БУДЕ ОНЛАЙН

infotecs®

«Технология и продукты квантовой защиты информации»

23 июня 12:00 мск

Квантовые атмосферные и космические каналы связи

Сергей Кулик

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени
М.В.Ломоносова

ЦЕНТР КВАНТОВЫХ ТЕХНОЛОГИЙ
МГУ имени М.В. Ломоносова

Центр Квантовых Технологий

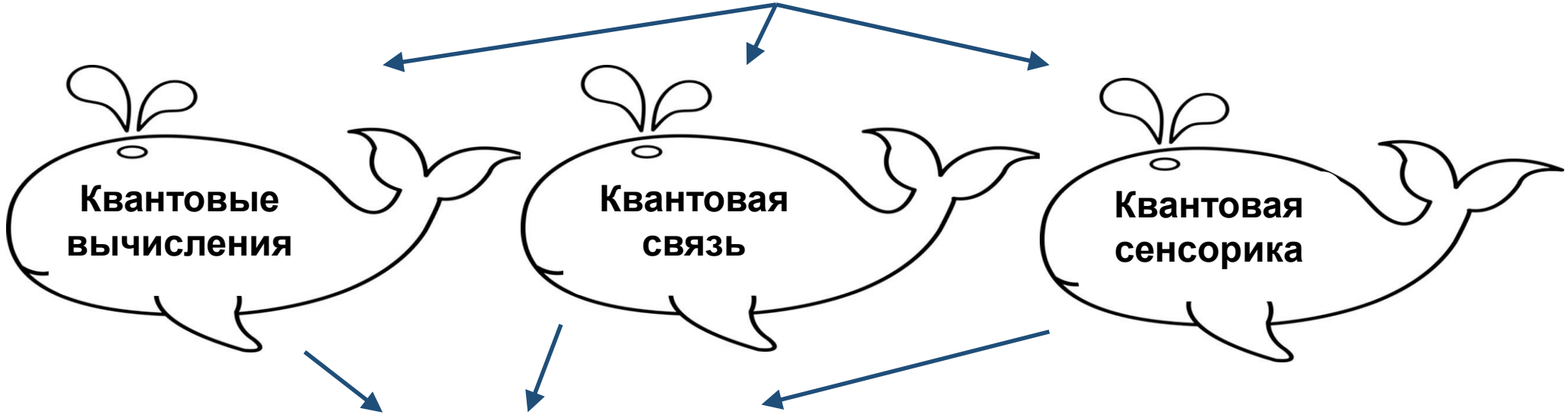
БИБ онлайн «Технология и продукты квантовой защиты информации»
23.06.20

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Центр Квантовых Технологий

Квантовая обработка информации. КВАНТОВЫЕ ТЕХНОЛОГИИ: три кита

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА



Оптоволоконные каналы связи: сетевая топология

Атмосферные/ космические каналы: мобильные, стационарные

Квантовая память, квантовые повторители

Глобальная Защищенная сеть

Центр Квантовых Технологий

Квантовая коммуникация/связь

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Волоконно-оптические Системы

Свободное пространство

Квантовые интерфейсы и память

ВЫВОД ЗАЩИТЫ ИНФОРМАЦИИ НА ПРИНЦИПИАЛЬНО ИНОЙ УРОВЕНЬ!

Квантовая коммуникация – это область знаний/техники о передаче квантовых состояний между удаленными объектами

Центр Квантовых Технологий

Основные направления мировых разработок

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

1. Волоконно-оптические линии связи

- шифрование квантовыми ключами данных, передаваемыми по магистральным линиям связи
- создание локальных защищенных сетей с электронным документооборотом
- создание крупномасштабных сетевых структур через доверенные узлы

2. Атмосферно-космические каналы связи

- распределение квантовых ключей между мобильными и стационарными объектами
- распределение ключей между низкоорбитальными спутниками и наземными объектами
- распределение ключей между низко- и высокоорбитальными спутниками
- создание глобальных квантовых сетей, охватывающих значительные территории

По всем направлениям работа ведется на физическом факультете МГУ

при поддержке

Фонда перспективных исследований, НТИ (Центр квантовых технологий),
Министерства обороны РФ, ФСБ России, Министерства науки и высшего образования и др.
Индустриальный партнер — ОАО «ИнфоТеКС»

Центр Квантовых Технологий

Квантовое распределение ключей через открытое пространство

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ МГУ имени М. В. ЛОМОНОСОВА

1. Квантовое распределение ключей – демонстрационные эксперименты

2000-2001 Первые работы по распределению ключей на расстояния порядка 1 км
2007-2009 Рекорд дальности по распределению ключей и передаче запутанности на 144 км
2012 Распределение перепутанности и квантовая телепортация на 97 км

2. Квантовое распределение ключей на движущиеся объекты

2013 Квантовое распределение ключей на самолет
2015 Квантовое распределение ключей на движущийся автомобиль
2017 Распределение ключей между дронами

3. Спутниковые системы квантовых коммуникаций

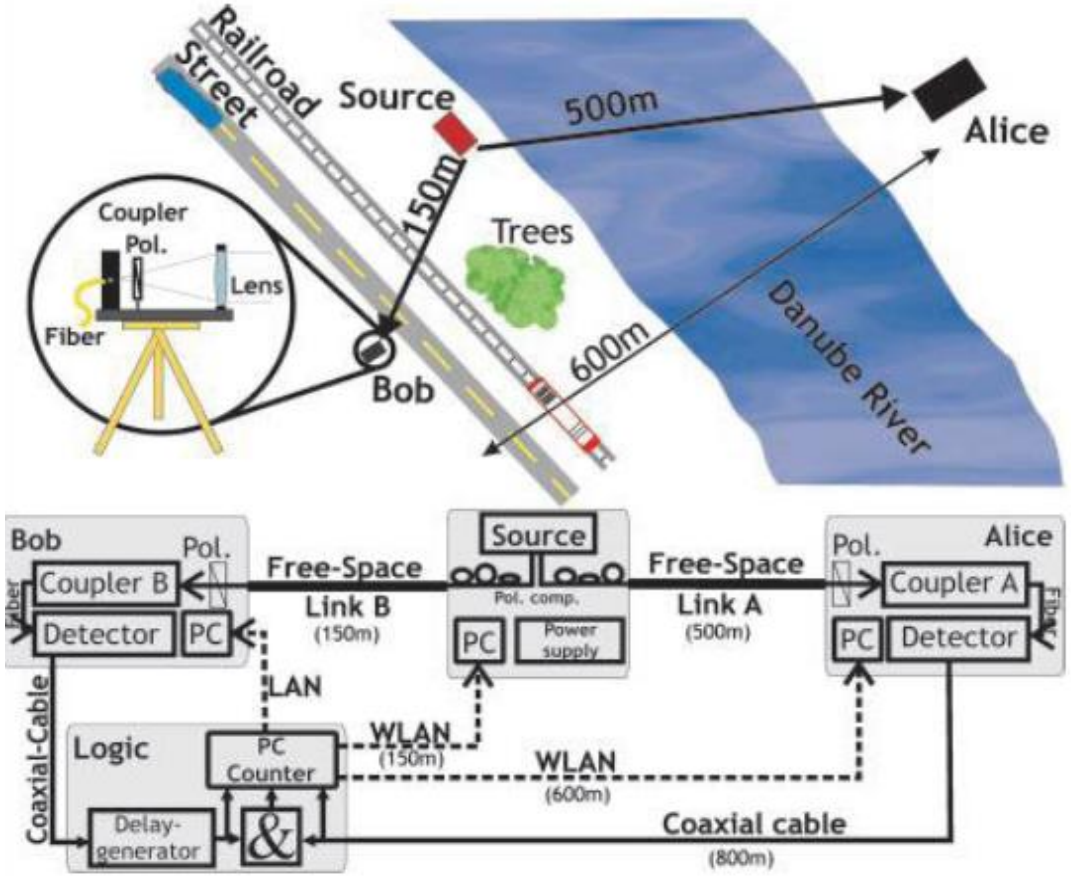
2014 SOTA/SOCRATES optical space terminal (NICT, Japan)
2016 Источник пар фотонов на орбите (Сингапур); Micius satellite (China)
2017 Квантово-ограниченная передача с геостационара (Alphasat)

Центр Квантовых Технологий

Long-Distance Free-Space Distribution of Quantum Entanglement

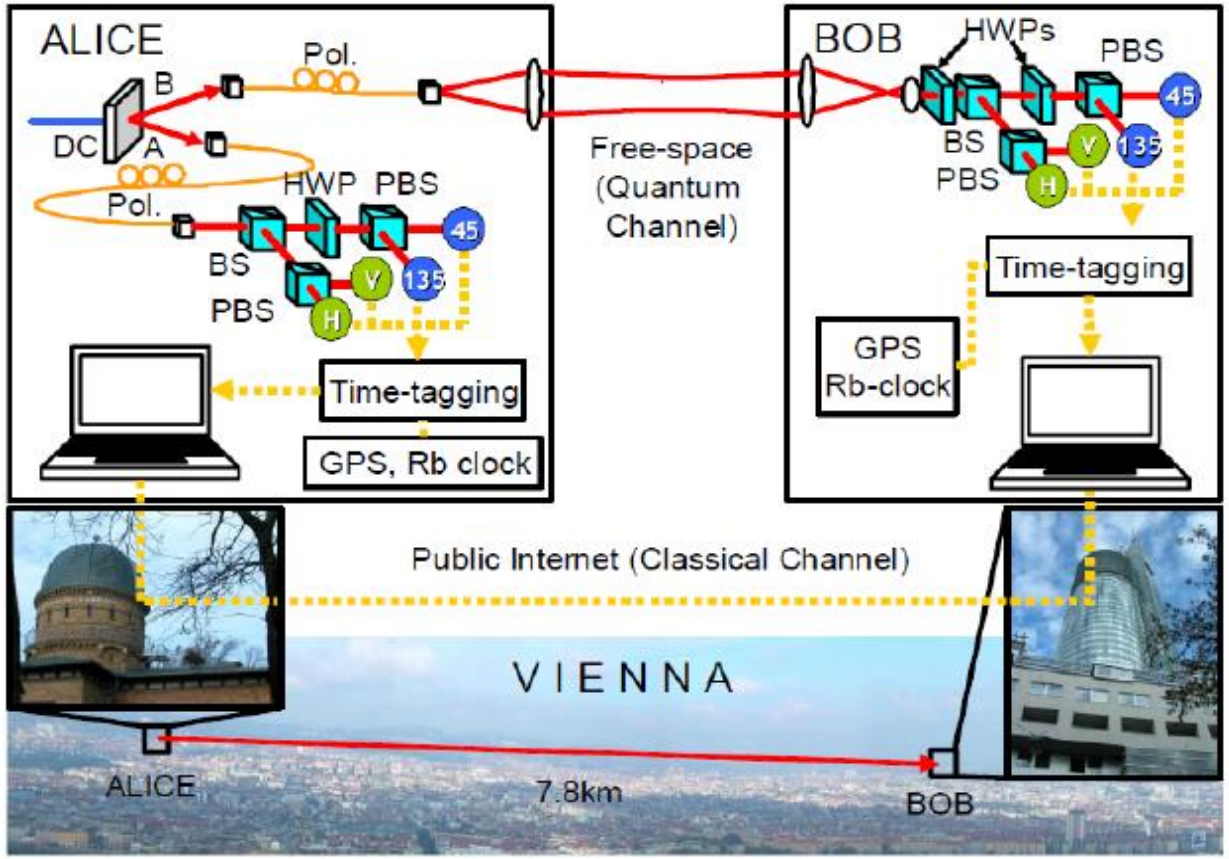
ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Over 600m



Experiment in Vienna, Austria, 2003

Over 7.8km



Experiment in Vienna, Austria, 2005

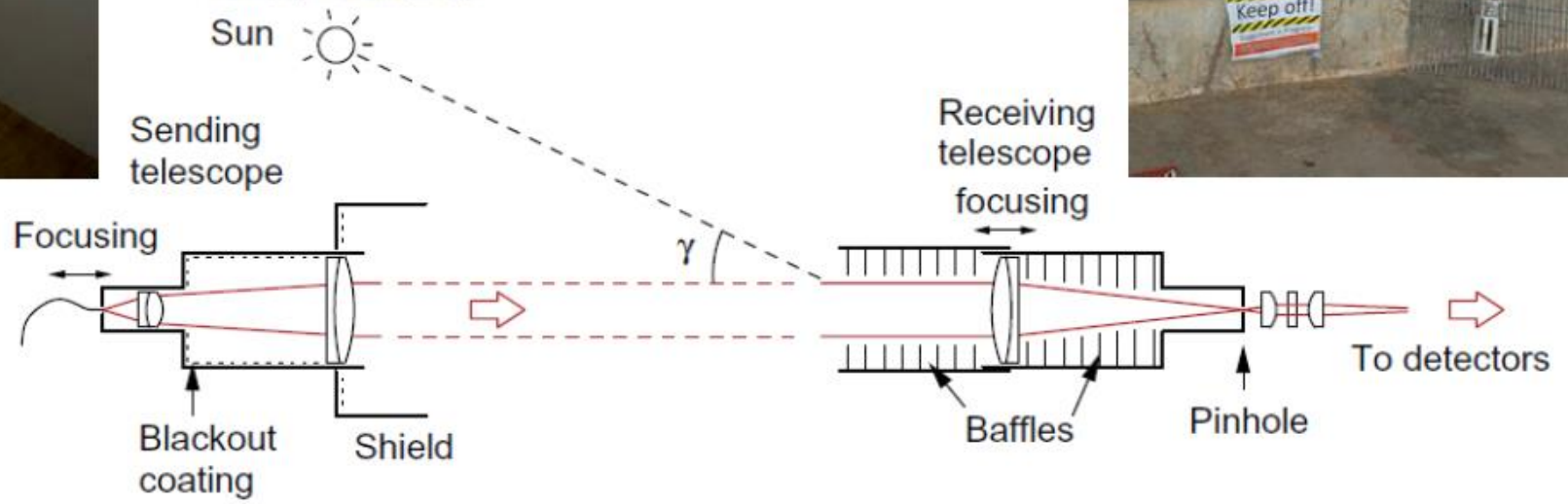
M. Aspelmeyer, et al. "Long-Distance Free-Space Distribution of Quantum Entanglement" Science 301, 621 (2003)
K.J. Resch at al. "Distributing entanglement and single photons through an intra-city, free-space quantum channel" OPTICS EXPRESS Vol. 13, No. 1 p.202 (2005).

Центр Квантовых Технологий

КРК на расстоянии 350 м при дневном освещении

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

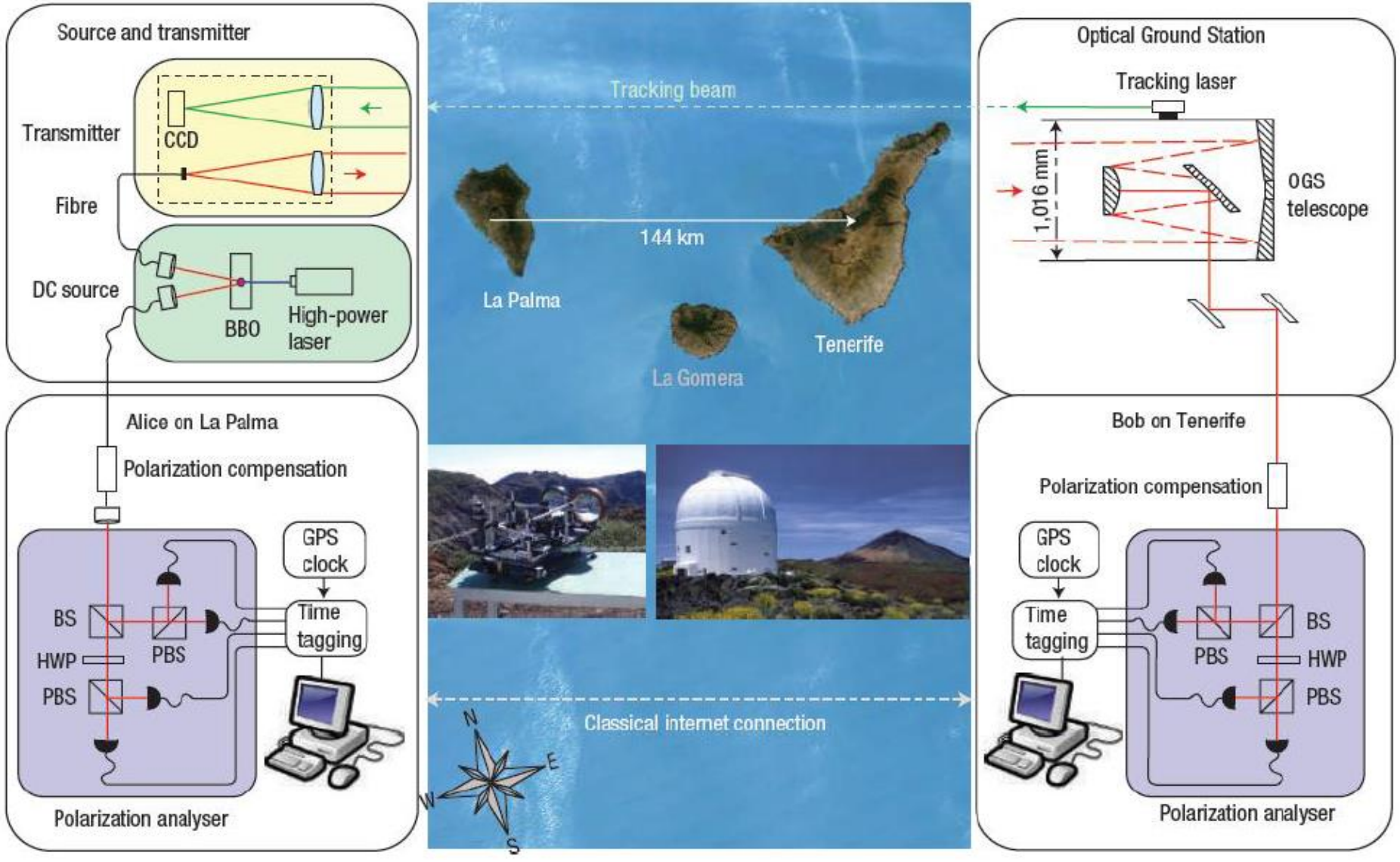
APL 89, 101122 (2006)



M.P. Peloso at al. "Daylight operation of a free space, entanglement-based quantum key distribution system" New Journal of Physics 11 (2009) 045007

NUS National University of Singapore

КРК на расстоянии 144 км. Распределение запутывания между Канарскими островами

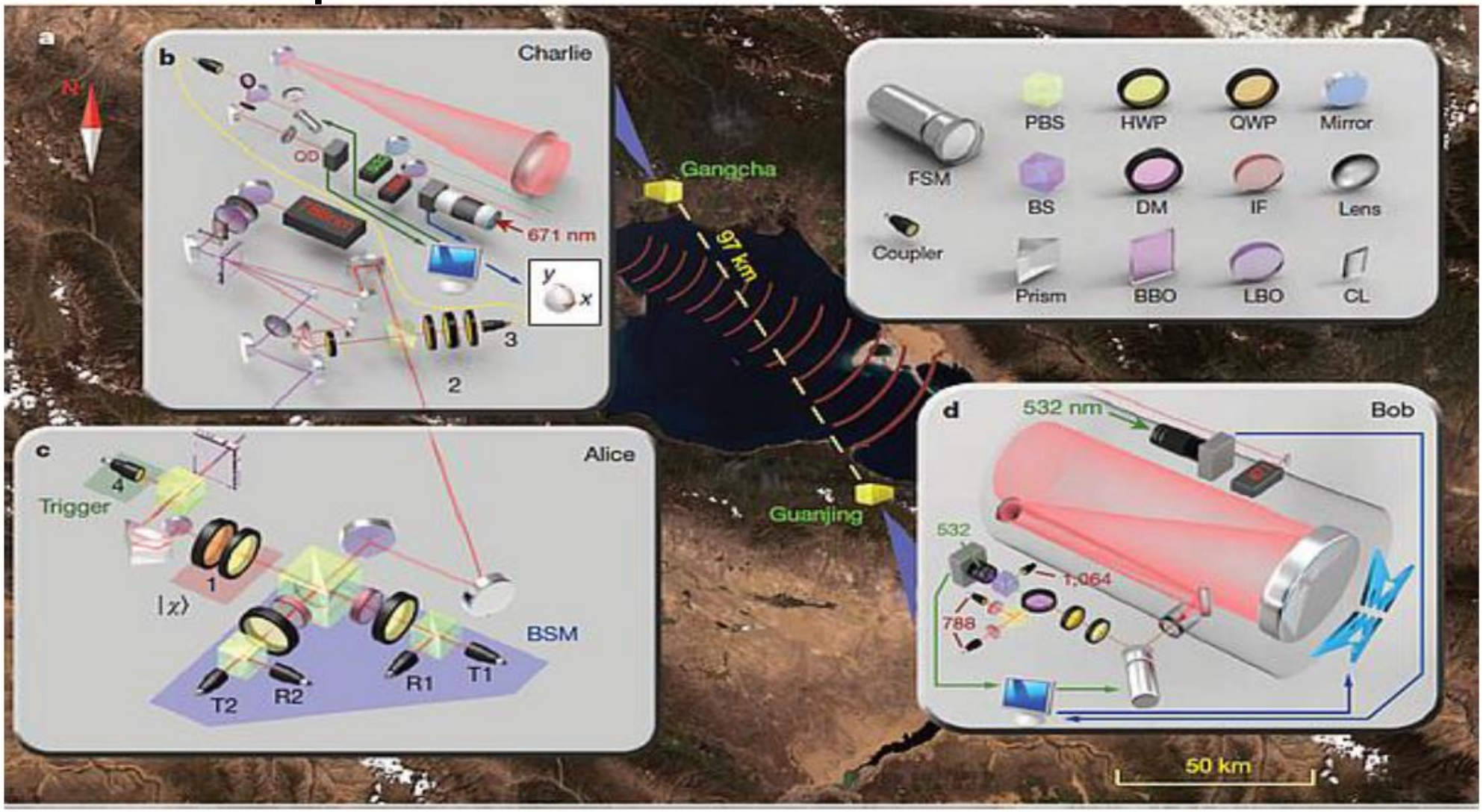


Ursin, R. et al. Entanglement-based quantum communication over 144 km. Nature Phys. 3, 481-486 (2007).

