



**SMARTS
КВАНТТЕЛЕКОМ**

Практическое применение многопользовательских квантовых сетей с промежуточными доверенными узлами для задач защиты информации

Сантьев Алексей Альбертович,
Руководитель направления развития и продвижения продуктов

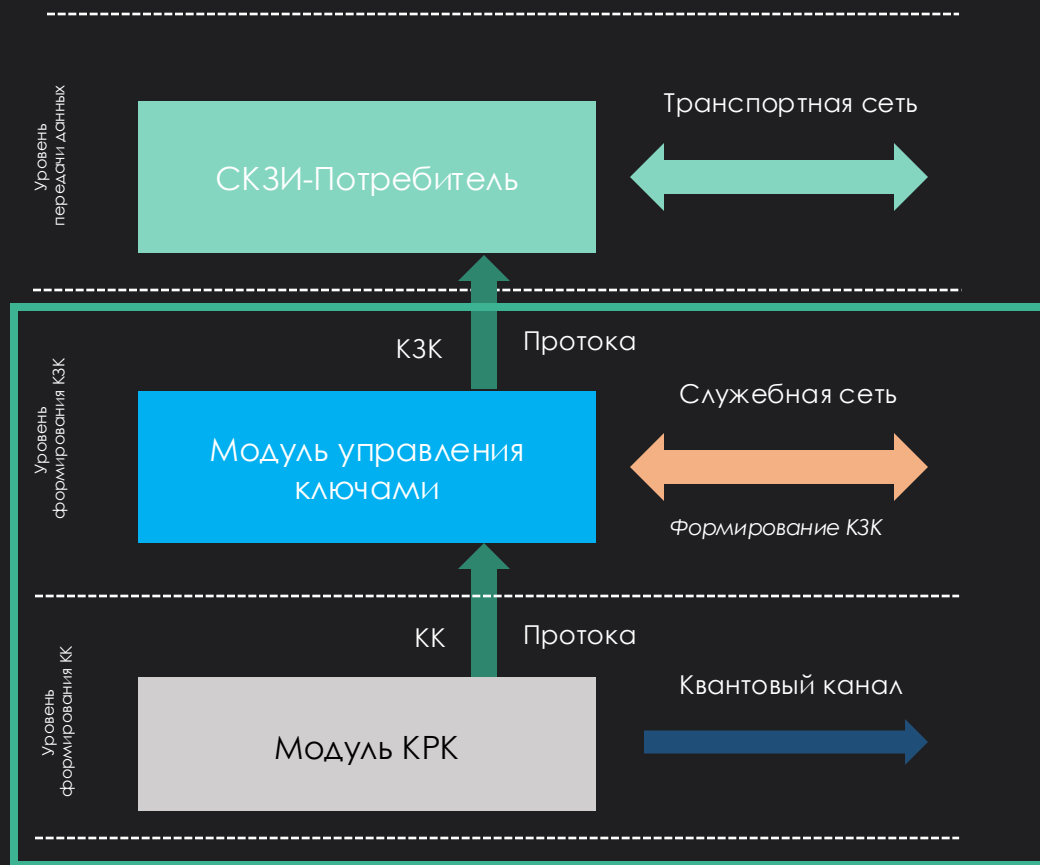
кванттелеком.рф

Структура магистральной квантовой сети

Основные принципы оказания сервисов и услуг



SMARTS
КВАНТТЕЛЕКОМ



Доверенный промежуточный узел квантовой сети

КК – квантовые ключи

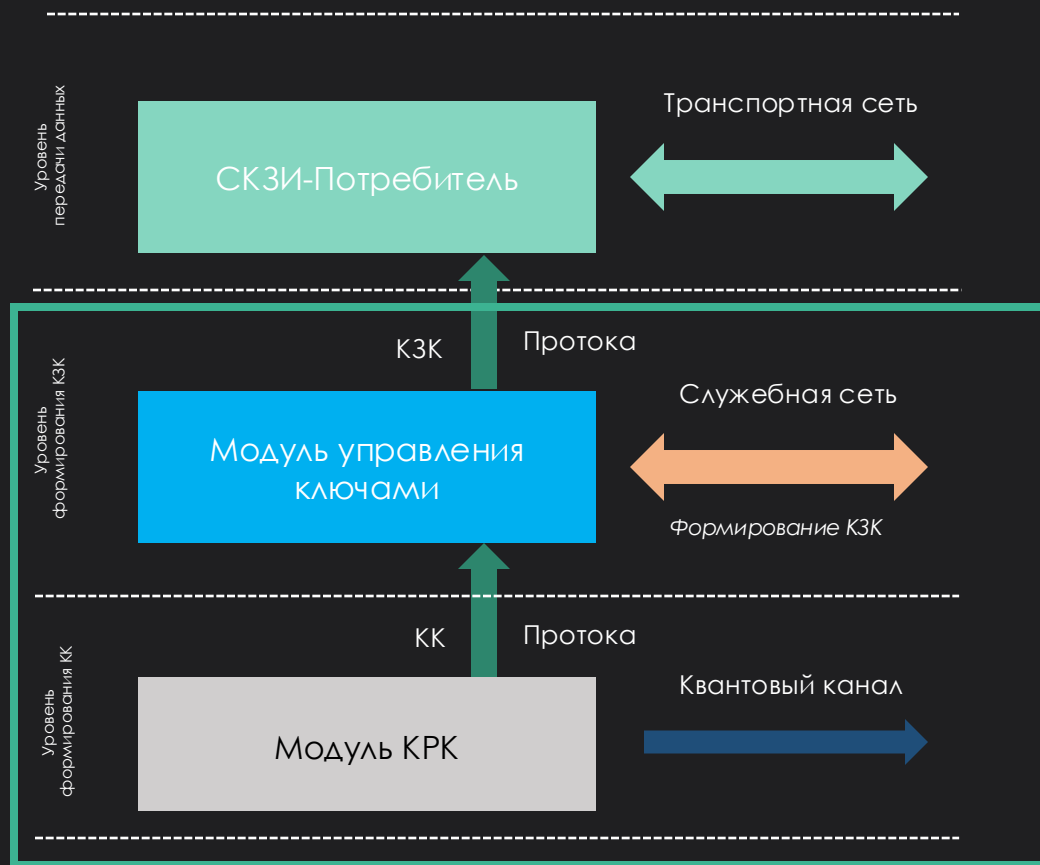
КЗК – квантовозащищенные ключи

Структура магистральной квантовой сети

Основные принципы оказания сервисов и услуг



SMARTS
КВАНТТЕЛЕКОМ



Где здесь
сервисная модель?

Доверенный промежуточный узел квантовой сети

КК – квантовые ключи

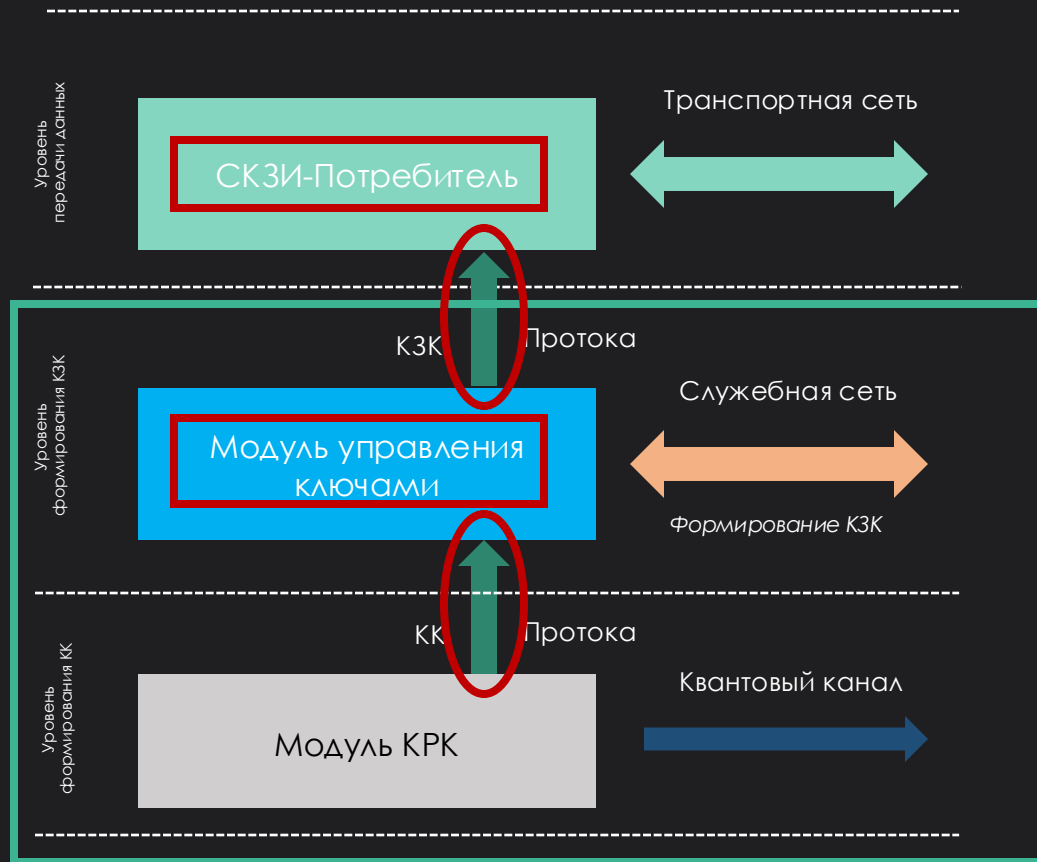
КЗК – квантовозащищенные ключи

Структура магистральной квантовой сети

Основные принципы оказания сервисов и услуг



SMARTS
КВАНТТЕЛЕКОМ



1. Какие устройства выступают в роли СКЗИ-Потребителей и по какому протоколу получают ключи?

Доверенный промежуточный узел квантовой сети

КК – квантовые ключи

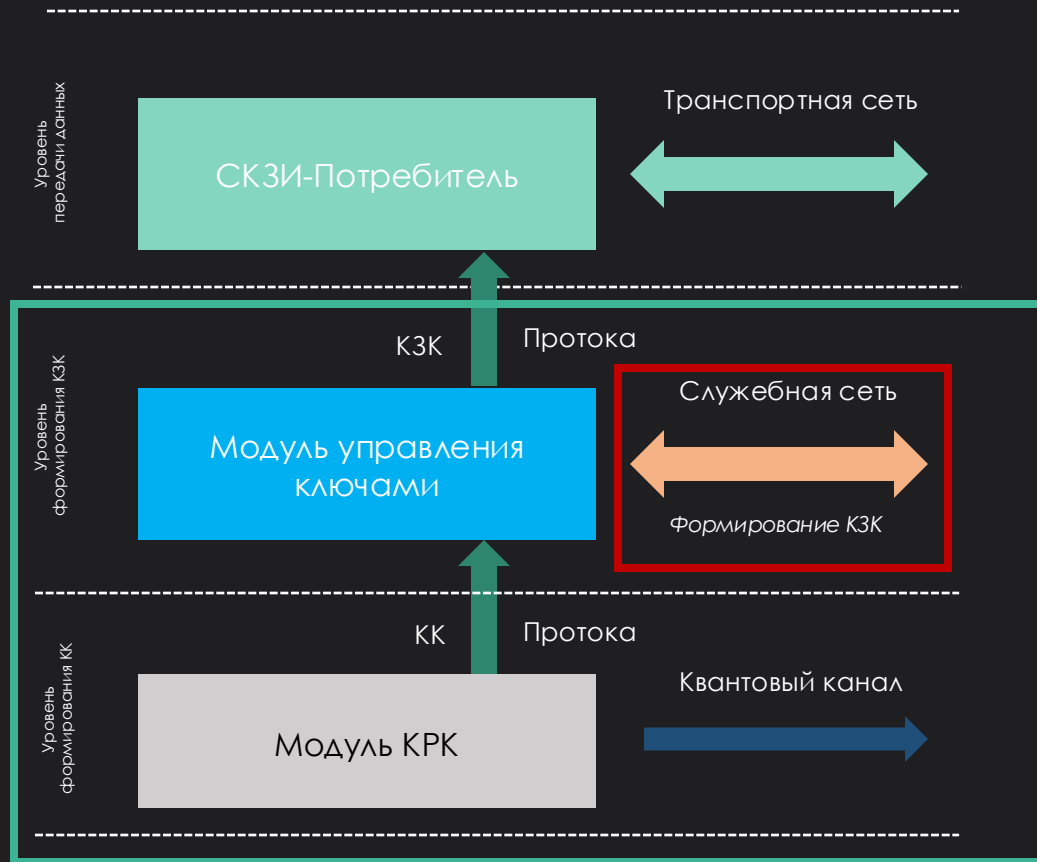
КЗК – квантовозащищенные ключи

Структура магистральной квантовой сети

Основные принципы оказания сервисов и услуг



SMARTS
КВАНТТЕЛЕКОМ



1. Какие устройства выступают в роли СКЗИ-Потребителей и по какому протоколу получают ключи?
2. Способы управления жизненным циклом квантовых и квантовозащищенных ключей в квантовой сети, включая способы формирования, накопления и выдачи потребителям

Доверенный промежуточный узел квантовой сети

КК – квантовые ключи

КЗК – квантовозащищенные ключи

Структура магистральной квантовой сети

Основные принципы оказания сервисов и услуг



SMARTS
КВАНТТЕЛЕКОМ



1. Какие устройства выступают в роли СКЗИ-Потребителей и по какому протоколу получают ключи?
2. Способы управления жизненным циклом квантовых и квантовозащищенных ключей в квантовой сети, включая способы формирования, накопления и выдачи потребителям
3. Архитектура и принципы эксплуатации магистральных квантовых сетей, региональных и городских квантовых сетей, локальных квантовых сетей

Доверенный промежуточный узел квантовой сети

КК – квантовые ключи

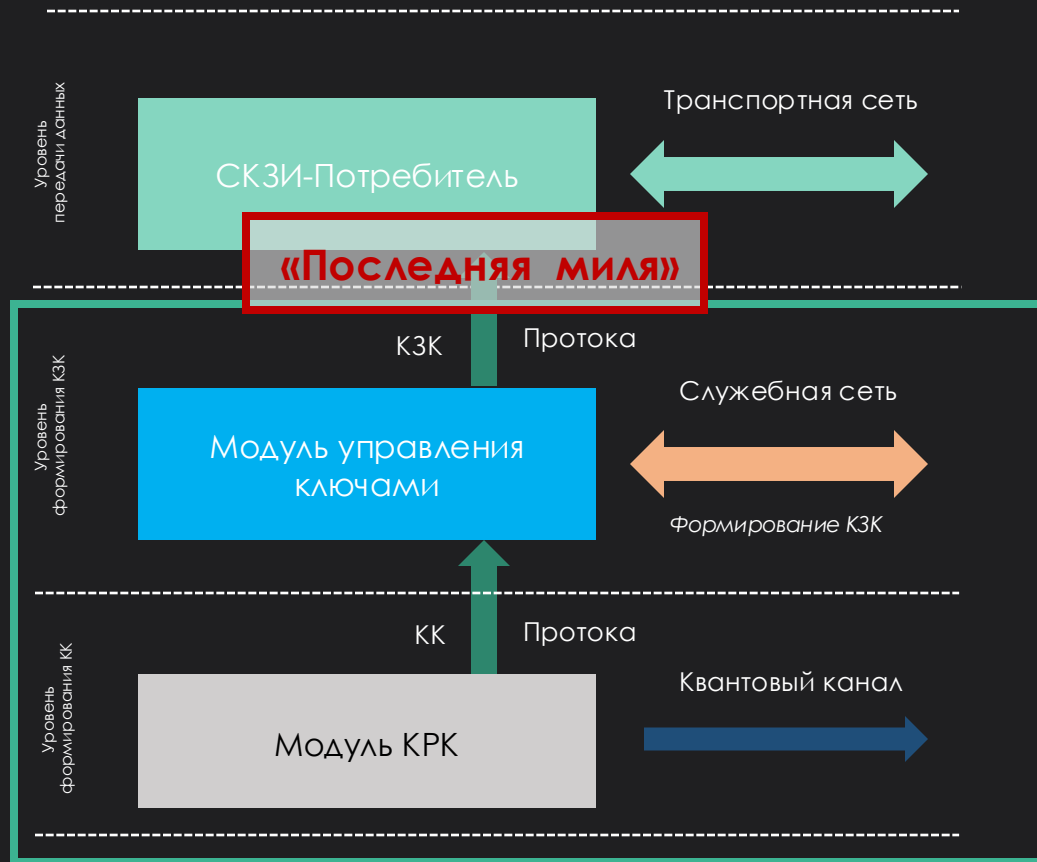
КЗК – квантовозащищенные ключи

Структура магистральной квантовой сети

Основные принципы оказания сервисов и услуг



SMARTS
КВАНТТЕЛЕКОМ



1. Какие устройства выступают в роли СКЗИ-Потребителей и по какому протоколу получают ключи?
2. Способы управления жизненным циклом квантовых и квантовозащищенных ключей в квантовой сети, включая способы формирования, накопления и выдачи потребителям
3. Архитектура и принципы эксплуатации магистральных квантовых сетей, региональных и городских квантовых сетей, локальных квантовых сетей
4. Способы подключения различных видов потребителей, в том числе в составе сетей фиксированной связи, сетей беспроводной связи («последняя миля»)

