# Квантовая коммуникация

Сыч Денис


Квантовая физика
Теория информации
Квантовая теория информации

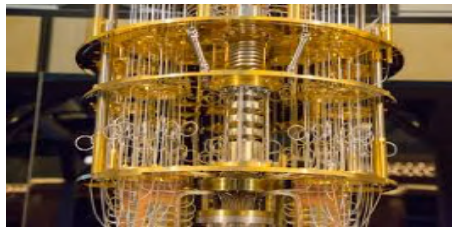
$\alpha|0\rangle + \beta|1\rangle$

# Qubit (кубит)


100 кубитов
=
Суперкомпьютер

# Qubit number contest in 2019

IBM



## Cloud access

IBM creates cloud-accessible quantum computer with **16 qubits**

MAY 2017

China announces world's largest investment centre to support development of quantum technologies: **US$10 billion**

SEPTEMBER 2017

## 50 qubits

IBM creates quantum computer with **50 qubits**

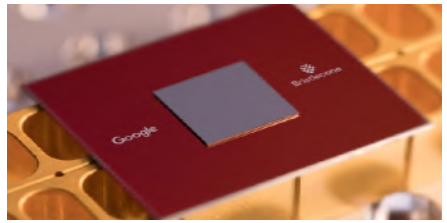
NOVEMBER 2017

## 1st in China

Alibaba launches cloud-accessible quantum computer with **11 qubits**

FEBRUARY 2018

Google



## 72 qubits

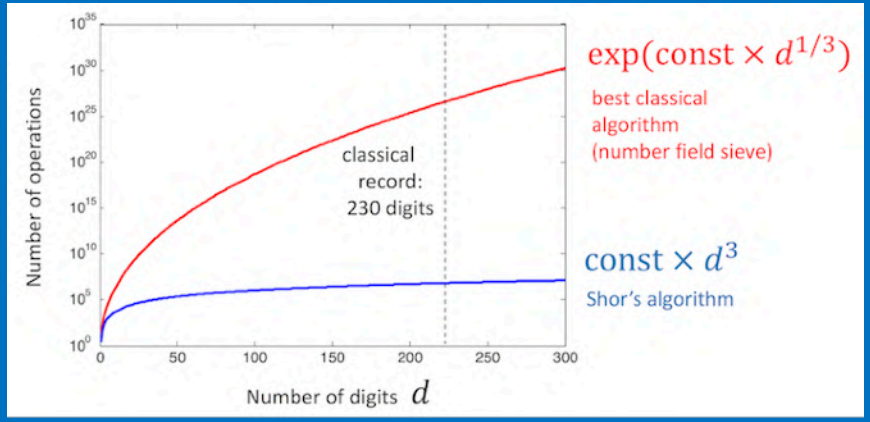
Google release Bristlecone quantum chip with **72 qubits**

MARCH 2018

# THREAT OF QUANTUM COMPUTERS

Ассиметричные алгоритмы

Peter Shor




| RSA | cracked in | CPU years | Shor |
|---|---|---|---|
| 453 bits | 1999 | 10 | 1 hour |
| 768 bits | 2009 | 2000 | 5 hours |
| 1024 bits | | 1000000 | 10 hours |

Симметричные алгоритмы

Lov Kumar Grover

| Algorithm | Key Length | Effective Key Strength / Security Level | |
|---|---|---|---|
| | | Conventional Computing | Quantum Computing |
| RSA-1024 | 1024 bits | 80 bits | 0 bits |
| RSA-2048 | 2048 bits | 112 bits | 0 bits |
| ECC-256 | 256 bits | 128 bits | 0 bits |
| ECC-384 | 384 bits | 256 bits | 0 bits |
| AES-128 | 128 bits | 128 bits | 64 bits |
| AES-256 | 256 bits | 256 bits | 128 bits |

**Applying Grover's algorithm to AES: quantum resource estimates**

Markus Grassl[1], Brandon Langenberg[2], Martin Roetteler[3] and Rainer Steinwandt[2]

[1] Universität Erlangen-Nürnberg & Max Planck Institute for the Science of Light

[2] Florida Atlantic University

[3] Microsoft Research

February 24, 2016

> For public key cryptography, the damage from quantum computers will be **catastrophic**.

— US National Institute of Standards and Technology

# Сохраним сейчас – расшифруем потом

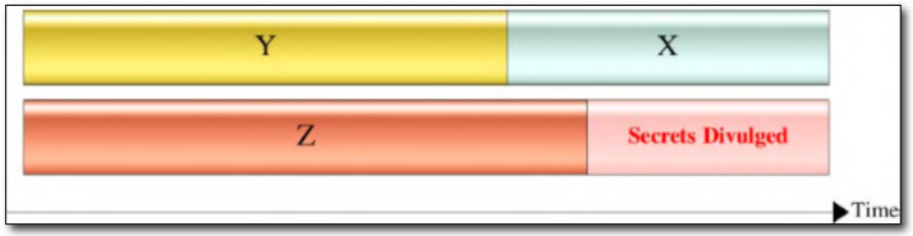
NSA data center Utah – $3x10^{18}$ - $10^{24}$ bytes

x: "how many years we need our encryption to be secure“

y: "how many years it will take us to make our IT infrastructure quantum-safe"

z: "how many years before a large-scale quantum computer will be built"

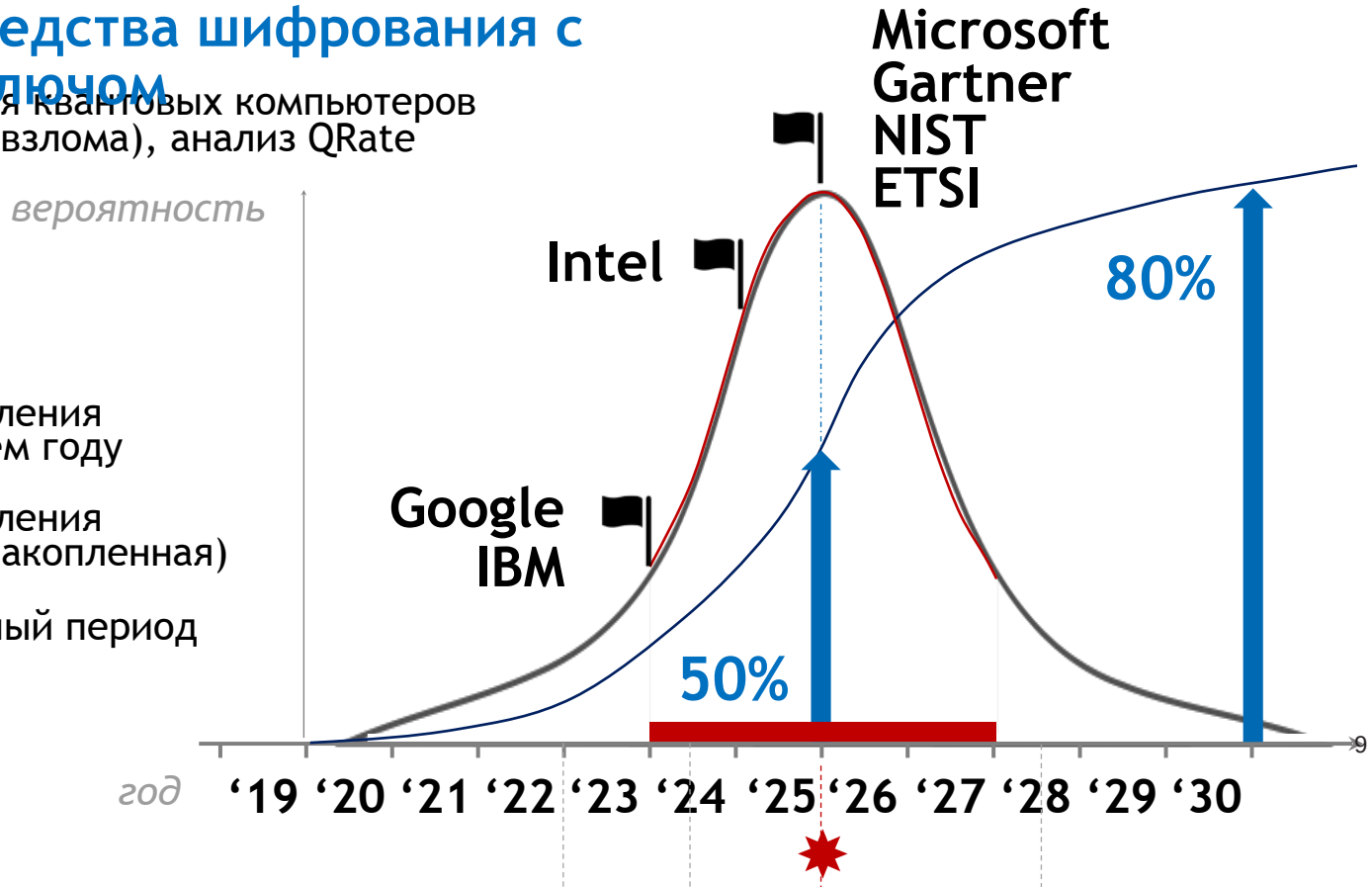
Figure 4 - Lead time required for quantum safety



# РАЗРАБОТКУ ПЕРСПЕКТИВНЫХ РЕШЕНИЙ НЕОБХОДИМО НАЧИНАТЬ СЕЙЧАС, ЧТОБЫ ВЫВЕСТИ ПРОДУКТ НА РЫНОК К ВСПЛЕСКУ ЕГО ВОСТРЕБОВАННОСТИ

## Квантовые компьютеры позволят взломать средства шифрования с открытым ключом

прогноз появления квантовых компьютеров (подходящих для взлома), анализ QRate




- оценка экспертов
- вероятность появления в соответствующем году
- вероятность появления к данному году (накопленная)
- наиболее вероятный период

**5-10 лет**
2023-2027

**вероятное появление квантовых компьютеров, подходящих для взлома существующей защиты**

оценка вероятности:

**50% к 2025**
**80% к 2030**

**необходимые алгоритмы уже есть (алгоритм Шора)**

длительность разработки

продолжительность внедрения КРК

срок чувствительности данных

**угроза взлома информации !!!**

ценная информация может быть записана
в зашифрованном виде и декодирована позднее с помощью новых технологий

