовых коммуникационных сетях

Внутри ДПУ данные могут передаваться в открытом виде (на рисунке показаны штриховой линией), т. к. защита от несанкционированного доступа к данным обеспечивается конструкцией ДПУ.



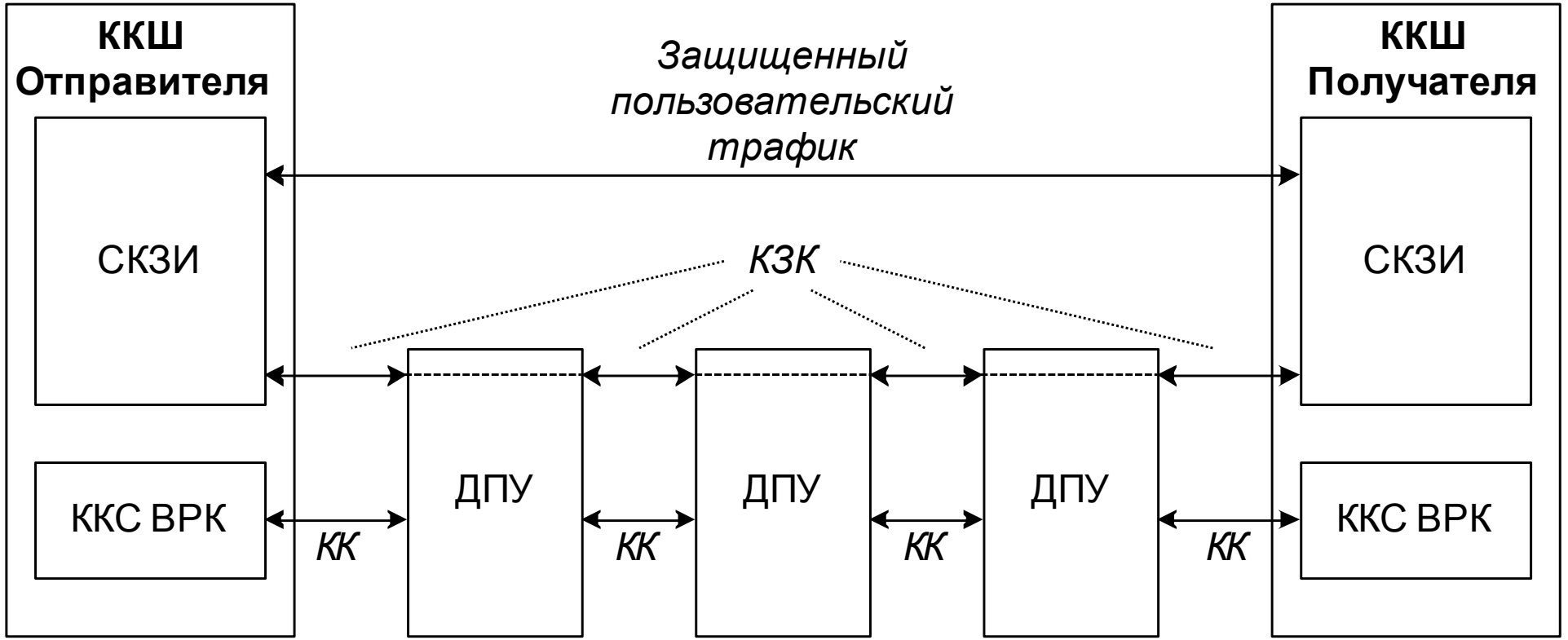
Состав доверенного промежуточного узла

Перешифрование **данных** в сетях на основе доверенных промежуточных узлов



ПКС передачи данных

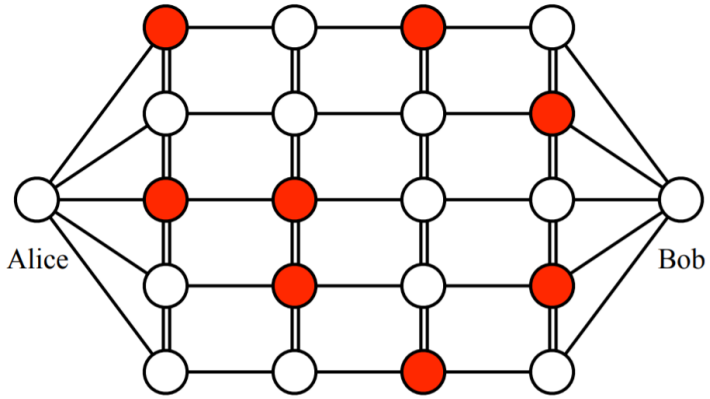
Перешифрование **ключей** в сетях на основе доверенных промежуточных узлов



ПКС передачи ключей

Способы передачи ключей с перешифрованием и частичным перешифрованием

Наиболее распространенный подход к реализации квантовых сетей (например DARPA [1], SECOQC [2]) – метод квантового реле [3].



