СМАРТС
КВАНТТЕЛЕКОМ

Перспективы применения технологии квантового распределения ключей в дорожной инфраструктуре

Егоров Владимир Ильич,
Советник генерального директора по науке,
ООО «СМАРТС-Кванттелеком», к.ф.-м.н.

История развития решений компании

В кооперации с Университетом ИТМО

СМАРТС КВАНТТЕЛЕКОМ

2006 - 2015

- Старт научных исследований в ИТМО
- Создание первого лабораторного макета, переход к R&D
- Первая квантовая сеть в России между двумя корпусами ИТМО
- Создание компании «Квантттелеком», резидентство Сколково
- Первые продажи лабораторных систем КРК

2016 - 2019

- Запуск четырехузловой квантовой сети в Казани между корпусами КНИТУ-КАИ
- Старт проекта по исследованию подходов к созданию программно-конфигурируемых квантовых сетей
- Запуск квантовой сети между ЦОД в Самаре при участии АО «СМАРТС»
- Старт дорожной карты «Квантовые коммуникации».

2020 - 2021

- Создание промышленных образцов систем КРК в нескольких модификациях
- Исследование систем КРК на новых принципах (протоколы, атмосферный канал)
- Первый «квантовый» звонок на пилотном участке магистральной квантовой сети Москва - СПб
- Завершение гранта Сколково и старт проектов Дорожной карты

2022 - 2024

- Квантовая сеть между городами Самарской области при поддержке РФРИТ
- Завершение проекта Минпромторга России на создание системы КРК с отечественной ЭКБ
- Испытания квантовой сети Москва - Нижний Новгород
- Монтаж квантовой сети Нижний Новгород - Казань
- Испытания на инфраструктуре TEA NEXT

Как взаимодействовать «умным дорогам» и «умным машинам»

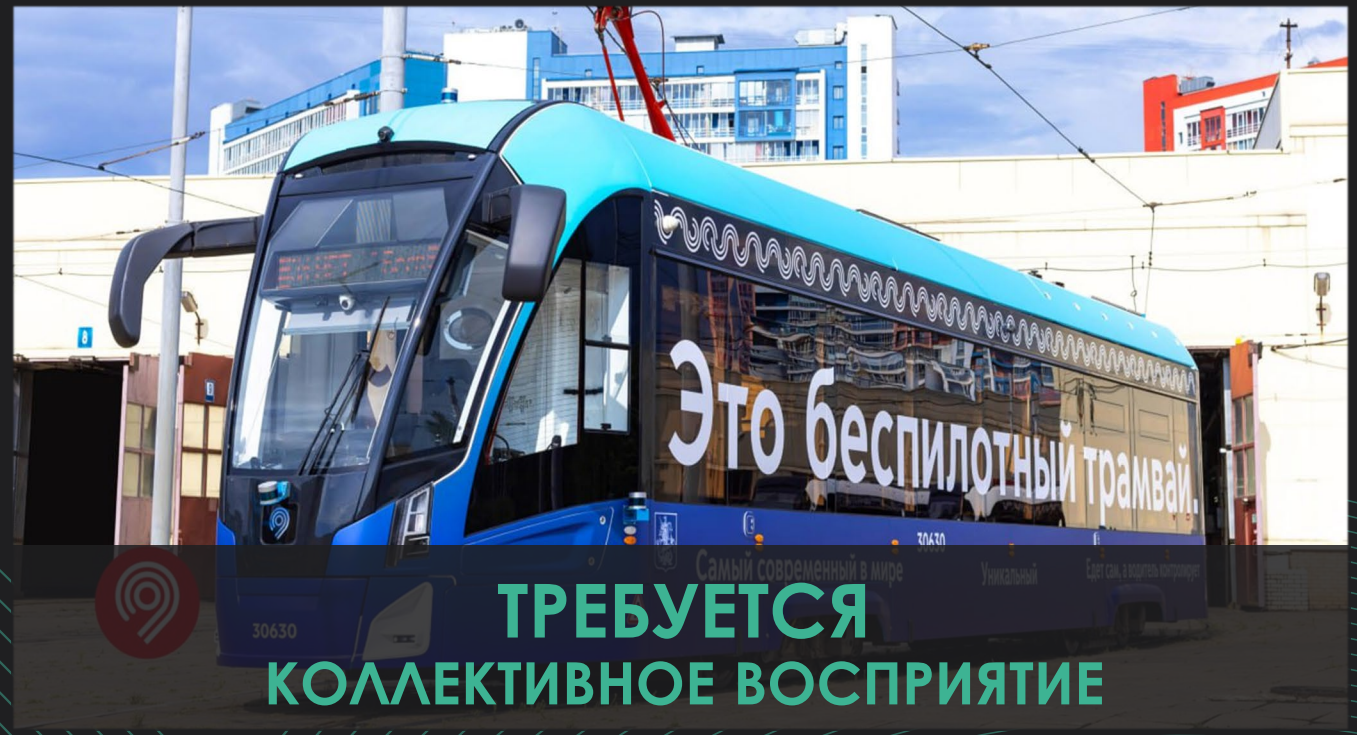
СМАРТС

Как обеспечить приоритетный проезд?

Как автоматизировать стрелки?

ПЕРВОСТЕПЕННО:

- Безопасность
- Контроль
- Взаимодействие



Защита данных сегодня

Проблемы существующих методов шифрования

СМАРТС КВАНТТЕЛЕКОМ

Криптография с симметричным ключом

- Необходим защищенный канал передачи секретного ключа;
- В особо важных случаях (гос. тайна, банковская информация) передача ключа отправителю и получателю осуществляется в ручном режиме на физическом носителе;
- Для обеспечения высокого уровня безопасности передачи данных необходима частая смена ключа, что влечет проблему его передачи.