Доверенный промежуточный узел квантовой сети

КК – квантовые ключи

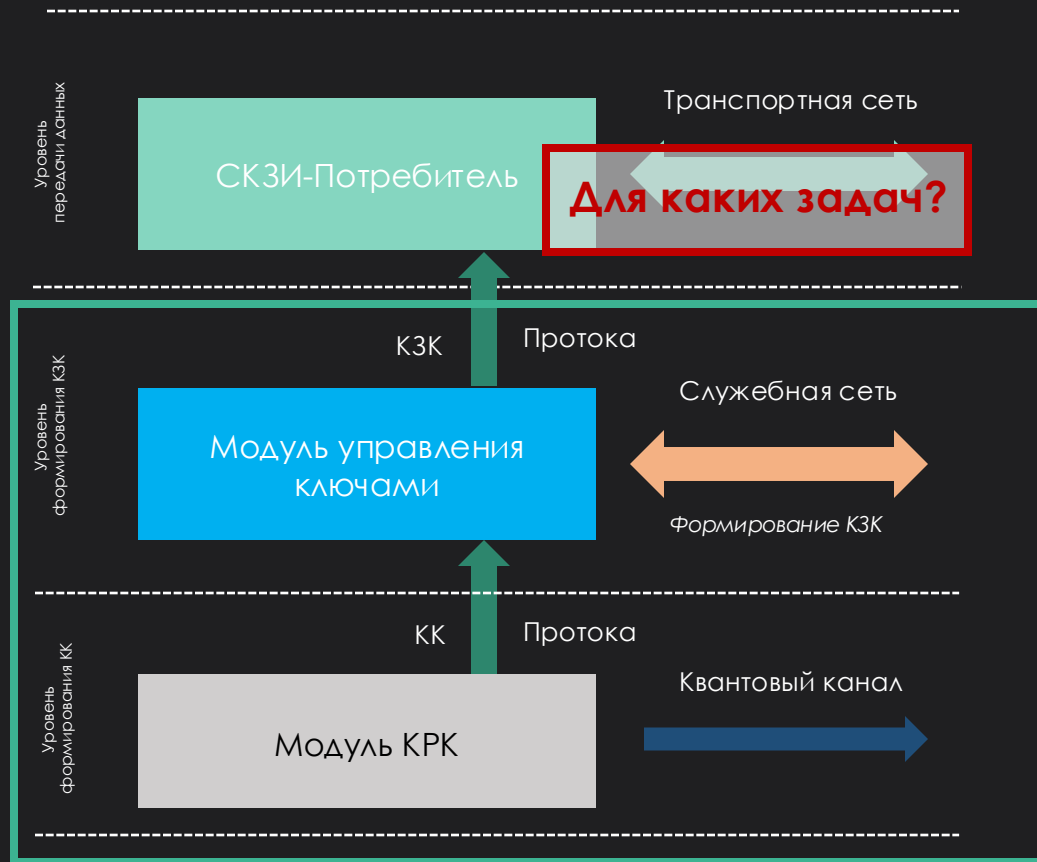
КЗК – квантовозащищенные ключи

Структура магистральной квантовой сети

Основные принципы оказания сервисов и услуг



SMARTS
КВАНТТЕЛЕКОМ



Доверенный промежуточный узел квантовой сети

КК – квантовые ключи

КЗК – квантовозащищенные ключи

1. Какие устройства выступают в роли СКЗИ-Потребителей и по какому протоколу получают ключи?
2. Способы управления жизненным циклом квантовых и квантовозащищенных ключей в квантовой сети, включая способы формирования, накопления и выдачи потребителям
3. Архитектура и принципы эксплуатации магистральных квантовых сетей, региональных и городских квантовых сетей, локальных квантовых сетей
4. Способы подключения различных видов потребителей, в том числе в составе сетей фиксированной связи, сетей беспроводной связи («последняя миля»)
5. Пользовательские приложения (задачи) для применения полученных от квантовой сети криптографических ключей (КК или КЗК)

1. Какими бывают потребительские устройства в квантовых сетях?

Мировая и отечественная практики

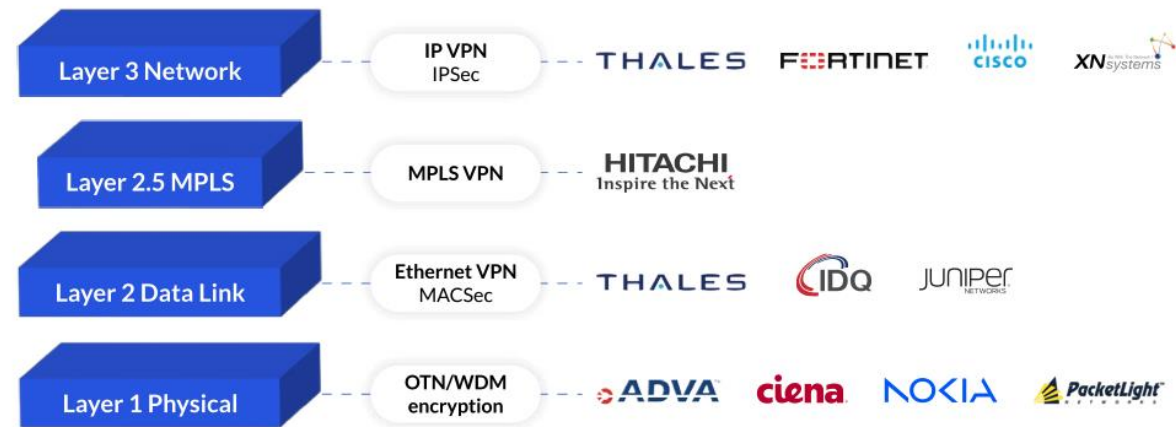
Зарубежный подход: протокол ETSI

ETSI GS QKD 014 V1.1.1 (2019-02)



Quantum Key Distribution (QKD);
Protocol and data format of REST-based key delivery API

Стандартный интерфейс выдачи ключей



Подключение различных вендоров

GROUP SPECIFICATION

Аппаратные модули безопасности



The diagram illustrates the IDQ Cerberis XG architecture, showing a Primary Datacenter and a Backup Datacenter connected via a Quantum Channel & Service Channel.

Primary Datacenter:

- Thales CN6140 Network Encryptor
- IDQ Cerberis XG - Alice

Backup Datacenter:

- Thales CN6140 Network Encryptor
- IDQ Cerberis XG - Bob

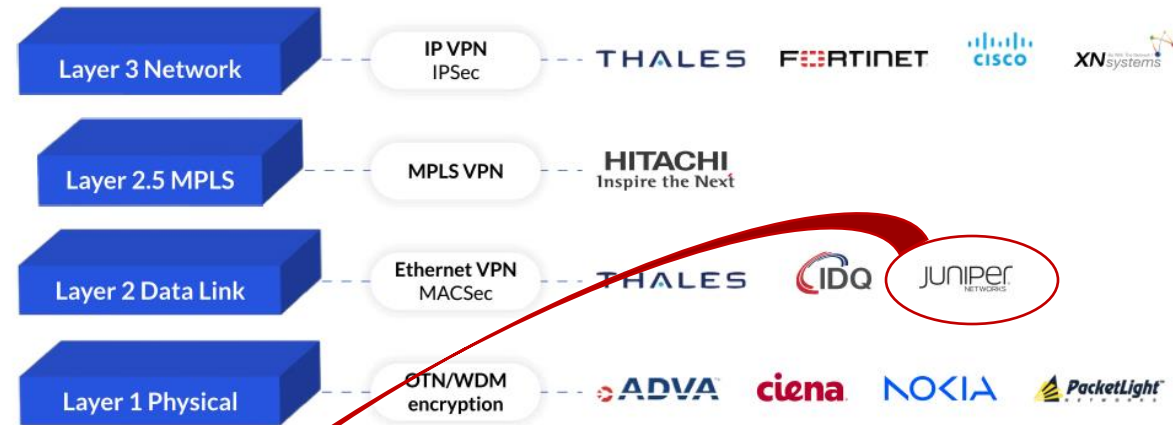
Connections:

- The Thales CN6140 Network Encryptors are connected to the IDQ Cerberis XG devices via a **Standard Interface (ETSI REST API - QKD 0.14)**.
- The IDQ Cerberis XG devices are connected via a **Quantum Channel & Service Channel**.

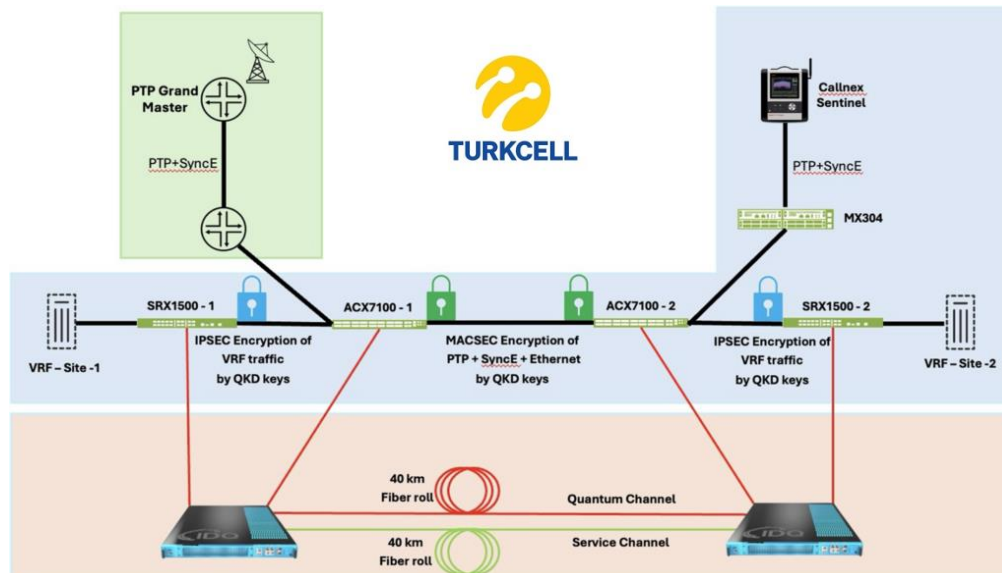
<https://makeing.idquantique.com/acton/attachment/11868/f-12253b9e-5c7b-454f-b2a8-cd78566fd70/1/-/-/-/IDQ-Thales-Brochure.pdf?ch=189aam%20a%20MT03OTU2NDa5Nv4xNzUwNTc4OTk%3a%20a%20DYzhTcwM4NzUyNTc4OTk%3a%20440NW49CK5%20czE3NTc5MjU0NzlkbnkzZkdkDE3NTc5MzZM3OTYkYUwJGwwJGgzNzVmTlVnZm>

Зарубежный подход: протокол ETSI

ETSI GS QKD 014 V1.1.1 (2019-02)



Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API



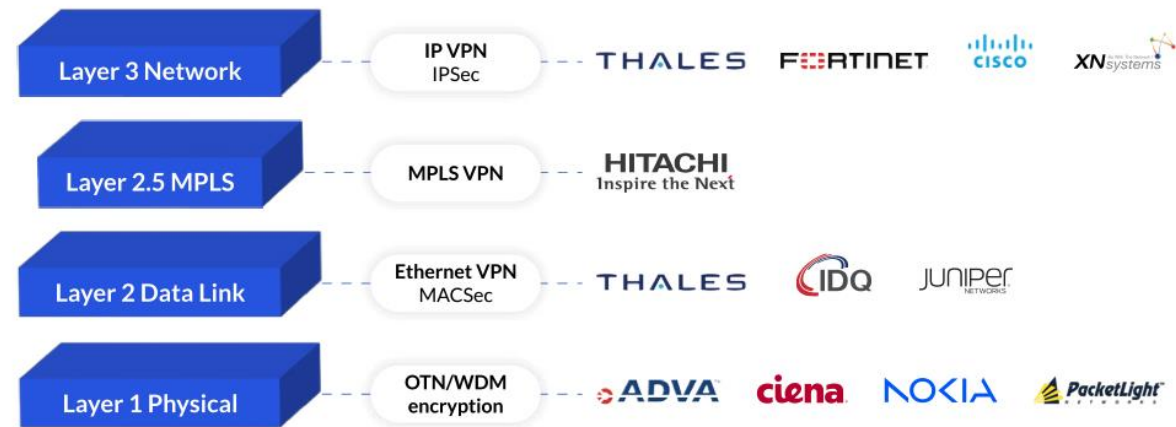
- Шифрование на канальном уровне (MACsec) на базе стандартного маршрутизатора SRX1500
- Шифрование на сетевом уровне (IPsec) на базе межсетевого экрана нового поколения (NGFW) SRX1500

Февраль 2025, Стамбул

ETSI GS QKD 014 V1.1.1 (2019-02)



Quantum Key Distribution (QKD);
Protocol and data format of REST-based key delivery API



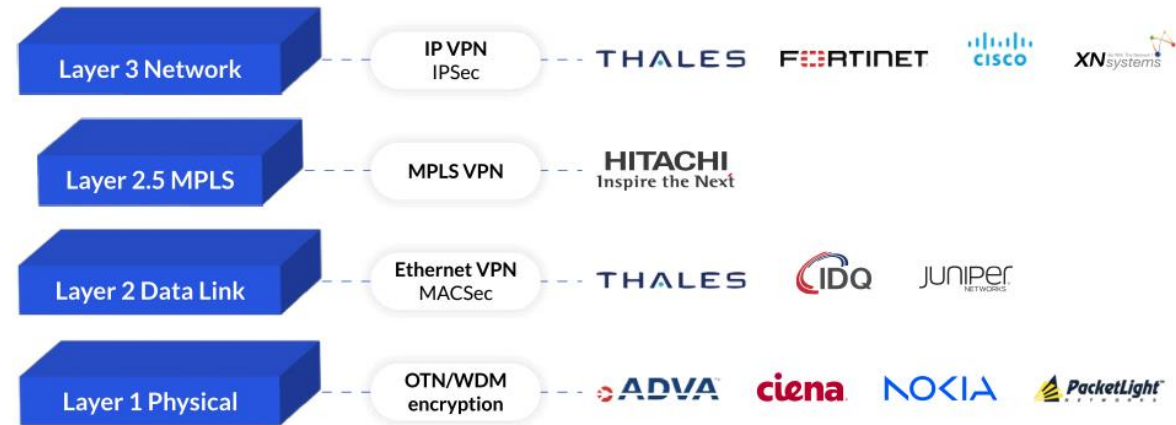
Есть ли интероперабельность между вендорами?

Зарубежный подход: протокол ETSI

ETSI GS QKD 014 V1.1.1 (2019-02)



Quantum Key Distribution (QKD);
Protocol and data format of REST-based key delivery API



Нет!

Интероперабельность
протокола взаимодействия
аппаратуры разных вендоров
является проблемой и за
рубежом!