# Вызовы современной коммуникации

## Проблемы передачи данных и идентификации

**Рост трафика**

Увеличение нагрузки на ключ

**x 5** вырастет объем данных в мире за 7 лет - с 2018 к 2025 [1]

**x 10** с 2010 скачок скорости передачи данных за 10 лет [2]

**40%** доля данных, требующих защиты, к 2020 [1]

**Рост числа потребителей ключей**

IoT, беспилотники

**Секретность ключей**

Необходимо распределять ключи для симметричного шифрования

**Прогресс квантовых компьютеров**,

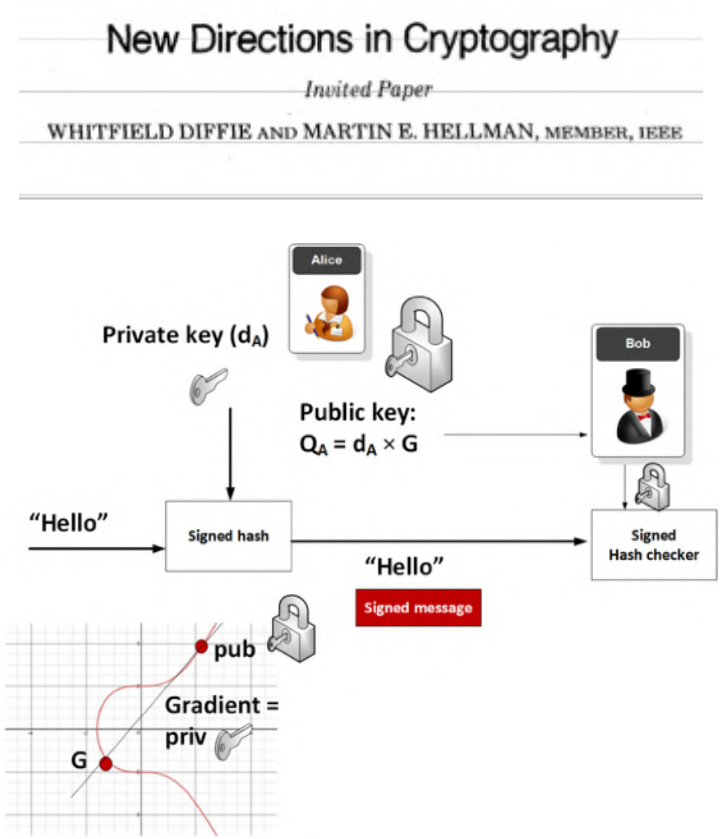
Которые могут взломать алгоритмы с открытым ключом

[1] **IDC**: Data Age 2025: The Evolution of Data to Life-Critical; [2] **infinera**: Super-Channels: DWDM Transmission at 100Gb/s and Beyond;