Криптография с открытым ключом

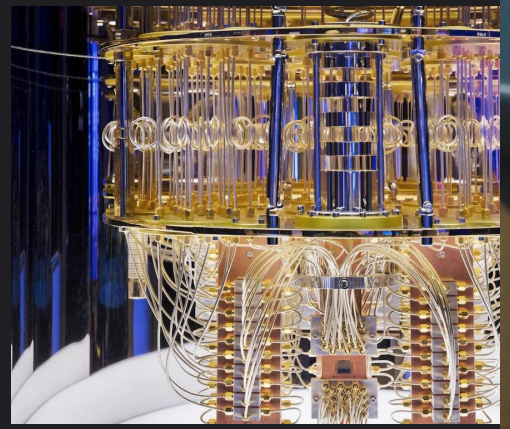
- Безопасность широко используемых методов основана на том, что перехватчик не успеет расшифровать информацию, пока она актуальна;
- Сложность дешифровки сообщений зависит от длины ключа. Увеличение его длины значительно перегружает инфраструктуру и уменьшает скорость обмена сообщениями;
- Подобрать ключ ограниченной величины возможно (RSA 768 бит был подобран на электронных компьютерах в 2010г.*)

* http://www.emc.com/emc-plus/rsa-labs/historical/rsa-768-factored.htm

Угрозы криптосисте

Мотивация к поиску новых ре

Существующие криптосистемы с от
могут быть полностью взломаны кванто



Крупные компании, занимающиеся создани
компьютера:

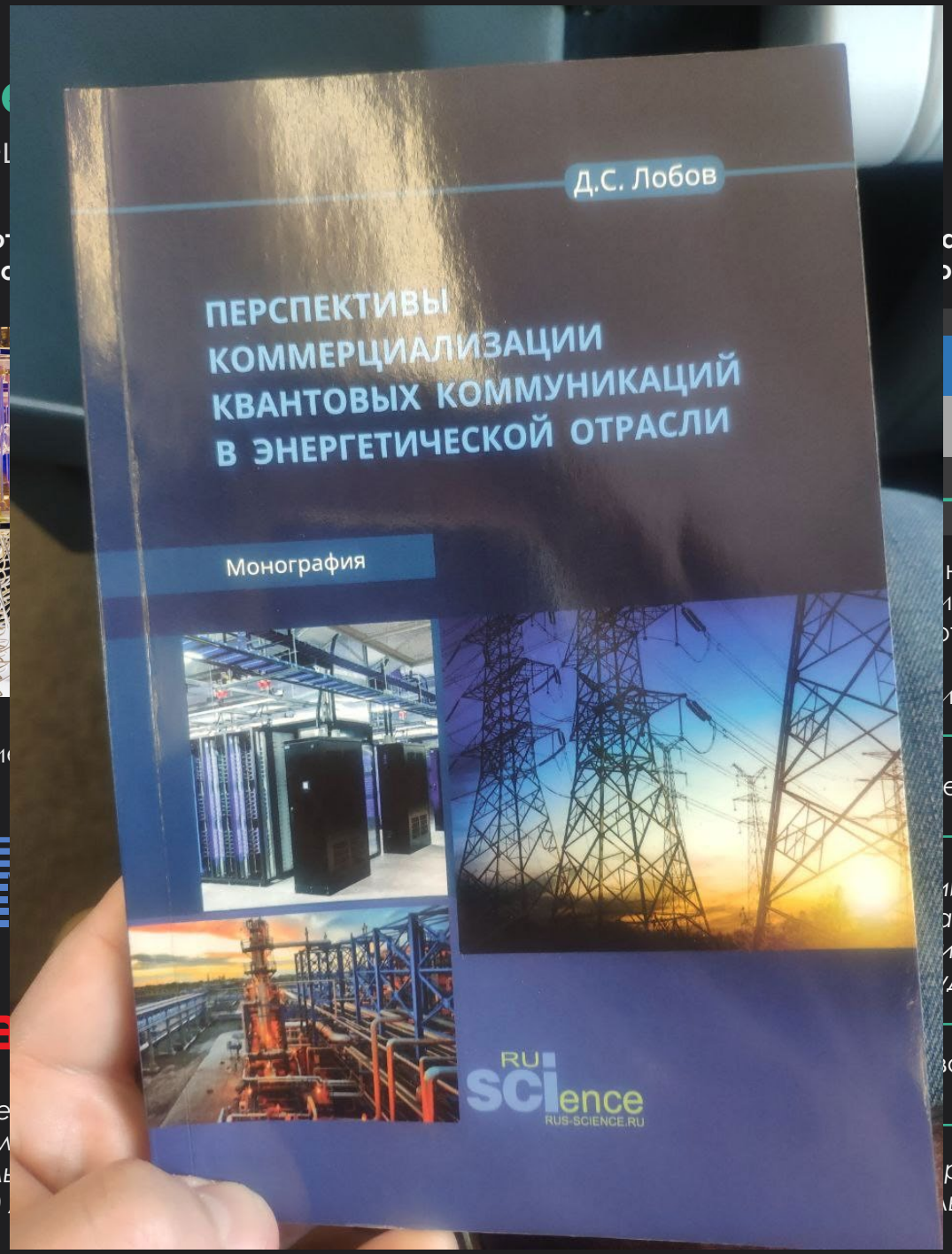
D:Wave

IBM

Alibaba.com

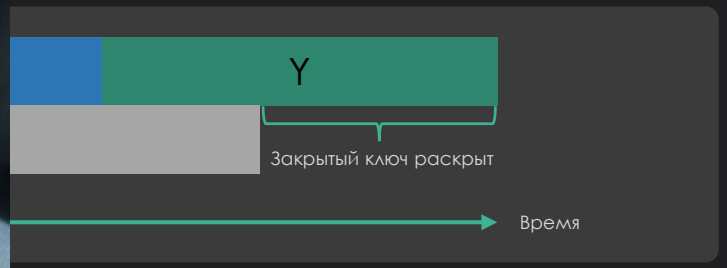
Ba

*В 2021 году компания **Google** впервые*
***квантового превосходства:** квантовый ком*
решил задачу, на решение которой самы
компьютерам понадобилось бы более 1000



СМАРТС
КВАНТТЕЛЕКОМ

аться о смене криптосистем с
ткрытым ключом?