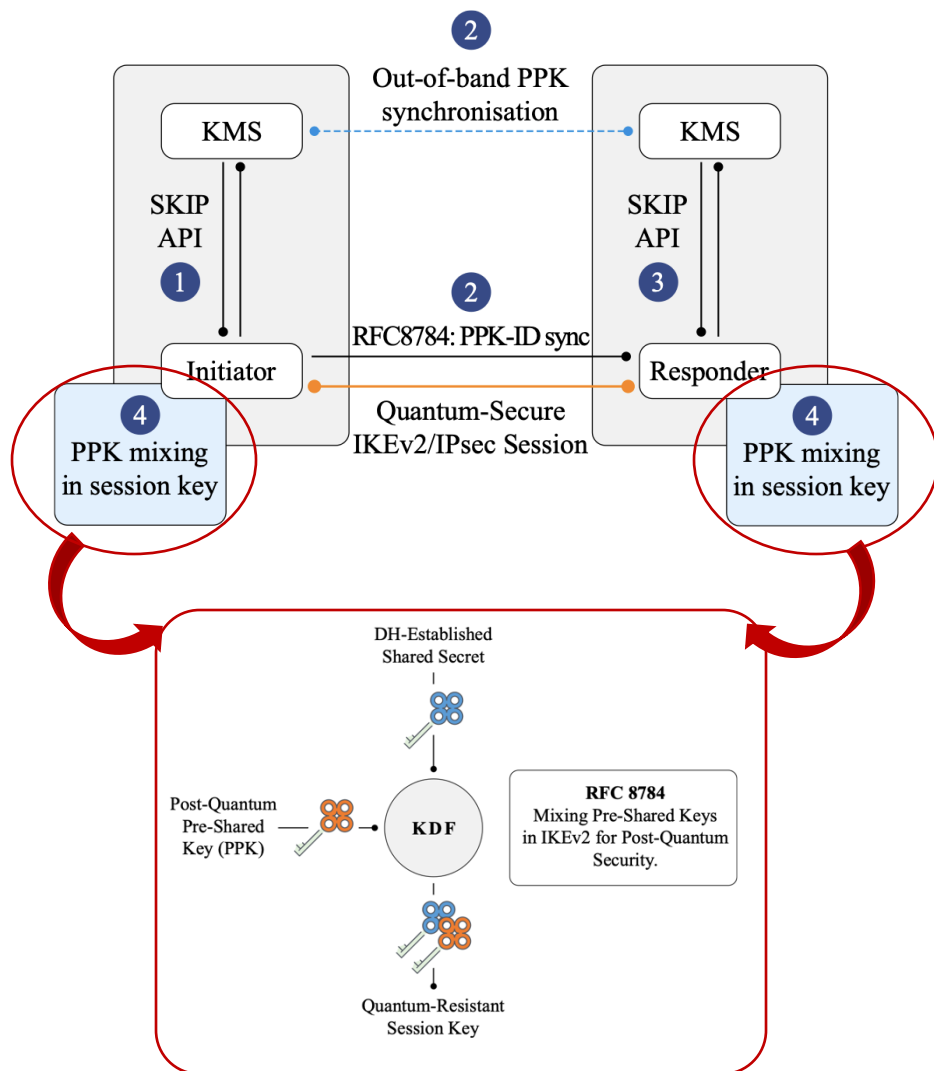
5 Key challenges and future directions

This section presents a concise list of challenges and future endeavors in key management in QKD networks. Key management is the foundational task of QKD networks; without it, the key generation process would be ineffective. However, the development and optimization of the key management layer are significantly constrained due to the limited number of testbeds and real-world applications of QKD network services. These are identified key challenges to guide future directions:

- **Standardization of interfaces for communication between QKD modules and key managers:** To facilitate fair representation of all QKD equipment manufacturers in the market, it's imperative to establish clear guidelines for communication and interoperability between various QKD module manufacturers and key managers. Currently, there is no standardized interface that delineates this communication.

Проприетарный протокол SKIP от Cisco

Secure key integration protocol (SKIP)



- ✓ Компания Cisco разработала собственный протокол сопряжения с внешним источником ключей, в том числе с модулями КРК
- ✓ Полученные ключи используются в протоколе IKEv2 посредством функции диверсификации ключей вместе с ключами DH



Quantum-Safe Encryption Using Postquantum Preshared Keys

This chapter explains how to use Postquantum Preshared Keys (PPK) for quantum-safe encryption of IKEv2 and OTNsec data, through the implementation of RFC 8784 and the Cisco Secure Key Integration Protocol (SKIP).

- [Quantum-Safe Encryption Using Postquantum Preshared Keys, on page 2](#)
- [Verify the PPK Configuration, on page 10](#)
- [View IKEv2 Session Detail, on page 14](#)

Реализация протокола ProtoQa

Профиль протокола от СМАРТС-Кванттелеком (профиль СКТК)



СМАРТС
КВАНТТЕЛЕКОМ



ProtoQa,
профиль
СКТК

ProtoQa,
профиль
СКТК

ProtoQa,
профиль
СКТК



СПБ | СИСТЕМЫ
ПРАКТИЧЕСКОЙ
БЕЗОПАСНОСТИ

Решение в едином корпусе



Р 1323565.1.046-2023. Рекомендации по стандартизации. «Информационная технология. Криптографическая защита информации. Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации»

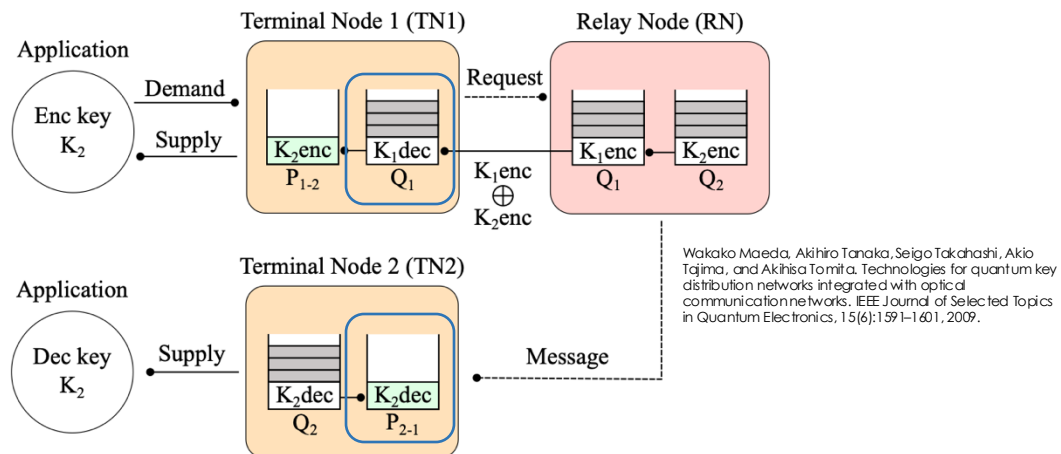


2. Модуль управления ключами – основная проблематика развития решений.

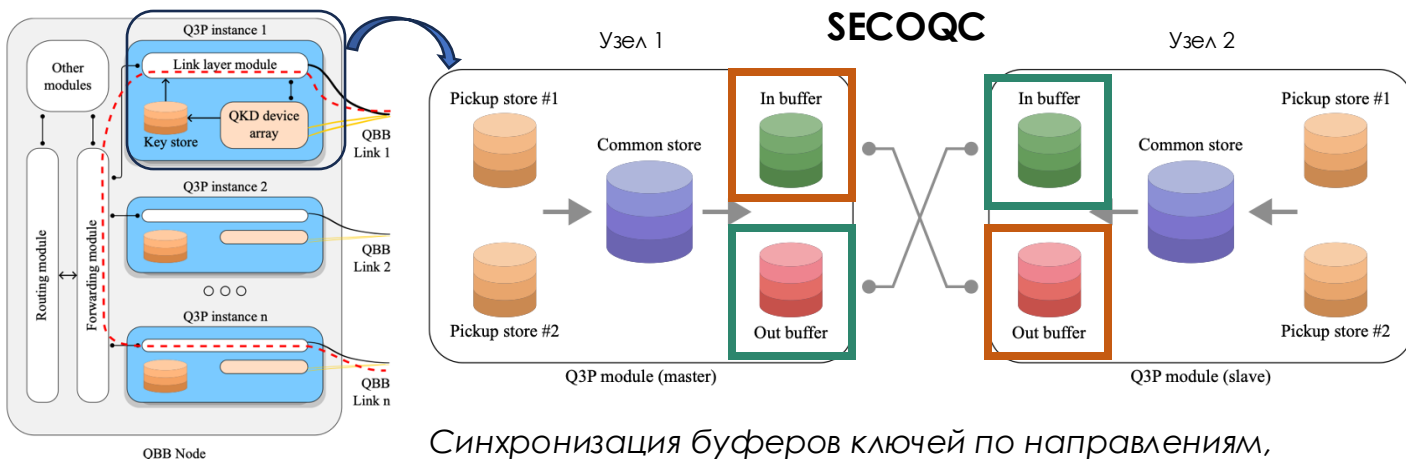
Решение	Год	Логические уровни в архитектуре	Локальное хранение ключей	Преобразование ключей	Логическое разделение ключей	Хранение глобальных ключей	Пороговые значения в хранилищах ключей
DARPA key Management	2002-2007	Нет	Да	Нет	Нет	Нет	Нет
SECOQC key management	2007-2009	Да	Да	Да – после приема. Нет – при распределении	Да, ключи шифрования и расшифрования	Нет	Минимальный уровень по количеству ключей для пополнения хранилища
NIST manager	2008	Нет	Да	Да	Да, сессионные ключи	Нет	Нет
QCC security processor key manager	2008	Нет	Да	-	Да, сессионные ключи	Нет	Минимальный уровень по количеству ключей для пополнения хранилища
NEC key management	2009	Да	Да	Нет	Да, ключи шифрования и расшифрования	Да	Нет
Magiq Tehnologies key manager	2010	Да	Да	Нет	Да, сессионные ключи	Нет	Нет
SwissQuantum key management	2009-2011	Да	Да	-	Да, сессионные ключи	Да	-
QoS-suported key manager	2011	Нет	Да	-	-	-	-
NECTEC key management	2012	Да	Да	-	Да, сессионные ключи	Да	Нет
Toshiba key management	2016	Да	Да	Да – после приема. Нет – при распределении	Да, ключи шифрования и расшифрования и сессионные ключи	Да	Нет
NICT QKD platform	2017	Да	Да	-	-	Да	Нет
Quantum Canada key management	2018	Да	Да	-	Локальные ключи и ключи для сетевого распределения . Ключи шифрования и расшифрования	Да	Не
NSFC SDQaaS framework	2019	Да	Да	-	Да, сессионные ключи	Да	Нет
NKPs DDKA-QKDN scheme	2022	Нет	Да	Да – после приема. Нет – при распределении	Нет	Да	Минимальный уровень по количеству ключей для старта процедуры сетевой рассылки ключей
KISTI key management	2022	Да	Да	Да, НКДФ	-	Да	Нет
AIT key manager	2023	Нет	Да	Да	-	-	Минимальный уровень по количеству ключей для пополнения хранилища

Модуль управления ключами: методы и принципы

NEC



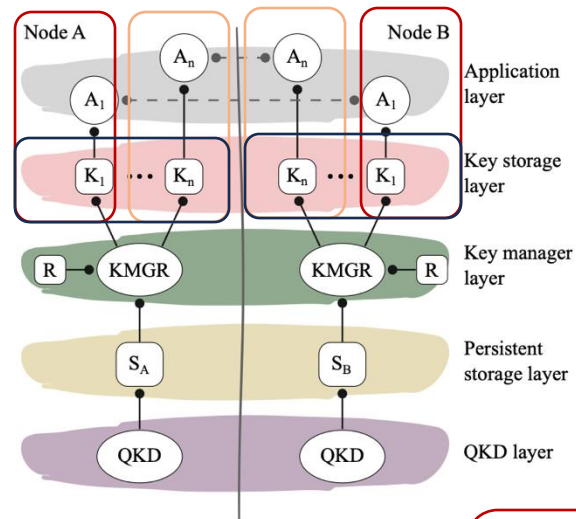
Раздельное хранение
«ЛОКАЛЬНЫХ» и «ГЛОБАЛЬНЫХ» КВАНТОВЫХ КЛЮЧЕЙ



Синхронизация буферов ключей по направлениям,
разграничение прав по принципу master/slave

Magiq Technology

Keun Lee and Audrius Berzanskis. Key manager for qkd networks, U.S. Patent US20060062392A1, Jan. 2010.

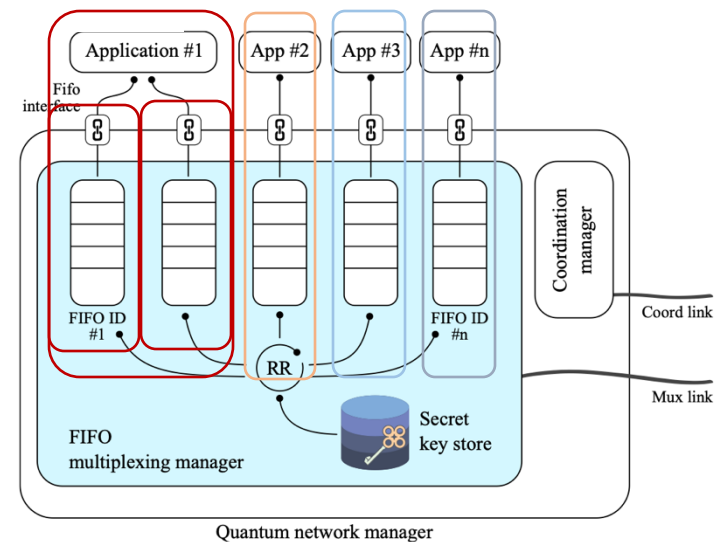


Хранение ключей с
разделением
буферов по потребителям
после формирования
квантовозащищенных
ключей (КЗК)

До формирования КЗК
хранение в едином
буфере квантовых ключей

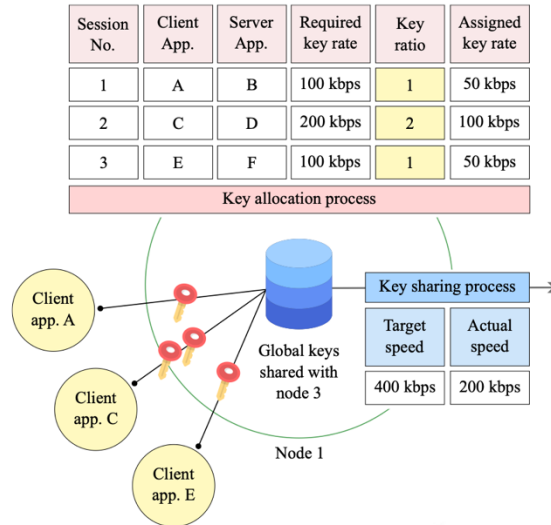
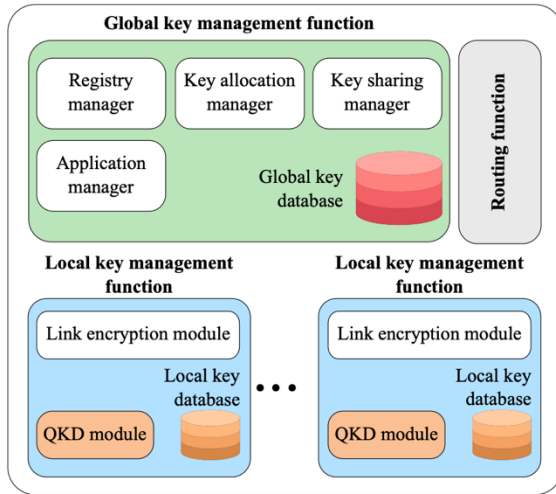
NIST

Alan Mink, Lijun Ma, Tassos Nakassis, Hai Xu, Oliver Slattery, Barry Hershman, and Xiao Tang. A quantum network manager that supports a one-time pad stream. ICQNM 2008, pages 16-21. IEEE, 2008.