Центр Квантовых Технологий

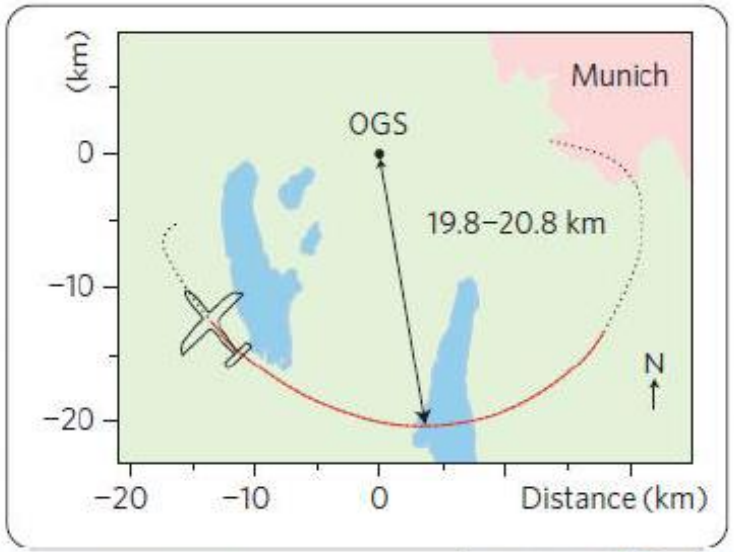
Квантовая телепортация на расстоянии 97 км

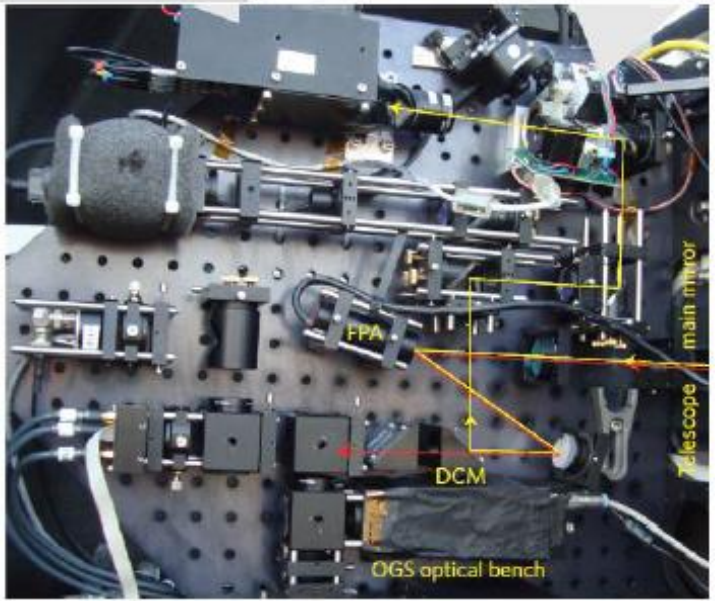
ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА



J. Yin, J.-G. Ren, H. Lu, at al. "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels", Nature, vol. 488, p.185.

BB84 на ослабленных когерентных состояниях, поляризационное кодирование, дальность – 20 км, полная эффективность -38 дБ



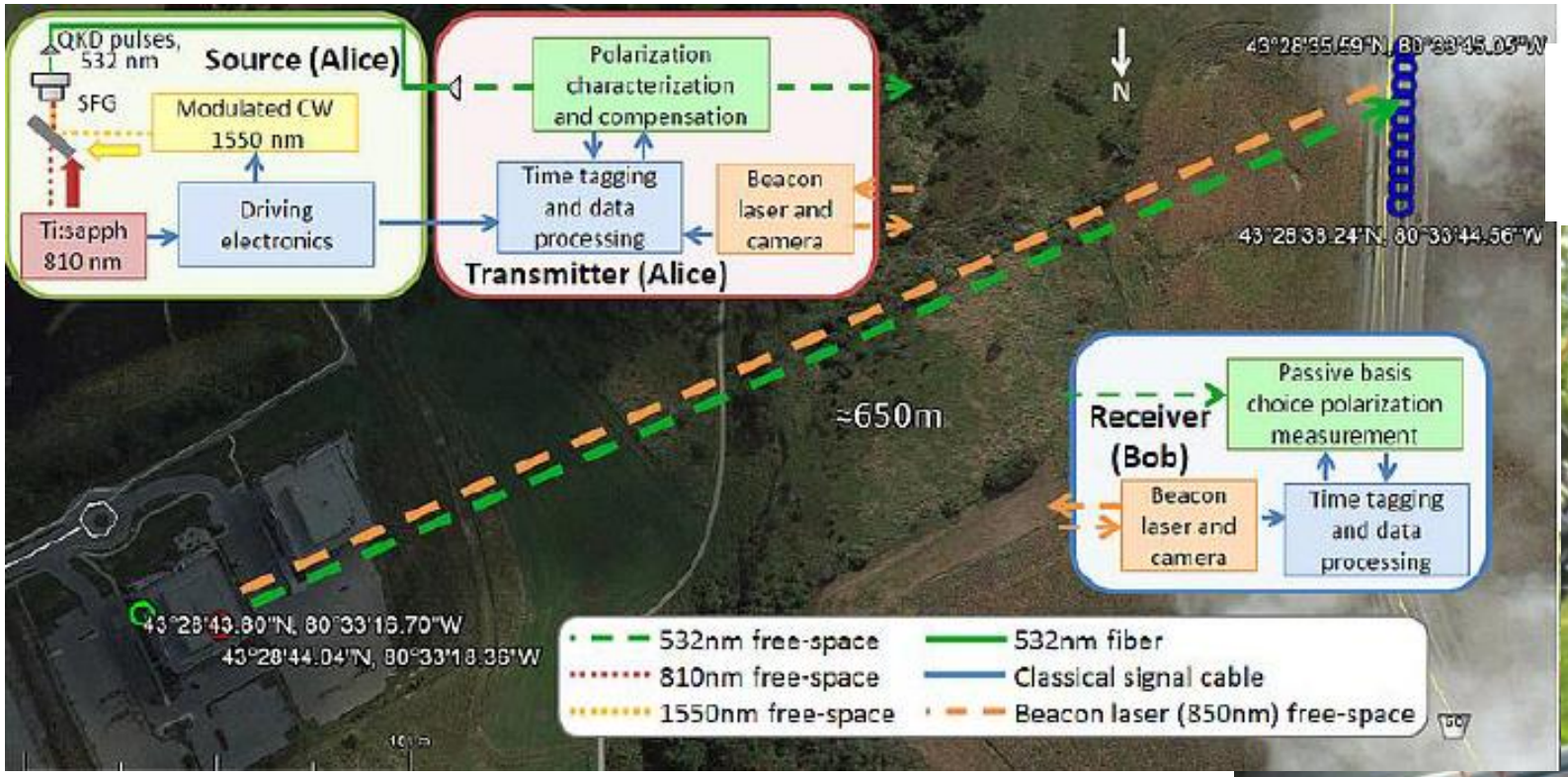


S. Nauerth at al. "Air-to-ground Quantum communication", Nature Photon. 2013

Центр Квантовых Технологий

КРК между стационарной станцией и движущимся автомобилем

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ МГУ имени М. В. ЛОМОНОСОВА

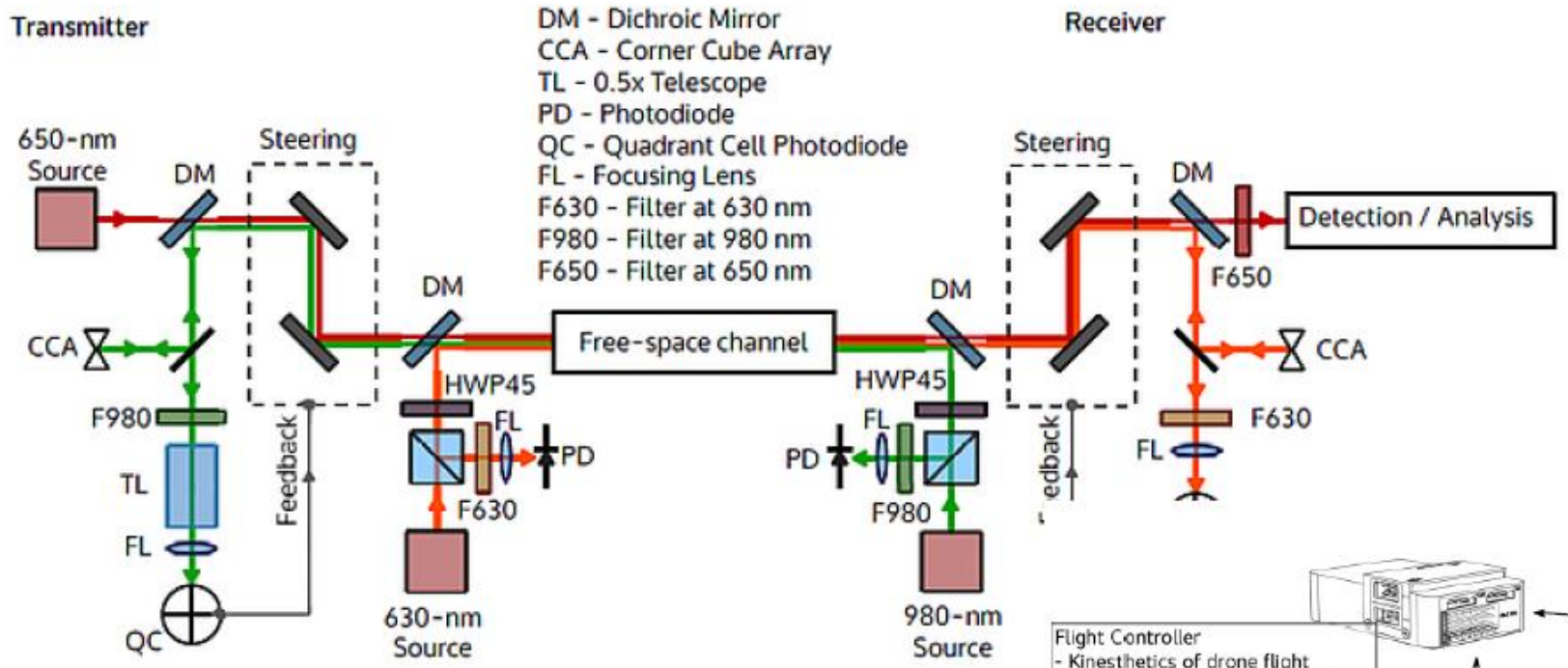


BB84 decoy-state

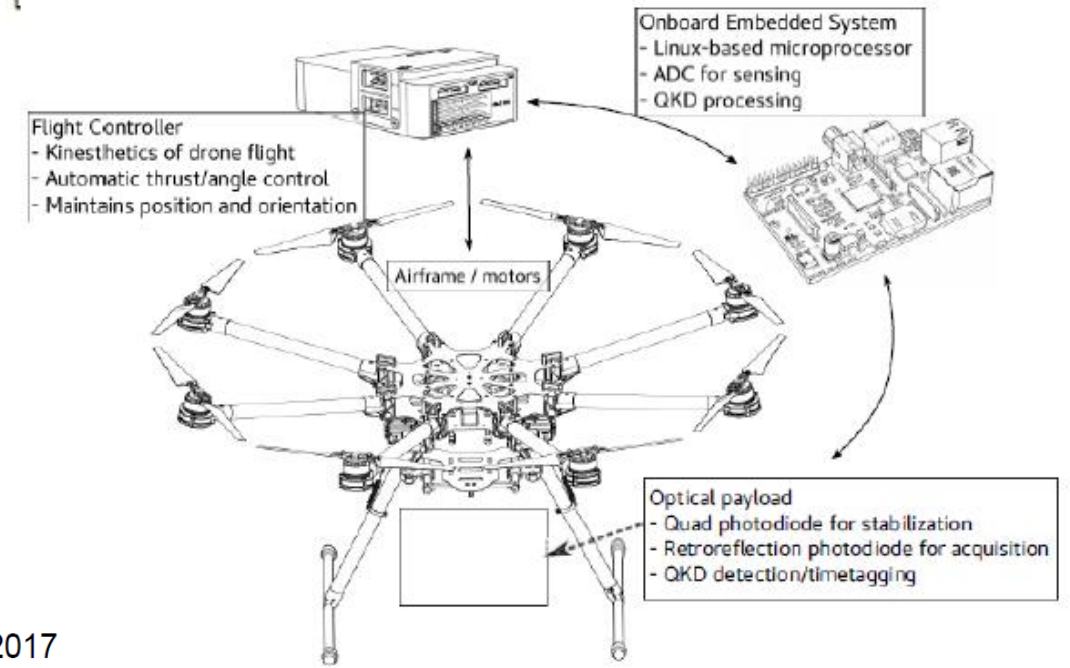
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

J.-P. Bourgoin, B. L. Higgins, N. Gigov, at al.
“**Free-space quantum key distribution to a moving receiver**”, Opt. Express v. 23, 33437 (2015)

КРК между стационарной станцией и ДРОНом



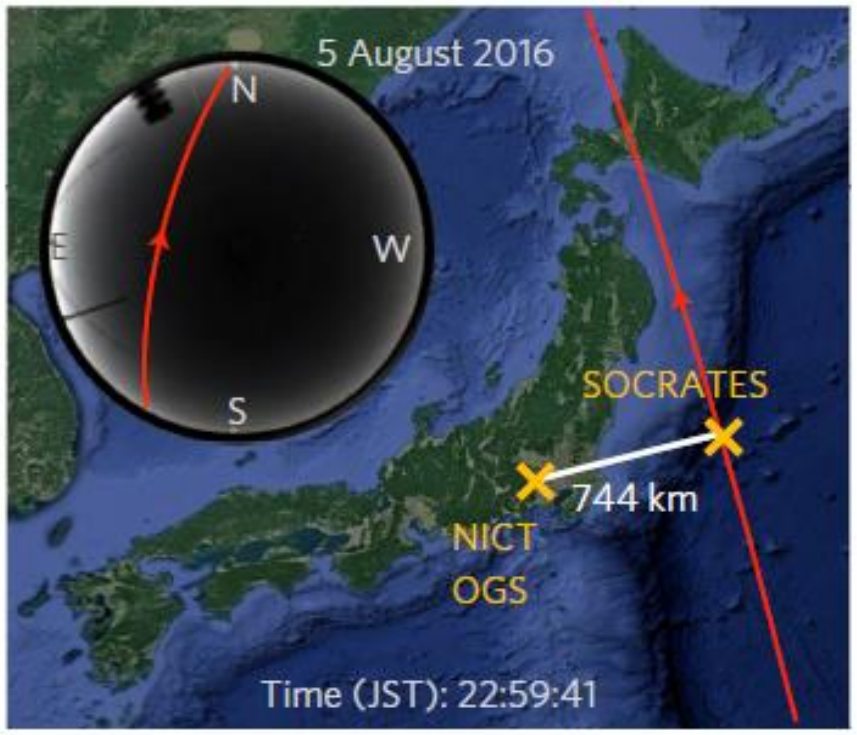
3-state protocol

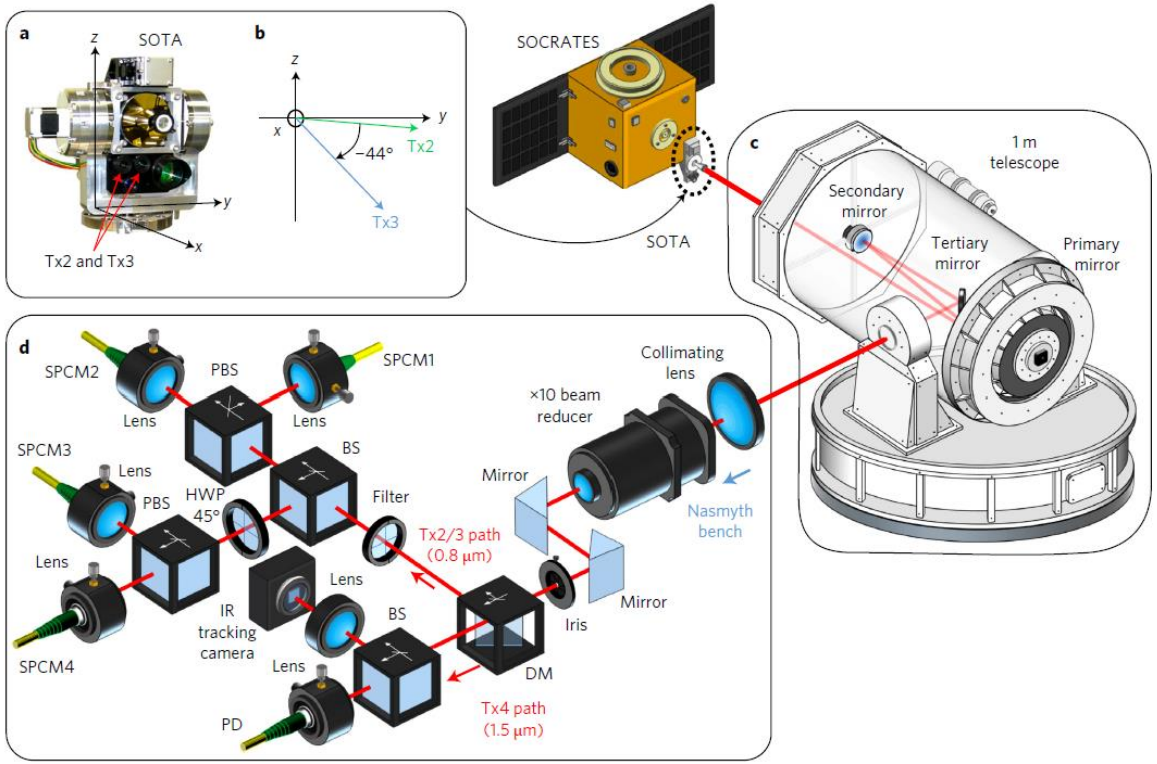


A. D. Hill, J. Chapman, K. Herndon, C. Chopp, D. J. Gauthier, Paul Kwiat, 2017

Квантовая спутниковая связь (2014)

2014 – SOTA/SOCRATES optical space terminal (NICT, Japan): микроспутник 50 кг.
Измерение поляризационных состояний, «квантово-ограниченная» передача данных на землю.
Передатчик на спутнике, прием наземным 1,5 м телескопом.