# Центральная проблема – распределение ключей

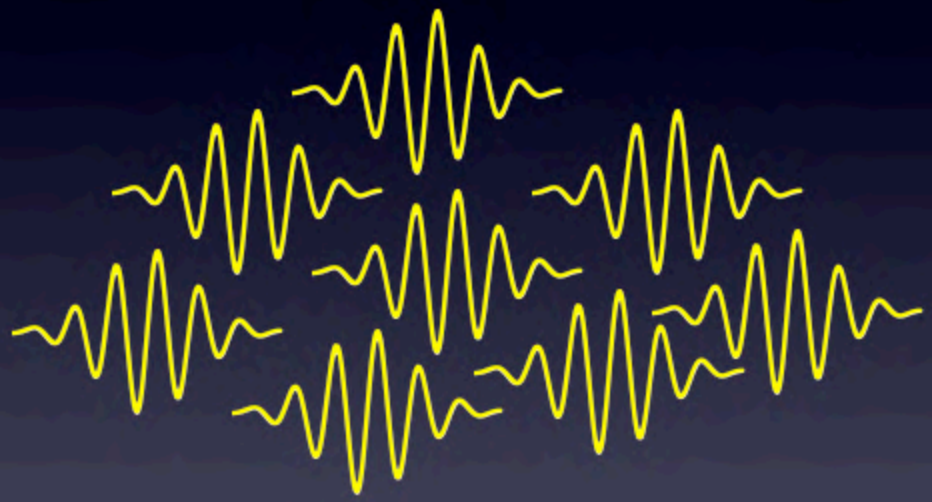
## Доверие человеку

## Доверие алгоритму



# Носитель информации

## классический



$10^6$ фотонов/импульс

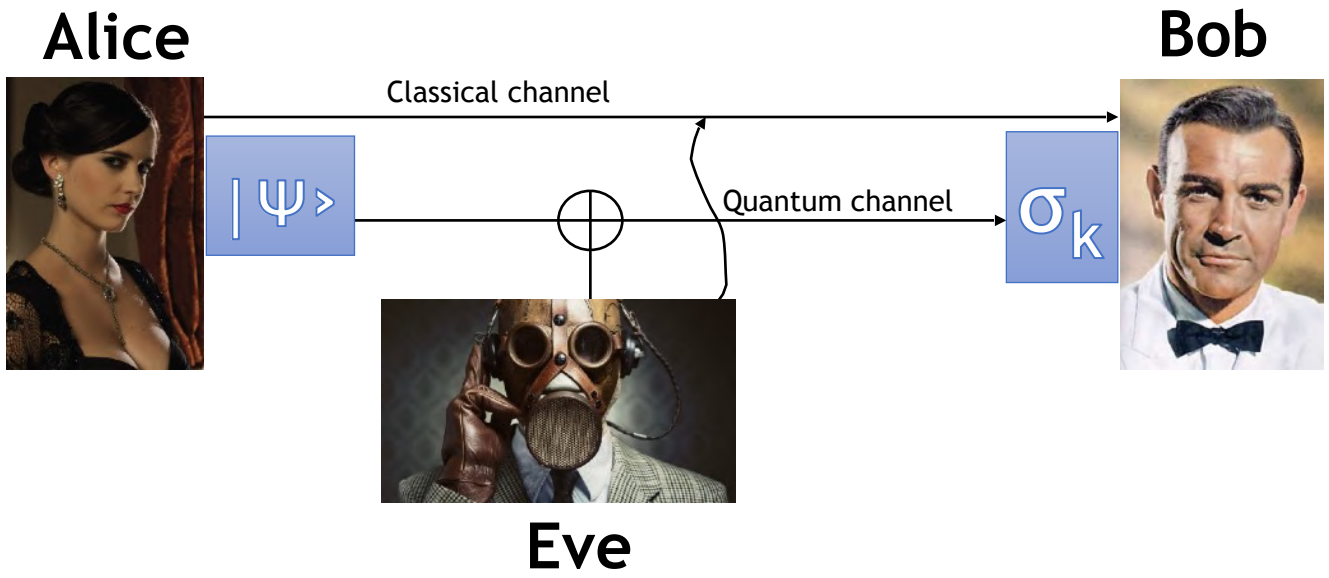
## квантовый

1 фотон/импульс

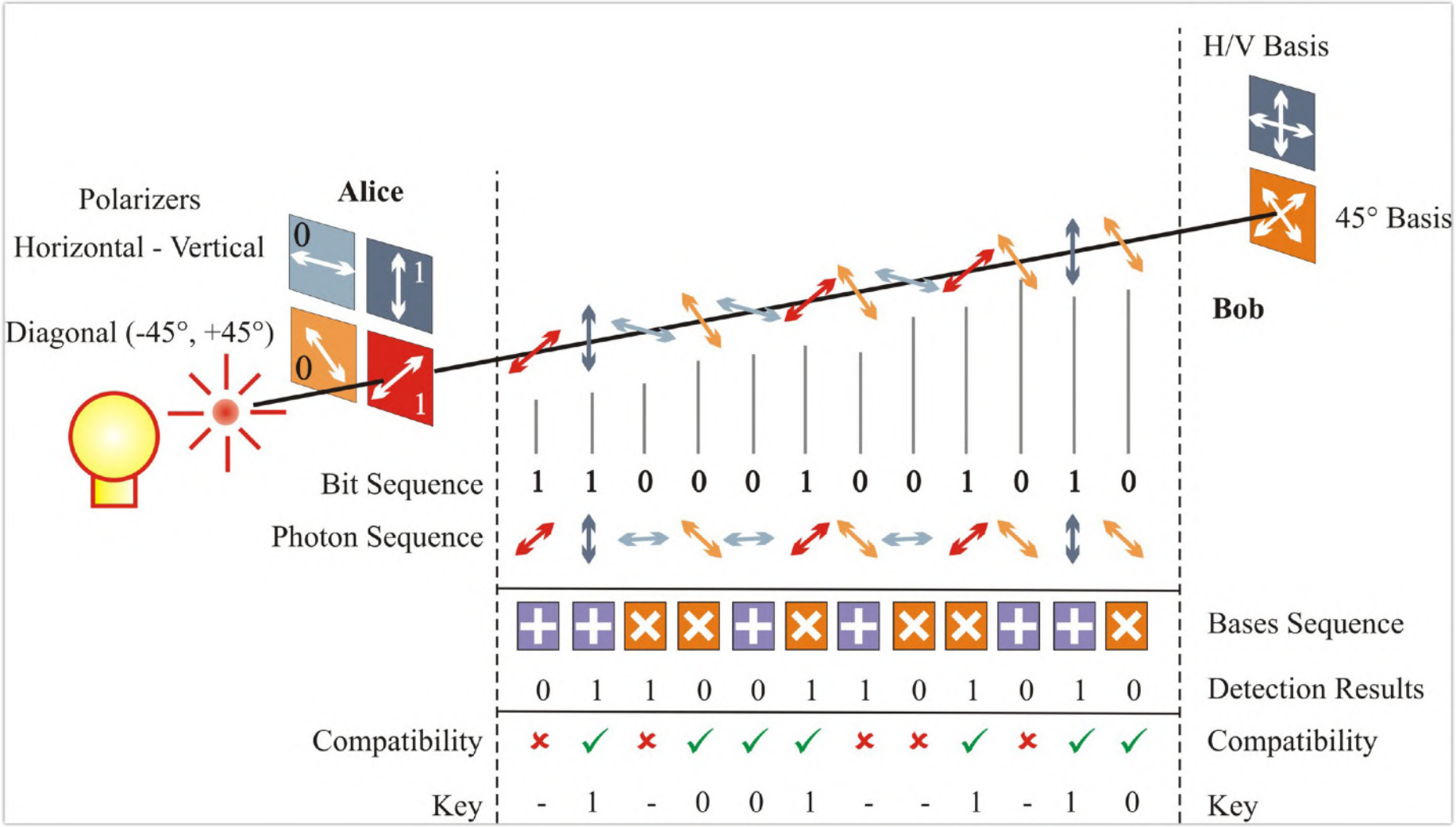
# Квантовая передача данных

**Главные особенности:**

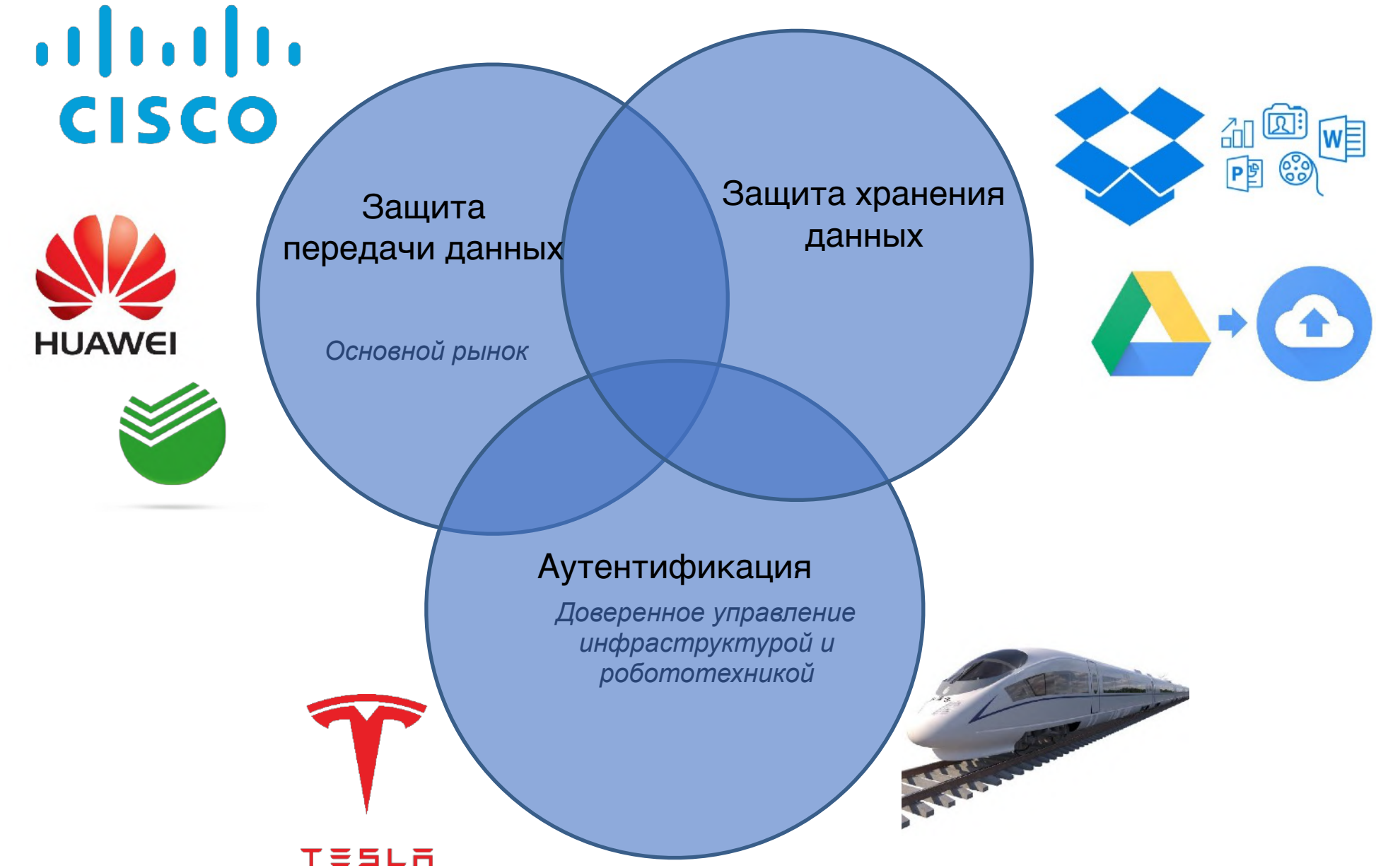
- Фотон невозможно разделить
- Квантовое состояние одиночной частицы невозможно скопировать
- Любое взаимодействие изменяет состояние фотона



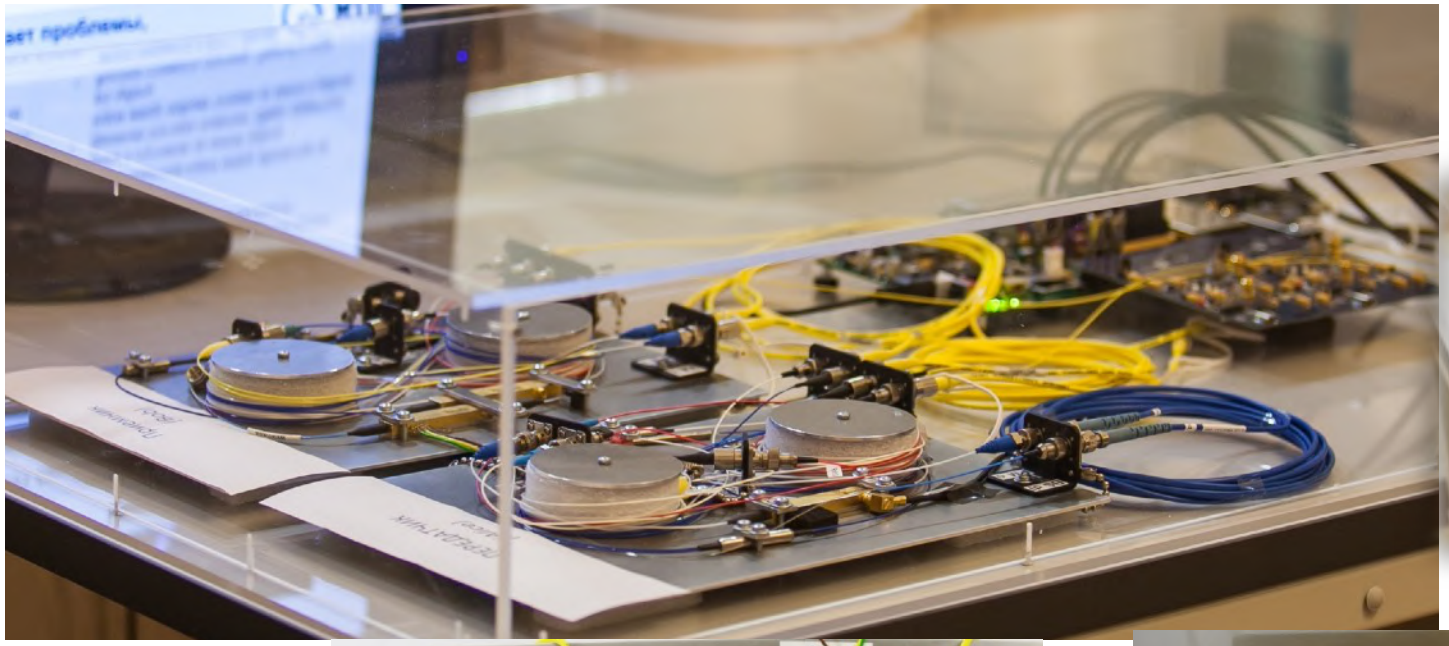
# Протокол BB84

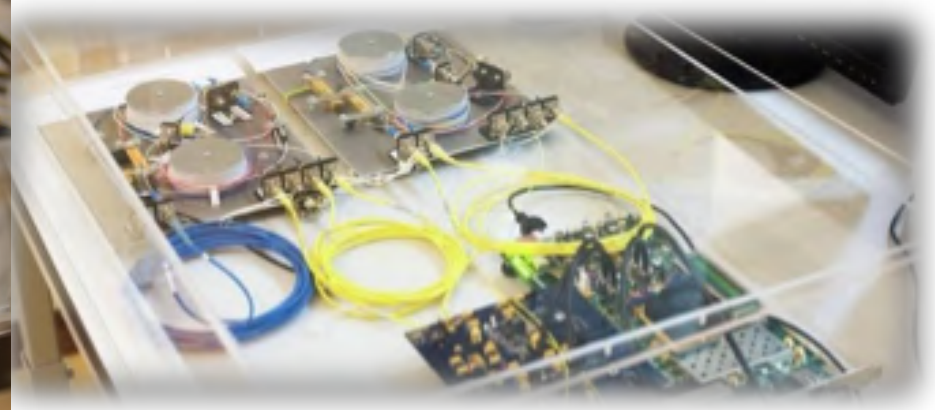


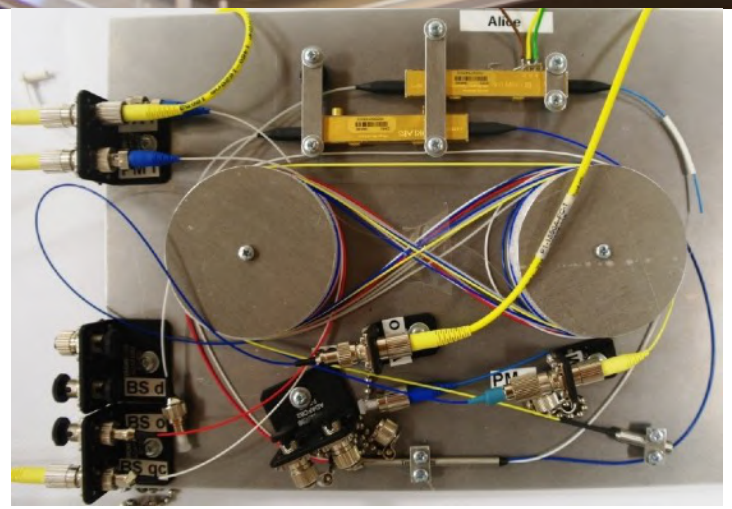
# Направления применения КРК

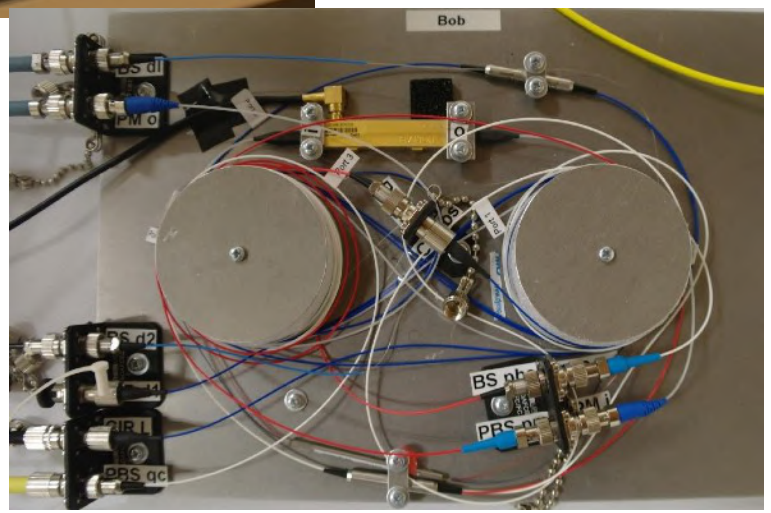


# Как это выглядит в реальности?







# Лидеры коммерциализации – Швейцария и Китай

IDQ
FROM VISION TO TECHNOLOGY

- First product announced in 2001
- Demonstrated successful exit in 2018 with SK telecom