Раздельные буферы ключей для каждого потребителя

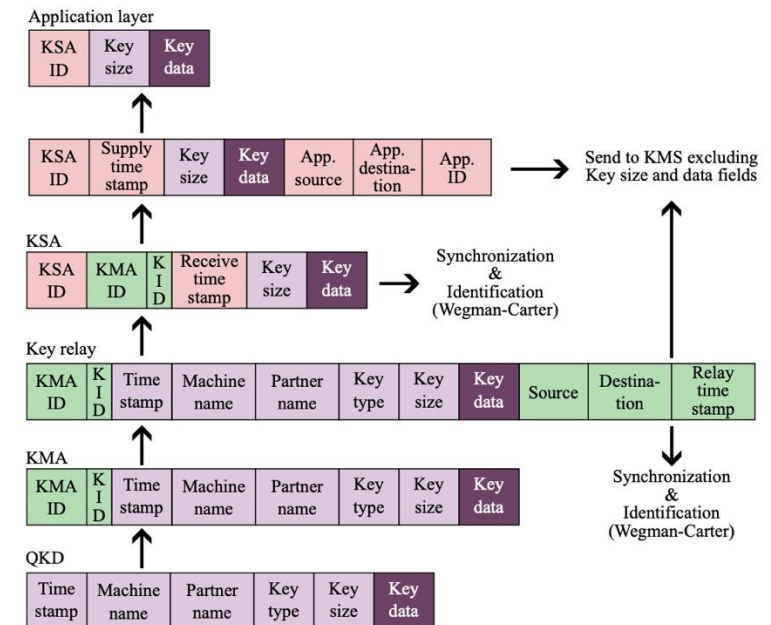
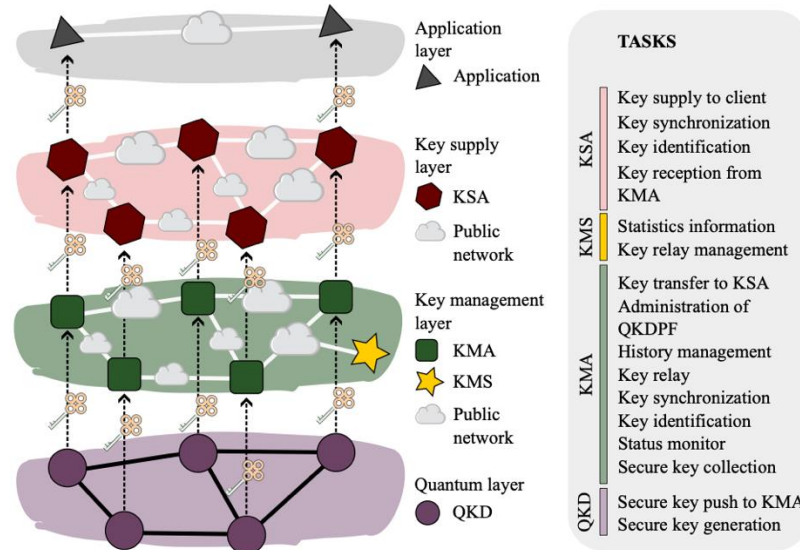
Модуль управления ключами: методы и принципы



- Раздельное ведение буферов «локальных ключей» от разных модулей КРК в одном узле
- Наличие общего буфера «глобальных ключей» в модуле управления ключами
- Скорость выработки «глобальных ключей» делится пропорционально частоте запросов пользовательских приложений
- Доступная скорость выработки может быть ниже необходимой потребителям

Появление метаданных на каждом уровне обработки ключей (получение от КРК, сетевое распределение и выдача потребителям):

- Уникальный ID ключа и модуля управления ключами при получении квантового ключа;
- ID узлов сети КРК, временная метка отправки
- ID модуля выдачи ключей, временная метка получения ключа
- ID устройства потребителя и время выдачи ключа



Актуальные проблемы при создании модулей управления ключами за рубежом:

Эффективные методы ведения **буферов ключей**.
Минимизация задержек при запросе ключей в критических важных приложениях.

- **Effective key storage approaches:** The key manager is required to effectively manage cryptographic keys, which includes key storage and formatting. It is critical that keys are stored in a manner that allows for efficient key addition and retrieval. Key formatting should also be supported and performed efficiently on demand because the application in critical infrastructures requires a minimum delay in key supply. There are no studies analyzing the effectiveness of key storage designs, nor are there detailed approaches to effective key formatting.

Приоритезация потребителей в соответствии с метриками качества обслуживания для распределения приоритета выдачи ключей.
В критически важных приложениях **не должно быть отказа в обслуживании**.

- **Effective resource sharing and quality of service support:** With the growing push for enterprise integration of QKD networks, it's anticipated that a large number of users, i.e., cryptographic applications, will need to share limited key resources. The key manager must prioritize applications of varying backgrounds and even support quality of service requirements for the most critical applications. Most approaches utilize desired key rates as a metric for allocating available resources. However, it's essential to consider the nature of the applications.

Создание и стандартизация **единого интерфейса взаимодействия для модулей управления ключами** разных вендоров.
Сопряжение сегментов квантовых сетей на аппаратуре **разных вендоров**.

- **Standardization of interfaces for communication between remote key managers:** To achieve interoperability and ensure fair representation of different key manager vendors, it's crucial to define the methods and protocols between remote key managers. This point presents a significant obstacle to developing and integrating QKD networks. As vendors endeavor to incorporate their QKD devices and key managers into a single device and rely on proprietary interfaces, the result is the imposition of a QKD network reliant on the catalog of a single vendor. The absence of a standardized interface between key managers hinders the broader integration of QKD networks, particularly in terms of key relaying, which is aimed to be addressed through the ETSI QKD 020 standard. However, there are concerns that this solution may not scale effectively and could potentially slow down the traffic within the QKD network.

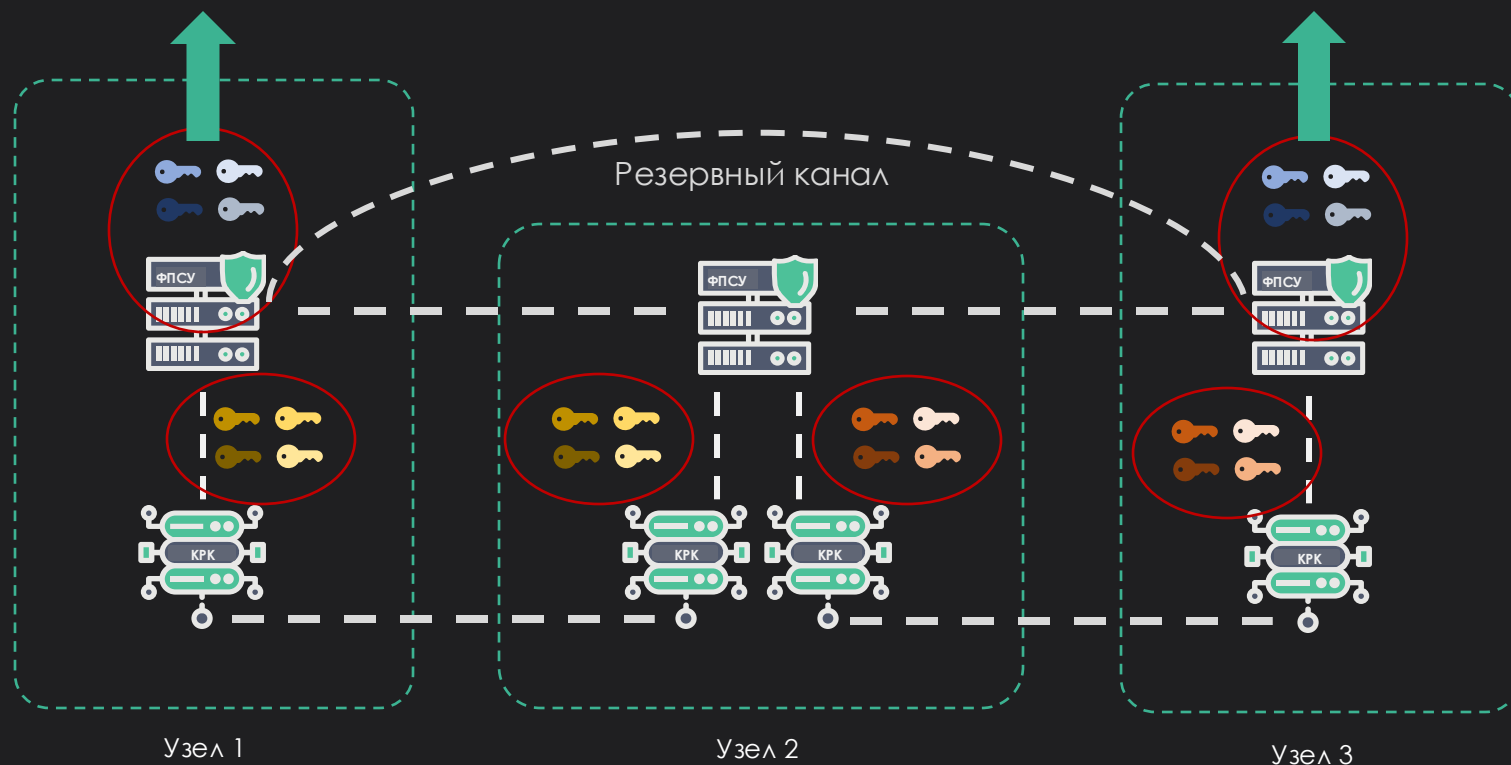
Накопление буферов КЗК

Повышение



СМАРТС
КВАНТТЕЛЕКОМ

- Формирование буферов квантовых и квантовозащищенных ключей в ФПСУ
- Сохраняет возможность предоставления услуги при отказе одного или нескольких модулей КРК и ФПСУ на разных сегментах квантовой сети



Основные принципы

- Буферы КК и КЗК формируются непрерывно
- Выдача КК и КЗК происходит по запросу СКЗИ-Потребителя без ожидания времени на формирование нового ключа
- Для КК и КЗК администратор СКЗИ может устанавливать различную длительность использования (с учетом максимальной допустимой нагрузки на ключ)
- Минимальная емкость буферов ключей может рассчитываться исходя из суточных лимитов на запрос ключей СКЗИ-Потребителями или нормативного времени замены вышедших из строя устройств

СКЗИ для построения квантовых сетей

Решение для построения магистральных сетей произвольной топологии



1. Идентификатор узла, состоящий из идентификатора сети и номера узла

Идентификатор сети состоит из 4-х символов, среди которых могут быть цифры и заглавные латинские буквы. Количество возможных вариантов — около 1.7 млн. ($36^4 = 1\,679\,616$).

2. Тип устройства. 01 – модуль управления ключами, 02 – ККС ВРК, 03 – СКЗИ-Потребитель, 04- межсетевой шлюз.

Количество вариантов от 1 до 254

3. Идентификатор клиента. Используется только для СКЗИ-Потребителей.

Структура аналогична Идентификатору сети.

4. Номер устройства.

Используется для идентификации клиентских устройств в пределах одного узла. Интервал значений — от 1 до 2^{32} (более 4 млрд.)

В ячейках указаны 16-ричные значения, либо ASCII символы в кавычках.

Структура для модуля управления ключами:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Идентификатор узла						Резерв									Тип уст.
Идентификатор квантовой сети [A..Z, 0-9]				Номер узла		=0									=1

Пример:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
`Q`	`K`	`D`	`1`	00	0F	00	00	00	00	00	00	00	00	00	01

Структура для ККС ВРК:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Идентификатор узла						Идентификатор соседнего узла						Резерв			Тип уст.
Идентификатор квантовой сети [A..Z, 0-9]				Номер узла		Идентификатор квантовой сети [A..Z, 0-9]				Номер узла		=0			=2

Пример:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
`Q`	`K`	`D`	`1`	00	0F	`Q`	`K`	`D`	`1`	00	10	00	00	00	02

Структура для СКЗИ-Потребителя:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Идентификатор узла						Идентификатор клиента				№ устройства				Резерв	Тип уст.
Идентификатор квантовой сети [A..Z, 0-9]				Номер узла		[A..Z, 0-9]								=0	=3

Пример:

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
`Q`	`K`	`D`	`1`	03	09	`R`	`T`	`K`	`1`	01	E2	40	00	00	03



3. Какими бывают магистральные квантовые сети в мировой практике?



Chen, H.Z., Li, M.H., Wang, Y.Z. et al. Implementation of carrier-grade quantum communication networks over 10000 km. *npj Quantum Inf* **11**, 137 (2025). <https://doi.org/10.1038/s41534-025-01089-8>

npj | quantum information

Published in partnership with The University of New South Wales

Article



<https://doi.org/10.1038/s41534-025-01089-8>

Implementation of carrier-grade quantum communication networks over 10000 km

 Check for updates

Hao-Ze Chen^{1,2,3}, Ming-Han Li^{1,2,3}, Yu Zhou Wang¹, Zhen-Geng Zhao², Cheng Ye^{1,2}, Fei Long Li^{1,2}, Zhu Chen², Sheng-Long Han², Bao Tang², Ya Jun Miao^{1,2} ✉ & Wei Qi^{1,2} ✉

Протяженность:
более 10 000 км

145 узлов магистральной сети

80 городов в **17 провинциях**

7 типов различных систем КРК

Опубликовано 8 августа 2025 года



Длительность недоступности сервиса по формированию ключей (часы в неделю)

Table 1 | List of the durations when KM-Links failed to provide service (hours)

	Harbin-Beijing (3 KM-Link)	Beijing-Wuhan (4 KM-Link)	Wuhan-Guangzhou (3 KM-Link)	Guangzhou-Shenzhen (2 KM-Link)
Week 1	0.51	0	1.01	0
Week 2	0	0	0	0
Week 3	1.69	0	0	0
Week 4	0.09	0	0.96	0
Week 5	1.21	0	0	0
Week 6	0	0	0	0
Week 7	0.49	0	0	0
Week 8	0.51	0	0.91	0
Week 9	0.17	0	0	0
Week 10	0.46	0	0	0
SUM	5.13	0	2.88	0

19 узлов

14 узлов

Chen, H.Z., Li, M.H., Wang, Y.Z. et al. Implementation of carrier-grade quantum communication networks over 10000 km. npj Quantum Inf 11, 137 (2025). <https://doi.org/10.1038/s41534-025-01089-8>