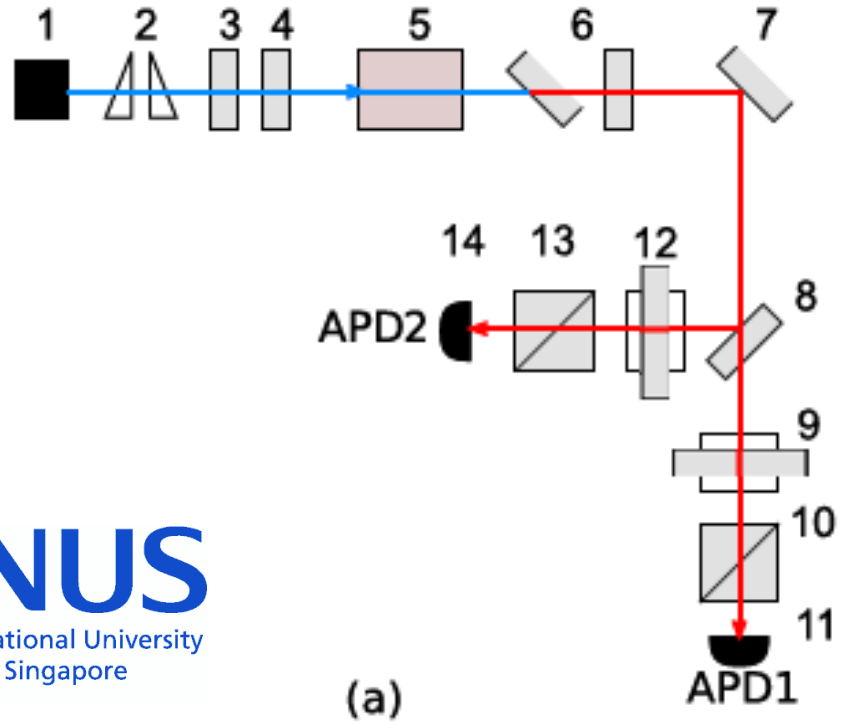
H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite" NATURE PHOTONICS, vol. 11, p. 502, 2017.

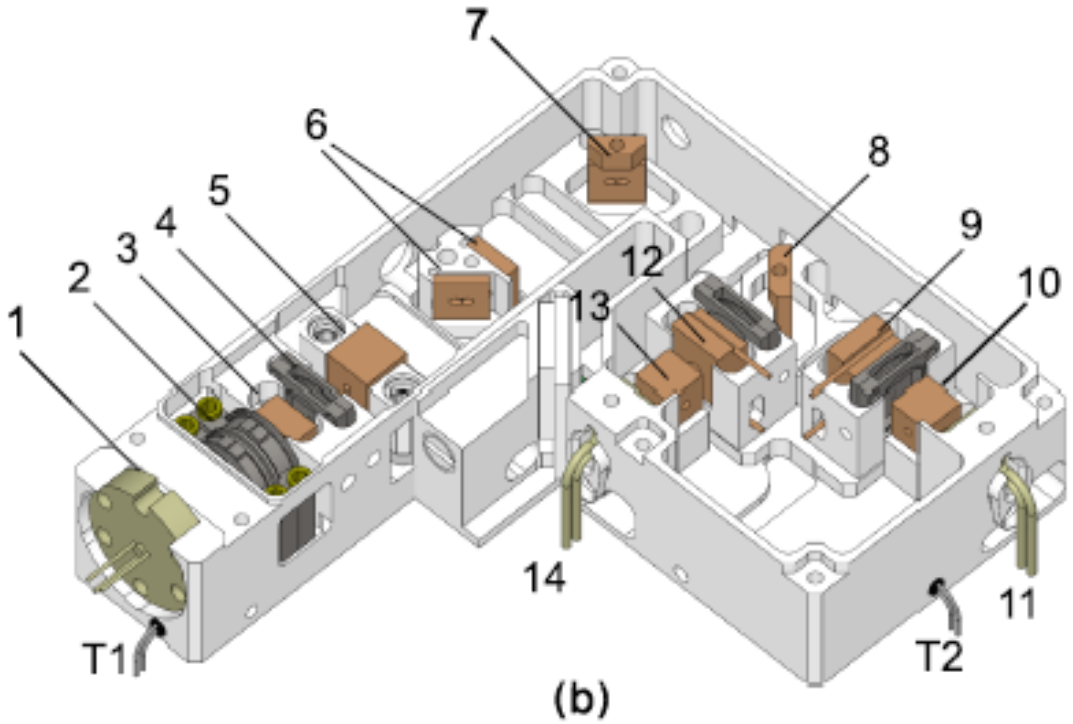
Центр Квантовых Технологий

Источник пар фотонов на орбите (2016)

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ МГУ имени М. В. ЛОМОНОСОВА

Первая попытка не удалась – взорвалась ракета-носитель, но источник в итоге остался цел.
Вторая попытка успешная. Режим генерации пар: невырожденный коллинеарный синхронизм типа I.





NUS National University of Singapore

Zhongkan Tang, Rakhitha Chandrasekara, Yue Chuan Tan, Cliff Cheng, Luo Sha, Goh Cher Hiang, Daniel KL Oi, Alexander Ling"Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite", PHYSICAL REVIEW APPLIED 5, 054022 (2016).

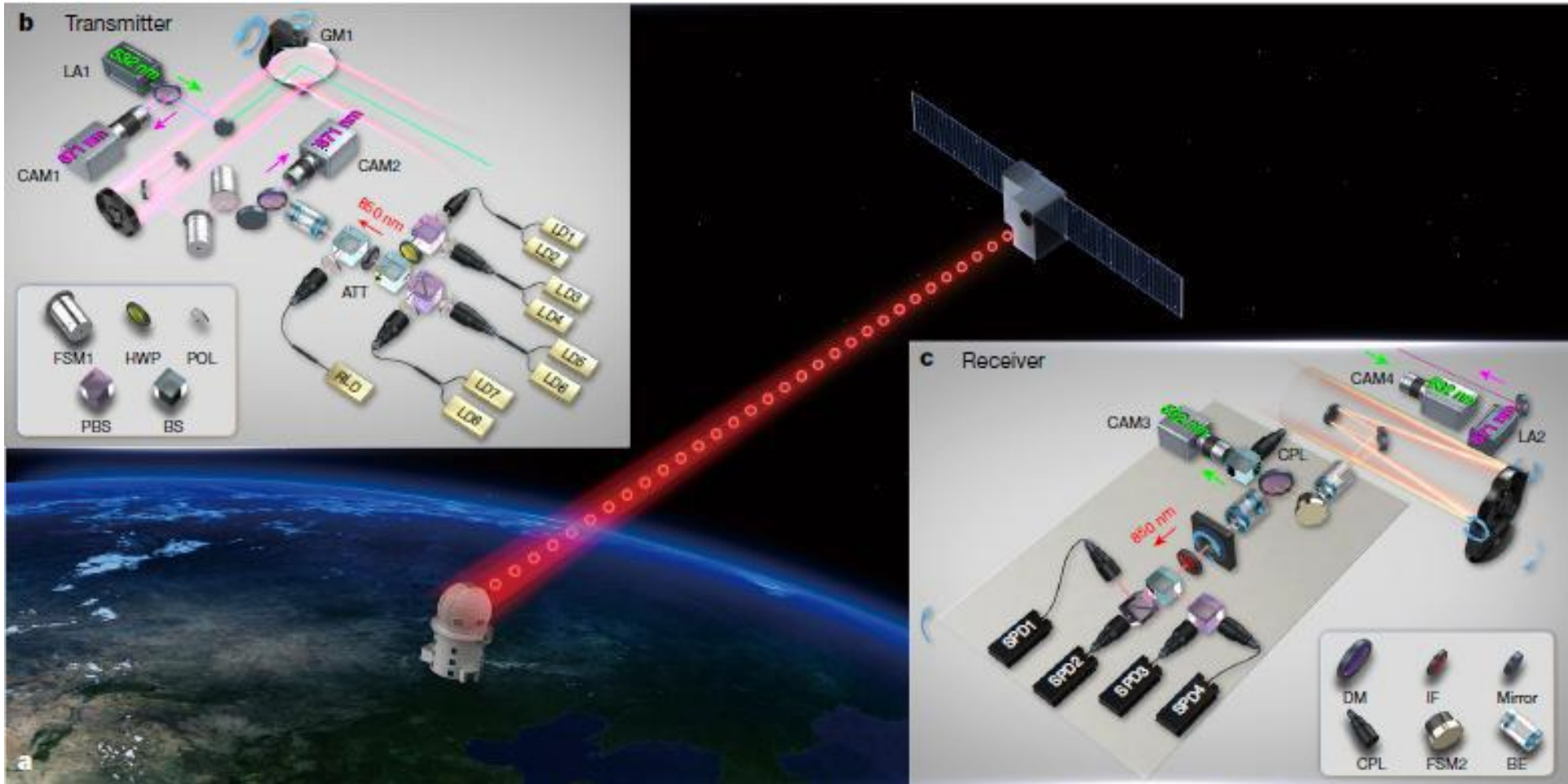
Центр Квантовых Технологий

Спутник Мисиус (Micius, China) 2016

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Источник пар фотонов на борту (KTP, 810 нм); Два передающих телескопа (30 см и 18 см)
Наземные станции: (2 телескопа 1 м, и еще один 1.8 м)

Основные результаты:
2017: Распределение запутанных фотонов на 1200 км
2017: Квантовое распределение ключей со спутника на землю
2018: Спутник как доверенный узел: распределение ключей на 7800 км

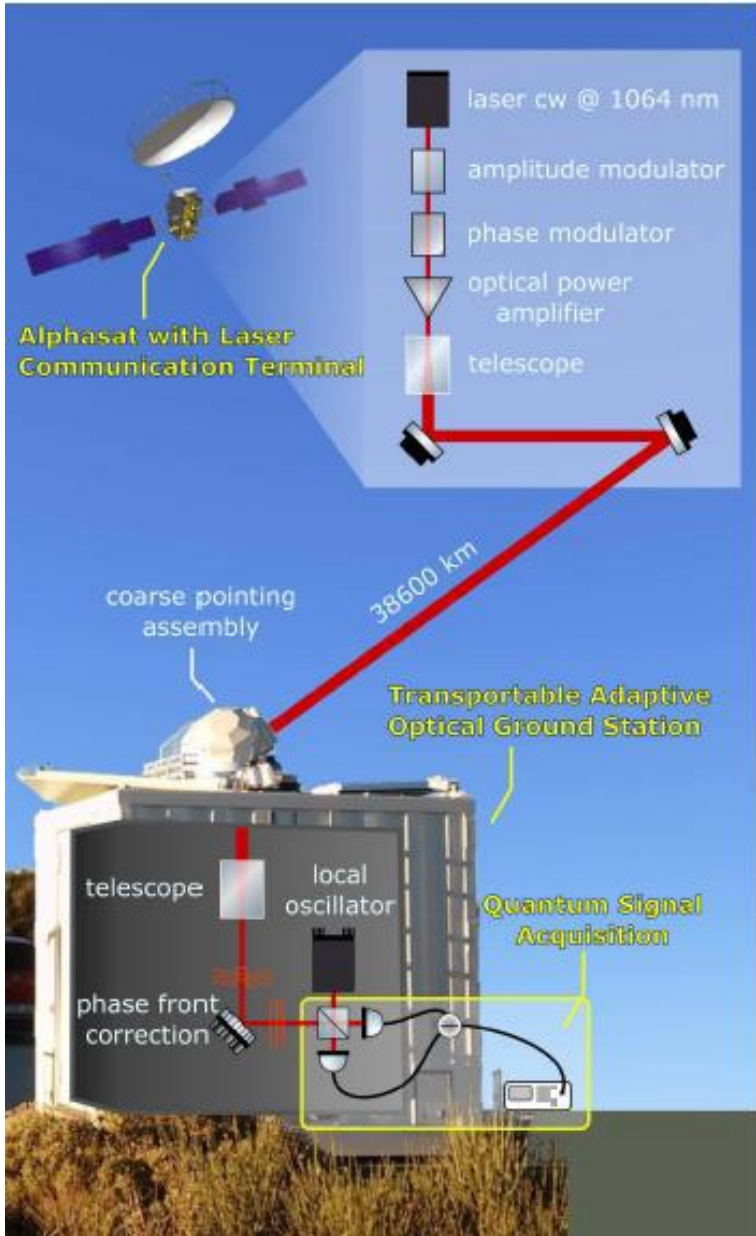


Центр Квантовых Технологий

Квантово-ограниченная передача с геостационарного спутника (Alphasat), 2017

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ
МГУ имени М. В. ЛОМОНОСОВА

Alphasat (Inmarsat-4A F4)
дальность передачи - 38 600 км
Приемная апертура на земле - 27 см
Полные потери - 85 дБ
Длина волны - 1064 нм
Скорость передачи данных - 2.8 Гбит/сек
Бинарная фазовая модуляция



K. Günthner "Quantum-limited measurements of optical signals from a geostationary satellite", Optica, Vol. 4, No. 6, p.611, 2017.

Центр Квантовых Технологий

Квантовая коммуникация: три крупных проекта в ЦКТ МГУ

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ МГУ имени М. В. ЛОМОНОСОВА

1. Квантовый шифратор 10G

МОСКВА, 11 апр 2017 — TADVISER

«На базе технологии, созданной в рамках проекта Фонда перспективных Исследований, Физический факультет МГУ имени М.В.Ломоносова и ОАО «ИнфоТеКС» разработают высокопроизводительный шифратор с квантовым каналом распределения криптографических ключей»

infotecs

2. «Квантовый телефон»

МОСКВА, 13 дек 2017 — РИА Новости

«Ученые из Московского государственного университета создали и проверили на практике линию телефонной связи, защищенную от прослушивания системой квантового шифрования, сообщает пресс-служба вуза»

infotecs

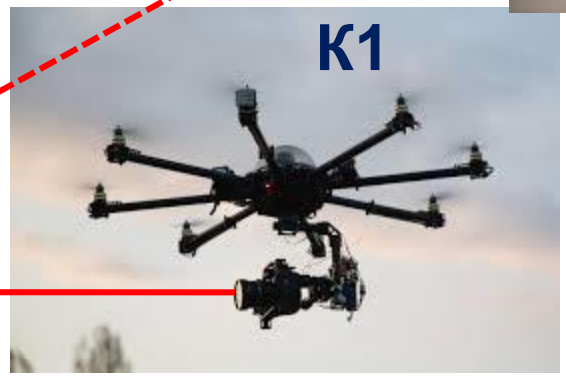
3. Квантовая космическая связь

Проект ФПИ «Звезда» - совместно с РКК Энергия, РФЯЦ-ВНИИЭФ (г. Саров)

КРК между стационарным Объектом и ДРОНом

Распределение ключей между стационарным объектом (Ш) и мобильными летательными аппаратами (К1, К2, К3…) через мобильный летательный аппарат (К).

ПРОТОКОЛ: на перепутанных парах фотонов
Расстояние до 100 м (проект 2019-2020 гг.)



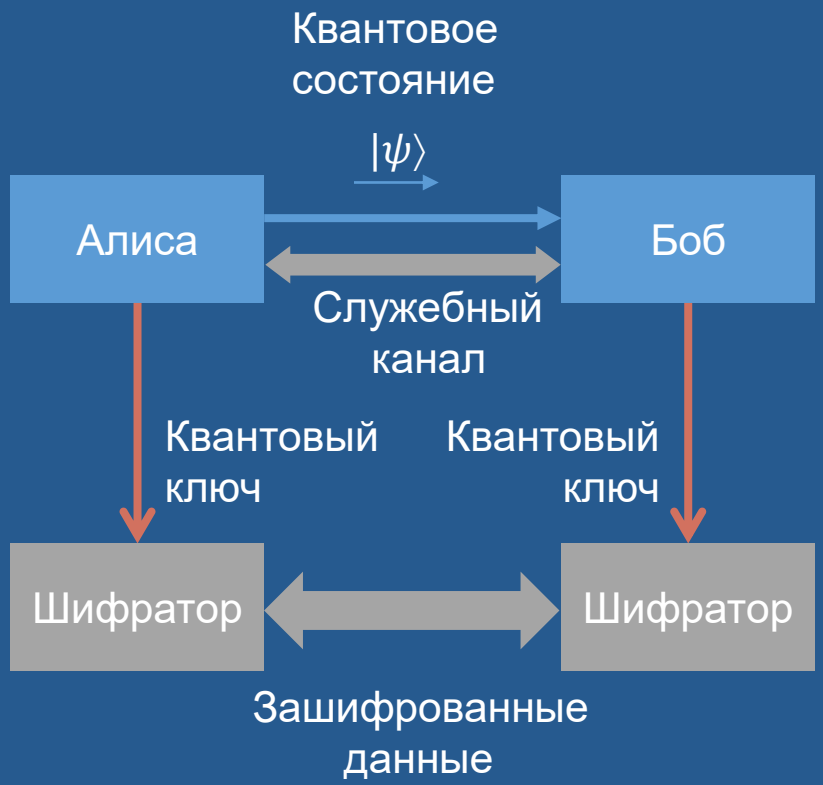
infotecs

Перспективные исследования технологии квантового распределения ключей для защиты информации

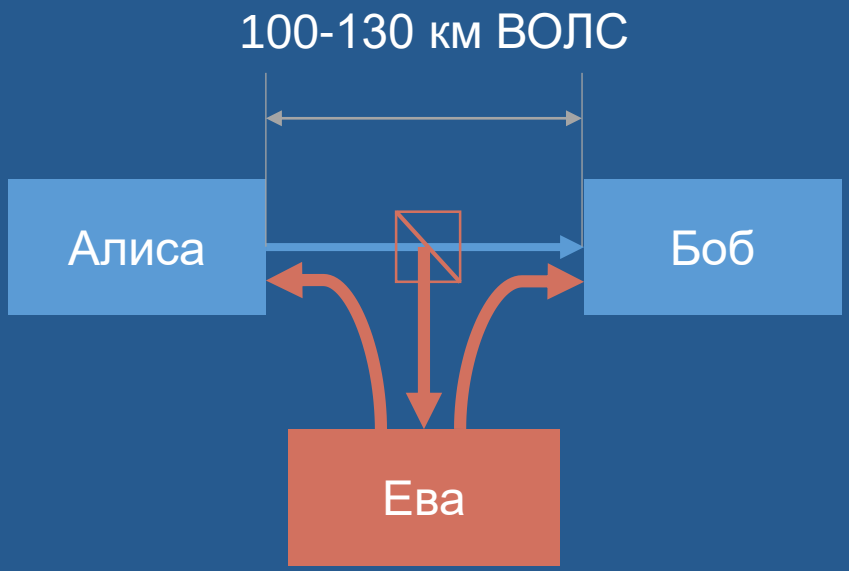
Владимир Елисеев

Что такое квантовое распределение ключей?