новых криптоалгоритмов на замену (с учетом
инфраструктуры и т.п.)
торого защищаемая информация остается

иверсального квантового компьютера

емая информация **будет скомпрометирована**

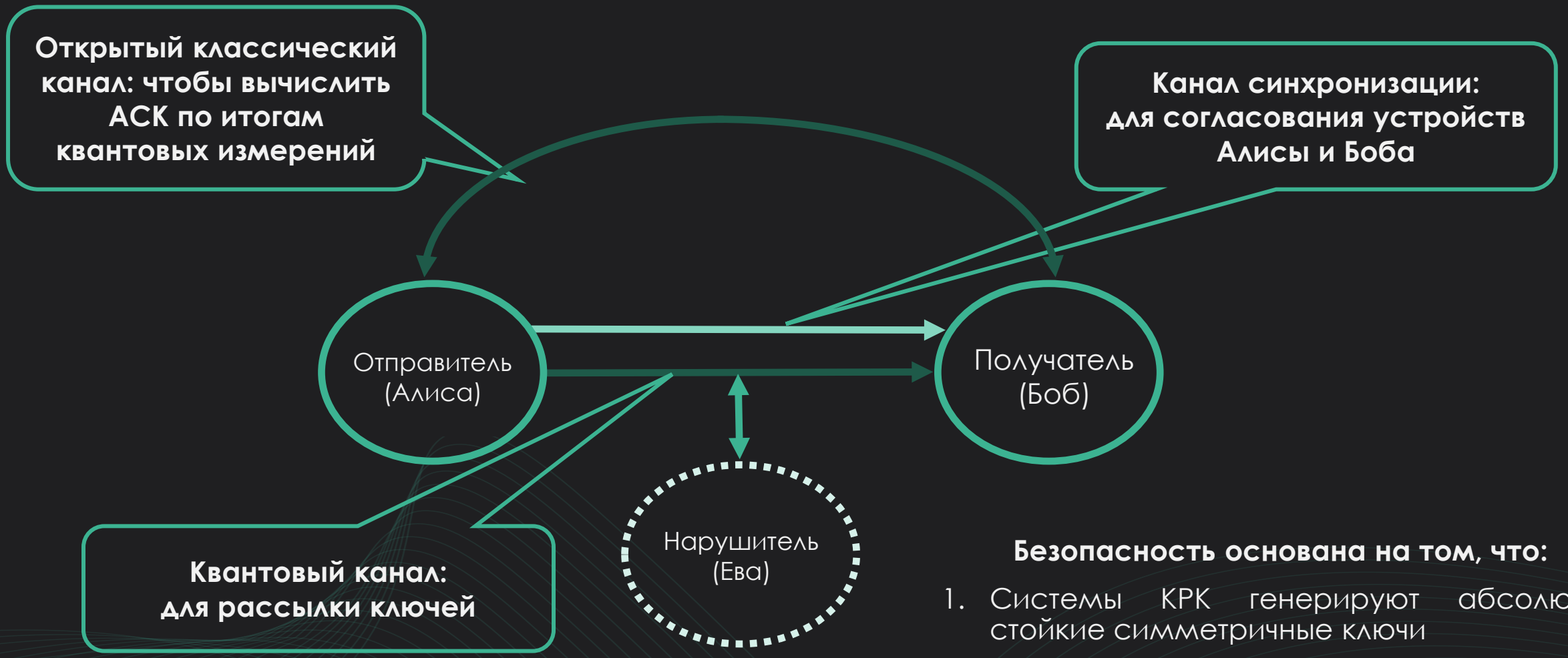
и не успеет перейти на квантовостойкие
ации, и при перехвате информации ее можно
использованием квантового компьютера в тот
удет актуальна

антовостойкие решения нужно до появления

ртным сообществом во всем мире квантовая
льной в перспективе 3-5 лет.