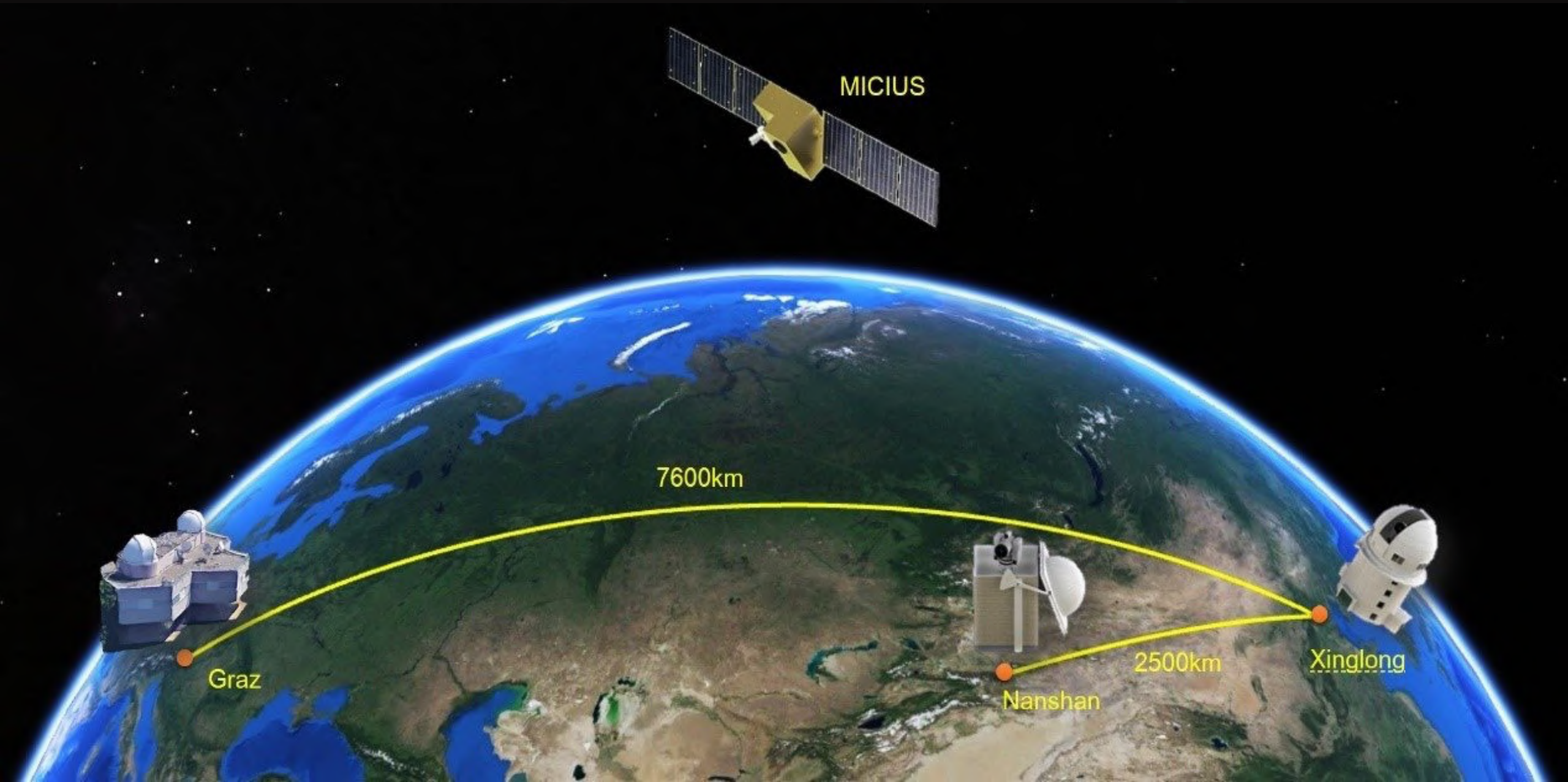
QuantumCTek

- Largest in the World production to supply network in China
- Number of products

# National Quantum Communication Backbone in China

- Inter-city quantum communication backbone with 32 trusted relays (~2000km)
- Inter-connection of four intra-city metropolitan networks
- For financial applications, public affairs, etc.
- Test-bed for quantum foundations (e.g. frequency dissemination)