- Цель квантового распределения ключей (КРК) – получить общий секретный ключ у двух абонентов, не передавая его
- КРК – это квантово-механический конкурент протокола Диффи-Хеллмана
- Наиболее удобным и надежным является формирование квантовых состояний фотонов, передаваемых по оптоволокну или по открытому пространству
- Квантовое состояние получается путем задания поляризации или сдвига фазы одиночного фотона
- Квантовые состояния невозможно скопировать или усилить, поэтому их невозможно «подслушать» в традиционном смысле этого слова



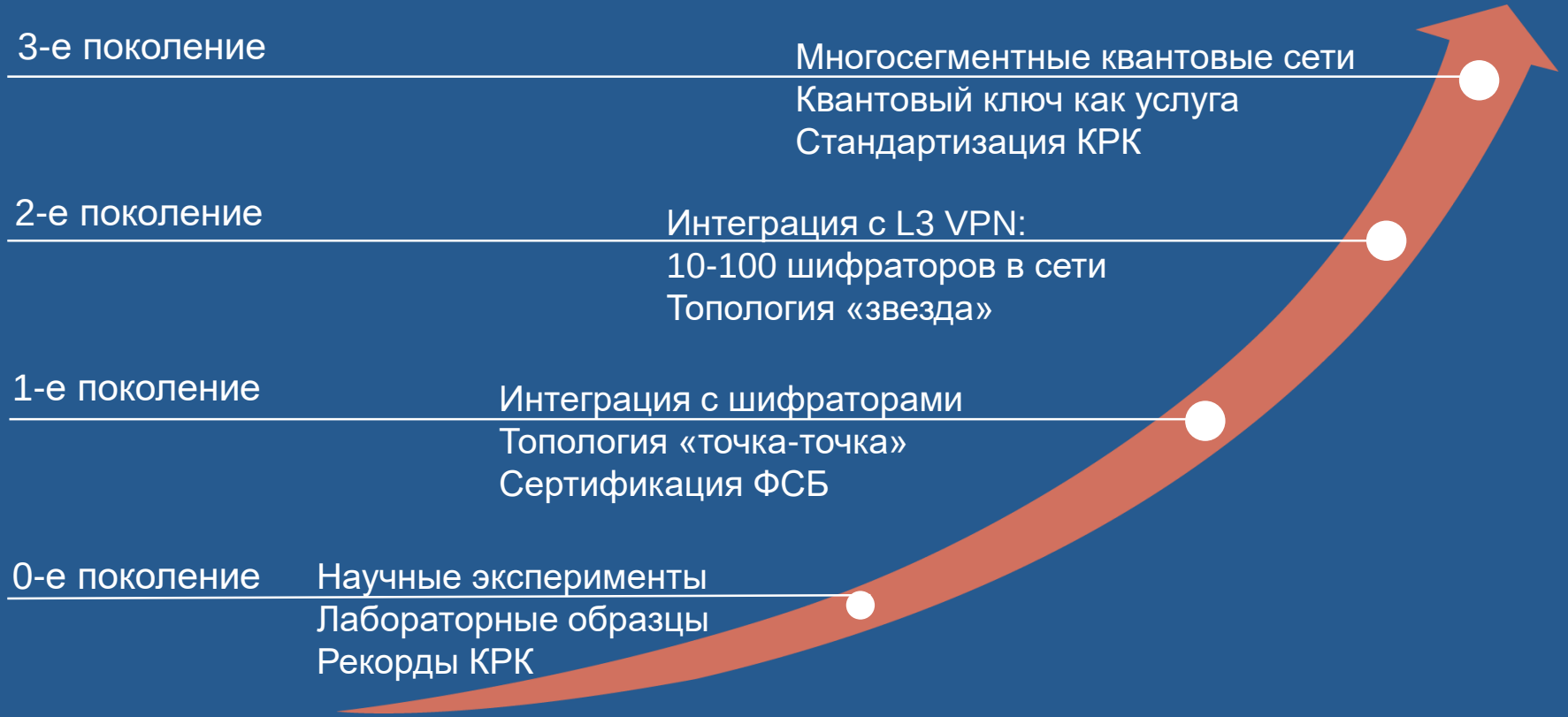
Свойства и ограничения КРК



- Принципиально топология «точка-точка» – не подходит напрямую для сети Интернет с адресацией «каждый с каждым»
- Ограничение по дальности одного сегмента ВОЛС
- Секретный квантовый ключ – только на одном сегменте ВОЛС
- КРК на околоземный спутник позволит кардинально решить вопрос ограничения расстояний
- Аппаратура КРК является частным случаем системы криптографической защиты информации (СКЗИ)
- Необходима сертификация ФСБ
- На протоколы и аппаратуру КРК тоже есть атаки, от которых необходимо защищаться

Развитие систем КРК

infotecs



Исследование точности и надежности аппаратуры КРК

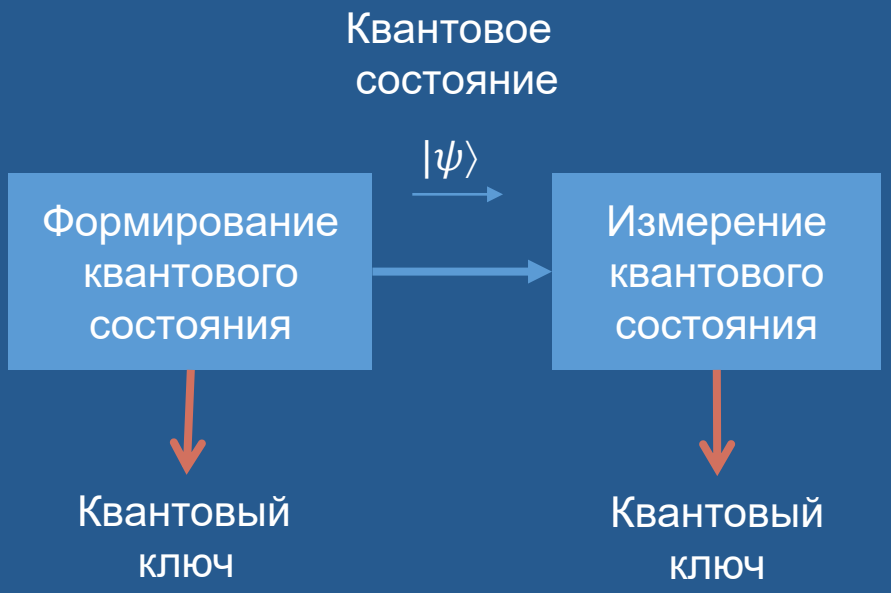
infotecs

Многие системы КРК можно представить в виде:

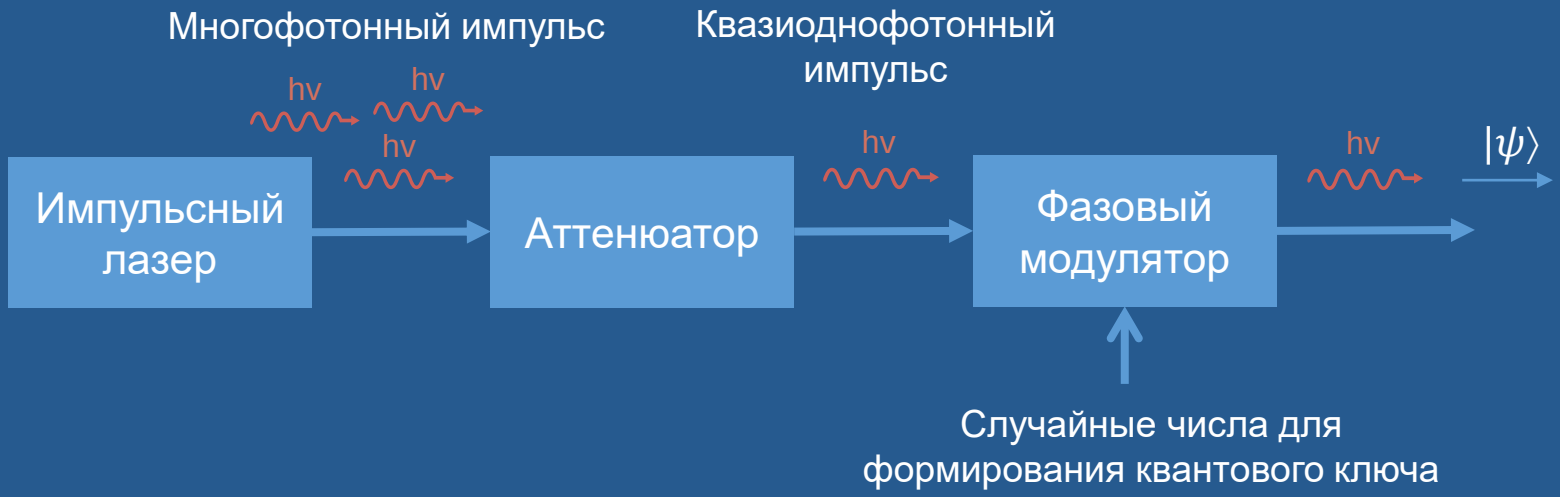
- Алиса – формирование квантового состояния
- Боб – измерение квантового состояния

Требования сертификации и эксплуатации:

- Точность реализации протокола КРК с учетом характеристик элементов
- Влияние надежности элементов на корректность и эффективность реализации протокола КРК
- Оценка реализованных мер защиты с учетом характеристик элементов

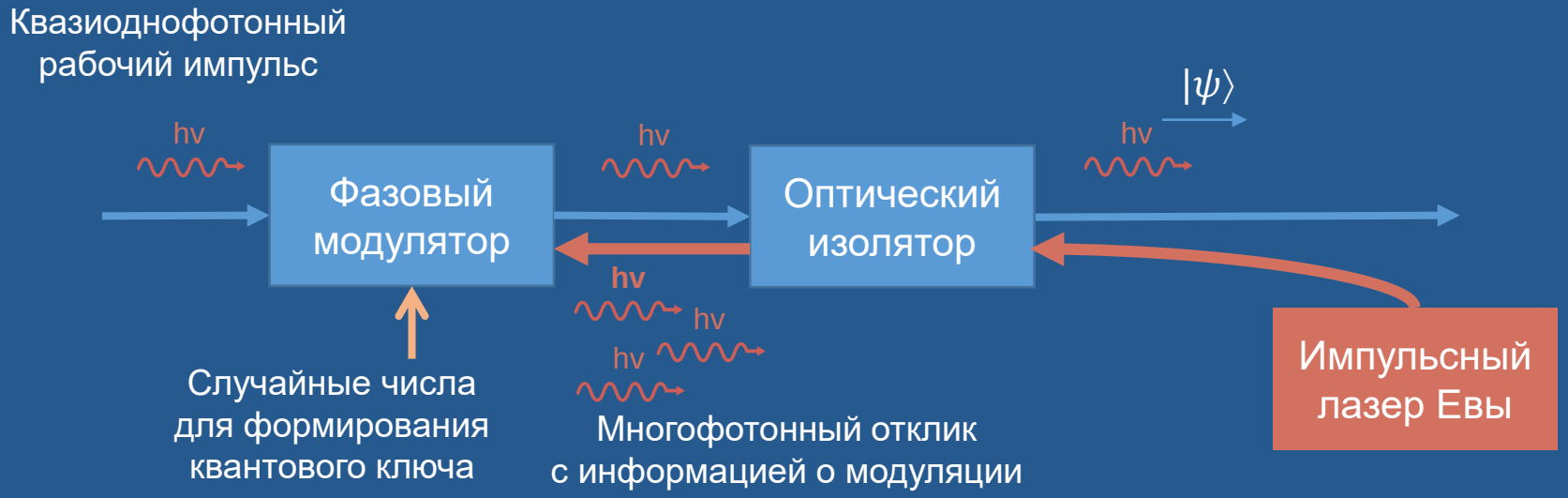


Точность и надежность переменного аттенюатора



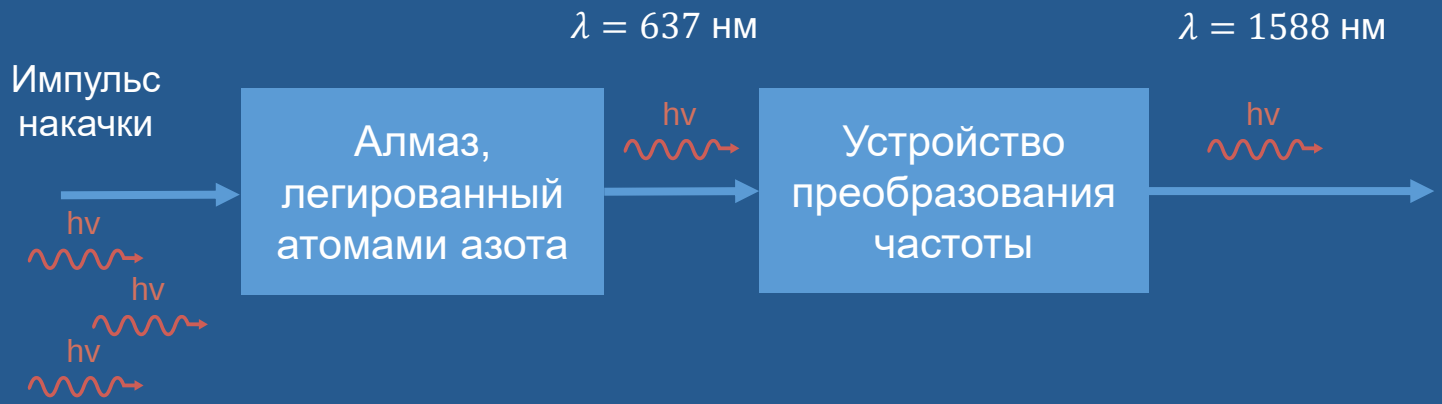
- Секретность систем КРК основана на формировании квантовых состояний на одиночных фотонах
- Реальные многофотонные импульсы делаются путем ослабления до почти однофотонного уровня
- Точность и надежность переменного аттенюатора – залог секретности формирования квантового ключа

Спектральные характеристики оптического изолятора



- В атаке активного зондирования Ева узнаёт случайные числа на фазовом модуляторе по отклику и нарушает секретность формируемого квантового ключа
- Для защиты от зондирования нужен оптический изолятор, пропускающий фотоны в одном направлении
- Необходимо исследовать спектральные характеристики оптического изолятора для предотвращения зондирования на нештатных для изолятора длинах волн, где его изолирующие свойства становятся хуже

Формирование истинно однофотонного импульса *



- Вероятность излучения двух и более фотонов существенно ниже, чем при ослаблении аттенюатором
- По этой причине у Евы значительно меньше возможностей для эффективной PNS атаки
- Большой потенциал не только для КРК, но и для оптических квантовых вычислителей

* Работа поддержана Минобрнауки России и ведется совместно с ВНИИОФИ

Выход за рамки одного сегмента волоконно-оптической сети

Основные ограничения базовой технологии КРК:

- Ограниченная дальность выработки квантового ключа в ВОЛС на уровне 100-130 км
- Квантовый ключ всегда вырабатывается в топологии «точка-точка»

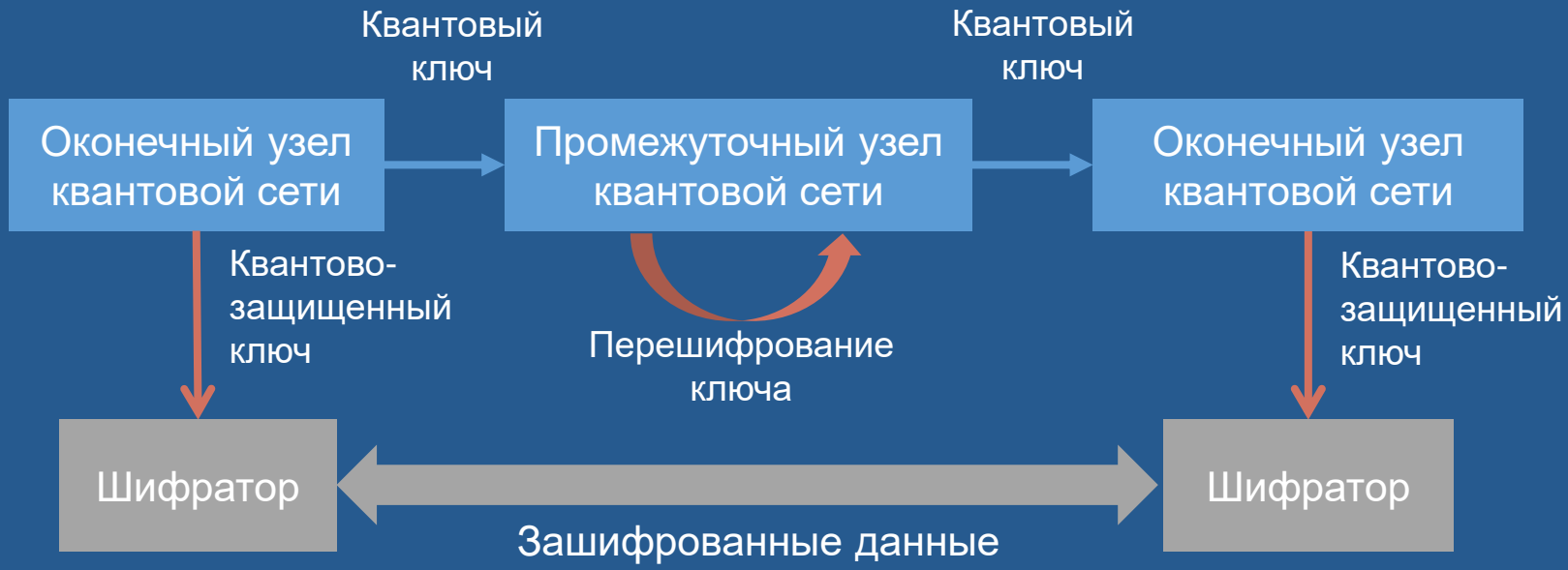
Современные потребности:

- Сети передачи данных реализуют логическую топологию «каждый с каждым»
- Протяженность телекоммуникационных линий может достигать тысяч километров

Многосегментные сети КРК с доверенными узлами:

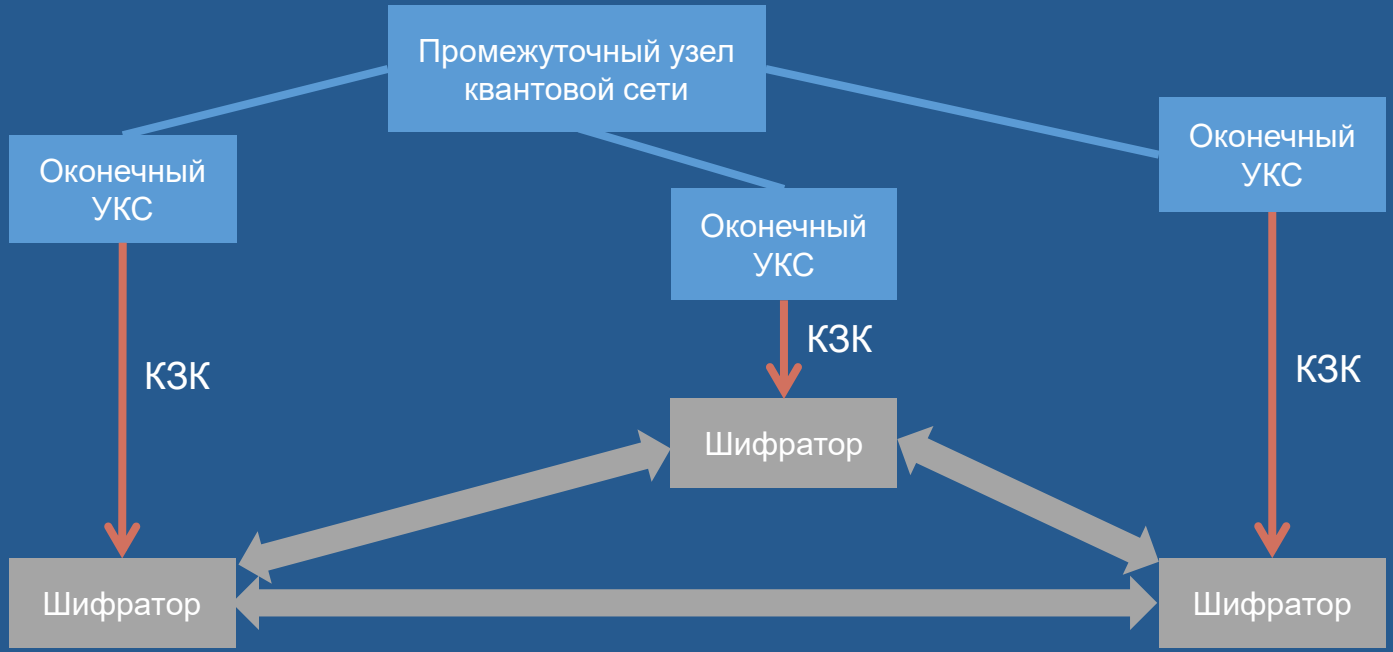
- На основе ВОЛС
- С сегментами открытого пространства
- С сегментами на космические спутники

Многосегментная сеть КРК с доверенными узлами



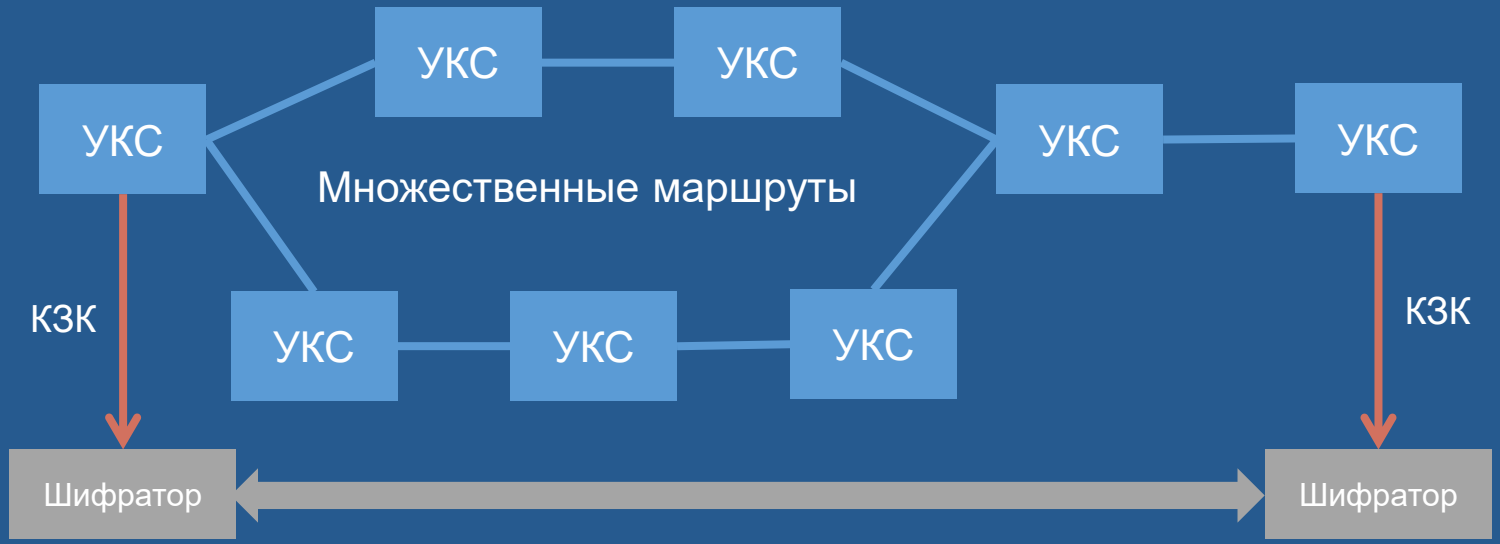
- Квантово-защищенный ключ (КЗК) передается по сети под защитой квантовых ключей на сегментах
- КЗК используется шифраторами как аналог квантового ключа