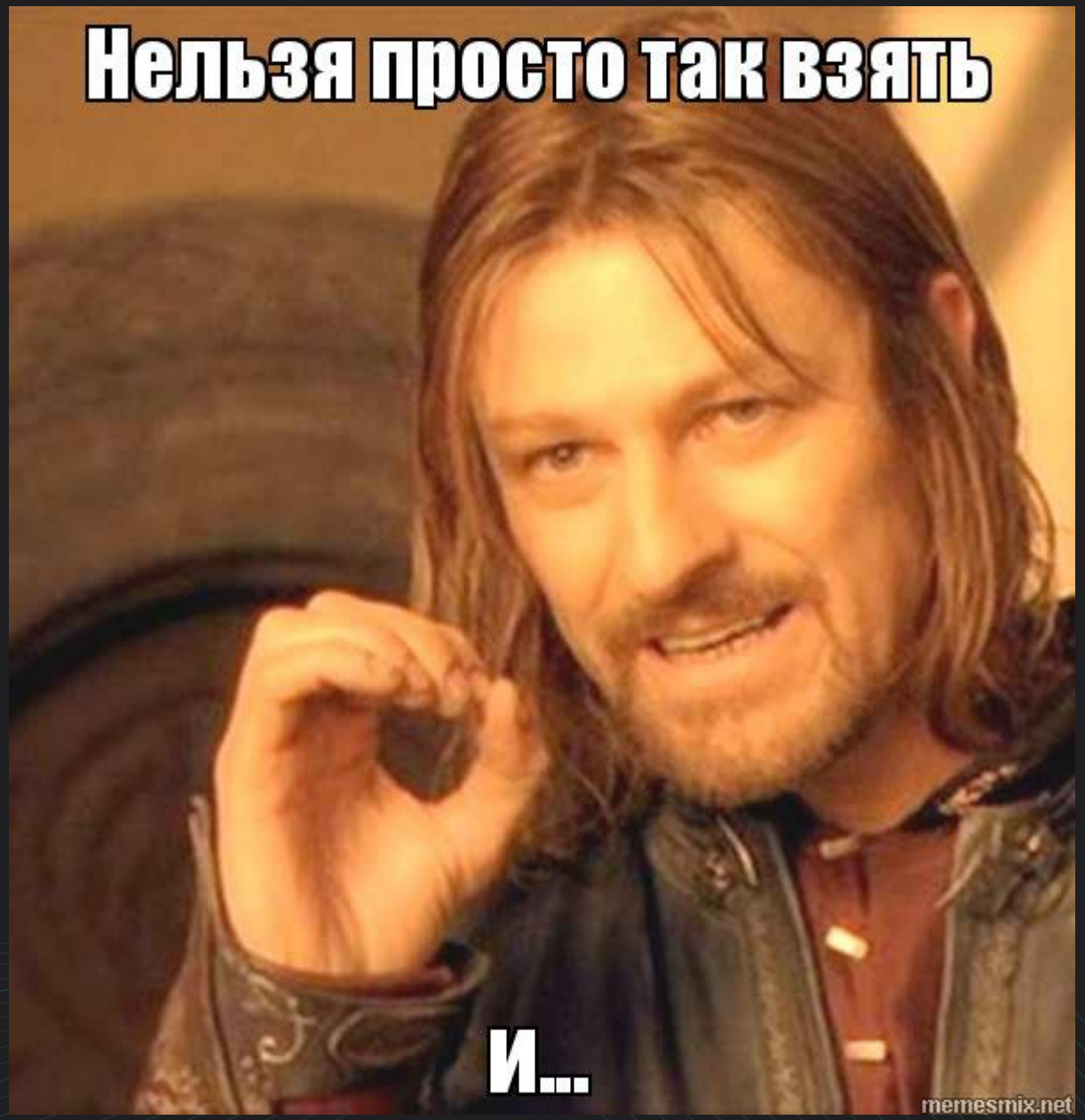
Схема квантового распределения ключей

СМАРТС КВАНТТЕЛЕКОМ



Безопасность основана на том, что:

1. Системы КРК генерируют абсолютно стойкие симметричные ключи
2. Ключи распределяются по каналу связи с помощью одиночных фотонов – квантов света



…разделить одиночный фотон

(используем квантовую природу)

…скопировать одиночный фотон

(используем неопределённость)

…повторно измерить одиночный фотон

(используем не-реализм)

Незаметно перехватить квантовый ключ невозможно!

Итог: новая парадигма безопасности

СМАРТС КВАНТТЕЛЕКОМ

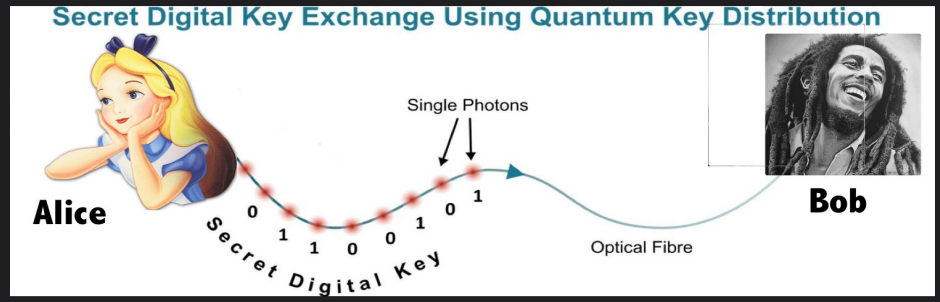
Современный подход:
Безопасность = математика

Легко

Сложно

Проблема

Решение



Подход будущего:
безопасность = физика

Квантовое распределение ключей (КРК)

но НЕ невозможно для:

- Квантовых компьютеров
- Новых алгоритмов?
- Облачных вычислений?
- Чего-то ещё?

Варианты применения КРК на «Умной дороге»

СМАРТС КВАНТТЕЛЕКОМ

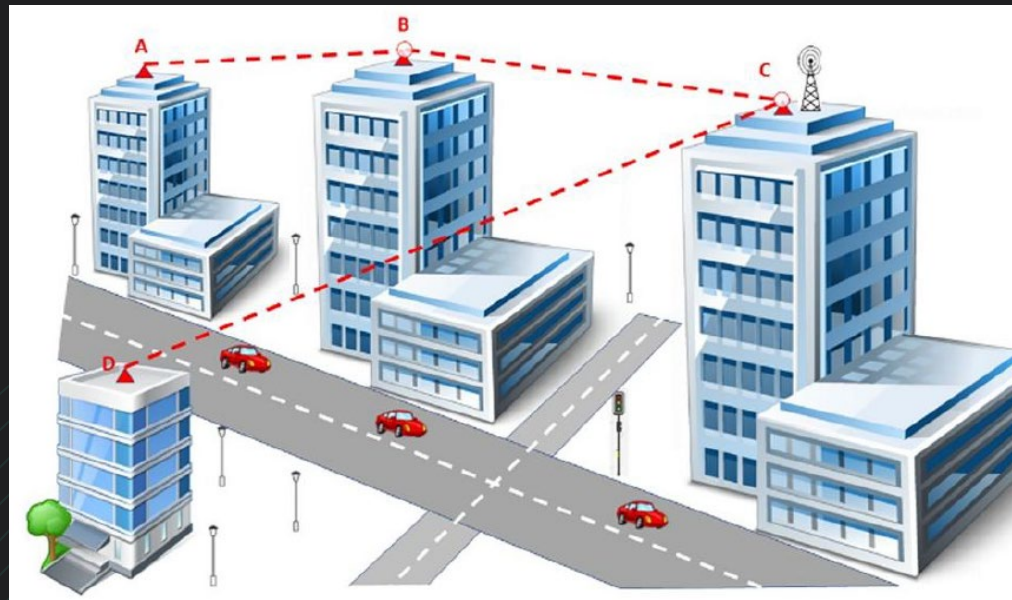
По оптическому волокну (можно сделать уже сейчас):

- Защита данных между соседними узлами связи одной автодороги
- Защищённая связь между изолированными умным дорогами (вдоль железных дорог, на инфраструктуре ОАО «РЖД»)
- Защищённая связь дорог с центрами управления и мониторинга

Атмосферная связь (требуется проведение ОКР):