# Единственная страна, эксплуатирующая спутниковую КРК - Китай




视频会议
数据库
量子信道
经典信道
视频会议
数据库
用户节点
单模复用技术

# Один из 32 узлов сети Пекин-Шанхай

Участники сети

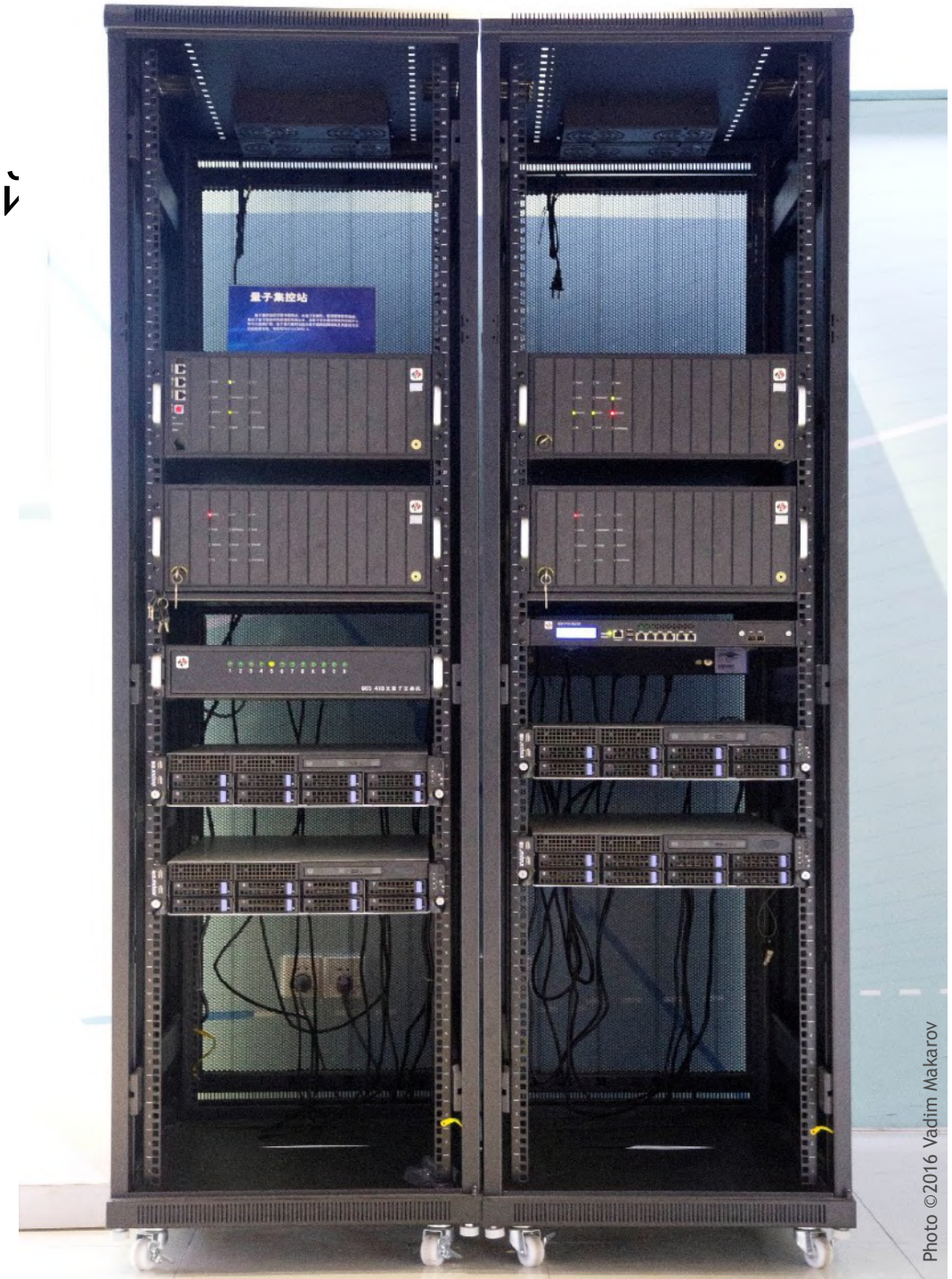




Photo ©2016 Vadim Makarov

# Мультивендорная квантовая сеть в Токио

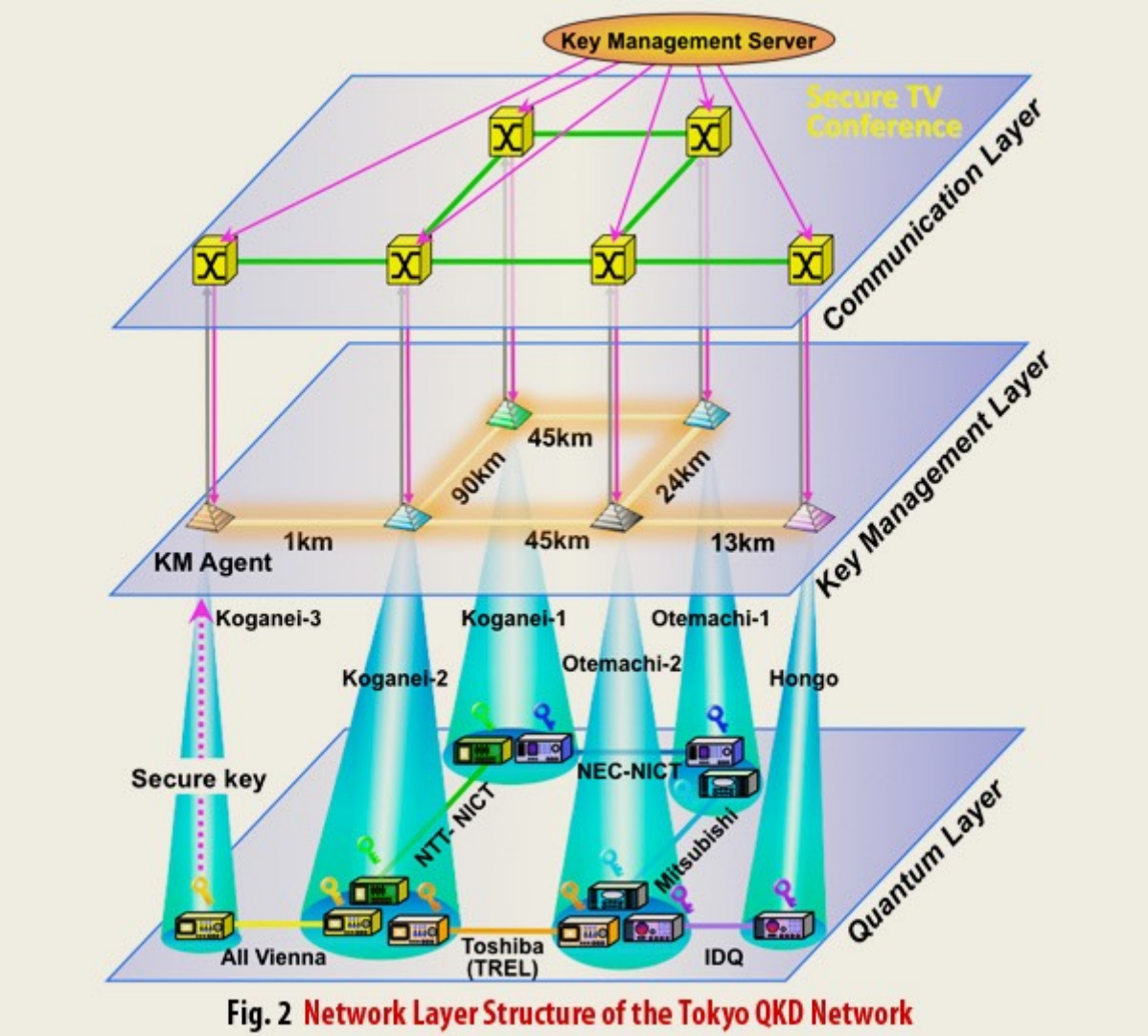


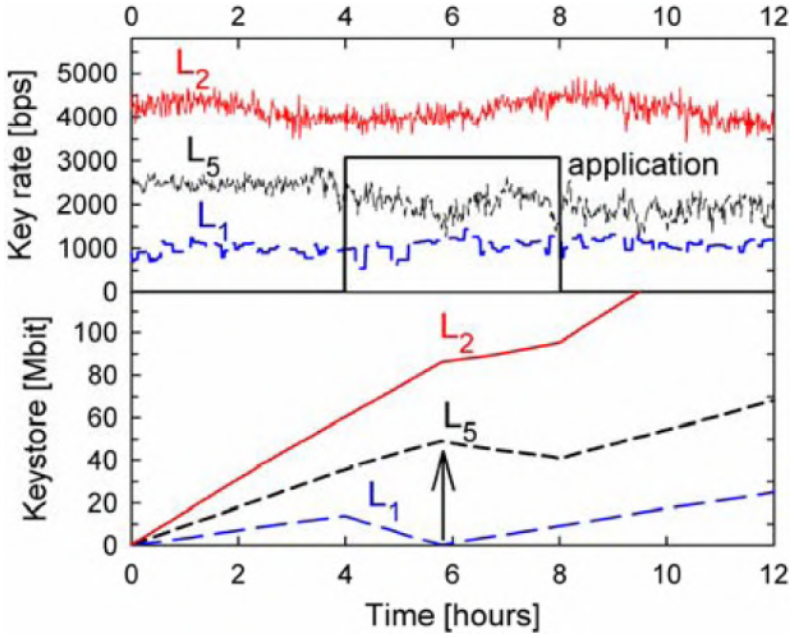
Fig. 2 Network Layer Structure of the Tokyo QKD Network

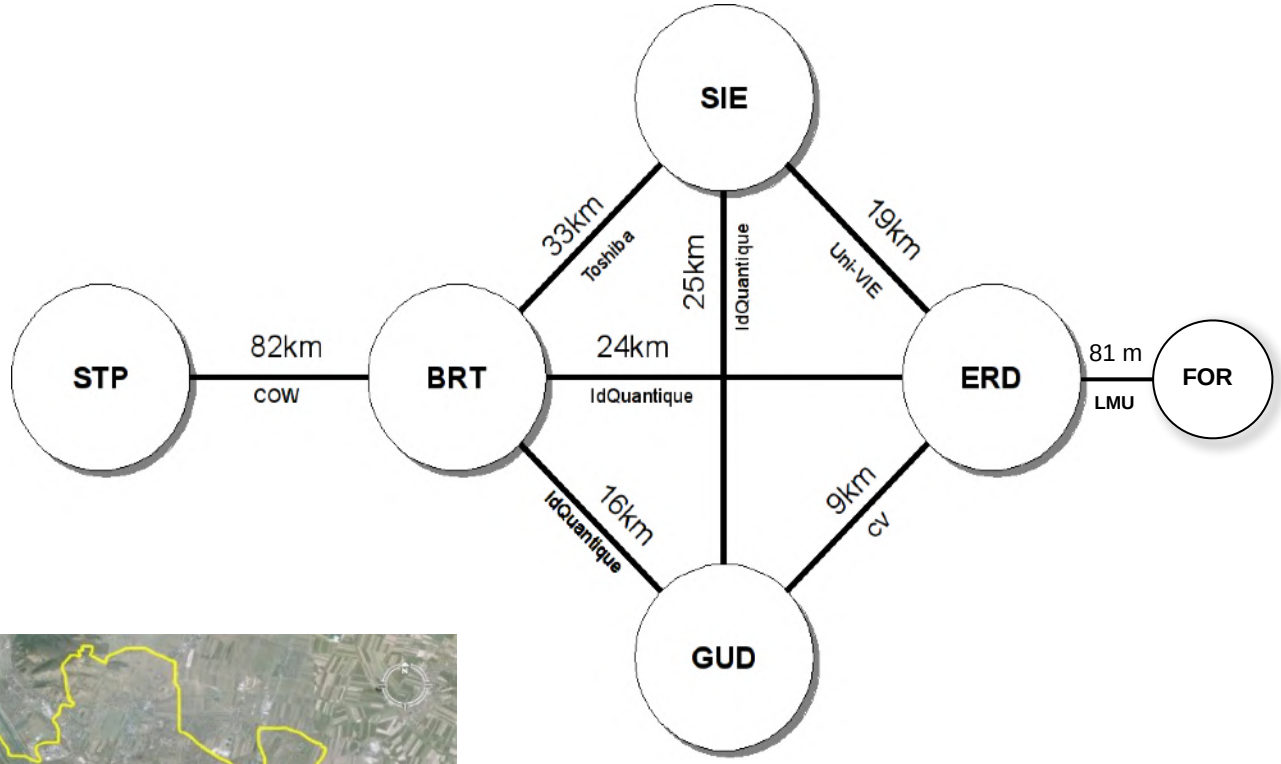
Communication layer

Key management layer

Quantum Layer

# Европейская сеть SECOQC





**По материалам презентации участника проекта:**
**M. Peev, 2008**

# С 2018 квантовые сети уже используются для бизнес-задач

| | | | |
|---|---|---|---|
| коммерческие сети | 2019 | **Южная Корея** | > 150 км, защита 5G и LTE связи<br>телеком – SK Telecom |
| | 2018 | **Китай** | **2000 км , 32 узла + 4 городские сети**<br>12 банков, энергетика, гос. сектор |
| пилотная эксплуатация | 2018 | **Великобритания** | > 120 км, 13 узлов, защита высокоскоростная связь - 500 Гб/с<br>телеком – British Telecom |
| | 2018 | **Испания** | 3 узла<br>телеком – Telefonica |
| | 2018 | **США** | критическая инфраструктура, Smart Grid, департамент энергетики, банки (Wall Street) |
| опытные сети | 2010 | **Япония** | 70 км, 4 узла (1 сегмент до 45 км) |
| | 2009 | **Австрия** | 184 км, 6 узлов (1 сегмент до 82 км) |
| | 2004 | **США** | 30 км, 3 узла (1 сегмент до 20 км) |

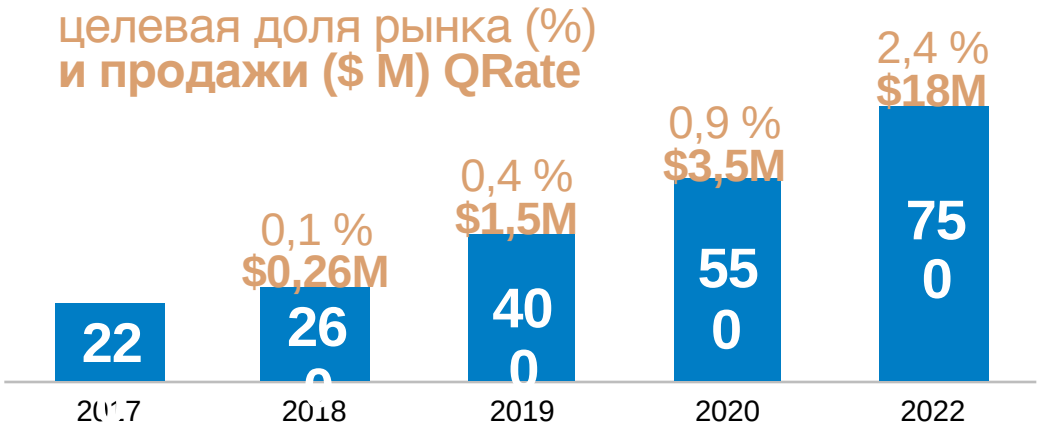
# Зарождение рынка – окно возможностей

## Сейчас на рынке преобладают стартапы

| | |
|---|---|
| IDQ | на рынке |
| QuantumCTek | на рынке |
| ASKY | на рынке |
| KETS | прототип |
| Quintessence Labs | прототип |
| TOSHIBA | нет в продаже<br>*лучшие параметры* |
| HUAWEI | начали показывать работы на конференциях |
| SEQURENET<br>A Quantum Key to Network Security | закрылись<br>*заработали на продаже IP* |

## Взрывной рост инвестиций

> SK Telecom покупает ID Quantique оценка $ 130 млн.

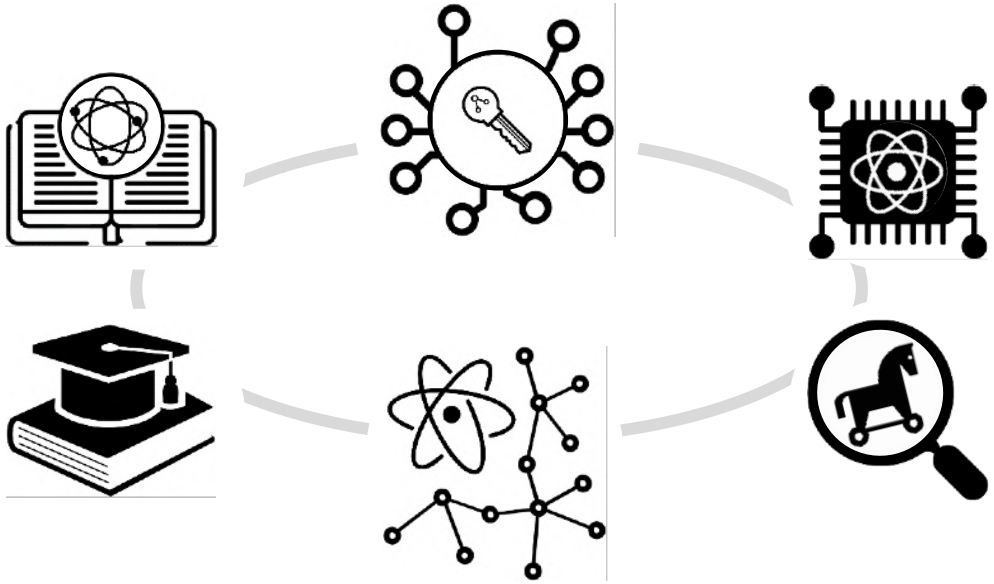




**Рынок оборудования квантовой криптографии, $ M** [1]

[1] **Markets&Markets:** Quantum cryptography market - 2017 to 2022

# Центр квантовых коммуникаций НТИ

Квантовое распределение ключа
и квантовая криптография



Теория
квантовых коммуникаций

Разработка базовых компонент
квантовых коммуникаций

Образовательные программы
в области квантовых
коммуникаций

Поиск уязвимостей
инженерных реализаций
квантовой криптографии

Распределенные
квантовые системы

**Консорциум ведущих исследователей и ключевых промышленных партнеров:**

РКЦ МИСиС s•terra КРИПТОПРО

QRATE SCONTEL ТИН ФОТОНИКА РАНХиГС МИАН ТГ

# Новые поколения решений откроют новые возможности

## Стандартное решение

Легкая интеграция в сетевую инфраструктуру

Магистральные каналы и бизнес-приложения (VPN, ВКС, KaaS[1])