Доступность сервисов квантовой сети КНР

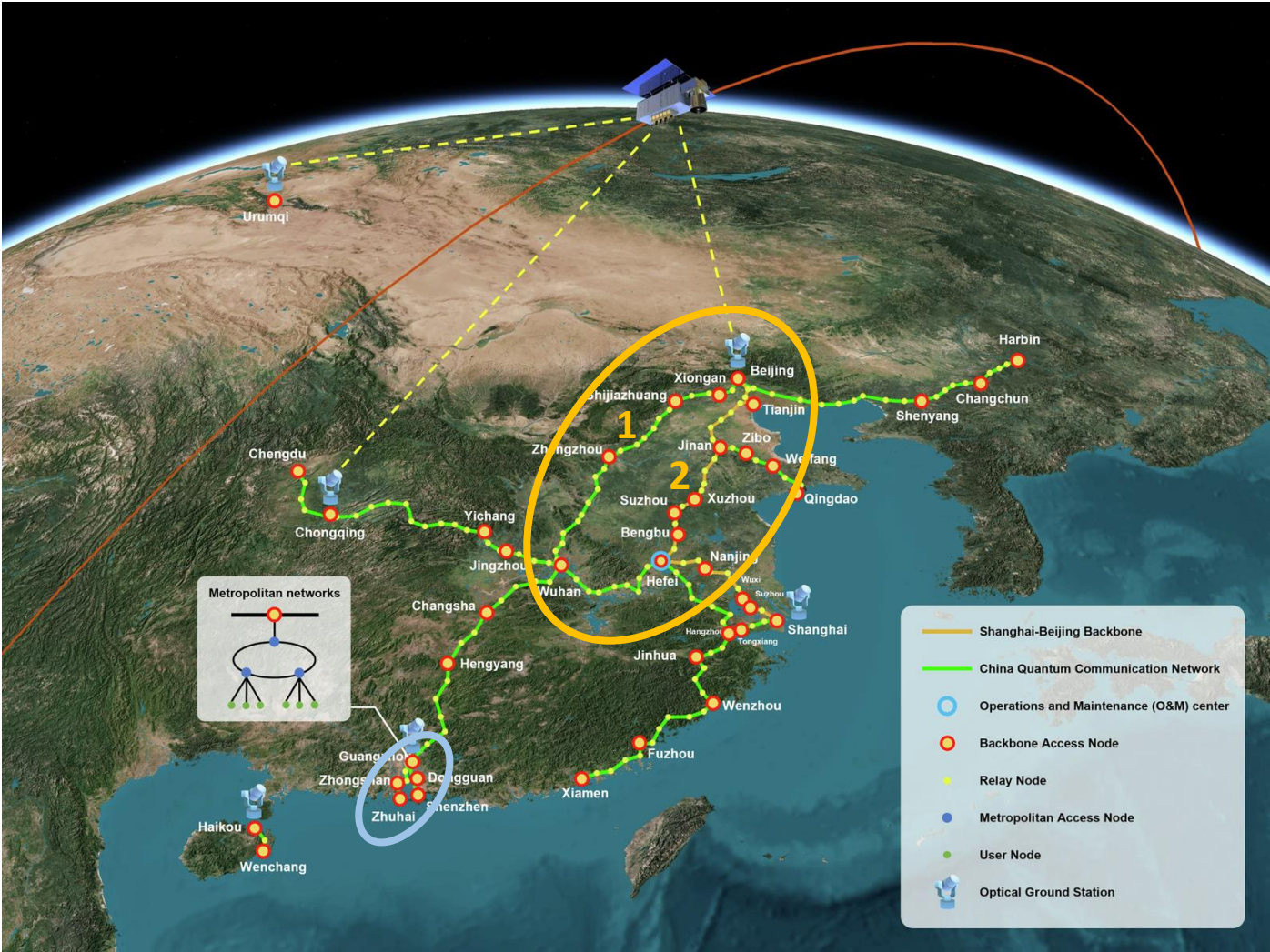


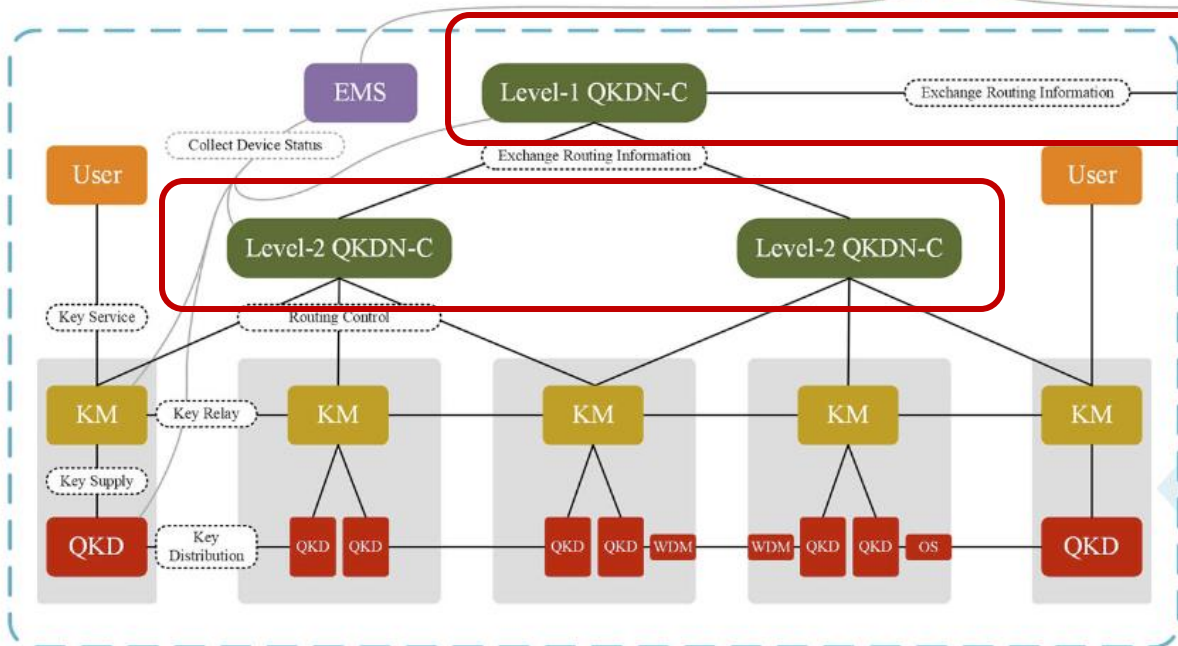
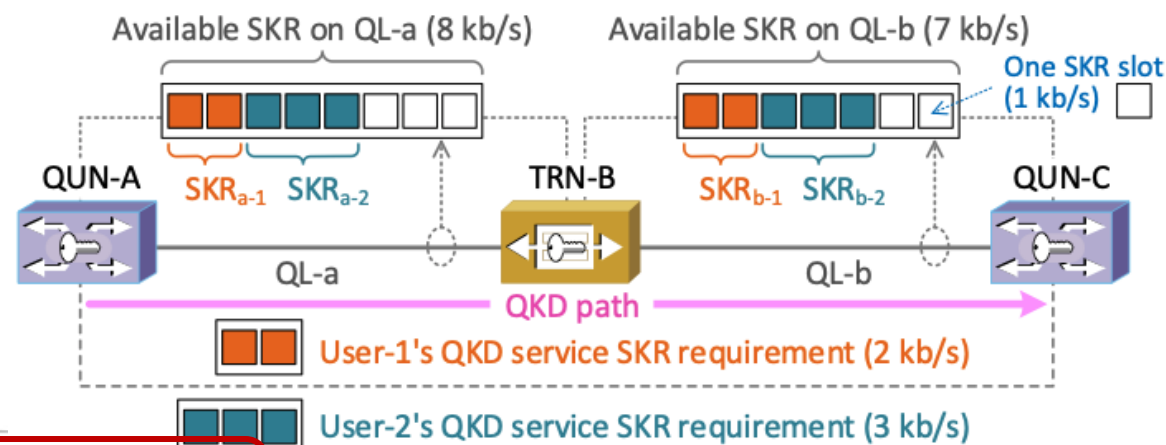
Table 1 | List of the durations when KM-Links failed to provide service (hours)

	Harbin-Beijing (3 KM-Link)	Beijing-Wuhan (4 KM-Link)	Wuhan-Guangzhou (3 KM-Link)	Guangzhou-Shenzhen (2 KM-Link)
Week 1	0.51	0	1.01	0
Week 2	0	0	0	0
Week 3	1.69	0	0	0
Week 4	0.09	0	0.96	0
Week 5	1.21	0	0	0
Week 6	0	0	0	0
Week 7	0.49	0	0	0
Week 8	0.51	0	0.91	0
Week 9	0.17	0	0	0
Week 10	0.46	0	0	0
SUM	5.13	0	2.88	0

1: 23 узла
2: 29 узлов

3 узла

- Разделение доступной скорости выработки ключей и потребностей пользователей на отдельные слоты
- Автоматизация поиска и использования слотов по запросу с помощью SDN контроллера



Иерархичная структура системы управления

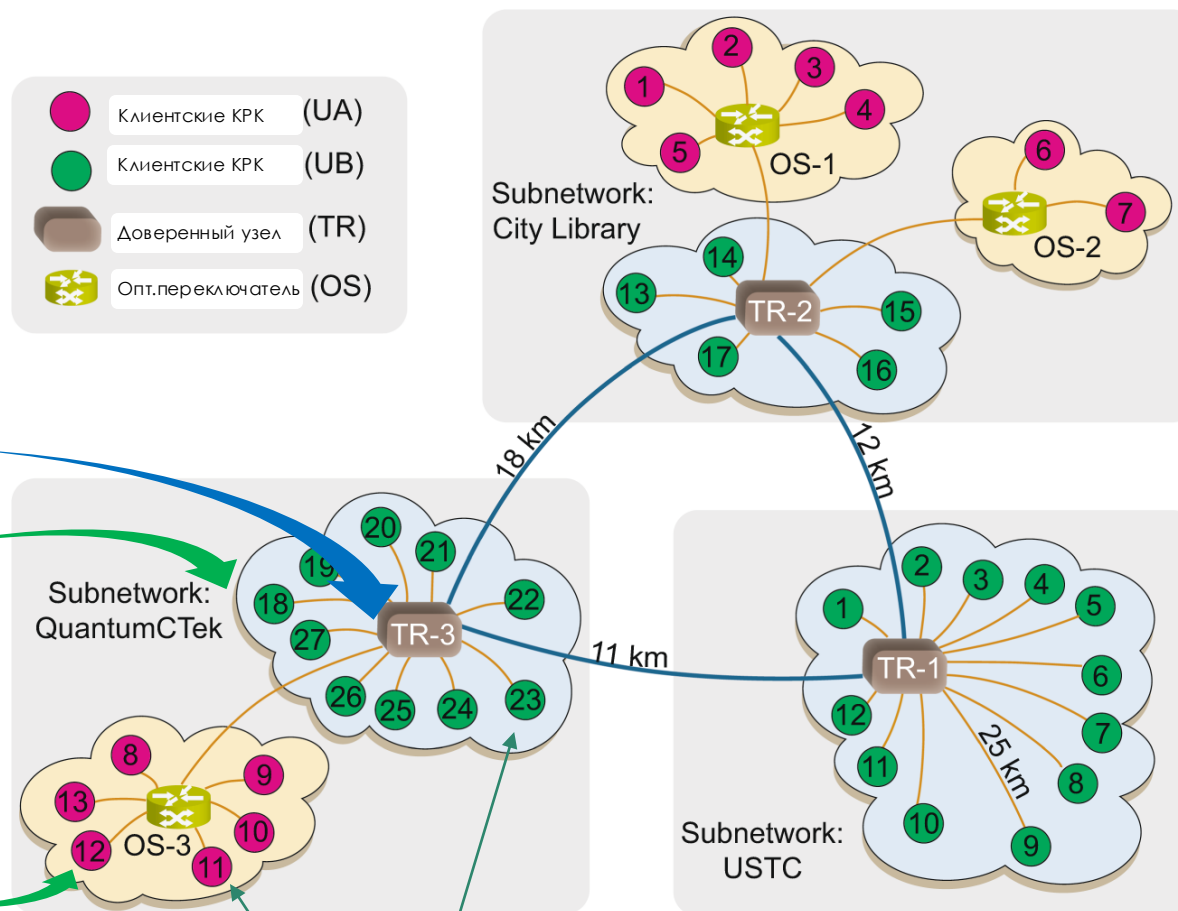
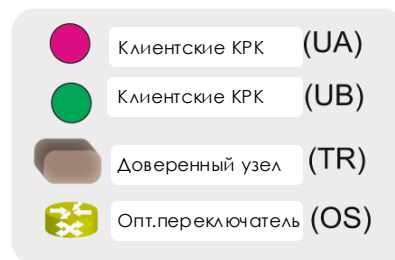
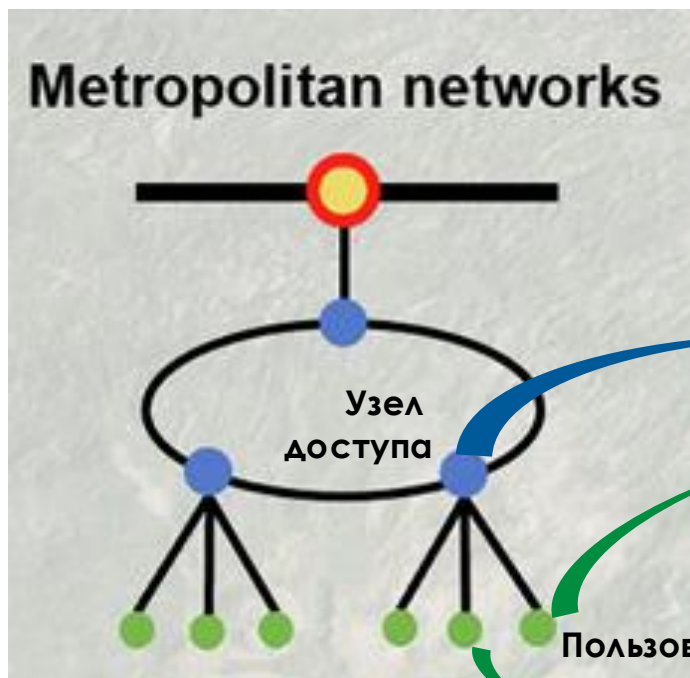
- **1 уровень** отвечает за управление внутри сегмента сети КРК
- **2 уровень** отвечает за взаимодействие между сегментами сетей КРК, в т.ч. передачу ключей между сегментами

Структура сети управления совпадает со стандартами ITU и рядом научных работ, использующих технологию SDN

Архитектура квантовой сети КНР: городские сети



SMARTS
КВАНТТЕЛЕКОМ

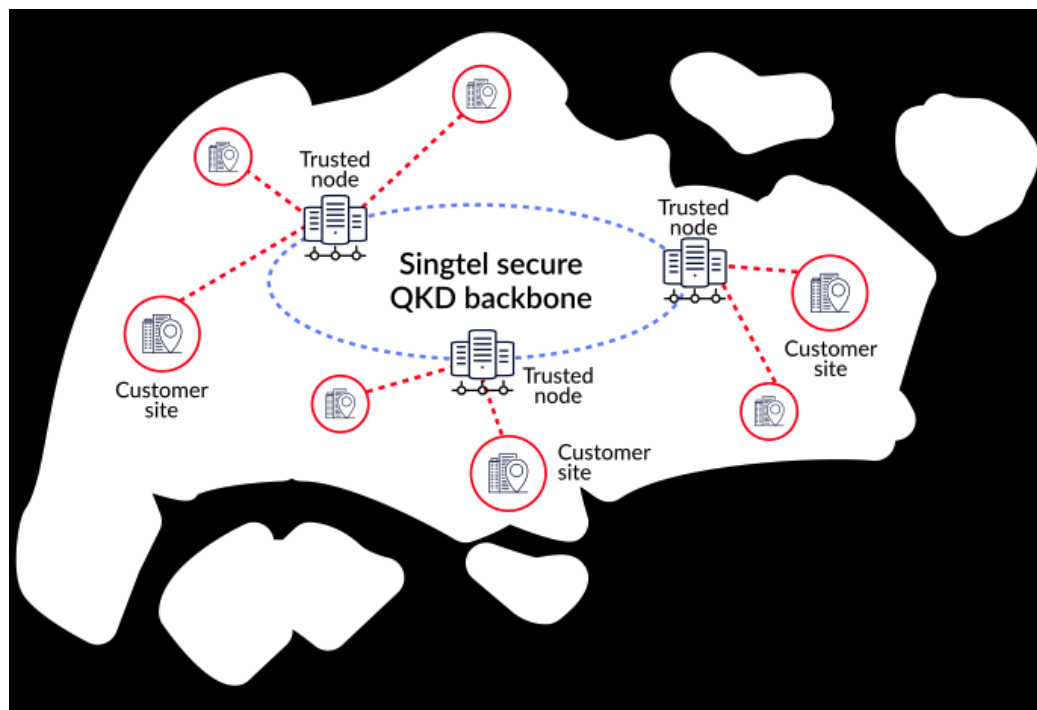


20 городских квантовых сетей,
в которых развернуто **36 узлов** доступа и
подключено более **800 пользователей**

К пользовательским узлам
может присоединяться набор шифраторов

Только ли в Китае кольцевая структура городских сетей?

Квантово-защищенная сеть Singtel
Сингапур, 2023-2025



 Singtel

 NOKIA

 CISCO

 FORTINET

 IDQ

<https://www.idquantique.com/quantum-safe-security/securing-singapore-into-the-quantum-era/>

Национальная квантовая сеть,
Республика Корея



Топология «кольцо» в
рамках магистральной
квантовой сети

2 городских сегмента
квантовой сети топологии
«кольцо»

 SK telecom

 IDQ

<https://www.idquantique.com/quantum-safe-security/nation-wide-quantum-safe-key-distribution-network-in-south-korea/>