Итоговый ключ K:

$$K = K_1 \oplus K_2 \oplus K_3 \oplus \cdots \oplus K_n$$

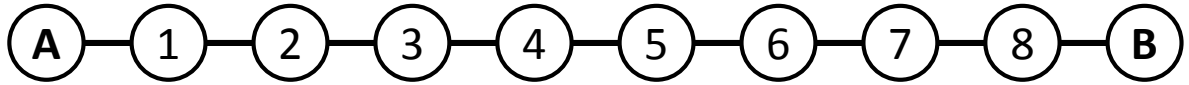
K_n - ключ, распределенный с помощью реле по n-му маршруту

Принципиальная схема квантового реле [3], позволяющего распределить криптографический ключ между двумя пользователями сети в присутствии компрометированных узлов. Кружками обозначены узлы сети, белые – нескомпрометированные, красные – подконтрольные перехватчику. Одинарные линии – магистральное соединение, двойные – локальное.

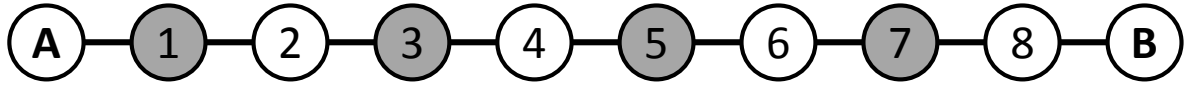
1. Sergienko A. V. (ed.). Quantum communications and cryptography. – CRC press, 2018.
2. Dianati M., Alleaume R. Architecture of the Secoqc quantum key distribution network //2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07). – IEEE, 2007. – С. 13-13.
3. Beals T. R., Sanders B. C. Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network //International Conference on Information Theoretic Security. – Springer, Berlin, Heidelberg, 2008. – С. 29-39.

Способы передачи ключей с перешифрованием и частичным перешифрованием

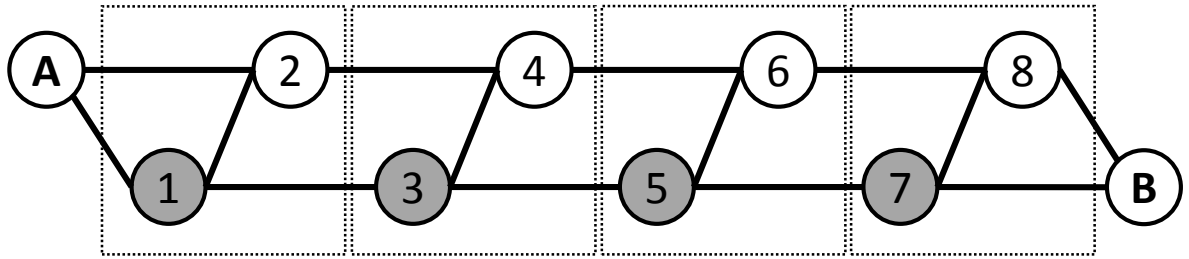
Тем не менее, метод квантового реле подходит к распределённым сетям с разветвленной структурой. Был предложен метод организации магистральных сетей аналогичным образом по следующей схеме [1]:

1) 

Изначальная последовательность узлов сети

2) 

Разбиение узлов на чередующие группы, например, на две (белые и серые)

3) 

Приведение к тождественной схеме организации сети, для которой представлено обоснование стойкости. Внутри прямоугольников «локальное» соединение узлов, между – «магистральное».