Многосегментная сеть КРК масштаба мегаполиса/региона



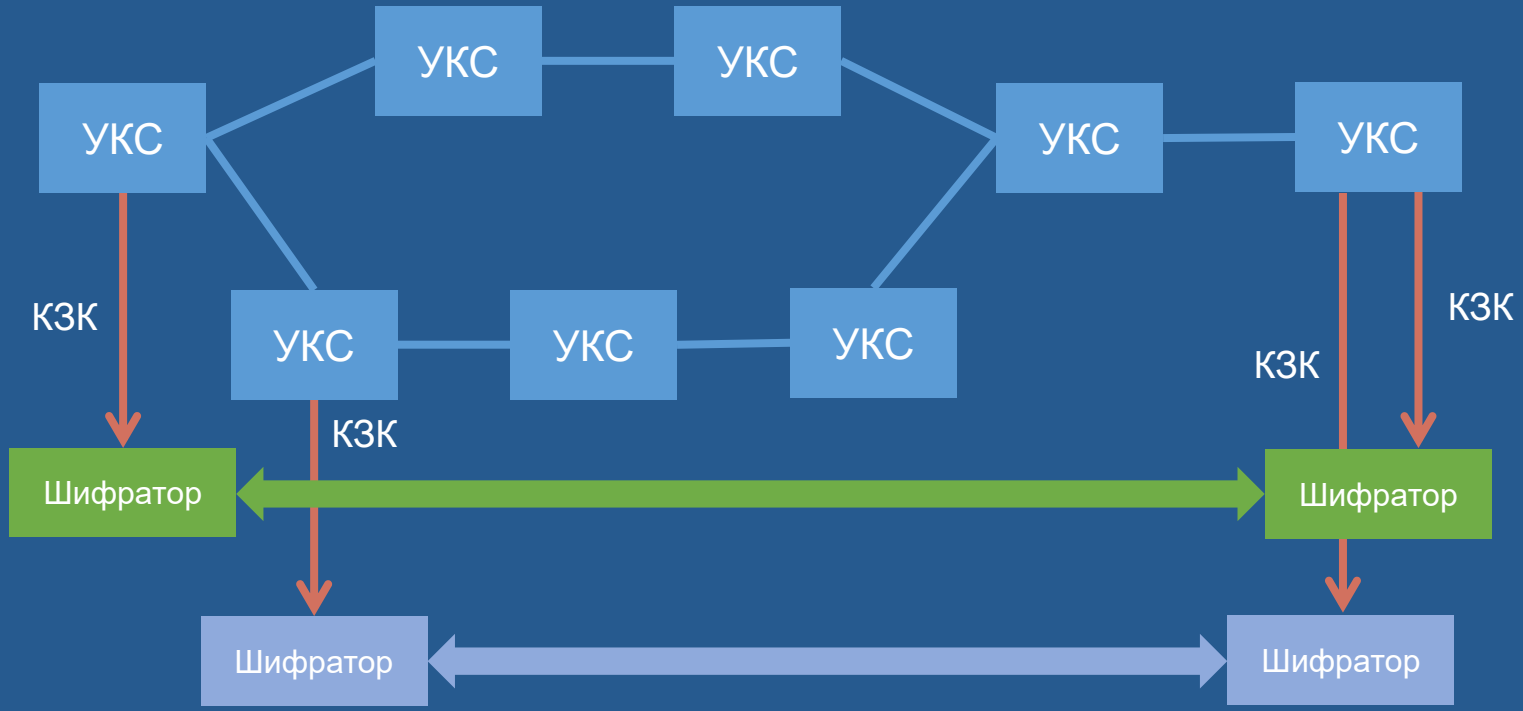
- Топология «звезда» сети КРК с помощью доверенного промежуточного узла в центре превращается в топологию «каждый с каждым» для шифраторов
- Технология отработана в проекте «Квантовый телефон» и реализуется в проекте ViPNet Quantum Security System (QSS)

Многосегментная сеть КРК масштаба страны



- Дублирование маршрутов для повышения производительности и отказоустойчивости
- Сочетание преимуществ топологии «магистраль» и «звезда»
- Подключение шифраторов различных производителей к узлам квантовой сети
- Технология построения квантовых сетей востребована лидерами рынка телекоммуникаций

Квантово-защищенный ключ как услуга квантовой сети



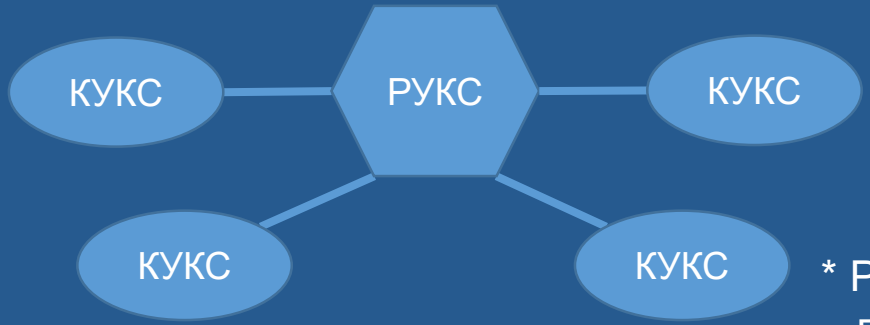
- Подключение шифраторов различных владельцев к узлам квантовой сети
- Необходимо стандартизовать протокол подключения шифраторов к узлам сети

Разработка технологии и аппаратуры квантовых сетей *

Базовые элементы квантовых сетей:

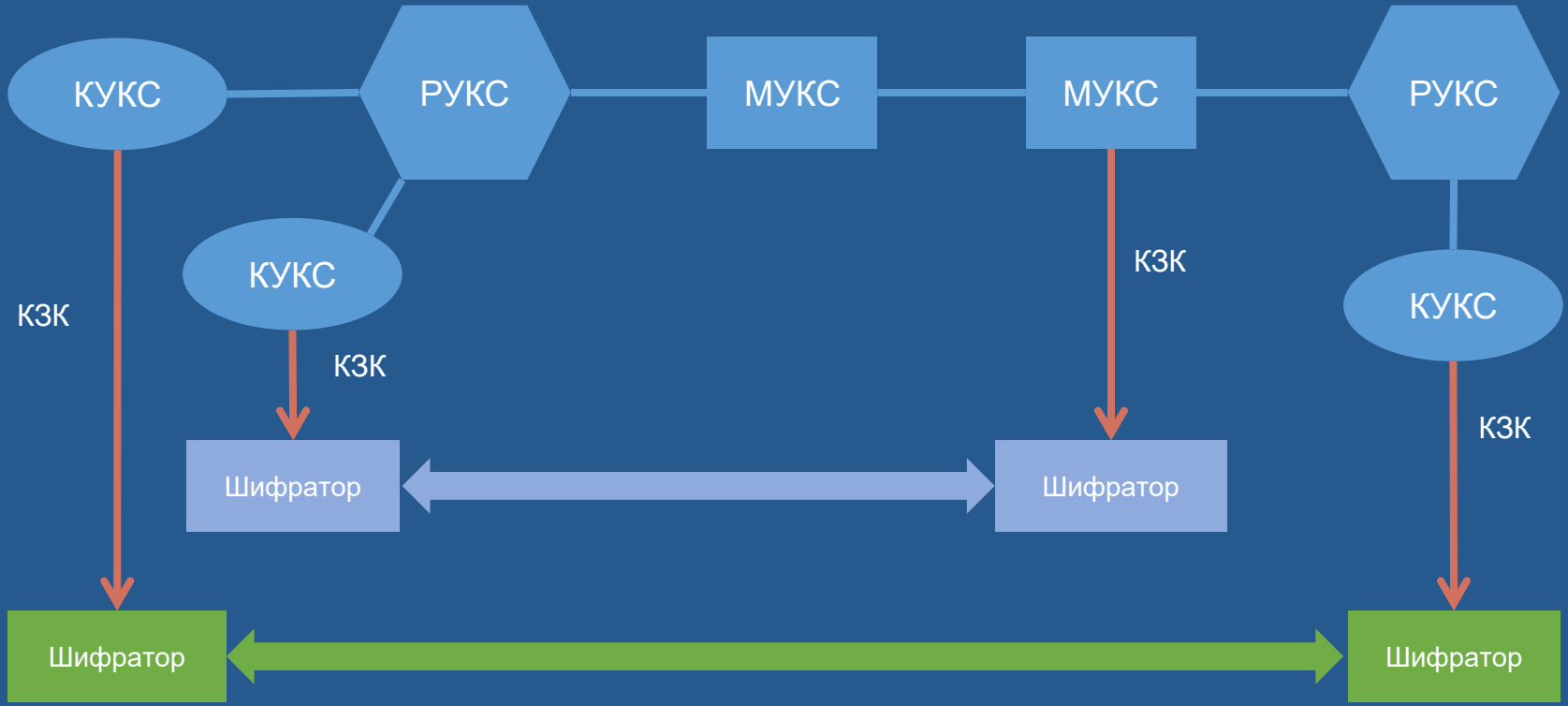
- Магистральный узел квантовой сети (МУКС)

- Распределительный узел квантовой сети (РУКС)
- Клиентский узел квантовой сети (КУКС)

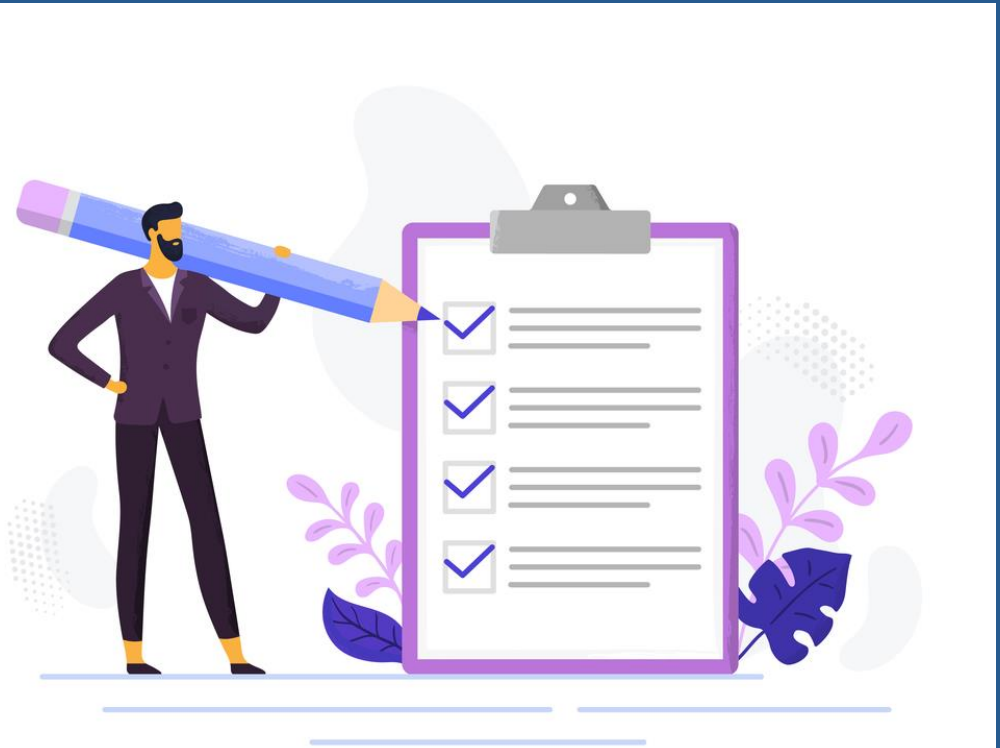


* Работа поддержана Министерством промышленности и торговли России

Пример квантовой сети на основе разрабатываемых узлов



План разработки технологии и аппаратуры квантовых сетей



2020

- Эскизное проектирование
- Техническое проектирование

2021

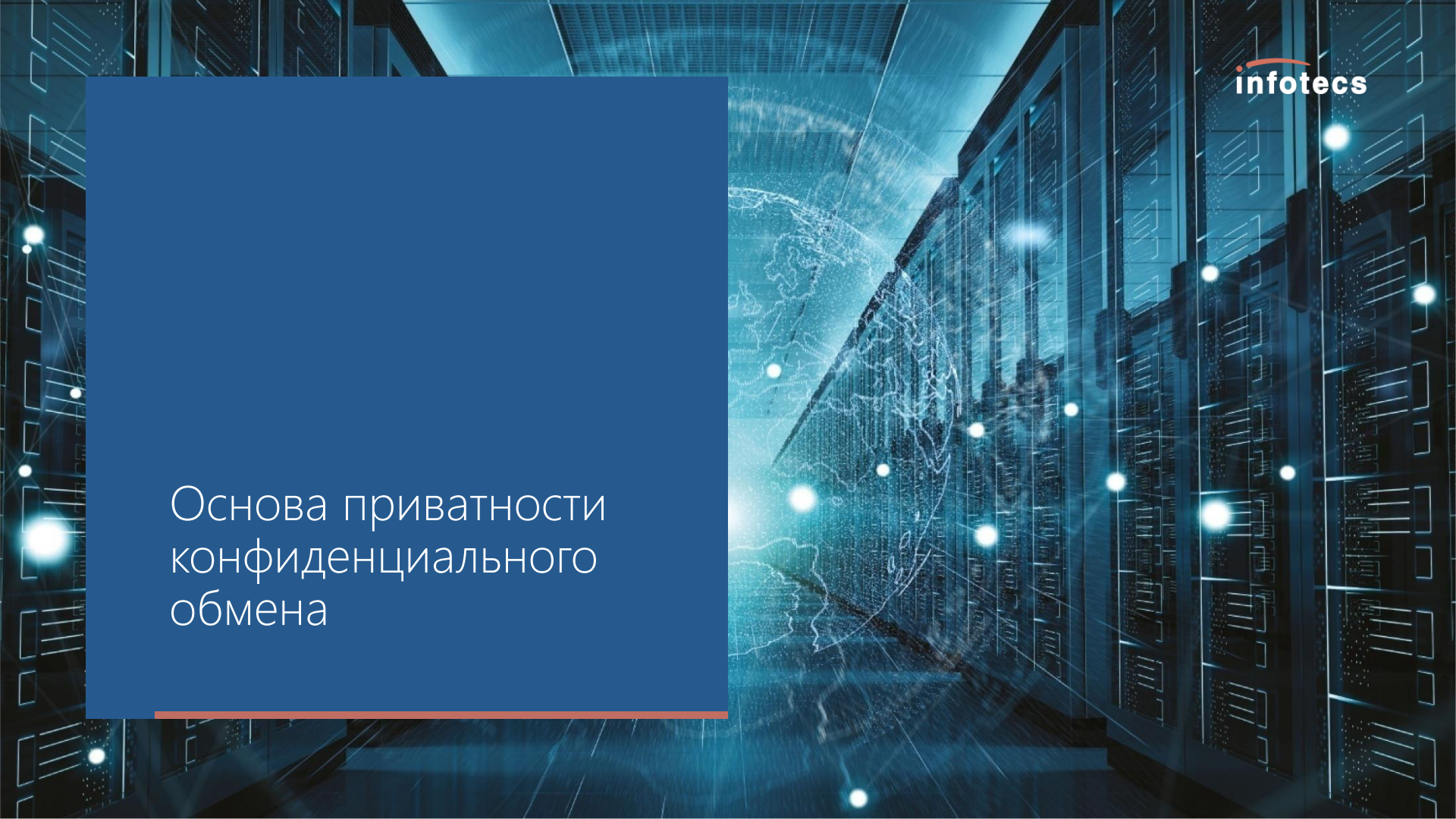
- Подготовка конструкторской документации
- Разработка опытных образцов
- Макет квантовой сети

2022

- Производство
- Сертификация

Технология КРК в продуктах ИнфоТеКС. Уровень готовности и планы развития

Александр Поздняков



Основа приватности конфиденциального обмена

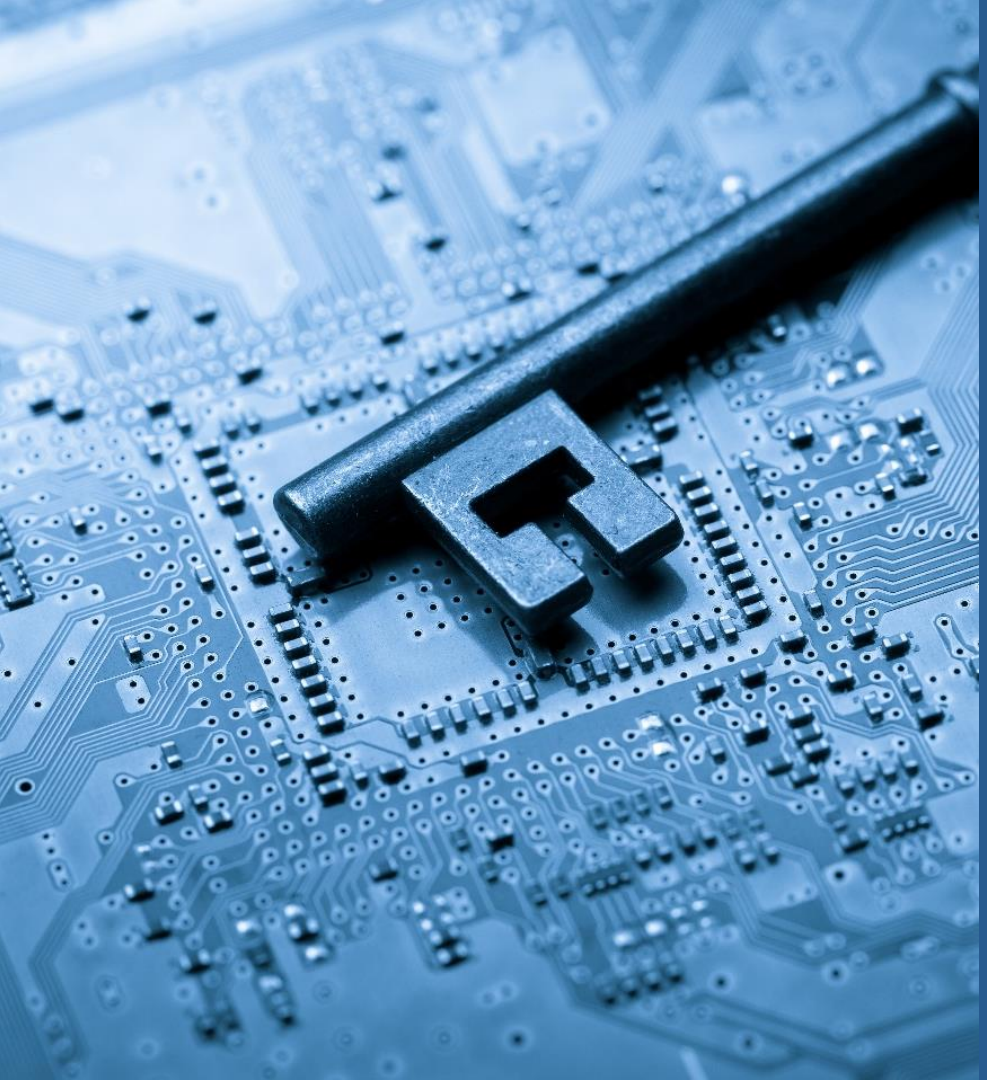
Враг знает систему» © Клод Шеннон

Из максимы Шенона следует:

- Секретность алгоритмов шифрования и аппаратной реализации **не определяют** стойкость криптосистемы
- Стойкость криптосистемы определяется лишь **секретностью ключа**

Остается главный вопрос:

Откуда взять ключ?



infotecs

Откуда обычно берутся секретные ключи?