- Загрузка ключей на авто во время остановки (сейчас идёт ОКР по обеспечению применения КРК на беспилотном поезде)
- Связь авто с умной дорогой во время движения
- Связь между авто во время движения

Спутниковая связь (дальняя перспектива, но есть задел)



Основные продукты компании

Решение для построения квантовых сетей произвольной топологии

СМАРТС КВАНТТЕЛЕКОМ

Коммерческие решения

- Для **магистральных квантовых сетей**

- *Для защиты* ***выделенных каналов связи***

Текущие разработки

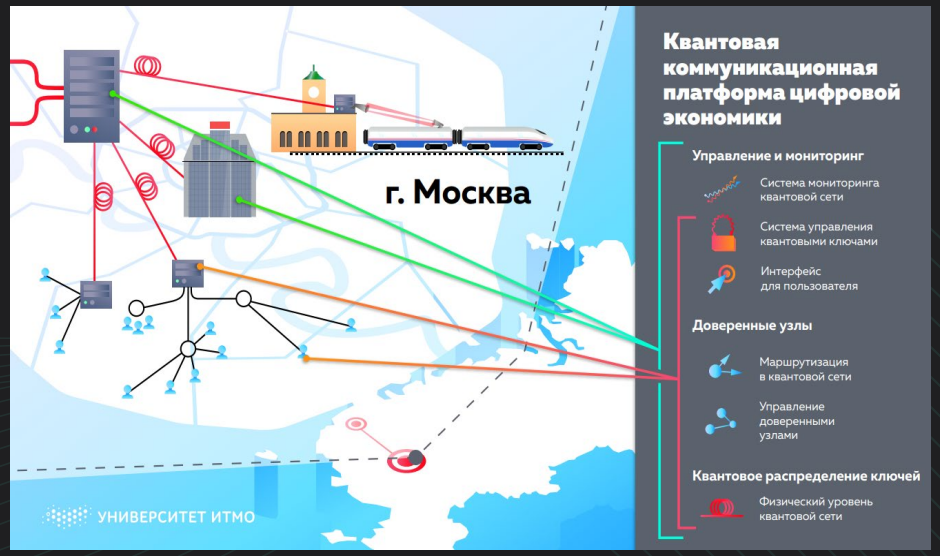
- **Многопользовательская система КРК** (топология «звезда») с **удешевленной стоимостью** клиентского модуля КРК (ОКР в рамках ДК «Квантовые коммуникации»)
  - Поддержка до **32** клиентов
  - Интегрировано **в один корпус** с СКЗИ
  - Формирование **КЗК** между любой парой клиентов и центральным узлом
- Система КРК **на основе отечественной компонентной базы** (продолжение импортозамещения узлов и модулей)
- Система КРК для **более высоких классов СКЗИ**
- **Высокоскоростной** квантовый генератор случайных чисел (**КГСЧ**)

Первый сегмент магистральной квантовой сети

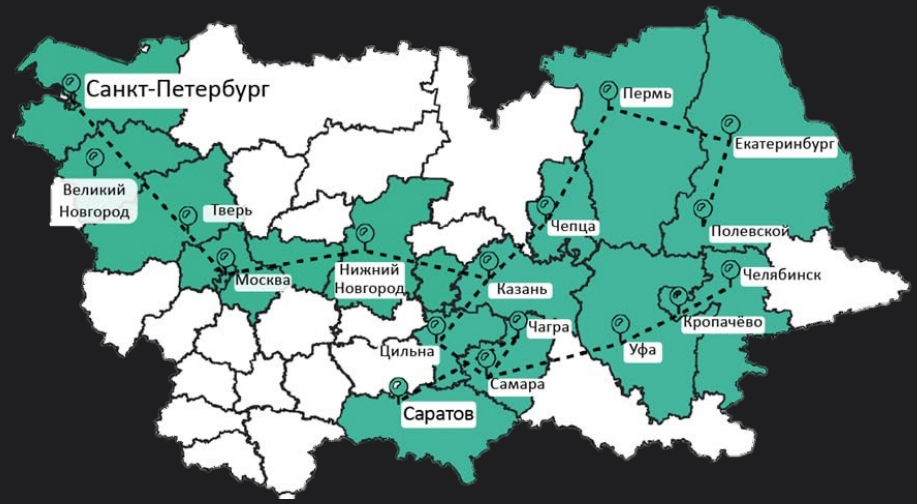
Опыт внедрения на пилотном участке Москва - Санкт-Петербург

ИТМО

СМАРТС КВАНТТЕЛЕКОМ



Российские железные дороги



Развитие магистральных квантовых сетей РЖД (восточное направление)

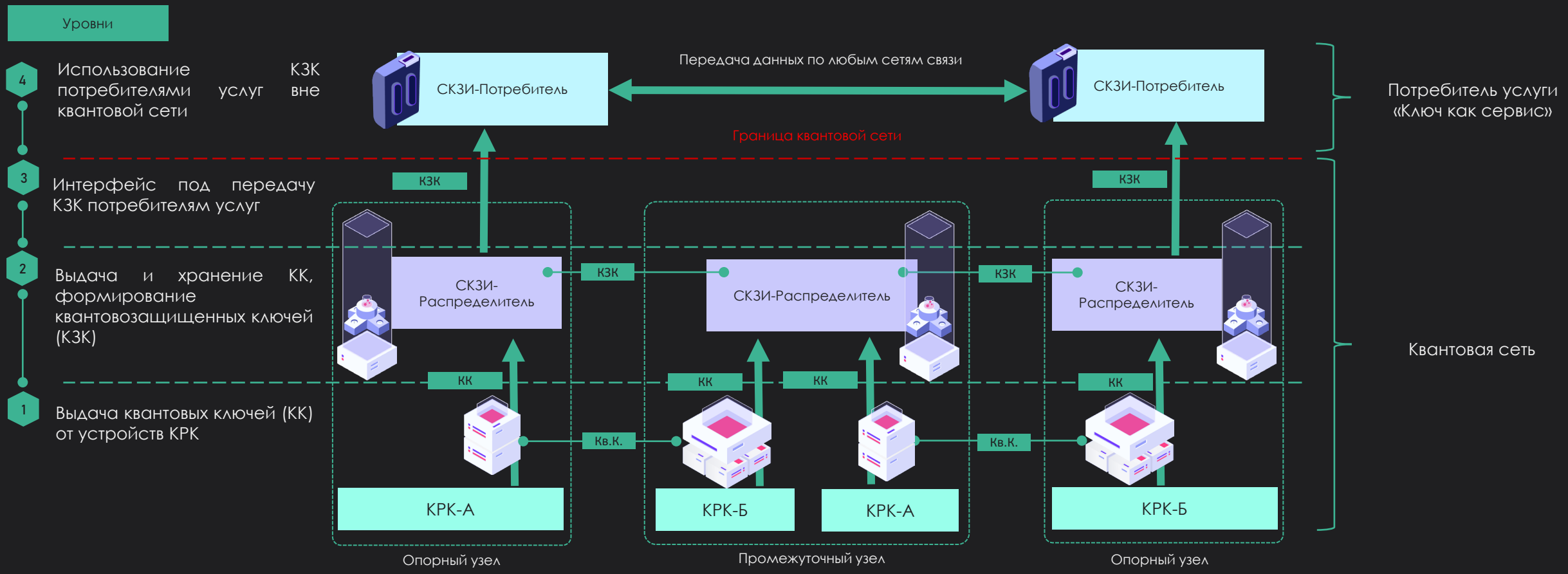
Сервисы:

- ✓ Выработка и рассылка ключей квантовыми методами
- ✓ Защита информации с применением квантовых ключей

Квантовые сети на основе промежуточных узлов

Принципы построения существующих магистральных квантовых сетей

СМАРТС КВАНТТЕЛЕКОМ



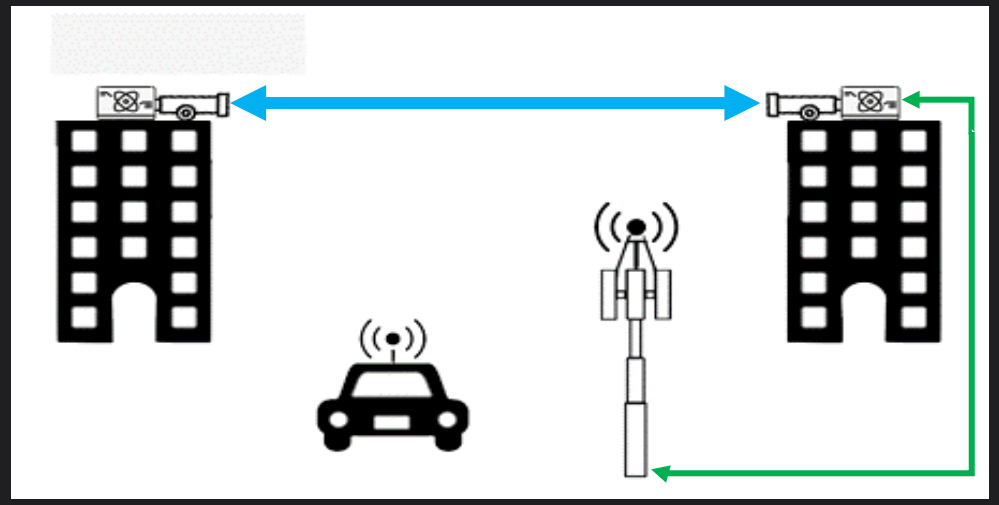
Принцип – квантовозащищенный ключ (КЗК) передается по цепочке промежуточных узлов с защитой на квантовых ключах (КК) смежных сегментов (т.е. в каждом промежуточном узле КЗК расшифровывается и зашифровывается разными КК). Этот функционал выполняется внутренними СКЗИ квантовых сетей (СКЗИ-Распределитель). Впоследствии КЗК поступает в потребительский сегмент (СКЗИ-Потребители), где с использованием КЗК защищается информация. При этом защищаемая информация может передаваться по любым видам сетей (не повторяя маршрут квантовой сети).

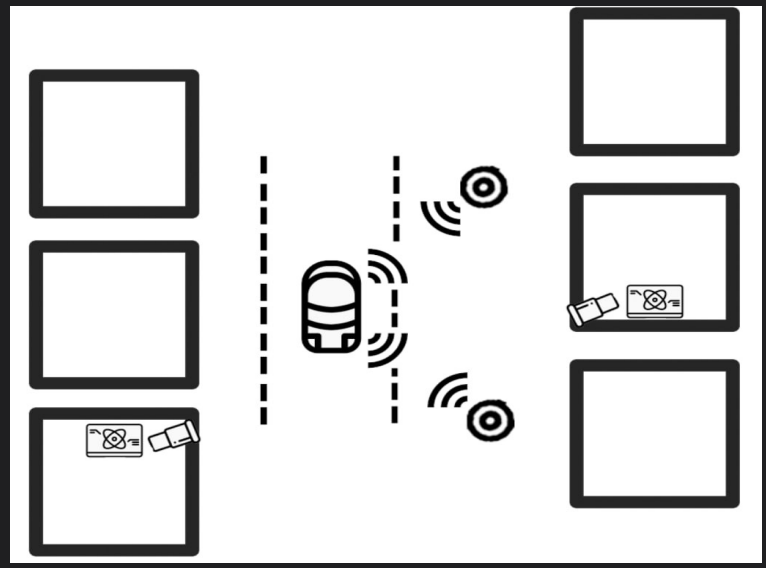
С промежуточными узлами можно реализовывать квантовые сети произвольной топологии и любой протяженности