Подключение к магистральной сети

Схема для решения Амикон/СМАРТС-Кванттелеком



AMICON

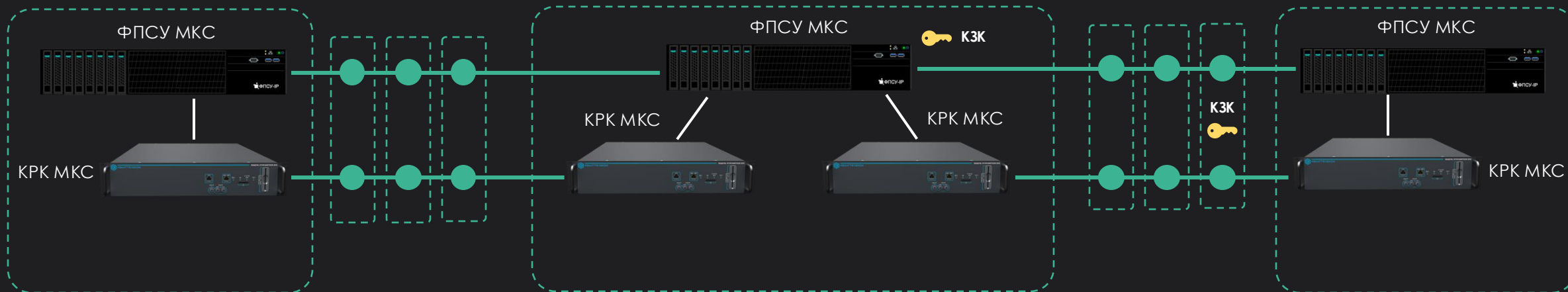


СМАРТС
КВАНТТЕЛЕКОМ

Узел МКС

Узел МКС

Узел МКС



Подключение к магистральной сети

Схема для решения Амикон/СМАРТС-Кванттелеком

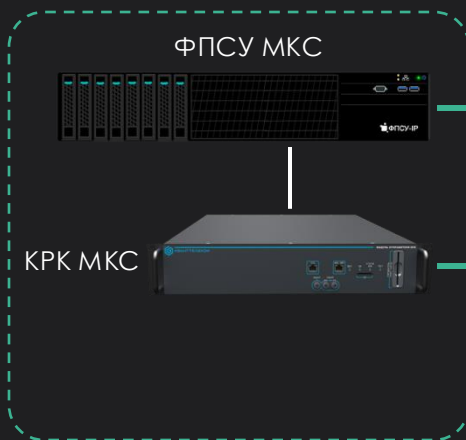


AMICON

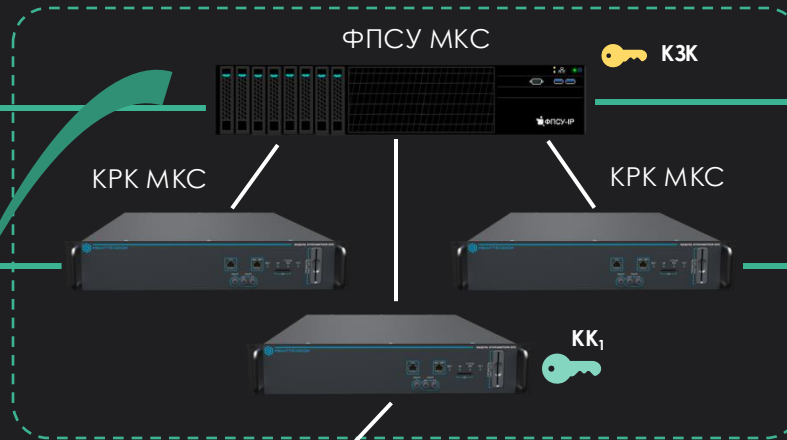


СМАРТС
КВАНТТЕЛЕКОМ

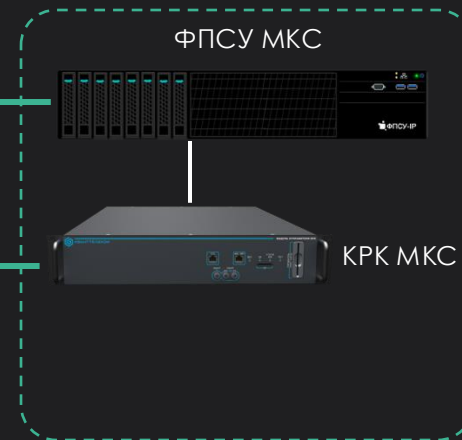
Узел МКС



Узел МКС

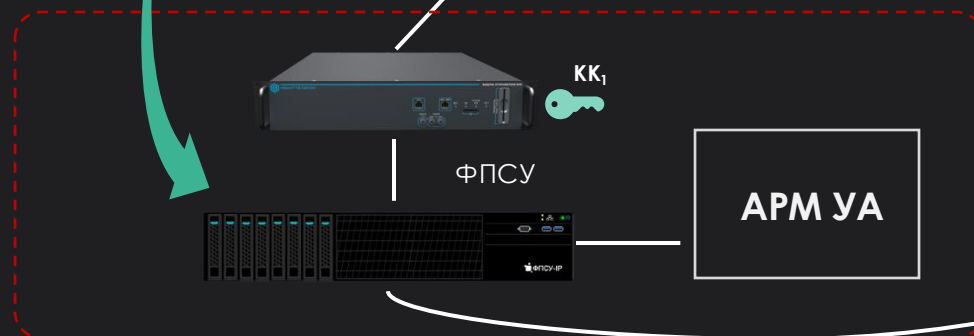


Узел МКС

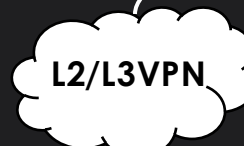


КЗК,
зашифрованный
на квантовом
ключе

Разделение зон
ответственности операторов
на уровне технических
решений и АРМ удаленного
администратора



Узел подключения



Узел
подключения



Пример реализации схемы подключения

Проект межуниверситетской квантовой сети (МУКС)

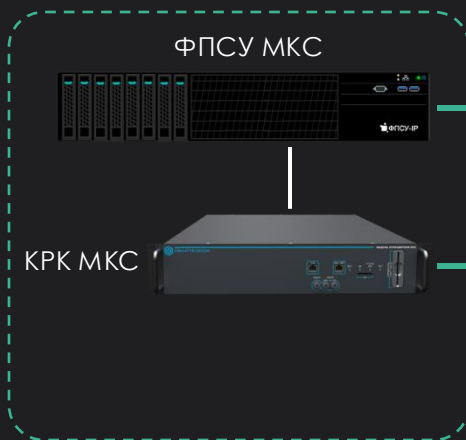


AMICON

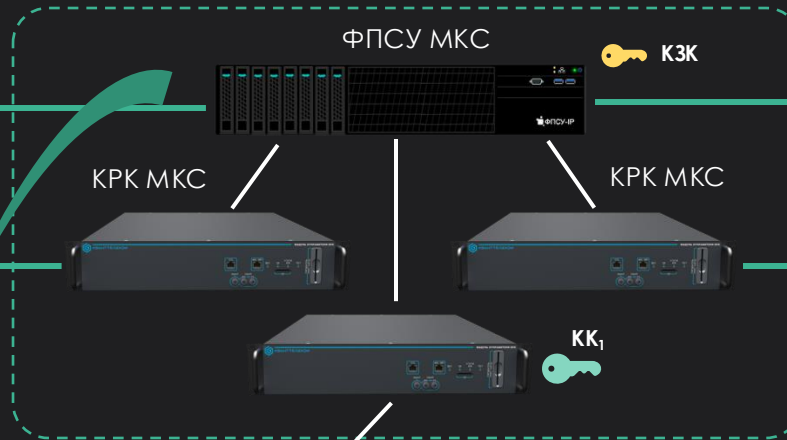


SMARTC
КВАНТТЕЛЕКОМ

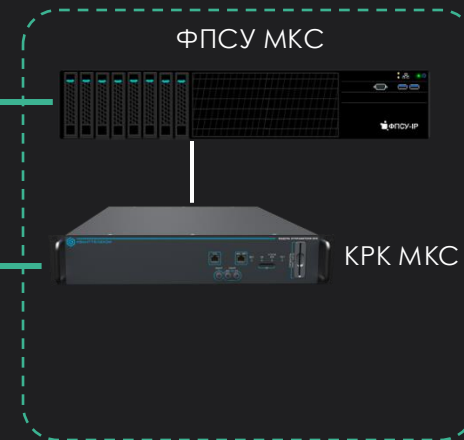
Узел МКС



Узел МКС



Узел МКС



КЗК,
зашифрованный
на квантовом
ключе

Сегменты подключения межуниверситетской квантовой сети

ИТМО

НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«КУРЧАТОВСКИЙ ИНСТИТУТ»



Узел подключения

АРМ УА



УНИВЕРСИТЕТ
ЛОБАЧЕВСКОГО

2024 год.

Подключение к
магистральной
квантовой сети.



САМАРСКИЙ УНИВЕРСИТЕТ

Возможности масштабирования

Присоединение произвольных городских и локальных сетей



AMICON

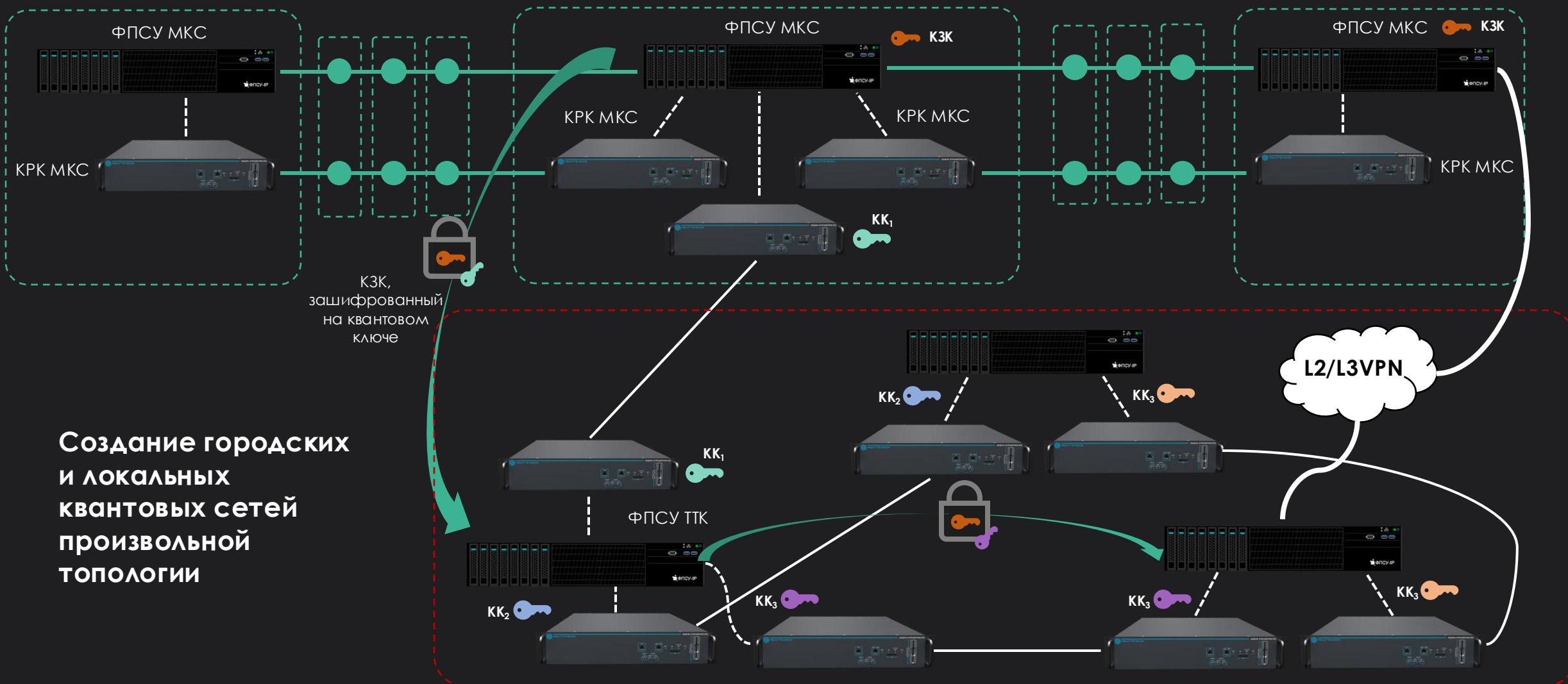


SMARTC
КВАНТТЕЛЕКОМ

Узел МКС

Узел МКС

Узел МКС

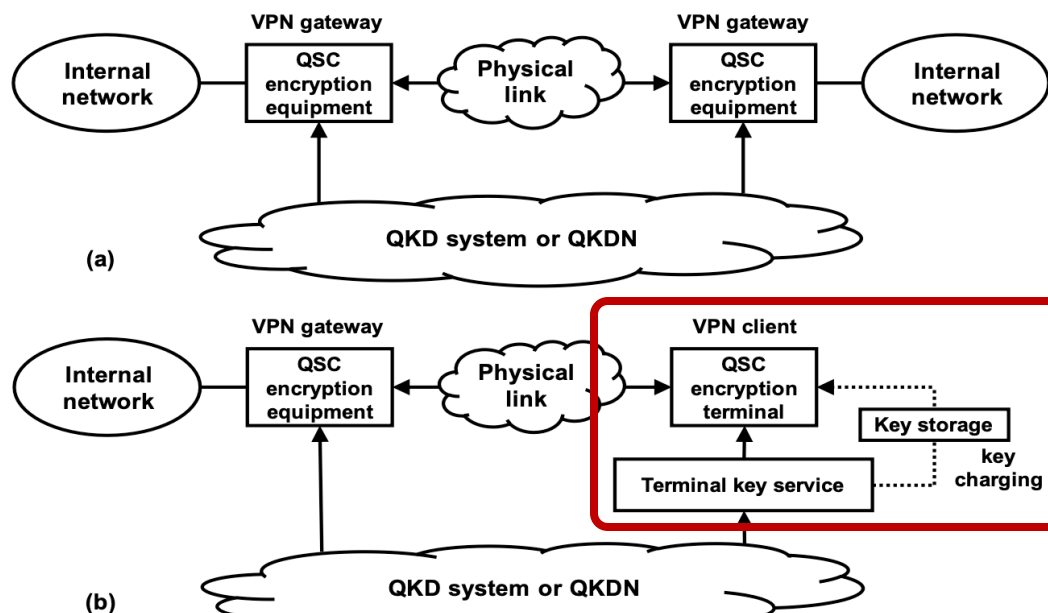




4. Какими бывают способы и примеры подключения беспроводных устройств?

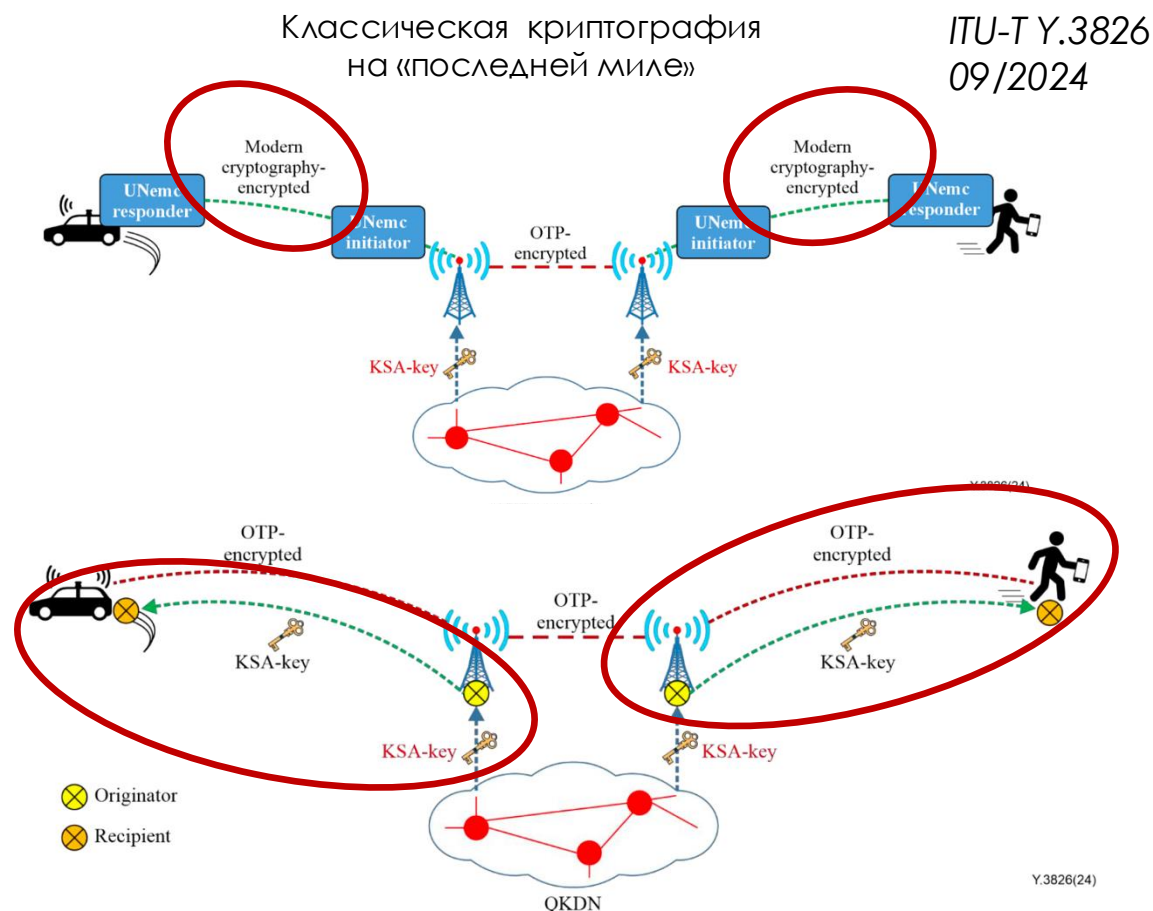
Решение проблемы «последней мили»

«Ключ как сервис» на базе квантовой сети Китая



Выдача ключей через терминал
для мобильных устройств на
«последней миле»