- Доверенный курьер **доставляет ключи** из ключевого центра

  или

- Ключи **вычисляют** при условии двусторонней аутентификации (ассиметричные алгоритмы)

Проблемы всех классических механизмов распределения ключей

- Не обеспечивается безусловная и доказуемая математически секретность ключей. Доверие к криптографическим ключам основано лишь на предположении, что у злоумышленника нет достаточного количества вычислительных ресурсов и предположении о том, что злоумышленнику не известен эффективный алгоритм взлома. (Доказать, что такого алгоритма нет, невозможно)
- Дорогостоящие организационно-технические меры. Чем больше людей, участвующих в процессе, тем сложнее обеспечить секретность
- Всегда есть «человеческий фактор»
- Создание квантового компьютера приведет к компрометации всех ассиметричных криптографических алгоритмов и протоколов на их основе (DH, RSA, ECDSA TLS/SSL, HTTPS, IPsec, X.509)
- Не обеспечивают быструю смену ключей автоматически, без участия администратора

Новый вид СКЗИ с использованием технологии квантового распределения ключей

Секретность выработки квантовых ключей основана на следующих квантовых принципах:

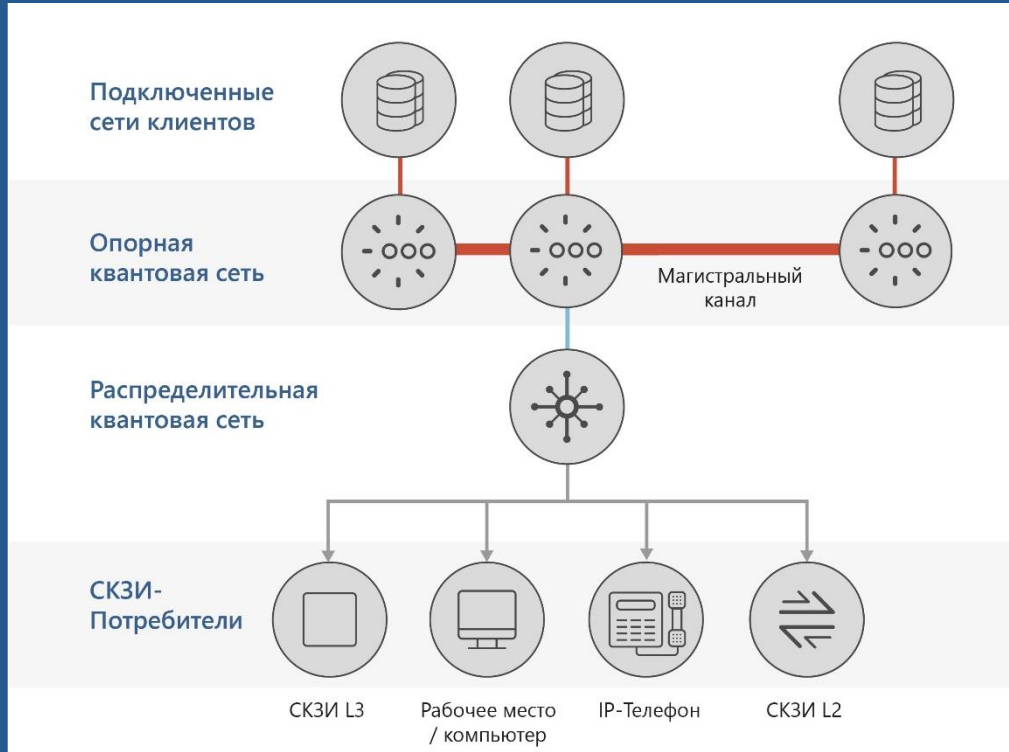
1. Фотон неделим
2. Невозможно клонировать неизвестное квантовое состояние
3. Невозможно измерить квантовое состояние без его изменения
4. Невозможно различить два неортогональных квантовых состояния

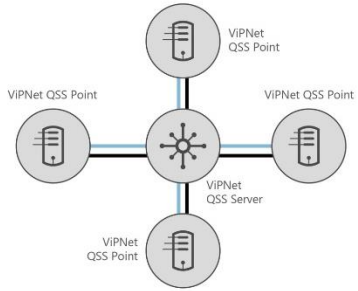
Преимущества технологии квантового распределения ключей

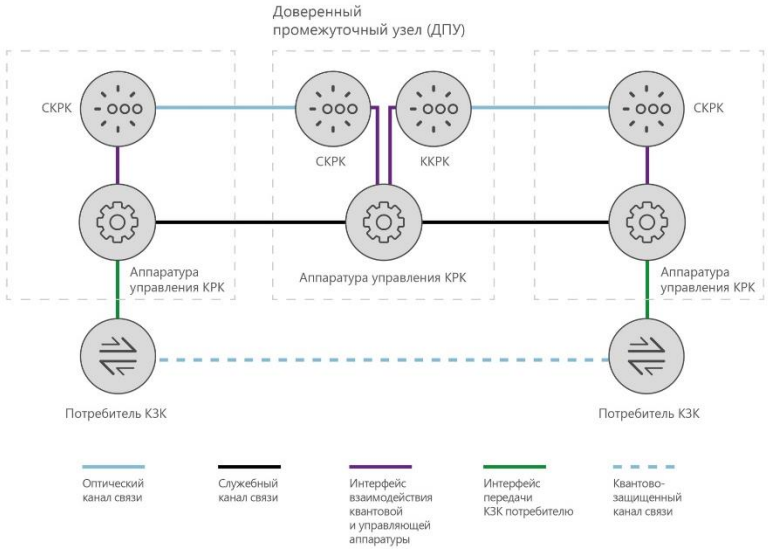
1. Безусловная **секретность** квантовых ключей **доказана** математически
2. Выработка ключей и загрузка в шифратор происходит автоматически – **без** участия администратора
3. Обеспечивается стойкость к криптографическим атакам при помощи квантового компьютера
4. Высокая скорость смены ключей

Концепция развития технологии квантового распределения ключей в ИнфоТеКС

- Квантовая сеть произвольной топологии
- Криптографические ключи с доказательством секретности
- Без использования асимметричных криптографических механизмов
- Ключи неизвестны администратору сети
- Автоматическая смена ключей во всей сети
- Не явная компрометация одного узла (например, увольнение администратора ИБ) не приводит к необходимости переинициализации всей сети





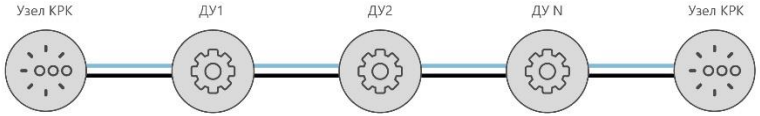


infotecs

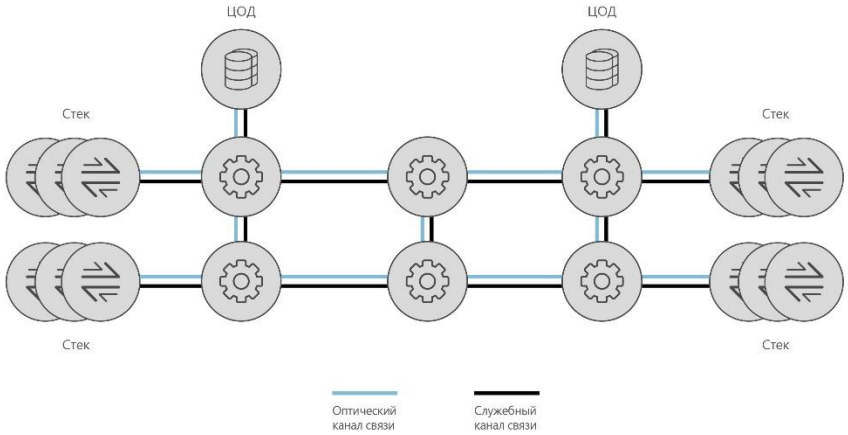
Пошаговое развитие топологии квантовых сетей

- В основе квантовой сети произвольной топологии – технология доверенного промежуточного узла
- Все «квантовые» продукты в одной сети

Квантовая магистраль



Квантовая сеть произвольной топологии на базе доверенных промежуточных узлов



Пошаговое развитие топологии квантовых сетей

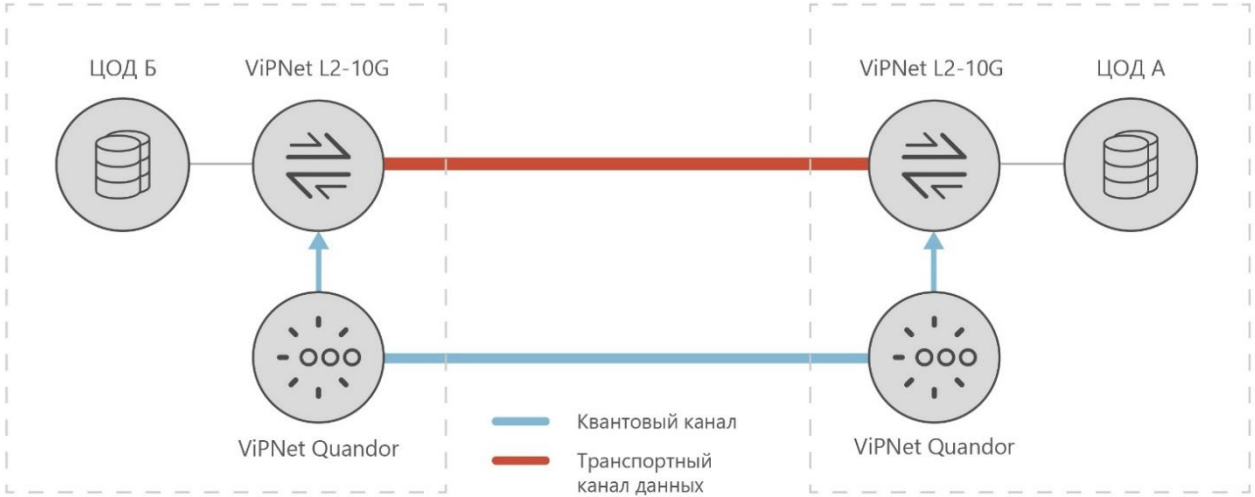
- В основе квантовой сети произвольной топологии – технология доверенного промежуточного узла
- Все «квантовые» продукты в одной сети
- Подключение к квантовой сети любых СКЗИ

ViPNet Quandor

Система автоматической доверенной доставки криптографических ключей

Совместный проект ОАО «ИнфоТеКС»
и МГУ имени М.В. Ломоносова

infotecs



ViPNet Quandor

Базовый сценарий – автоматическая доверенная доставка криптографических ключей для канальных шифраторов ViPNet L2.

Для использования квантовых ключей к шифратору по защищенному интерфейсу подключается аппаратура ViPNet Quandor, которая устанавливается в контролируемой зоне шифратора

infotecs

Стенд для внутренней эксплуатации ViPNet Quandor в ИнфоТеКС

Отечественное серийное производство

- Первый образец, изготовленный на собственном производстве
- Прошел все инженерные испытания
- На стадии сертификации в ФСБ России
- Готовность к поставкам

Комплект оборудования для пилотной эксплуатации ViPNet Quandor на сетях заказчика

- Мобильный комплект для быстрого разворачивания на сетях заказчика
- Защита во время транспортировки
- Минимальные затраты времени на ввод в эксплуатацию
- Демонстрация рабочего решения, готового к поставкам

ТТХ решения ViPNet Quandor

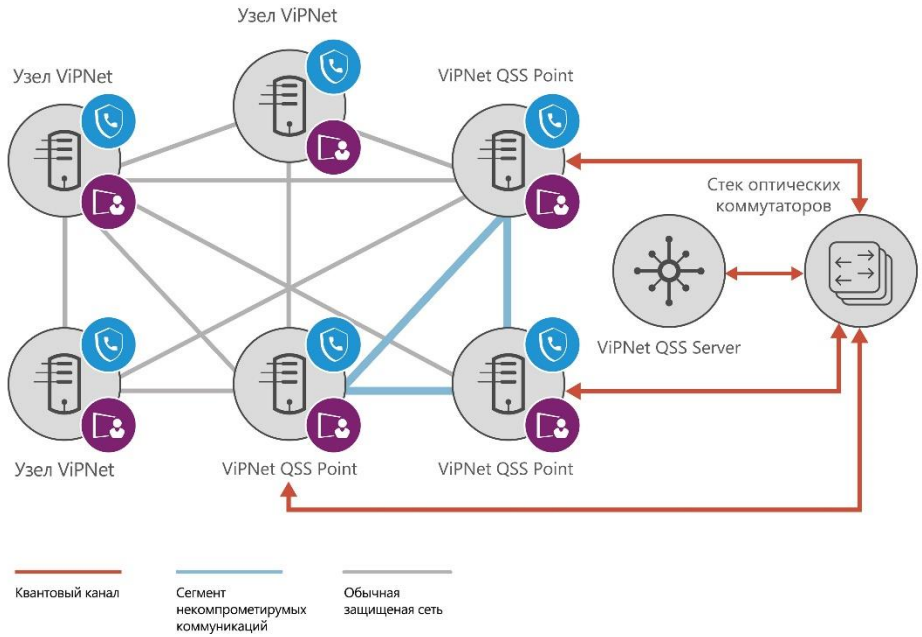
- Длина квантового канала 100 км (130 км – экспериментальный предел при идеальных условиях)
- Скорость шифрования и имитозащиты 20 Гбит/с в режиме дуплекс
- Задержка шифрования не более 15 мкс
- Не требует дополнительного охлаждения
- Устанавливается в стандартную стойку
- Автоматическая смена ключей 1 раз в минуту
- Гибридная ключевая система на квантовых и предраспределенных ключах. Физический вывод из строя квантового канала и оборудования не приведет к остановке шифрования
- Скорость загрузки нового КК – 1 ключ/мин.
- ФДСЧ на квантовых эффектах обеспечивает истинную случайность вырабатываемых ключей
- СКЗИ класса КС3 (все технические решения принимались с расчетом последующей сертификации на класс КВ, в плане на 2021 год)

В процессе исследования 8 центром ФСБ России

ViPNet QSS

ViPNet Quantum Security System

infotecs



Совместный проект ОАО «ИнфоТеКС» и МГУ имени М.В. Ломоносова

Оборудование квантового распределения ключей (КРК) сопряженное с ПО ViPNet Client и Connect на телефонах абонентов

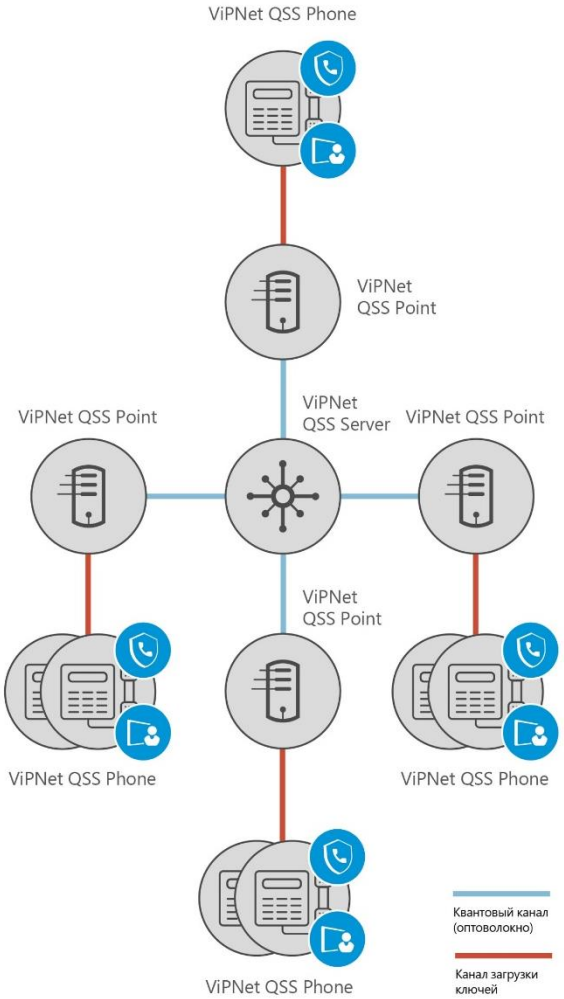
ViPNet **VPN**

ViPNet **Client**

ViPNet **Connect**

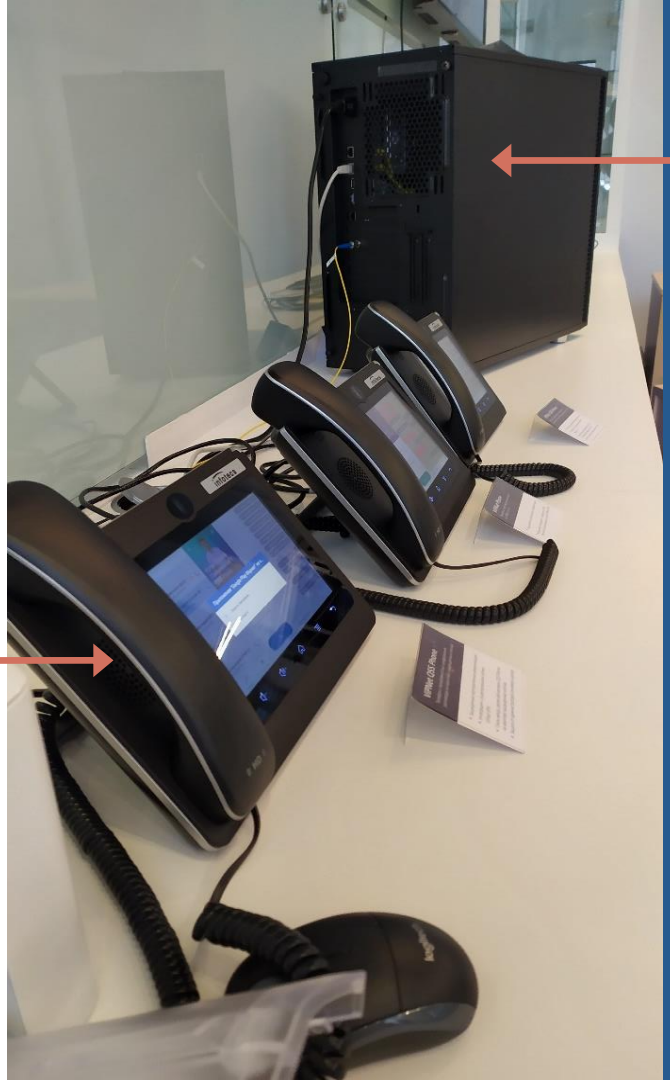
Особенности

- Распределяет квантовые ключи по сетевой топологии «Звезда» для практически неограниченного количества абонентов
- Бесшовная интеграция с существующими сетями на базе технологии ViPNet
- Не подвержен атакам, которые станут возможными при реализации эффективного квантового компьютера
- Стойкость квантового протокола математически доказана
- Шифрование телефонного трафика на ключах, не известных даже администратору сети
- Возможность выработки на одном Клиенте квантовозащищенных ключей для нескольких абонентов
- Полностью автоматическая регулярная смена ключей шифрования
- Пользователь сам может запросить выработку нового ключа в любой момент



Стенд в ИнфоТеКС

Потребители ключей. IP-телефоны – ViPNet QSS Phone



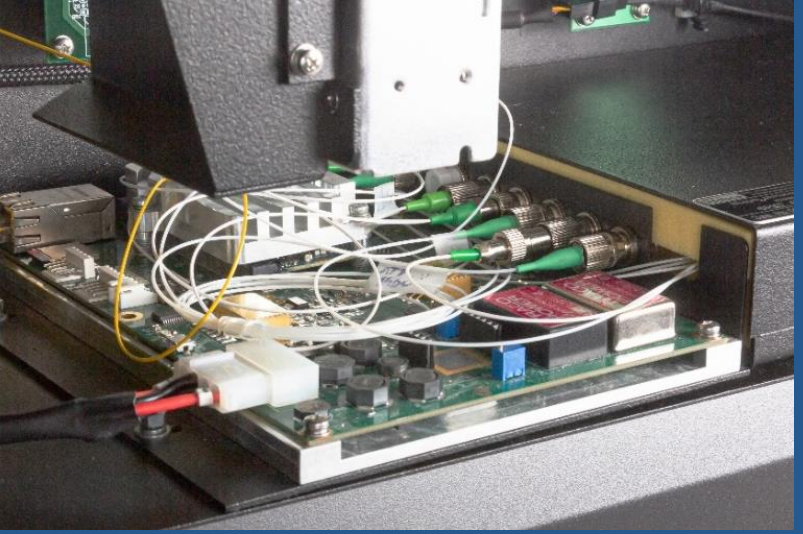
Клиент квантового распределения ключей – ViPNet QSS Point