Кейсы атмосферной квантовой связи: мировой опыт

Умная дорога – Великобритания, 2023

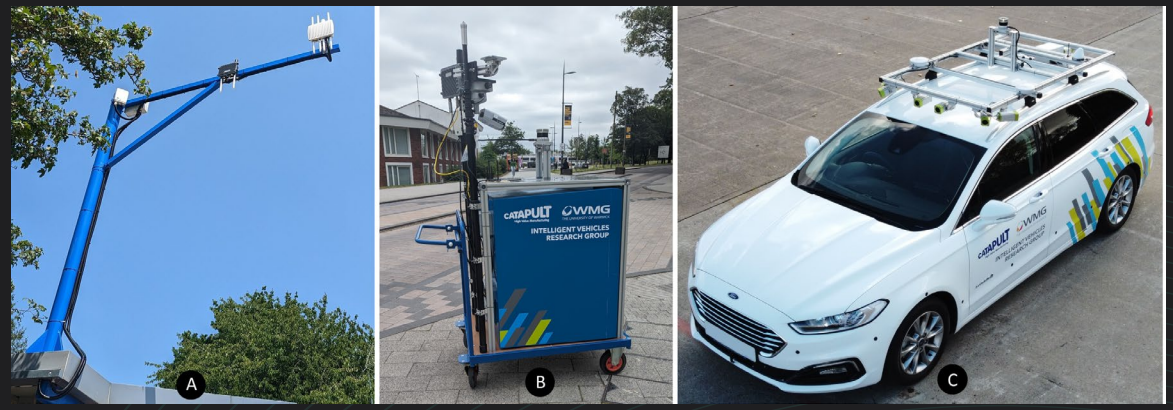
СМАРТС КВАНТТЕЛЕКОМ





- Автомобиль при поездке по городу защищен предраспределенными квантовыми ключами при обмене данными с дорожной инфраструктурой по радиочастотной сети

- Показана возможность масштабировать такие системы и применять для Умного города

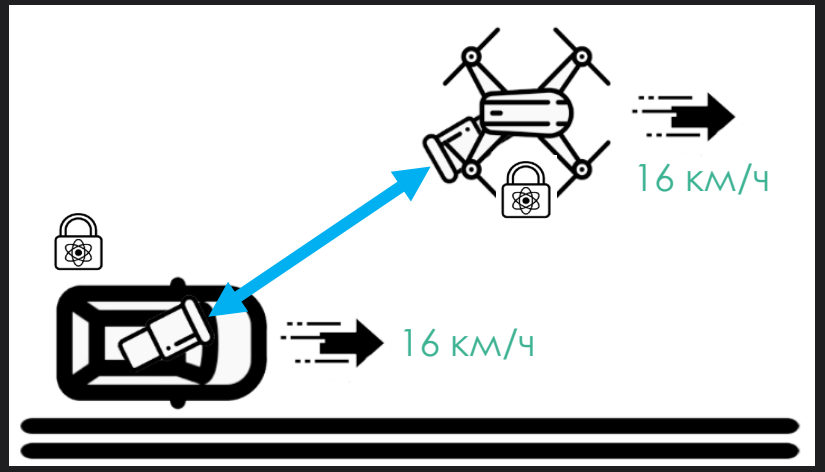


(Implementation of Quantum-Derived Keys for Secure Vehicle-to-Infrastructure Communications. Vehicles 2023, 5, 1586–1604.)

Кейсы атмосферной квантовой связи: мировой опыт

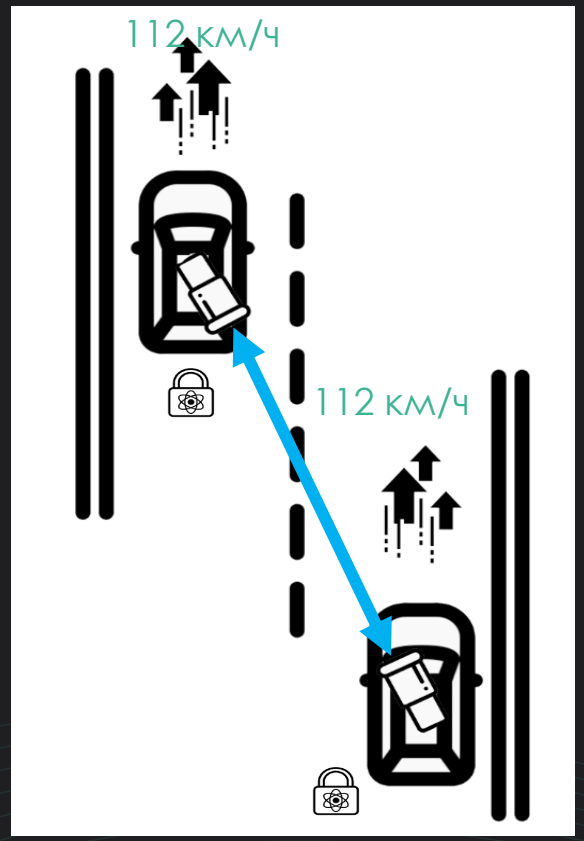
Автомобиль – дрон, автомобиль – автомобиль, США, 2023

СМАРТС КВАНТТЕЛЕКОМ



- Квантовое распределение ключей между дроном и автомобилем
- Расстояние – 10 метров
- Скорость движения – 16 км/ч
- Защищенный трафик данных

- Квантовое распределение ключей между автомобилями
- Расстояние – 10 метров
- Скорость движения – 112 км/ч
- Защищенный трафик данных между автомобилями **в отсутствии** дорожной инфрастуктуры



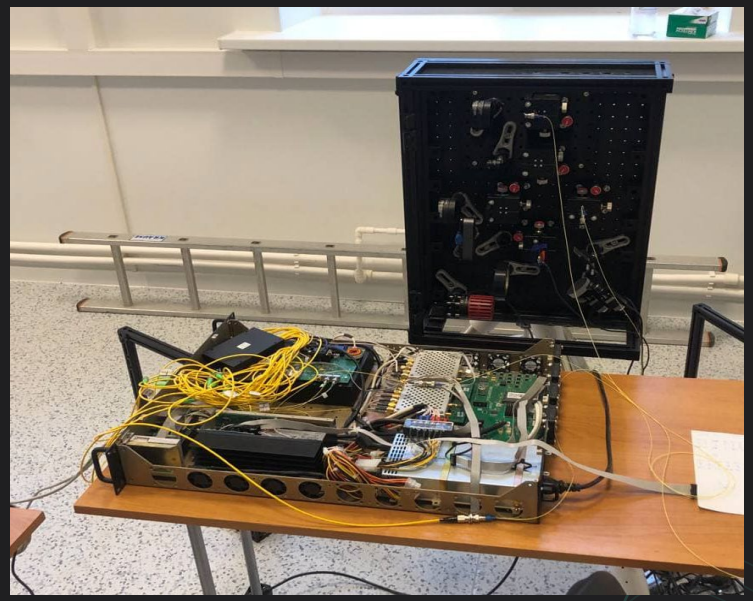
Quantum Key Distribution Links between Mobile Platforms, QCRYPT 2023