- Телекоммуникации
  - операторы
  - дата центры
- Банки

**Готово и доступно для приобретения**

## Компактное решение

Снижение стоимости квантового канала до 20 раз

Корпоративные каналы, конечные пользователи, приложения (authentication)

- Корпоративные сети
- Критическая инфраструктура
- Финансовый сектор
- Производители и операторы БП[2] транспорта

Разработка (прототип 2021)

## Распределение ключа по открытому пространству

Без оптоволоконной линии, расстояние не ограниченно

Ключи для БПА[2] и IoT, труднодоступные и удаленные объекты

- Производители IoT продуктов
- Гео-разведка (вкл. нефтегазовые кампании)
- ВПК и силовые ведомства
- Производители и операторы БП[2] транспорта

Разработка (прототип 2019)

## Миниатюрное решение (фотонные чипы)

Мобильные устройства и интеркоммуникации

Ключи для IoT и БПА[2], Бизнес- и пользовательские приложения (phone, storage)

- Производители электроники
  - носимые устройства
  - теле-медицина
  - пр.
- Промышленные системы
- Производители и операторы БП[2] транспорта

Исследования

**Поддержка в рамках дорожной карты Цифровой Экономики РФ**

*[1] KaaS – Key as a Service*
*[2] БП – беспилотные аппараты*

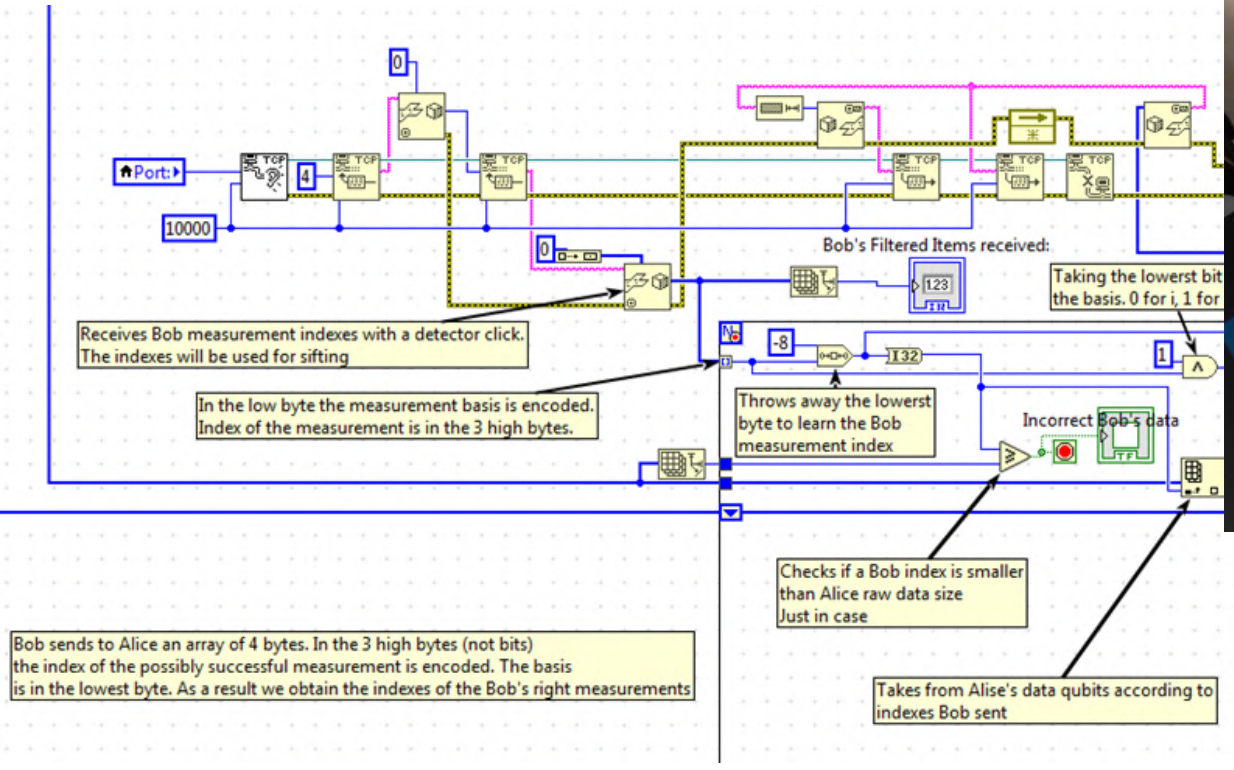
# Обучение квантовым технологиям и коммуникациям

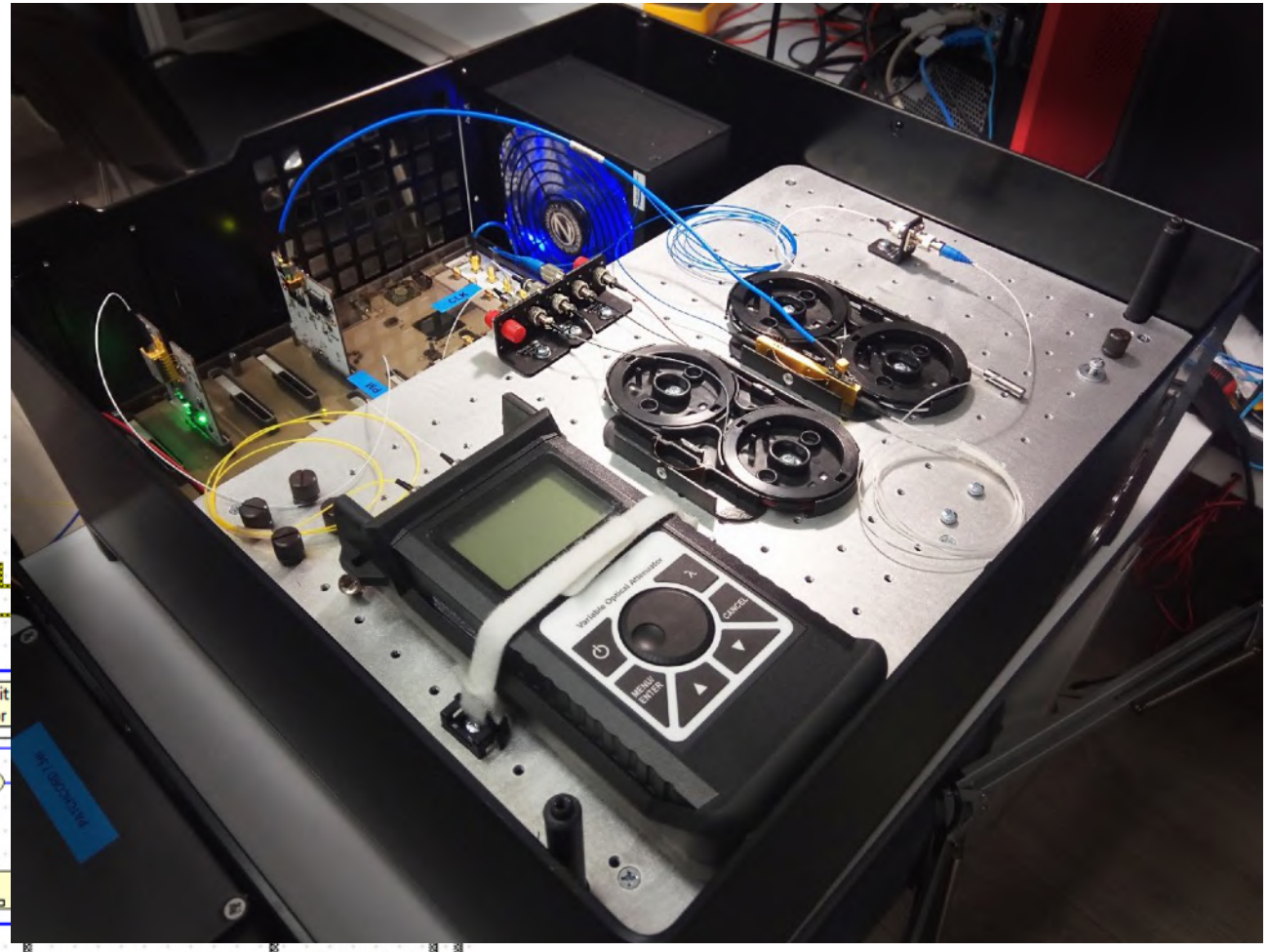
Программа открыта в МФТИ и в МИСиС

- Студенты трудоустраиваются в одну из лабораторий, ведут научную и практическую работу под руководством сотрудников РКЦ
- Под руководством бизнес-ментора со стороны кафедры РВК студенты готовят проекты коммерциализации разработок лабораторий.
- Междисциплинарность: технические знания + прикладные дисциплины из области экономики и управления.

# Учебно-исследовательская установка

- Модульная структура
- Простой доступ к компонентам
- Программируется на LabView
- Идеальная платформа для прототипирования