Стенд
в ИнфоТеКС

Оптический коммутатор –
ViPNet QSS Switch

Сервер квантового
распределения ключей –
ViPNet QSS Server

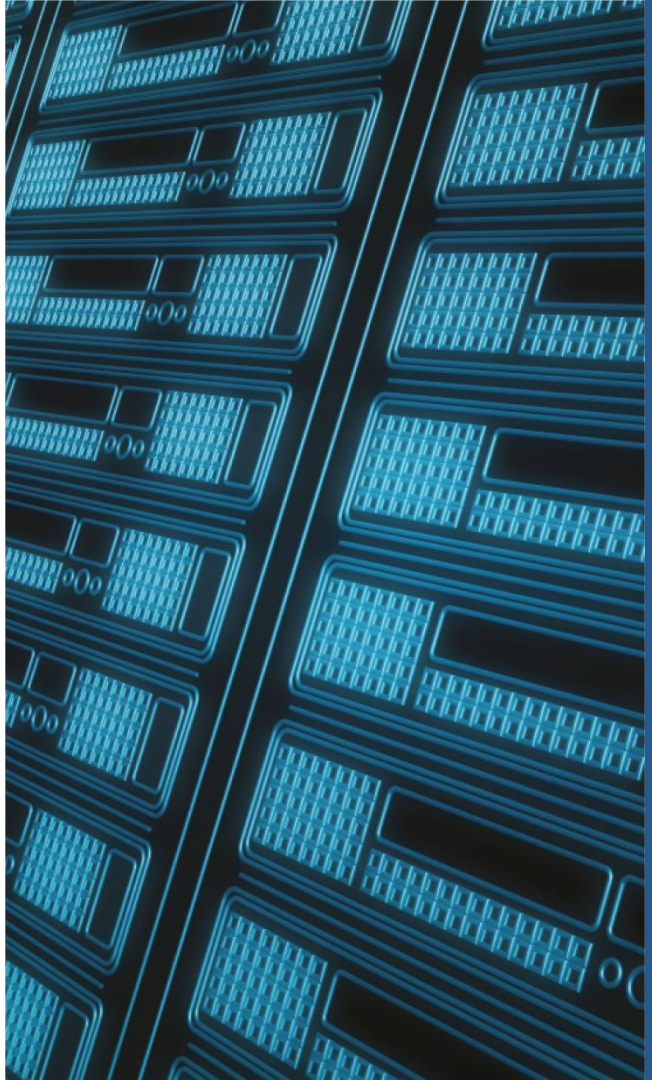
Отечественное серийное производство ViPNet QSS Point



- ✓ Высокий уровень локализации
- ✓ Оптимизирована логистика поставки комплектующих
- ✓ Отработан технологический процесс

Некоторые ТТХ ViPNet QSS

- Топология «Звезда»
- Расстояние между QSS Server и QSS Point до 44 км
- 3 уровня оптической коммутации с резервированием каналов
- До 1600 Клиентов КРК (ViPNet QSS Point, подключенных к серверу ViPNet QSS Server)
- К одному ViPNet QSS Point можно подключить много потребителей ключей (ViPNet QSS Phone) в пределах одной зоны доверия



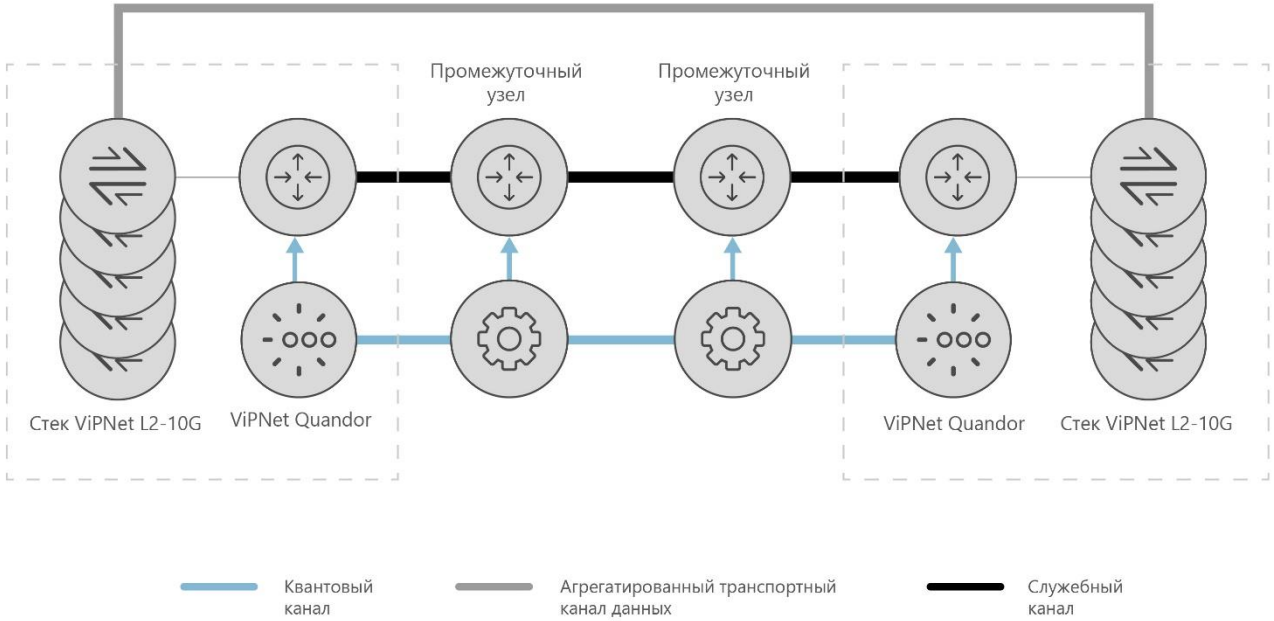
infotecs

- Класс защиты ViPNet QSS Server и ViPNet QSS Point - КС3 (Все аппаратные решения соответствуют классу КВ, в планах весь комплекс «дотянуть» до КВ)
- ViPNet QSS Phone (Android) – КС1
- В планах создание телефона на OS Linux на класс КВ
- Возможно размещение в категорируемых помещениях

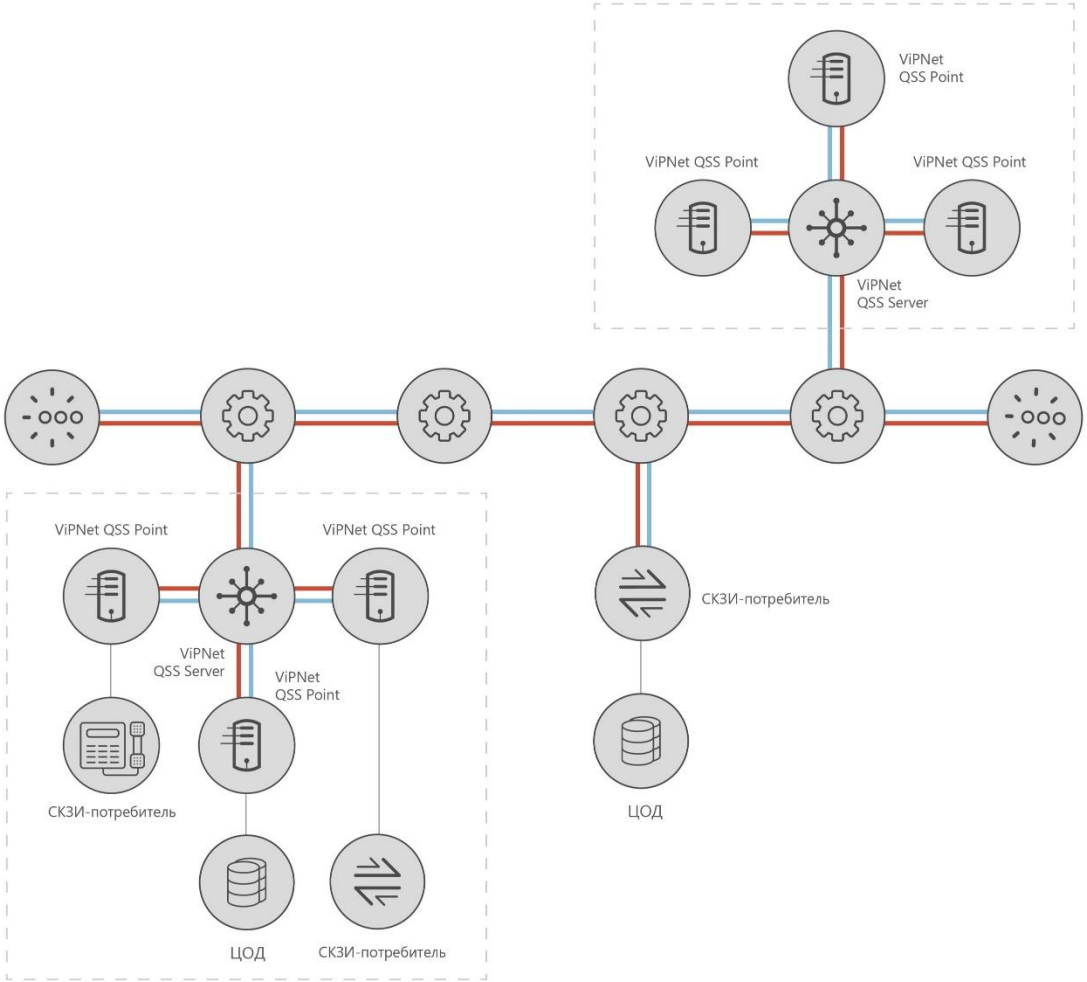
ТЗ согласовано с 8 центром ФСБ России

ViPNet Quantum Trusted Node

Магистральный сегмент. Опорная сеть



Перспективная квантовая магистраль



infotecs

Квантовая сеть произвольной топологии

- Сервис предоставления ключей
- Сервис предоставления защищенного канала
- Мультиарендность

infotecs

Обзор активностей по стандартизации в области квантового распределения ключей

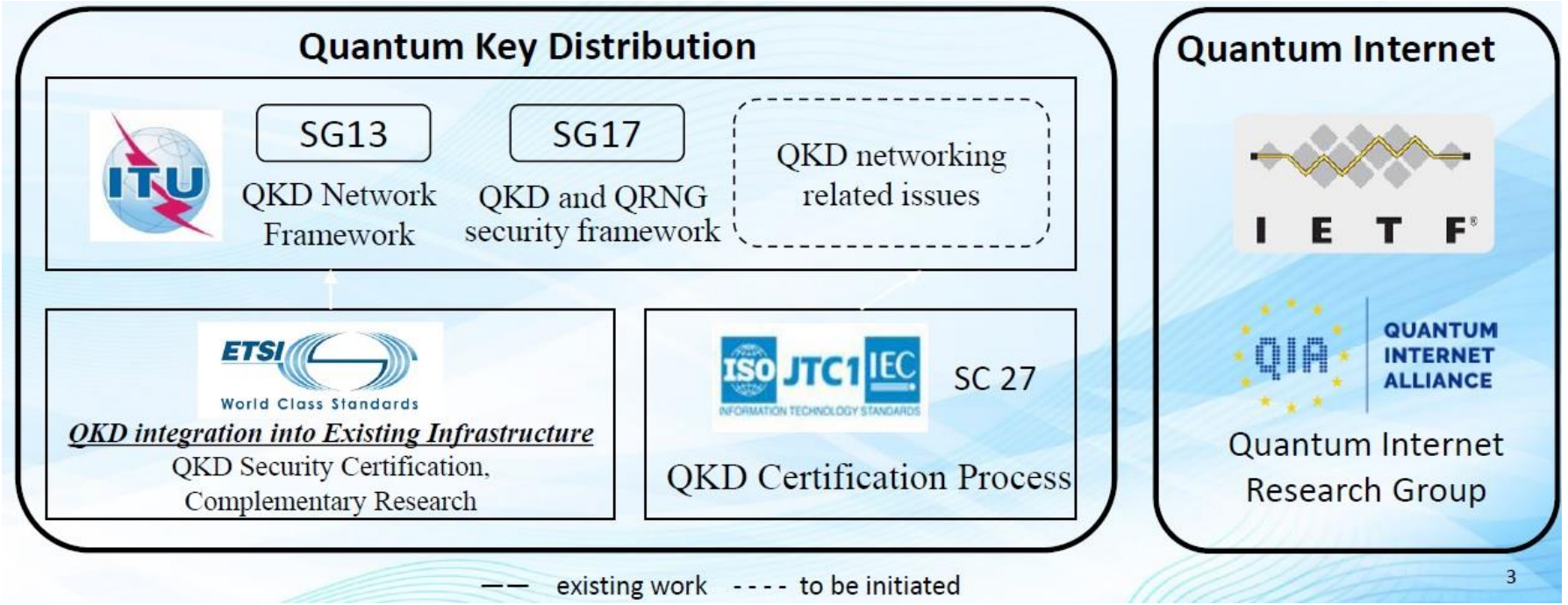
Алексей Уривский

Стандартизация КРК

Органы по стандартизации

- Отраслевые/индустриальные
- Региональные/национальные
- Международные

Организации и активности



Индустриальные органы по стандартизации

IETF – Quantum Internet Proposed Research Group (QIRG)

- **Draft "Architectural Principles for a Quantum Internet" (Inf)**
- **Draft "Applications and Use Cases for the Quantum Internet" (Inf)**
- **Draft "Connection Setup in a Quantum Network" (Inf, Deleted)**
- **Draft "The Link Layer service in a Quantum Internet" (Exp)**
- **Draft "Advertising Entanglement Capabilities in Quantum Networks" (?, Deleted)**

- Симулятор для разработки ПО для квантового интернета (SimulaQron)
  - http://www.simulaqron.org/

Национальные органы по стандартизации

NIST

- The Cryptographic Technology Group at NIST is **NOT** focusing on QKD

National Institute of Standards and Technology

Национальные: Китай

CCSA – China Communications Standards Association

- CCSA ST17 – 17th Special Task Group (ST17) «Quantum Communication and information technology» ->
  QKD-based Quantum Secure Communications
  - WG1 – Квантовые коммуникации
  - WG2 – Квантовая обработка информации
- www.ccsa.org.cn

CSTC – China Cryptography Standardization TC

- Quantum Cryptography Standard WG – 2012
- Работы по спецификации и тестирование KPK на базе протокола Decoy State BB84

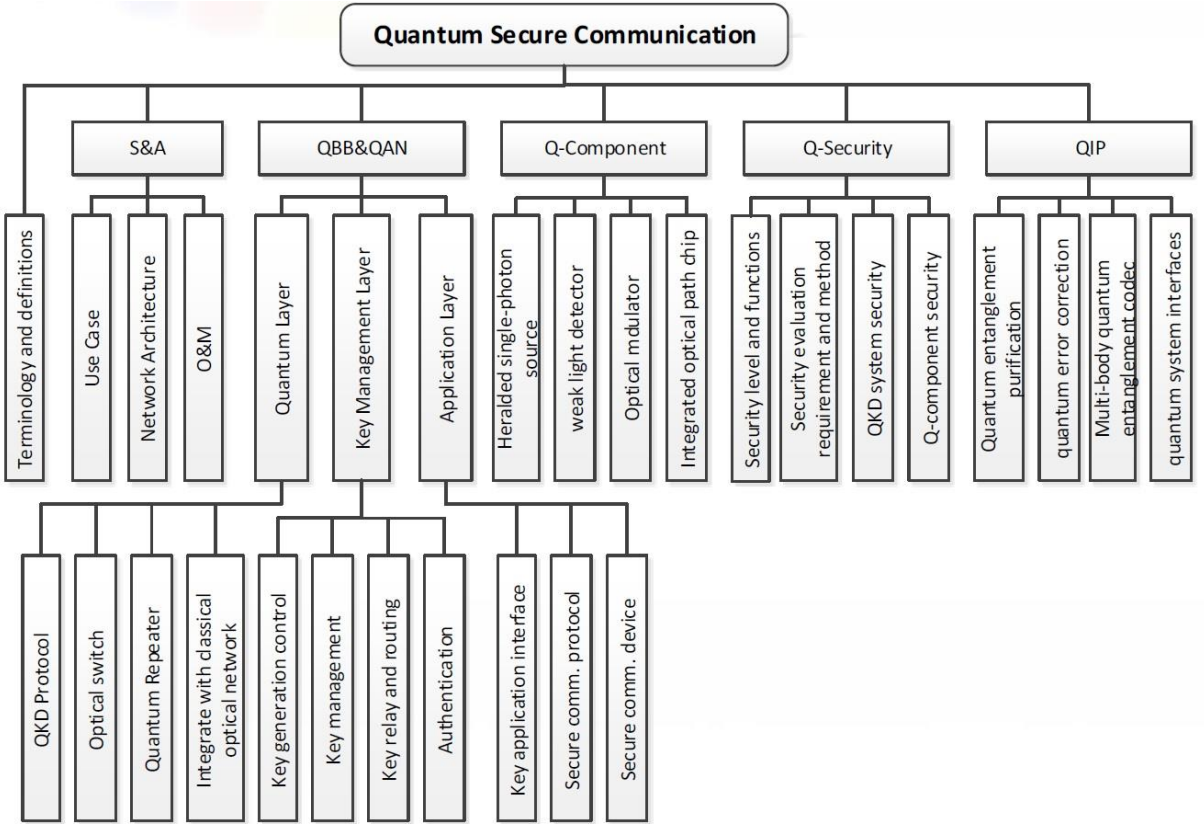
China Information Security Standardization TC (TC260)

- Работы по квантовым вычислениям и метрологии

Китай: CCSA ST17

5 групп стандартов

- S&A – система и архитектура
- QAN&QBB – квантовые магистральные сети и сети доступа
- Q-Component – квантовые компоненты
- Q-Security – квантовая безопасность
- QIP – квантовая обработка информации
- 25 документов



Китай: CCSA ST17

Национальные стандарты

1. **Quantum Communication Terms and Definitions**
2. **Quantum Secure Communication application scenario and requirements**

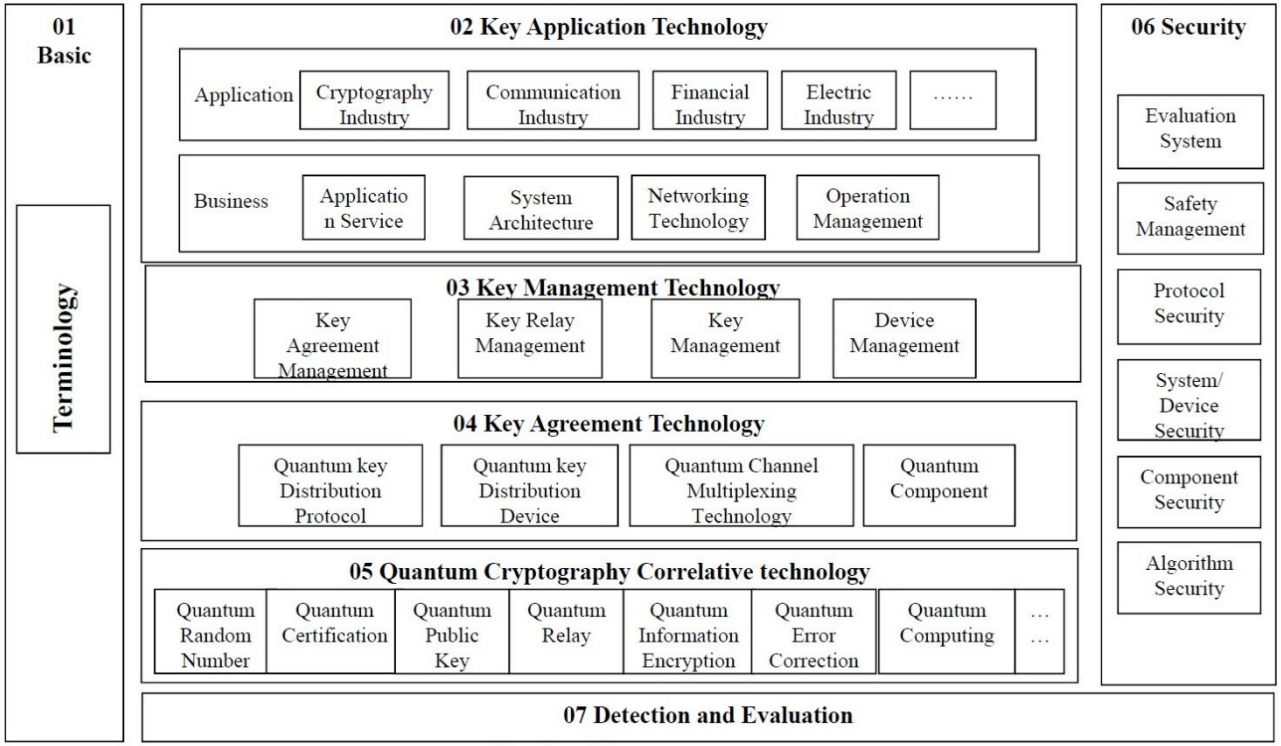
Промышленные стандарты

1	Quantum Key Distribution (QKD) application interface
2	Technical requirements for quantum key distribution (QKD) systems Part I: Decoy-state BB84
3	Test methods of optical quantum key distribution (QKD) system
4	Quantum Secure Communication Network Architecture
5	Technical Requirements of Co-Fiber Transmission System for Quantum Key Distribution and Classic Optical Communication
6	Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 1: optical source
7	Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 2: Single photon detector
8	Key components and modules for quantum key distribution (QKD) based on BB84 Protocol Part 3: Quantum random number generator(QRNG)