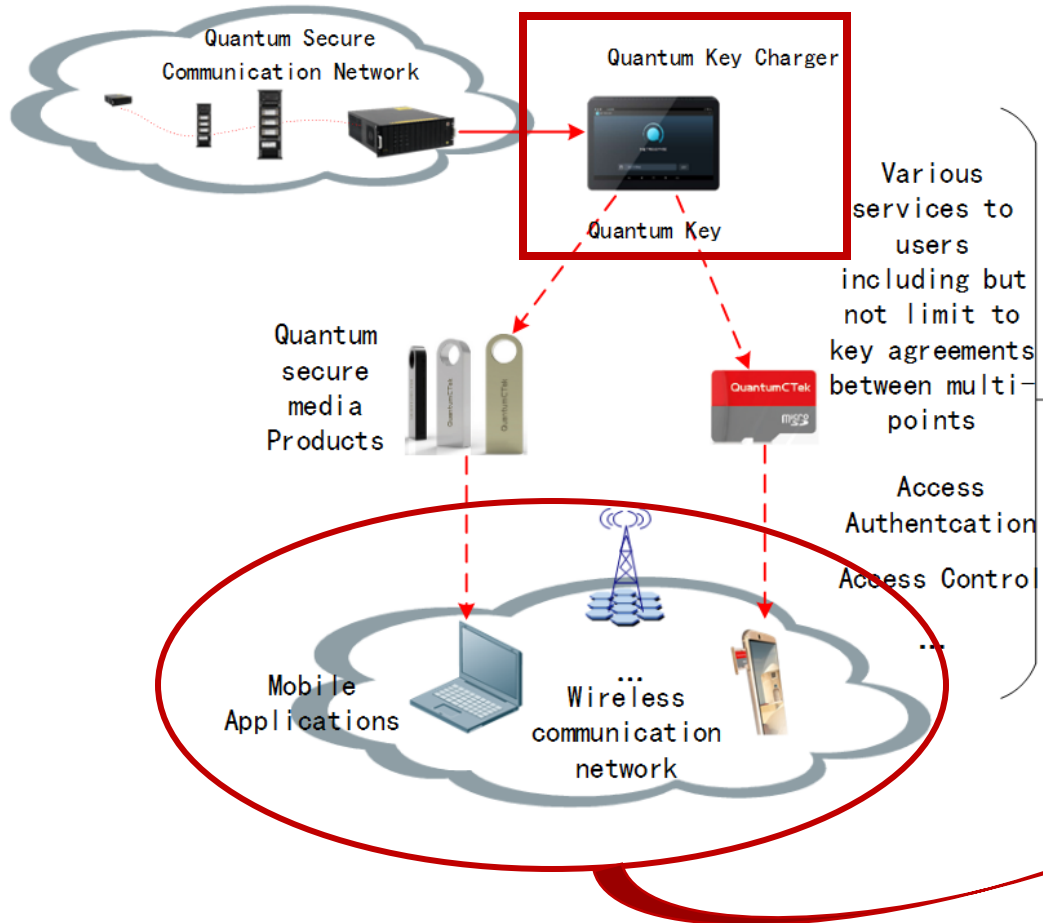
Рекомендации международного союза электросвязи



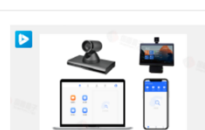
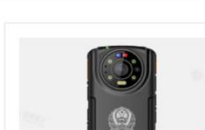
Доставка ключа от сети КРК
до конечного устройства в защищенном виде

Пример решений от QuantumCTek, КНР

«Ключ как сервис» с использованием оборудования QuantumCTek, Китай

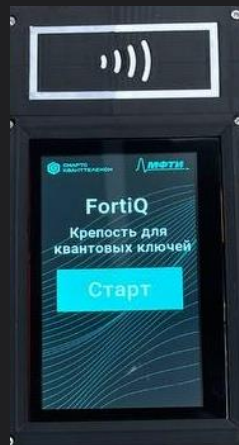


Перечень коммерчески доступных устройств для сервиса, QuantumCTek

	QuantumMail QuantumMail is a secure mail client product developed by QuantumCTek Co., Ltd. with independent IPRs. The product supports the key distribution technology of "one key at a time", providing end-to-end mail security receiving and sending services for users		Quantum Security Intelligent Office Books As an intelligent office equipment integrated with AI core technology and quantum encryption technology, quantum security intelligent office book supports handwriting recognition, voice recognition, real-time translation, quantum key protection, etc.,and
	Quantum Meeting Quantum Secure Meeting System is a series of meeting products developed by QuantumCTek Co., Ltd.. Combined with high-strength state secret algorithms, The product adopts quantum key to encrypt audio and video meeting data streams, in order to ensure the s... ..		Quantum Security HD Walkie-talkie Quantum security HD walkie-talkie is a two-way mobile communication tool, which supports the functions such as visual intercom, cluster conference, electronic map, etc. With the quantum encryption technology, the product can encrypt the terminal intercom
	Quantum Identity Security System Quantum Identity Security System is a series of products jointly developed by QuantumCTek Co., Ltd. and Bamboocloud Co.,Ltd., which can effectively ensure the access control security of application systems. Based on technologies such as quantum security e... ..		Quantum Security HD Walkie-talkie Quantum security law enforcement recorder is a device that can realize audio and video forensics on the scene of law enforcement. With such functions as camera, recording, photo, voice intercom, etc., It can realize visual remote command and dispatching b... ..

Мобильный ключевой центр

Интеграция профиля протокола ProtoQa SMARTC-Кванттелеком



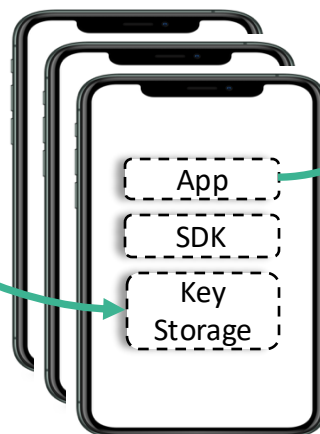
Демонстрация демо-версии на стенде «SMARTC-Кванттелеком», стенд №33

Мобильный
ключевой центр
выделенной
сети

ProtoQa,
профиль
СКТК

ККС ВРК

Хранение ключей на устройстве
Мобильное устройство



Защищенные коммуникации



В рамках программы
«Приоритет-2030»
МФТИ



**5. В каких сферах можно искать
сценарии применения для квантовых
сетей?**

Сценарий использования	Сфера применения	Описание	Вендор
Достоверность результатов выборов	Правительство, Швейцария	Применение технологии КРК при передаче данных между центром подсчета голосов и центром хранения данных о результатах выборов	ID Quantique
Резервное копирование для аварийного восстановления	Банковский сектор, Швейцария	Защита канала связи между штаб-квартирой банка и центром обработки данных с резервными копиями для аварийного восстановления информационных систем	ID Quantique
Защита финансовых данных	Финансовый сектор, США	Защита данных между двумя офисами финансовых организаций в Нью-Йорке (Уолл-Стрит) и Нью-Джерси	Toshiba
Система распознавания лиц	Биометрические данные, Япония	Защита канала передачи данных между точкой сбора биометрических данных и сервером их обработки через квантовую сеть с одним промежуточным узлом	NEC, квантовая сеть Токио
Хранение и резервное копирование ключей	Криптовалюты, Швейцария	Использование технологии КРК с шифрованием одноразовым блокнотом для защиты канала передачи ключей в распределенной системе хранения ключей криптобиржи.	ID Quantique
Передача медицинских изображений	Медицинские исследования, Австрия	Передача медицинских изображений и обеспечение удаленного доступа к ним с использованием распределенного хранения методом разделения секрета	ID Quantique Toshiba
Резервное копирование медицинских карт	Здравоохранение, Япония	Резервное копирование записей в медицинских картах с использованием технологии КРК со схемой разделения секрета для передачи в разные центры обработки данных.	Toshiba NEC
Соединение центров обработки данных	Телеком, Швейцария	Соединение двух территориально-распределенных центров обработки данных с использованием OTN-шифрования (L1 уровень)	ID Quantique ADVA
Генетические данные	Медицинские исследования, Япония	Защищенная передача данных и защищенная видеоконференцсвязь с обсуждением результатов генетических исследований (шифрование одноразовым блокнотом).	Toshiba
Соединение электростанций	Энергетика, Швейцария	Обеспечение защищенного соединения между несколькими электростанциями для управления ресурсами	ID Quantique
Аутентификация системы управления электросетями	Энергетика, США	Аутентификация трафика SCADA (т. е. данных измерений и управления) между центром распределения электроэнергии и электрической подстанцией	Qubitekk
Защита канала управления атомным реактором	Энергетика, США	Экспериментальный стенд с обеспечением доступа к полностью цифровой системе управления исследовательским атомным реактором PUD-1	Toshiba

Схема разделения секрета и технология КРК

Передача медицинских изображений и распределенное хранение с использованием схемы разделения секрета

Мотивация: большое время актуальности медицинских данных, в т.ч. генетических исследований

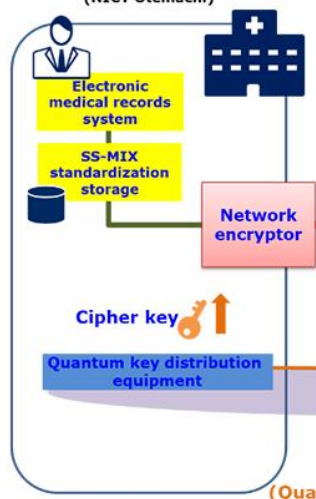
Япония, 2020

Обработка данных после передачи

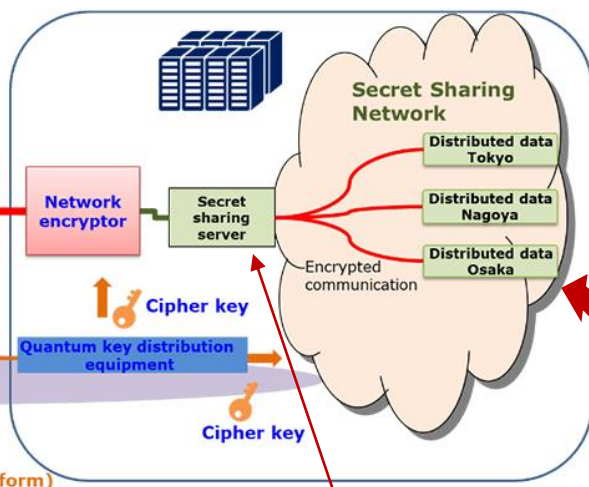
Грац, Австрия, 2020

Обработка данных до передачи
на обеих сторонах

In the simulated environment of
a Tokyo-based medical institution
(NICT Otemachi)



Distributed data backup system
(NICT Koganei)

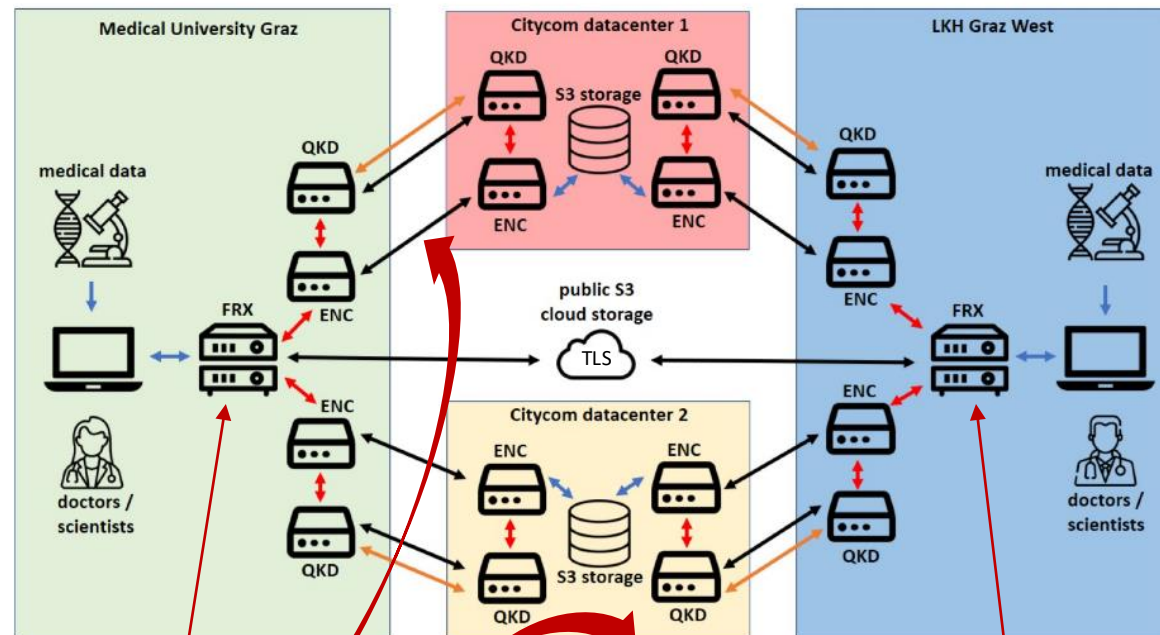


All-or-nothing transform (AONT)

Схема Шамира

Схема Шамира

Территориально-распределенные ЦОД. Хранение копий.
Защита каналов: симметричное шифрование и системы КРК



Высокопроизводительные вычисления в режиме реального времени и технология КРК

Лондон, 2021 год

Национальный центр композитных материалов (NCC)

Квантовозащищенный
канал

Операторский
кластер обмена
трафиком
British Telecom

Квантовозащищенный
канал

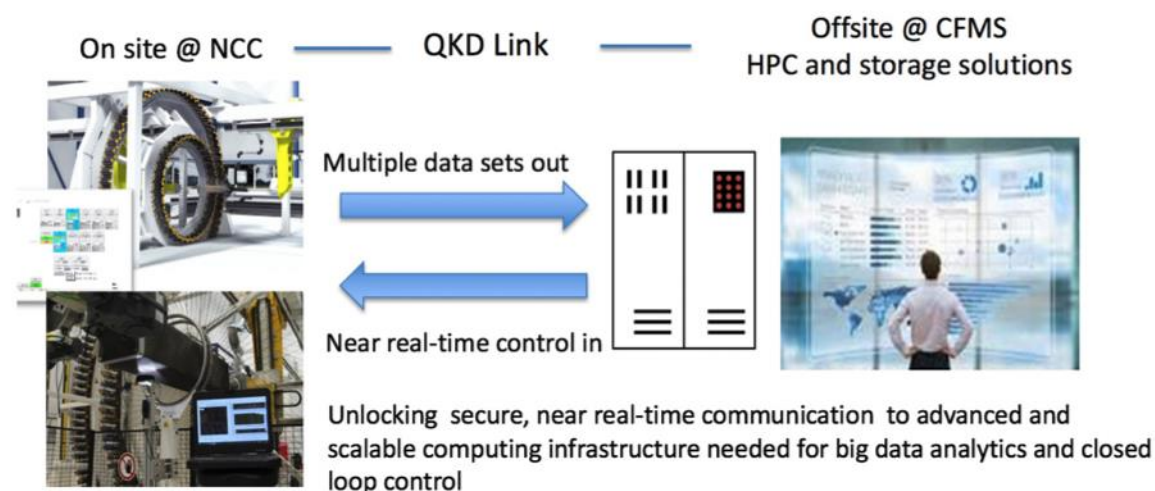
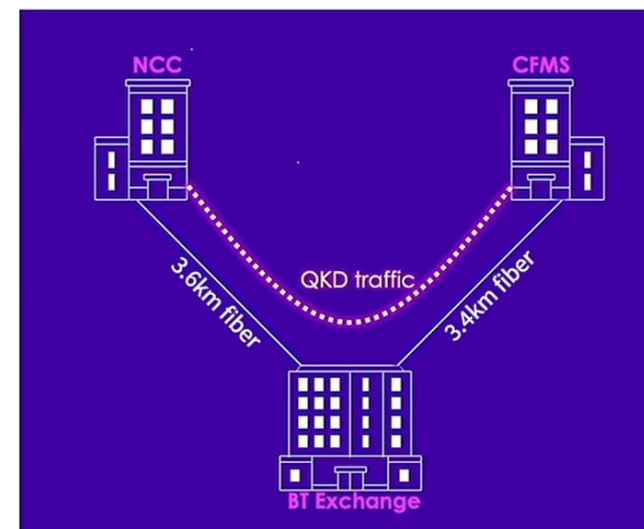
Центром моделирования и симуляции (CFMS)

Необходимо:

Вычислительные ресурсы для
моделирования новых
материалов с доступом в
режиме реального времени