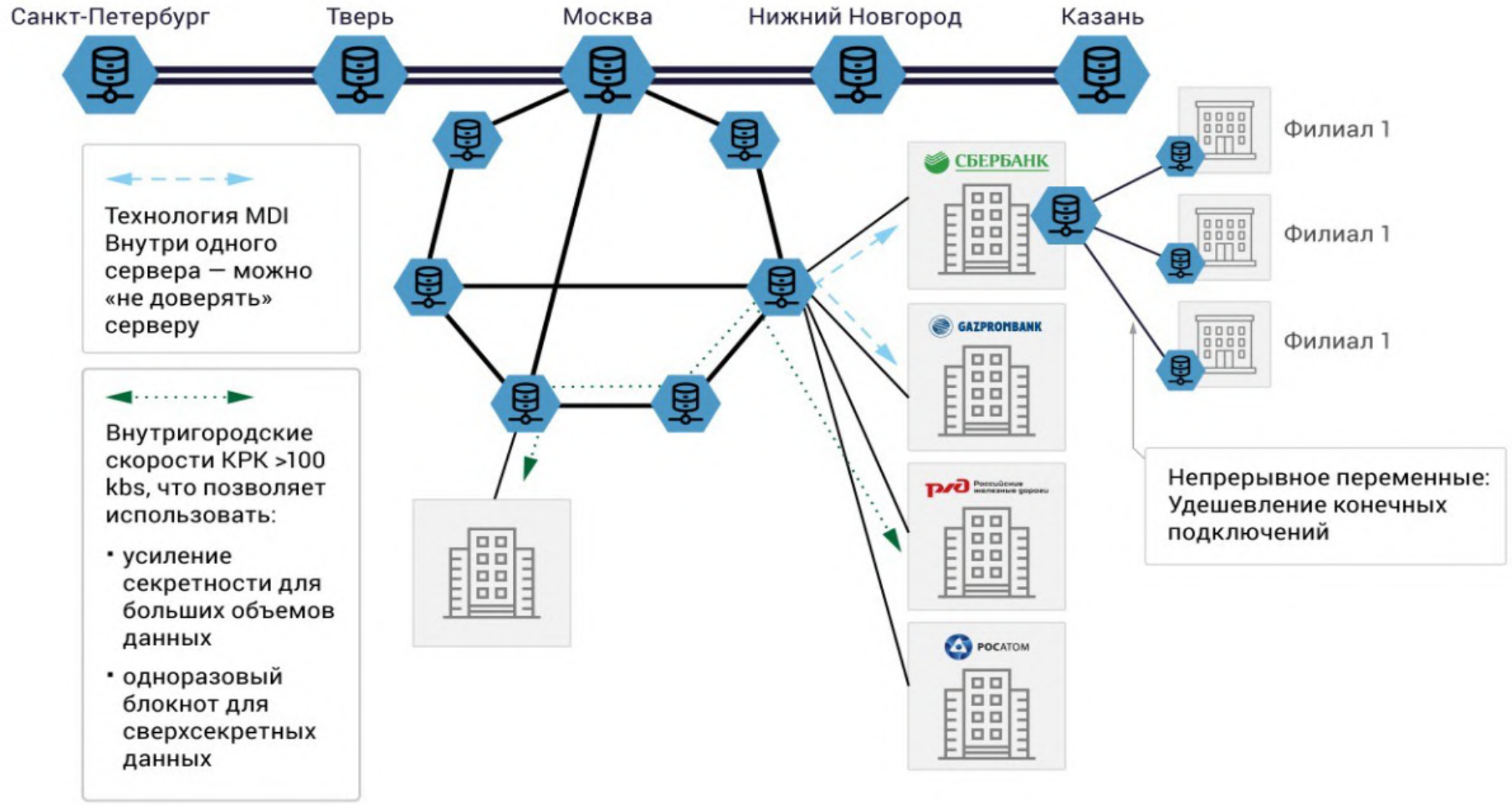


Университет партнер:

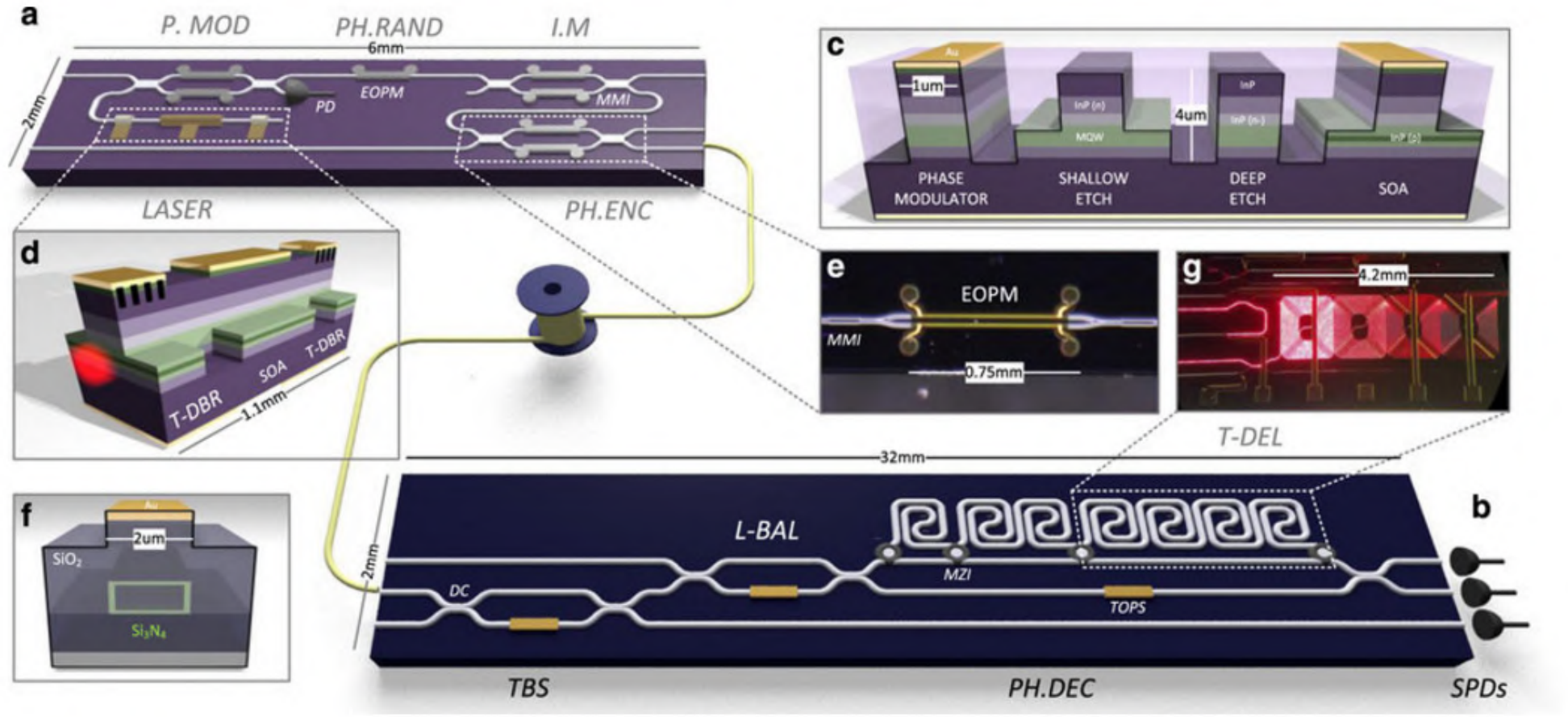
Томский государственный университет

# Российская квантовая сеть в 2024 году – 10 000 км.



# Интегральная оптика – перспективное решение

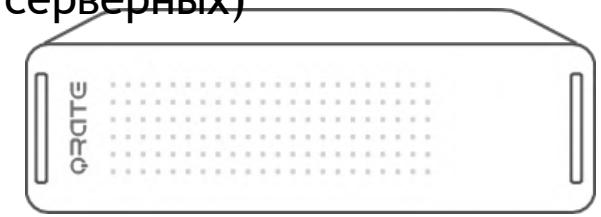
From: Practical challenges in quantum key distribution



# Миниатюризация открывает новые горизонты для решений КРК

## Существующий рынок КРК

**Исполнение для стойки 19”** (применение в дата-центрах и серверных)



**Соединение:** one to one

**Высокая тоимость 1 канала**

**Сегменты:**

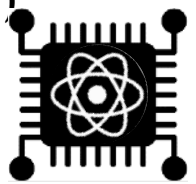
- корпоративные и гос сети (магистральные линии)

**Конкуренты:**

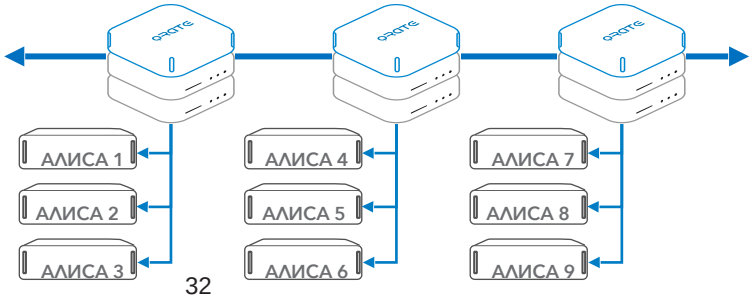
- ID Quantique
- Qubitekk
- QuantumCTek

## Новый перспективный рынок КРК за счет инновационных параметров:

**Миниатюрная клиентская часть** (интеграция в оборудование пользователя)



**Соединение:** one to many (до 1:100) архитектура клиент-сервер




32

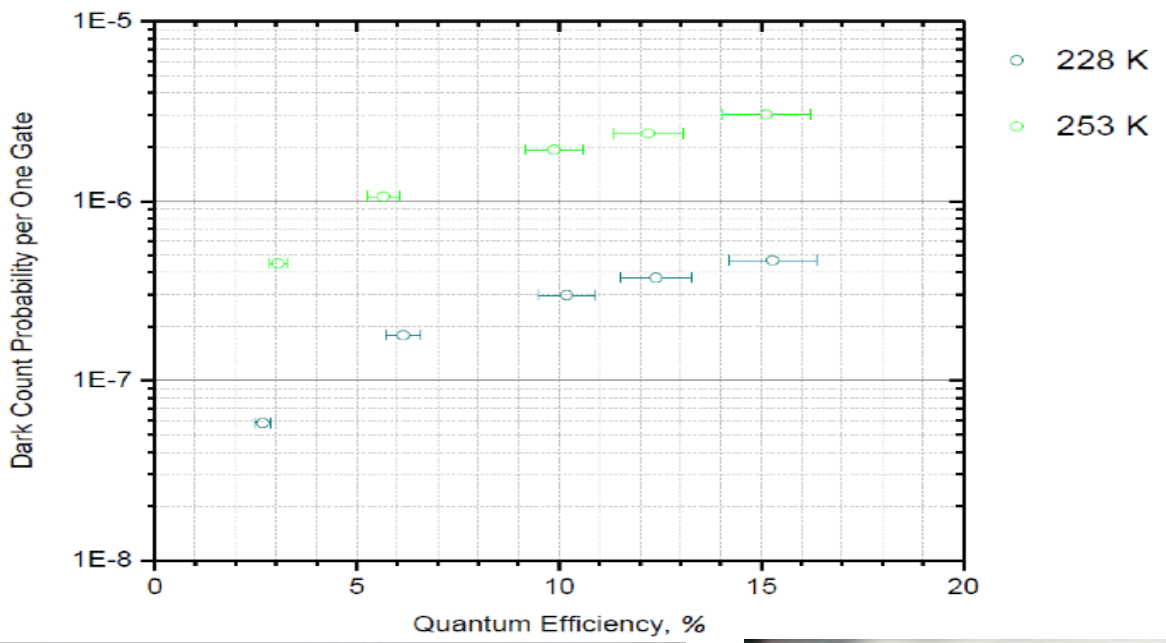
**Снижение стоимость 1 канала в 10 раз**