Отчеты об исследованиях

1	Study on Quantum secure communication network architecture
2	Study on security issues of Quantum Key Distribution
3	Study on test and evaluation of Quantum Secure Communication System
4	Study on the Co-Fiber Transmission of Quantum Key Distribution and Classic Optical Communication Systems
5	Study on Generation and Test method of Quantum Random Number
6	Study on quantum key distribution key device and module Technology requirements
7	Study on Quantum Secure Communication Network Management
8	Study on CV-QKD technique
9	Study on software defined QKD network
10	Study on trusted relay node in QKD network
11	Study on Quantum Secure Communication Networking Key Technologies
12	Study on Freespace Quantum Secure Communication Technology
13	Requirements of encrypted data carried in MPLS PW in quantum secure communication network
14	Study on optimization protocol based on decoy state method

Дорожная карта стандартов по квантовой криптографии



Китай: CSTC

- **TS “Network cryptographic server based on QKD” (2016)**
- **TS “Decoy state BB84 QKD Protocol Specification” (2016)**
  описание протокола с характеристиками безопасности на каждой стадии, технические требования к изделию в части набора функций, производительности и управления
- **TR “Evaluation Specification of Decoy state BB84 QKD System” (2017)**
- **TR “Encrypted Communication Technology Framework based on QKD” (2017)**
- **Research “Quantum RNG” (2018)**
- **TS “Decoy State BB84 QKD Test Specification” (2018)**
  цель тестирования, требования к окружению, процессам и оценке результатов; описание тестовых требований и методов в части набора функций, производительности, аппаратного и программного обеспечения и управления функциями безопасности
- **Research “Relay security of QKD Network” (2018)**
- **TS “Quantum key application Interface Specification” (2018)**
- **TS “Coherent State CV QKD” (2018)**

Региональные органы по стандартизации

ETSI Industry Specification Group on QKD

- Более 30 членов:
  - вендоры систем КРК, вендоры сетевого оборудования, сетевые операторы, системные интеграторы, университеты, академические организации, национальные лаборатории и т.д.
  - Европа, Япония, Южная Корея, США, Канада, Россия…
- Более 25 проведенных мероприятий
- Документы доступны бесплатно для скачивания
- Фактически: **международная стандартизация**
- www.etsi.org/qkd

Направления стандартизации

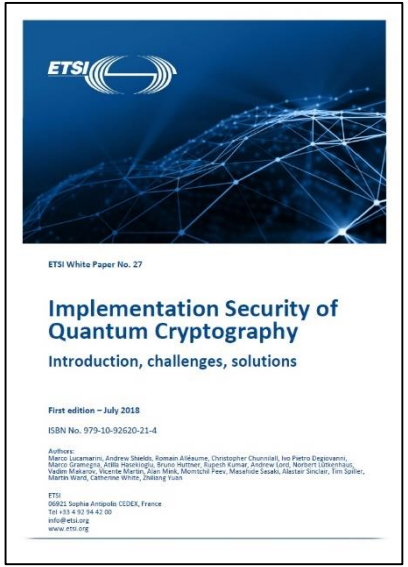
- Общие вопросы
- Безопасность практических реализаций систем КРК
- Интероперабельность для классических интерфейсов и протоколов, но не квантового канала и организация квантовых сетей
- Метрология компонентов и систем КРК (измерения на однофотонном уровне)

ETSI ISG QKD: Общие вопросы

- **GR QKD 007 v1.1.1 “Vocabulary” – 2018**
  глоссарий, согласующий остальные документы ETSI терминологически, предполагается регулярное обновление
- **GR QKD 003 v2.1.1 “Components and Internal Interfaces” – 2018**
  базовое функциональное описание компонентов систем КРК и их взаимосвязей
- **GS QKD 008 v1.1.1 “QKD Module Security Specification” – 2010**
  требования по безопасности к аппаратуре КРК как компоненту системы информационной безопасности

ETSI ISG QKD: Безопасность реализаций

- **White Paper 27**
  “Implementation Security of Quantum Cryptography” – 2018
  обзор реализаций и вопросов безопасности реализаций КРК
- **GS QKD 005 v1.1.1 “Security Proofs” – 2010**
  требования, определения, модели, ожидается обновление
- **Draft GS QKD 016 “Common Criteria Protection Profile for QKD” – 2020** (ожидается)
  профиль защиты для КРК в парадигме «Общих критериев»
- **Draft GS QKD 010 “Implementation security: protection against Trojan horse attacks in one-way QKD systems ” – 2020** (ожидается)
  рекомендации по защите КРК от зондирования состояния оптических компонентов засветкой



ETSI ISG QKD: Интероперабельность и сеть

- **GS QKD 014 v1.1.1 “Protocol and data format of REST-based key delivery API” – 2019**
  протокол и формат данных передачи квантовых ключей приложениям, но не в квантовой сети
- **GS QKD 004 v1.1.1 “Application Interface” – 2010**
  прикладной функциональный интерфейс передачи квантовых ключей приложениям, ожидается обновление
- **Draft GS QKD 015 “Control Interface for SDN” – 2020 (ожидается)**
  интерфейсы управления для интеграции на уровень управления сетевыми архитектура, и SDN в частности
- **GS QKD 012 v1.1.1 “Device and Communication Channel Parameters for QKD Deployment” – 2019**
  управление параметрами КРК при взаимодействии владельца КРК и потребителями
- **Draft GR QKD 017 “Network architectures“– ? (ожидается)**
  отчет по возможным архитектурам сетей КРК, автономные и интеграционные модели использования с телеком-системами

ETSI ISG QKD: Метрология компонентов и систем

- **GS QKD 011 v1.1.1 “Component characterization: characterizing optical components for QKD systems” – 2016**
  базовый документ («справочник») с требованиями к компонентам систем КРК
- **Draft GS QKD 013 v1.1.1 “Characterization of Optical Output of QKD transmitted modules” – 2020 (ожидается)**
  описание модуля оптического передатчика как целого, а не покомпоненто, как в GS QKD 011; измерения характеристик модуля в режиме «черного» и «серого» ящиков

Международные органы по стандартизации

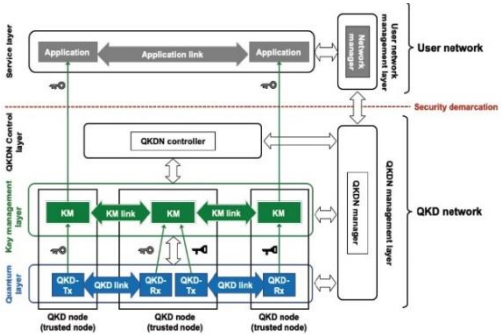
ITU-T Study Group 13: Future networks (& cloud)

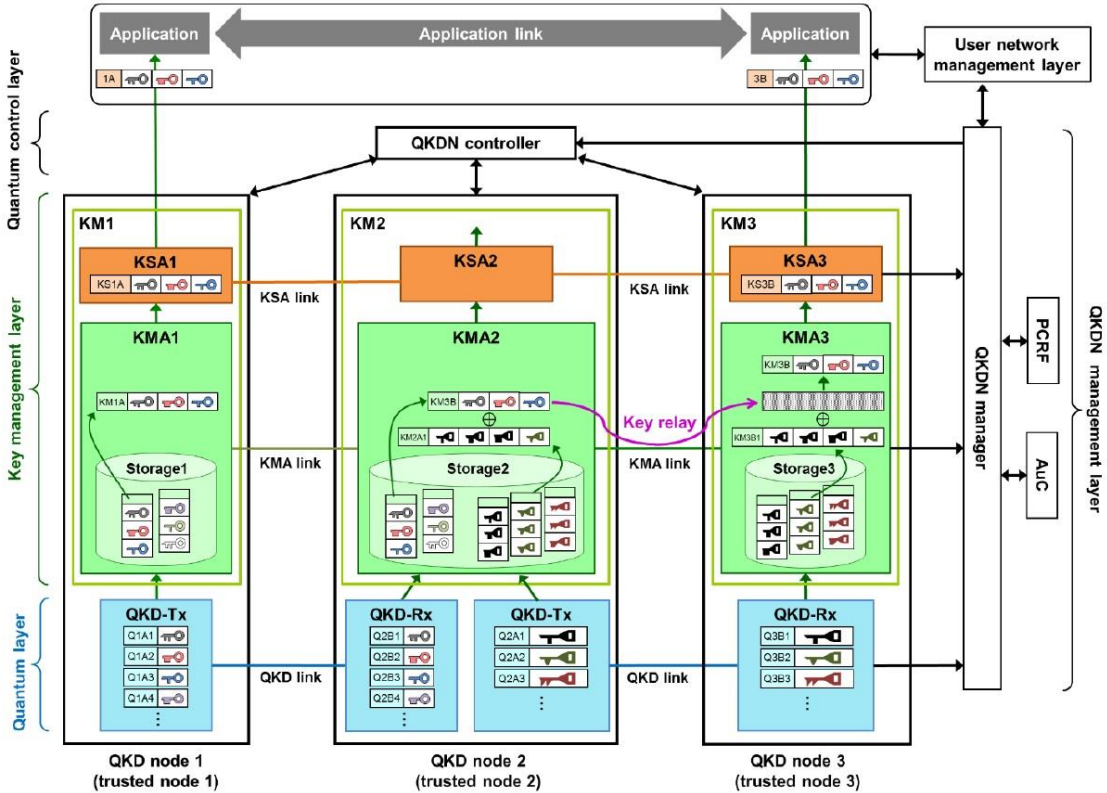
- **SG13 Q16 – Knowledge-centric trustworthy networking and services**
- **SG13 Q6 – Quality of service (QoS) aspects including IMT-2020 networks**
- https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.aspx
- Китай, Япония, Корея, Швейцария, Великобритания, США

infotecs

ITU-T SG13 Q16

- **Y.3800 “Overview on Networks supporting QKD” – 2019**
  Общий обзор сетей КРК (структура, функции, уровневая модель) и их взаимодействие с пользовательскими сетями
- **Y.3801 “Functional Requirements for QKD network” - 2020**
- **Rec Y.QKDN_Arch “Functional architecture of the QKD network” – 2020**
  эталонная модель квантовой сети, ее функциональные элементы, операционные процедуры и модель развертывания
- **Rec Y.QKDN_KM “Key management for QKD network” – 2020**
  требования к системе управления ключами, функциональные элементы, процедуры и форматы
- **Rec Y.QKDN_CM “Control and Management for QKD networks” – 2020**
- **Rec Y.QKDN_SDNC “Software Defined Network Control for QKD networks” – 2021**
- **Rec Y.QKDN_BM “Business role-based models in QKD network” – 2021**
- **Rec Y.supp.trust-roadmap “Standardization roadmap on trustworthy networking and services including quantum enhanced networks” – 2022**





Rec Y.QKDN_KM “Key management for QKD network”

ITU-T SG13 Q6

- **Y.QKDN-qos-gen“General Aspects of QoS on the QKD Network” – 2021**
  Общие вопросы обеспечения качества сервиса в сетях КРК: описание QoS и производительности для сетей КРК и их применимость, характеристики, классификация проблем производительности, требующих параметризации.
- **Y.QKDN-qos-req “Requirements for QoS Assurance of the Quantum Key Distribution Network” – 2021**
  Определяет требования к обеспечению качества сервиса в сетях КРК: пользовательские сценарии, высокоуровневые требования, функциональные требования.

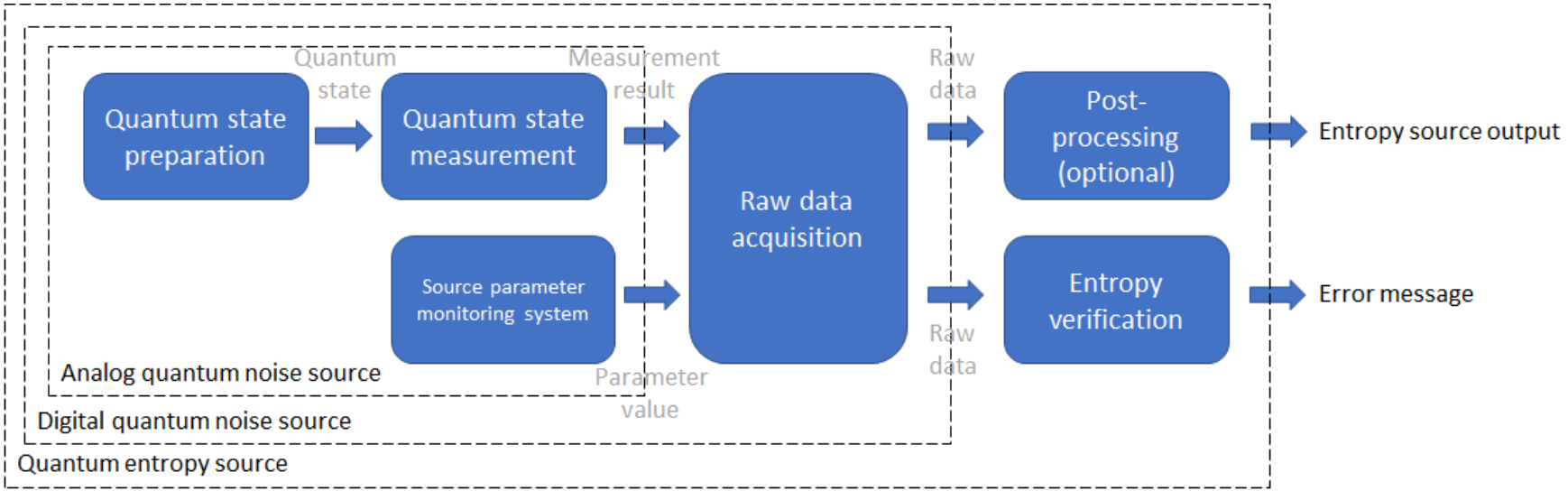
ITU-T Study Group 17: Security

- **SG17 Q4 – Cybersecurity -> Quantum Information Technologies**
- https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx
- Китай, Япония, Корея, Швейцария, США

ITU-T SG17 Q4

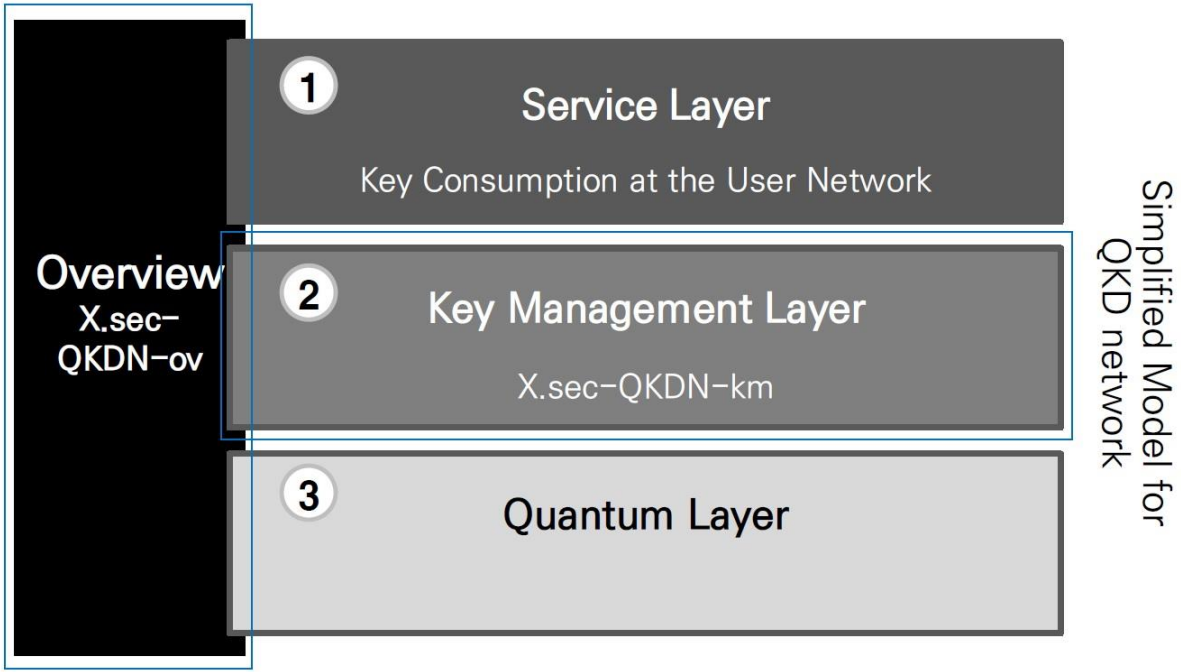
- **X.1702 “Quantum noise random number generator architecture” – 2020**
  Общая архитектура квантового источника энтропии
- **TR.sec-qkd “Security framework for QKD in telecom network” – 2021**
- **X.cf-QKDN “Use of cryptographic functions on a key generated in QKD networks” – 2020**
- **X.sec-QKDN-ov “Security requirements for QKD networks - overview” – 2020**
- **X.sec-QKDN-km “Security requirements for QKD networks - key management” – 2020**
- **X.sec-QKDN-tn “Security requirements for QKD networks - trusted node” – 2021**

X.1702 “Quantum noise random number generator architecture”



ITU-T SG17 Q4

Security Requirements for QKD



Международные: ITU-T FG QIT4N

ITU-T Focus Group on Quantum Information Technology for Networks

- https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx
- Изучение развития и применения квантовых информационных технологий (QIT) в сетях
- Терминология и пользовательские сценарии QIT для сетей
- Поддержка стандартизации QIT для сетей в других группах ITU-T и других организациях по стандартизации

ISO/IEC JTC1/SC27

- **WG3 – Security Evaluation, Testing and Specification**
- **ISO/IEC 23837 “Security requirements, test and evaluation methods for QKD” – 2022**
  - **Part 1: Requirements**
  - **Part 2: Test and Evaluation Methods**
- Основан на идеологии «Общих критериев» (ISO 15408) и уточняет методику оценки криптографических модулей ISO 19790 (FIPS 140-2) в части КРК.
- Common threats to QKD and specific threats to BB84 DS, MDI-QKD, CV-QKD.

ISO/IEC 23837 “Security requirements, test and evaluation methods for QKD”

- Security problem definition,
- Security functional requirements,
- security evaluation activities

Стандартизация КРК в России
… и не только

РОССИЯ

Технический комитет 26

"Криптографическая защита информации", https://tc26.ru/

- РГ "Квантовая криптография"
- Проект методических рекомендаций **"Протокол логического интерфейса взаимодействия" – 2021**

Технический комитет 194

"Киберфизические системы", http://tc194.ru/

- Проект ПНСТ **"Квантовые коммуникации. Общие положения и терминология" - 2020**

Российское **представительство** в международных организациях**:**

- ISO/IEC JTC1/SC 27 WG3 – эксперты (ТК26, Инфотекс)
- ITU-T FG QIT4N – сопредседатель (Ростелеком) https://www.itu.int/en/ITU-T/focusgroups/qit4n/Pages/default.aspx
- ITU-T SG17 – вице-председатель (Криптонит) http://www.itu.int/net4/ITU-T/lists/mgmt.aspx?Group=17&Period=16
- ETSI ISG QKD – эксперты (РКЦ, ИТМО) https://portal.etsi.org/TB-SiteMap/QKD/QKD-List-members

Контакты спикеров

Сергей Кулик

Научный руководитель Центра квантовых технологий МГУ

sergei.kulik@physics.msu.ru

Александр Поздняков

Менеджер развития продукта ИнфоТеКС

Aleksandr.Pozdnyakov@infotecs.ru

Владимир Елисеев

Руководитель центра научных исследований и перспективных разработок ИнфоТеКС

EliseevVL@infotecs.ru

Алексей Уривский

Заместитель генерального директора по науке и инновациям ИнфоТеКС

urivskiy@infotecs.ru

infotecs

Спасибо
за внимание!