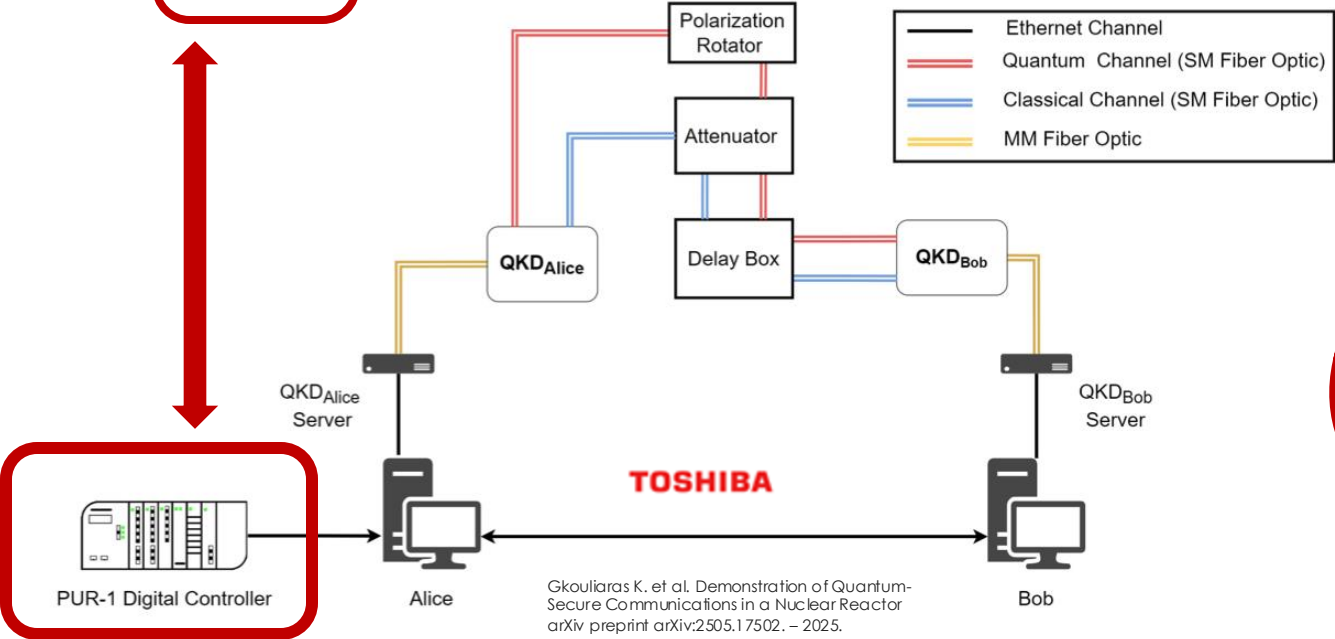
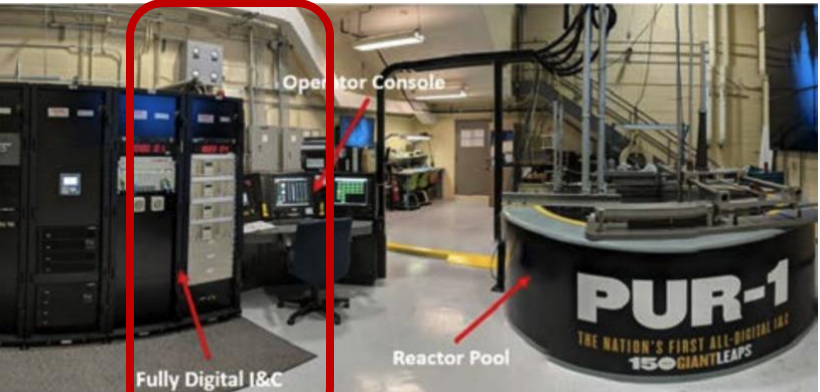
Ограничение:

Надежная защита
передаваемых данных для
построения моделей

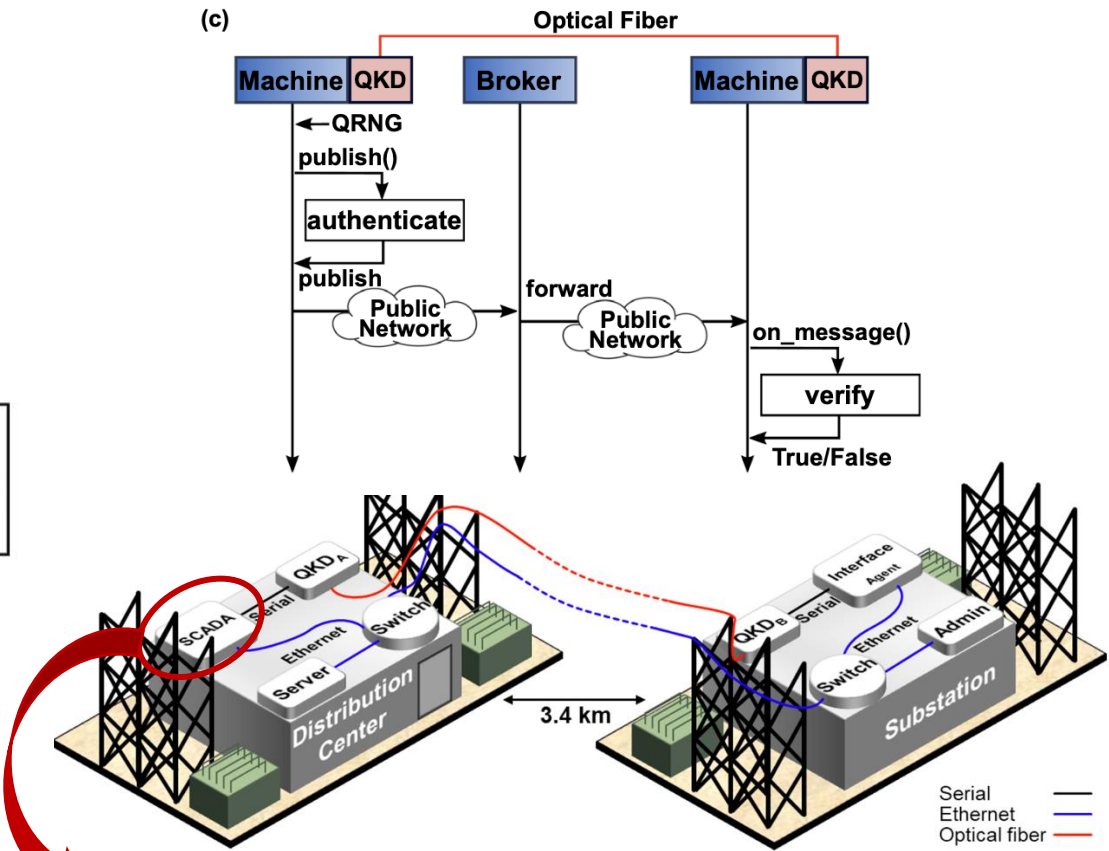


Применение технологии КРК в энергетическом секторе и на атомном реакторе

Защита канала доступа к цифровой системе управления
исследовательским **атомным реактором**



Аутентификация
электроподстанций с использованием
криптографических методов



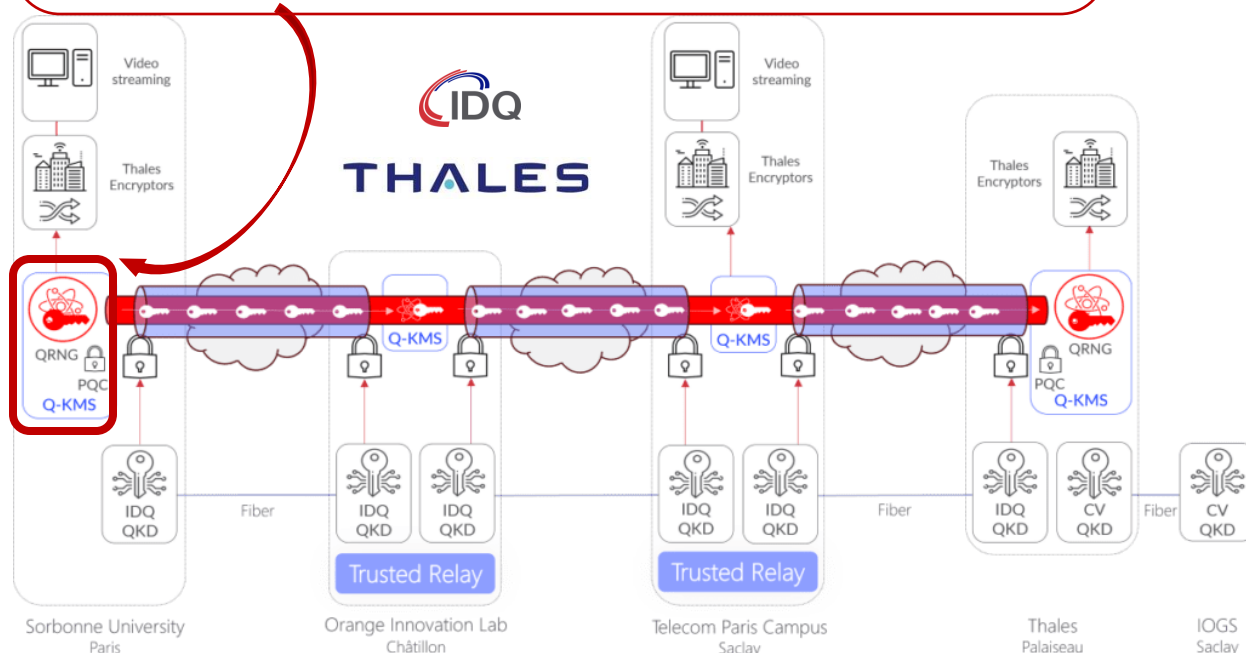
SCADA - система диспетчерского управления и сбора телеметрии

Alshowkan, M., Evans, P.G., Starke, M. et al. Authentication of smart grid communications using quantum key distribution. *Sci Rep* 12, 12731 (2022). <https://doi.org/10.1038/s41598-022-16090-w>

Совместное применение технологии КРК и постквантовой криптографии

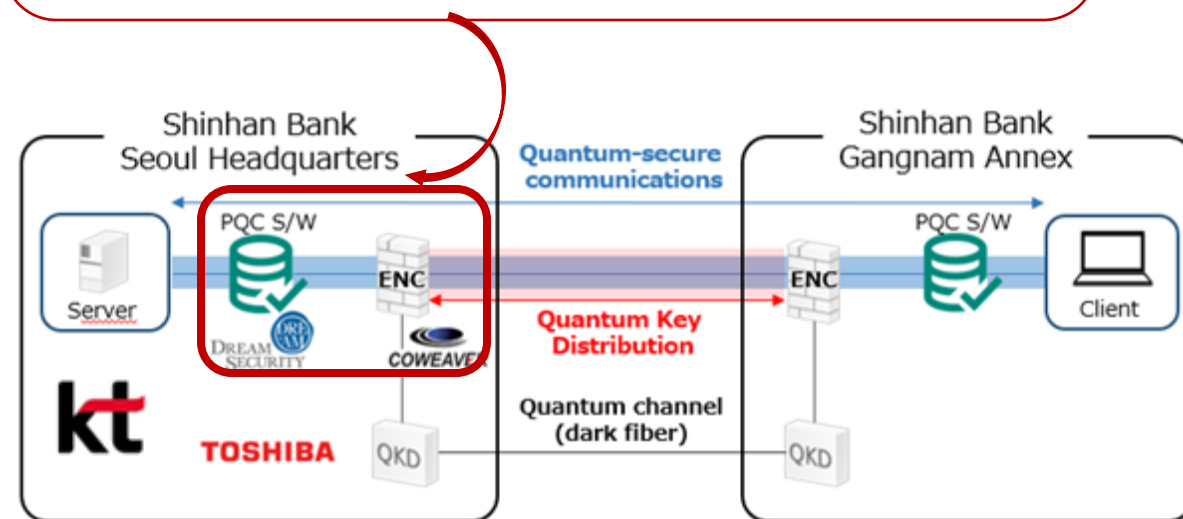
Интеграция постквантовой криптографии в составе сети КРК

- Источник криптографических ключей: квантовый генератор случайных чисел
- Постквантовая криптография используется для защиты ключей, передаваемых по сети КРК (объединение двух ключевых схем)



Интеграция постквантовой криптографии на уровне пользовательских систем

- Для защиты канала используются два контура шифрования.
- На канальном уровне - симметричное шифрование с квантовыми ключами
- На прикладном уровне – применение постквантовой криптографии



Пилотный проект с ГК «Автодор»

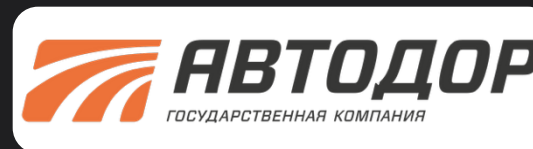
Применение технологии КРК на автодорожной инфраструктуре



СМАРТС
КВАНТТЕЛЕКОМ

Первая пилотная интеграция на сегменте автоматизированной системы управления дорожным движением (АСУДД)

При участии:



Цели проекта:

1. Анализ текущей сетевой инфраструктуры ГК «Автодор»
2. Разработка схемы организации сегментов сети КРК на инфраструктуре выделенной подсети существующей технологической сети связи (ТСС)
3. Проведение монтажных и пуско-наладочных работ на выделенных инфраструктурных объектах ТСС
4. Проведение испытаний схемы организации сегментов сети КРК на инфраструктуре выделенной подсети существующей ТСС

Автомобильная дорога: М-11 «Нева»

Длина ВОЛС: 21 км

Сроки: с 5 мая по 30 июня 2025 года

Техническое решение:

ККС ВРК «Квалион» и ФПСУ



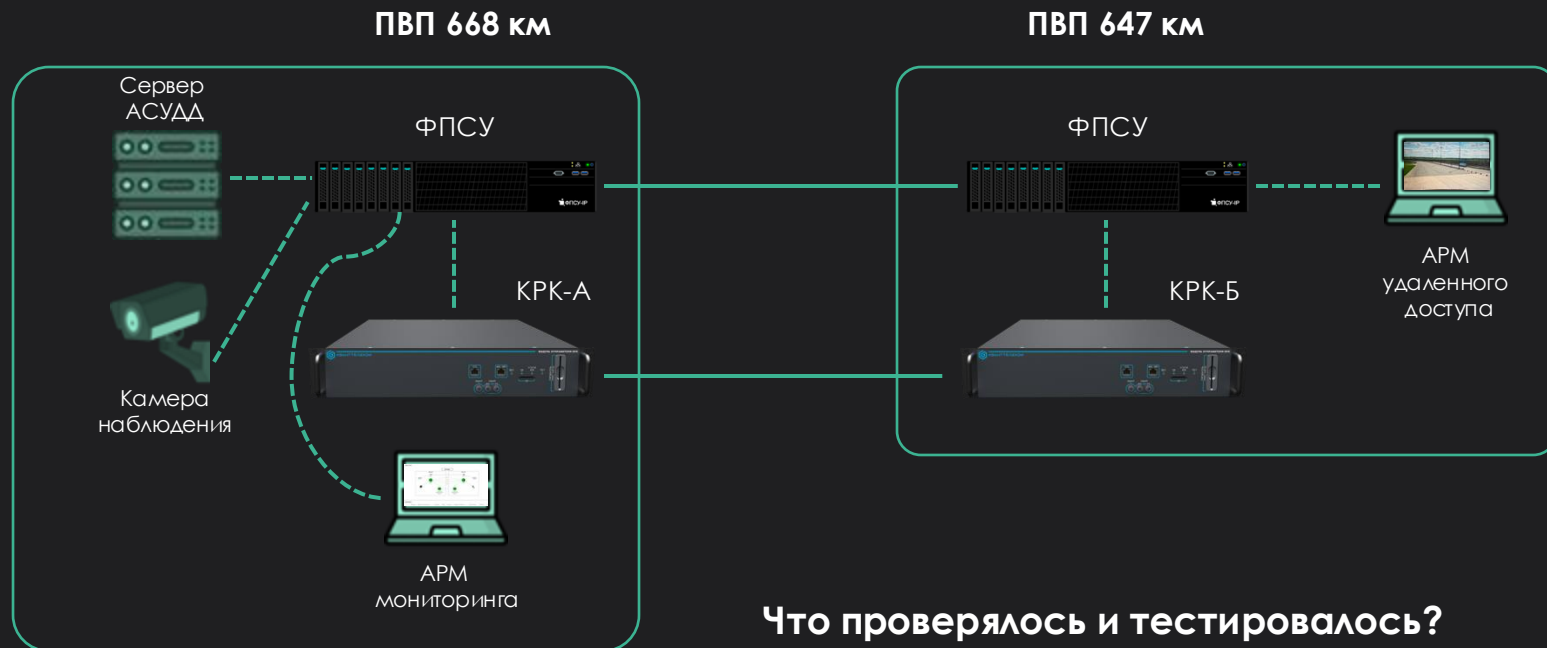
Пилотный проект с ГК «Автодор»

Применение технологии КРК на автодорожной инфраструктуре



СМАРТС
КВАНТТЕЛЕКОМ

Техническая схема решения



Что проверялось и тестировалось?

- ✓ Непрерывное функционирование ККС ВРК и сопряженных СКЗИ на длительном промежутке времени
- ✓ Отсутствие существенных сетевых задержек в канале КРК, критичных для АСУДД
- ✓ Отработка стандартных регламентов эксплуатации систем КРК
- ✓ Отработка внештатных ситуаций с выходом из строя систем КРК и СКЗИ





**SMARTS
КВАНТТЕЛЕКОМ**



Алексей Сантьев

Руководитель направления
развития и продвижения
продуктов

Контактная информация



199178, Санкт-Петербург, В.О., 6 линия д.59, корп. 1, лит. Б



a.santev@quanttelecom.ru

info@quanttelecom.ru



кванттелеком.рф