Кейсы атмосферной квантовой связи: Россия

Университет ИТМО, 2023

ИТМО

СМАРТС КВАНТТЕЛЕКОМ



Стационарная система с автоматическим наведением и удержанием канала связи

Расстояние

от 25 м до 1 км

Потери в канале

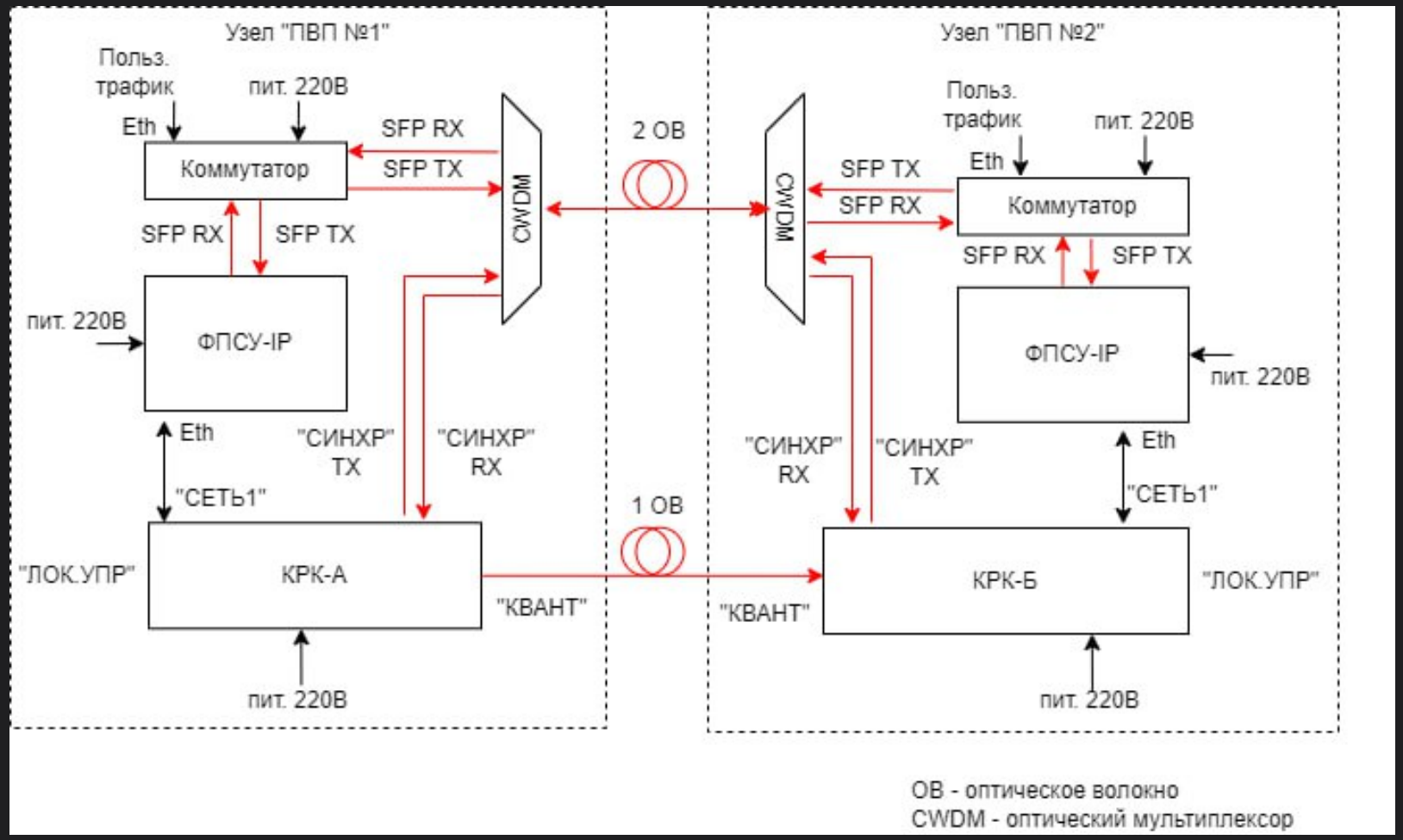
10 дБ

Скорость передачи квантовых ключей

2,1 кбит/с

Схема пилотирования совместно с ГК «Автодор»

СМАРТС КВАНТТЕЛЕКОМ



Квантовая защита канала между двумя пунктами взимания платы (ПВП) в волоконно-оптической сети.

Первый пилотный сегмент квантовых коммуникаций в автодорожной отрасли!

Цели пилотирования:

СМАРТС КВАНТТЕЛЕКОМ

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 пусконаладочных работ на выделенных инфраструктурных объектах ТСС;
4. Проведение испытаний схемы организации сегментов сети КРК на инфраструктуре выделенной подсети существующей ТСС.

Сроки: с 5 мая по 30 июня 2025 года. Место проведения: трасса М11

Задачи, требующие решения:

СМАРТС КВАНТТЕЛЕКОМ

1. Разработка архитектуры безопасности умной дороги на **симметричных ключах** (шифрование, имитозащита, подпись, система свой-чужой, центры сертификации)
2. Разработка решений по атмосферной связи между транспортными средствами, между ними и дорожной инфраструктурой
3. Разработка дешевых и портативных модулей КРК для транспортных средств
4. Разворачивание сетей КРК вдоль автодорог
5. Модернизация центров управления и мониторинга
6. Стандартизация

Спасибо за внимание!