**Сегменты:**

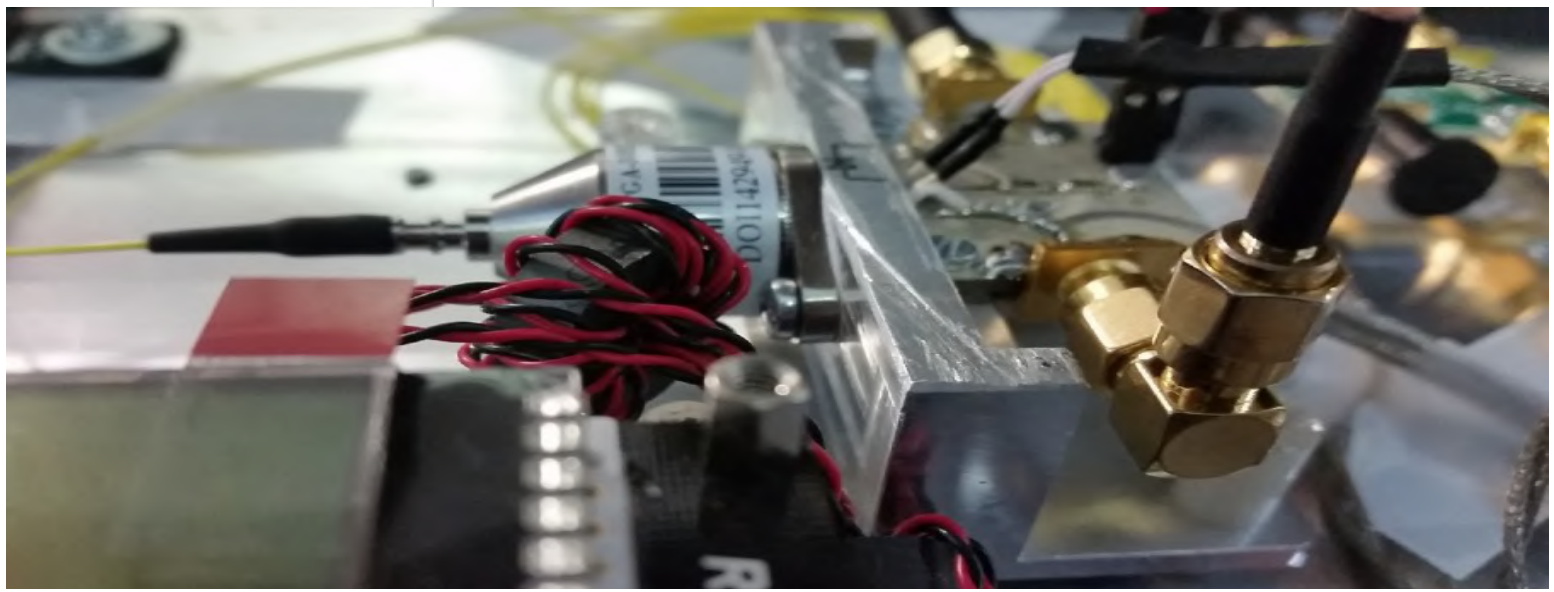
- Корпоративные сети
- Критическая инфраструктура
- Беспилотный транспорт

**Конкуренты:** нет в данном ценовом сегменте

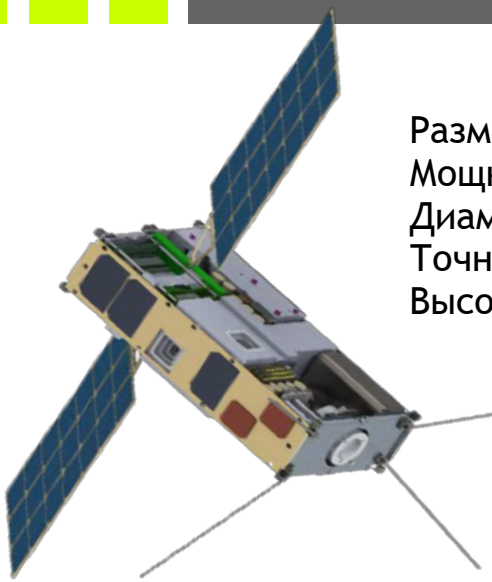
# Детектор одиночных фотонов



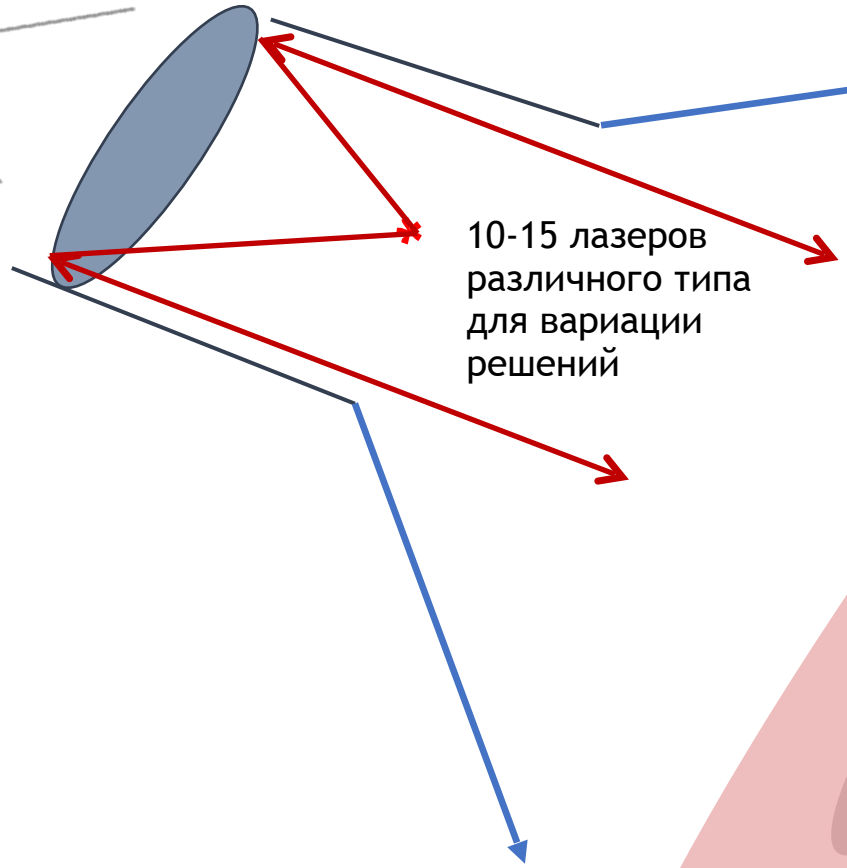

- Квантовая эффективность 10%
- Шумы 3*10^(-7)
- Частота повторения стробов 300 MHz.
- Ширина окна приема сигнала 400 ps



# Спутниковая квантовая коммуникация

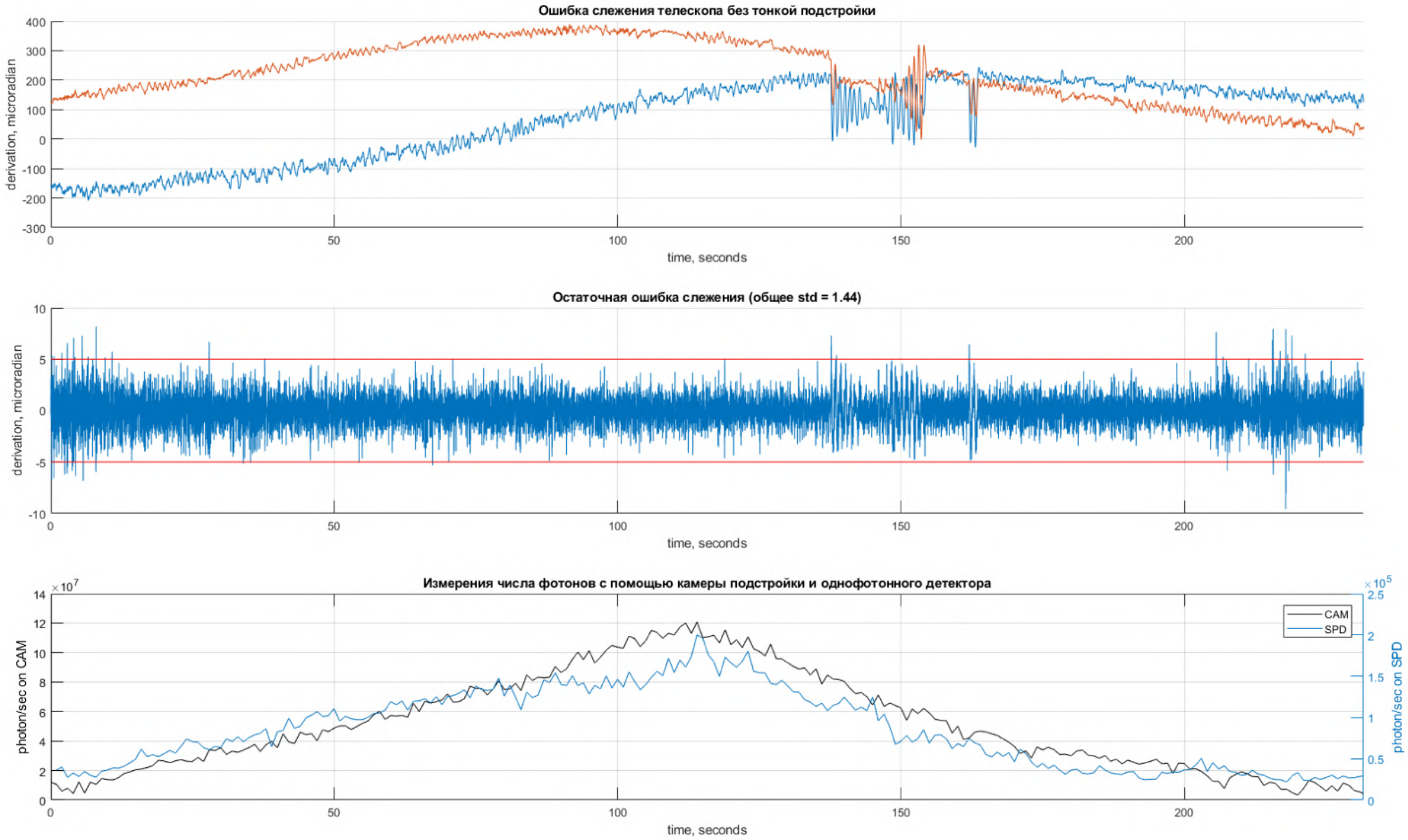


Размер 6U
Мощность 10-15 Вт
Диаметр телескопа на спутнике 80 мм
Точность позиционирования 15 угловых секунд
Высота орбиты 160-600 км




Диаметр луча (информационный канал) на земле более 10 м
Диаметр пучка (синхронный канал) на Земле до 40 м
Точность наведения на наземную станцию до 40 м
Диаметр принимающего телескопа более 0,6 м
1 сеанс в сутки продолжительностью 5 минут

# Подстройка поворотным зеркалом позволяет принять сигнал



# QRate сегодня это:

## Исследования

- ✔ Научная работа мирового уровня: квантовая механика, оптика, математика и др.
- ✔ Публикаций в изданиях с высокими рейтингами

## Разработка

- ✔ Сильные команды разработчиков электроники и ПО (в т.ч. ПЛИС), конструкторов
- ✔ Портфель IP по всем основным направлениям работ

## Производство

- ✔ Своя сборочная площадка и персонал
- ✔ Качественная сборка сложных высокотехнологичных устройств

## Продажи

- ✔ Специалисты с успешным опытом в индустрии
- ✔ Завершенные сделки, работа с партнерами и большой пул потенциальных клиентов в “pipeline”

## Перспективные области применения:

- Телеком
- Банки
- Транспорт
- IoT
- Критическая инфраструктура
- Аэрокосмическая отрасль
- Образование

У нас есть все необходимые ресурсы и компетенции для самостоятельной работы с полным жизненным циклом продуктов