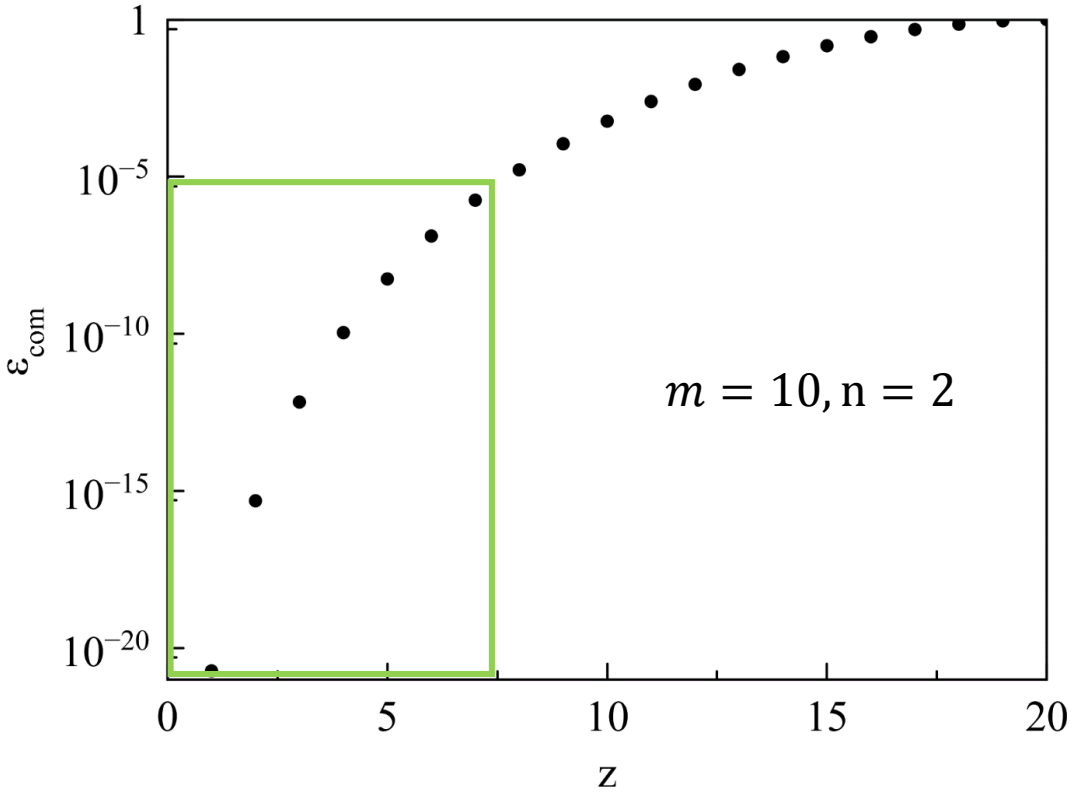
1. Barnett S. M., Phoenix S. J. D. Securing a quantum key distribution relay network using secret sharing //2011 IEEE GCC Conference and Exhibition (GCC). – IEEE, 2011. – С. 143-145.

Способы передачи ключей с перешифрованием и частичным перешифрованием

Вероятность скомпрометировать передачу ключа по квантовому реле [1], которая определяет криптографическую стойкость сети [2]:

$$\varepsilon_{com} \geq (1-(1-t^2)^n)^{m-1}$$

где $t = \frac{z}{mn}$ – доля компрометированных узлов, z – число компрометированных узлов , n – число узлов с «локальным» соединением, m – число узлов с «магистральным» соединением



1. Barnett S. M., Phoenix S. J. D. Securing a quantum key distribution relay network using secret sharing //2011 IEEE GCC Conference and Exhibition (GCC). – IEEE, 2011. – С. 143-145.
2. Salvail L. et al. Security of trusted repeater quantum key distribution networks //Journal of Computer Security. – 2010. – Т. 18. – №. 1. – С. 61-87.

Система управления ключами и система управления сетью

Задачи, решаемые системой управления ключами:

- генерация, распределение между пользователями сети,
- хранение и управление циклом жизни квантово-защищенных ключей.

Смена ключей шифрования должна производиться в полностью автоматическом режиме на регулярной основе.

Задачи управления и мониторинга протяженных квантовых сетей:

- управление сервисами,
- ресурсное планирование,
- контроль параметров качества оказания услуг.

Контроль скорости генерации квантовых ключей, контроль значений квантового коэффициента ошибок (QBER) для различных участков сети. Выдача предупреждений о превышении порога QBER, так как данная ситуация может быть вызвана попыткой НСД к квантовому каналу.

Выводы

Вопросы

Контактная информация

Электронная почта:

vereschagina@qcphotonics.com

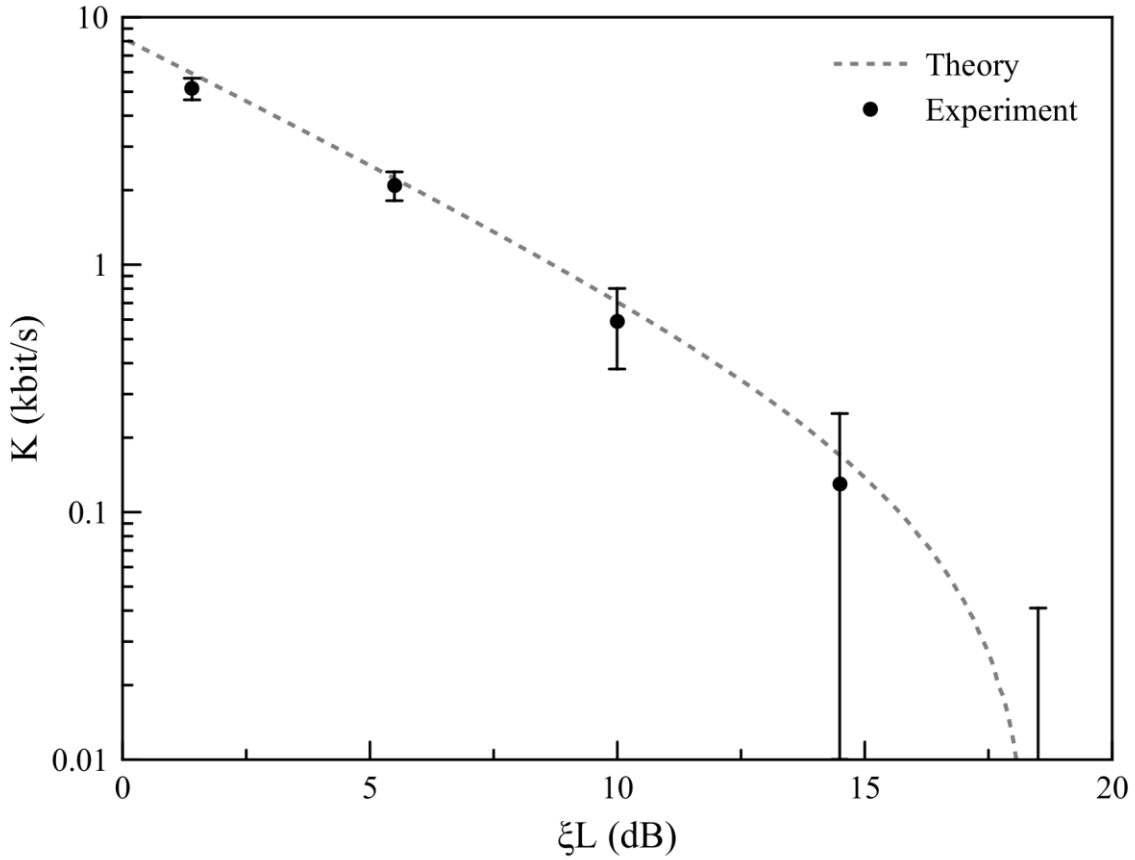
Телефон:

+7 981 803-79-11

Сайт:

www. quanttelecom.ru

Коллективная атака со светоделителем



- G - частота детектирования
- E - частота ошибок
- h(x) - бинарная энтропия Шеннона
- m - индекс модуляции
- μ_0 - среднее число фотонов на центральной моде
- $\tilde{\eta}(L)$ - потери в канале
- $J_0(x)$ - функция Бесселя

$$K(\mu_0, m, L) = \frac{1-G}{2T}\left[1 - h\left(\frac{E}{1-G}\right) - h\left(\frac{1}{2}\left(1 - e^{-\mu_0 \overline{\eta}(L)(1-J_0(2m))}\right)\right)\right]$$

G.P. Miroshnichenko, **A.V. Kozubov**, A.A. Gaidash, A.V. Gleim, D.B. Horoshko Security of subcarrier wave quantum key distribution against the collective beam-splitting attack // Optics express. - 2018. - Vol. 26. - № 9. - Pp. 11292-11308

Перешифрование **данных** в сетях на основе доверенных промежуточных узлов

- При передаче данных от одного квантового участка к другому происходит смена квантовых ключей. Таким образом, пользовательские данные приходят в доверенный промежуточный узел, зашифрованные на одном квантовом ключе, полностью расшифровываются внутри узла, а затем зашифровываются на другом квантовом ключе перед передачей в следующий доверенный промежуточный узел.
- Необходимость перешифрования большого объема информации, увеличение задержки при передаче данных.
- Отсутствие необходимости в поддержке дополнительной ключевой системы.

Перешифрование **ключей** в сетях на основе доверенных промежуточных узлов

- В этом случае на квантовых ключах перешифровываются не пользовательские данные, а т. н. квантово-защищенные ключи. В итоге квантово-защищенные ключи распределяются между конечными пользователями и в дальнейшем служат для шифрования пользовательских данных. Перешифрования данных в этом случае уже не требуется.