



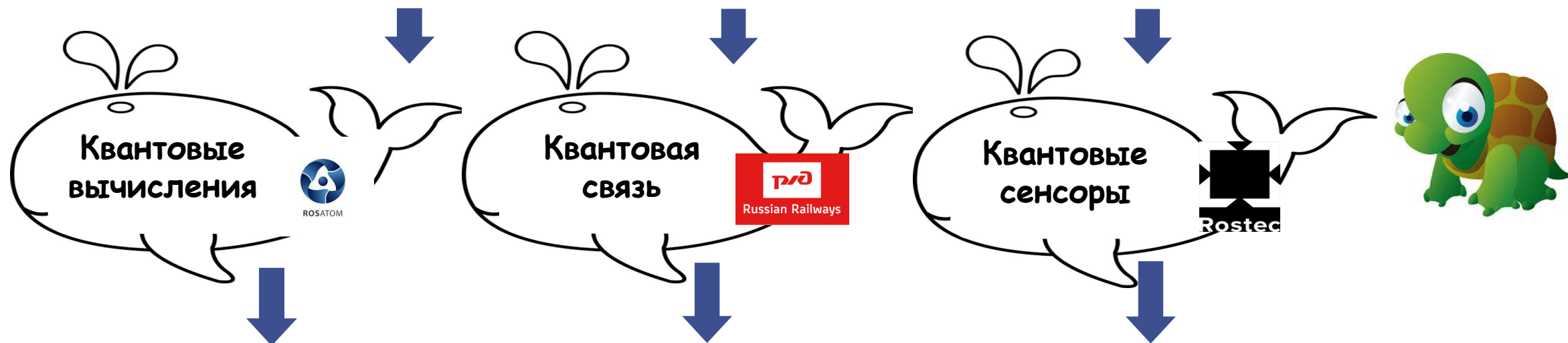
Квантовые коммуникации: проблемы и перспективы

Сергей Кулик

*Центр квантовых технологий, физический факультет МГУ
имени М.В.Ломоносова*



КВАНТОВЫЕ ТЕХНОЛОГИИ: три кита



Ионы и нейтральные атомы
в ловушках

Линейно-оптические
вычисления
(фотонные чипы)

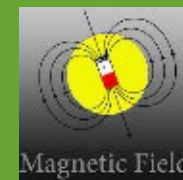
Сверхпроводниковые кубиты

Оптоволоконные каналы

Атмосферные/космические
каналы:
мобильные и стационарные

Квантовая память,
квантовые интерфейсы...

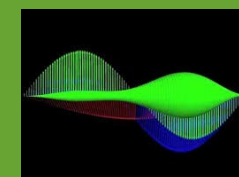
Сенсоры
электрических и
магнитных полей



Часы,
гравиметры,
гироскопы



Квантовая
метрология



ОСНОВНЫЕ ЦЕЛИ И ИНСТРУМЕНТЫ

Цель:

понять, как фундаментальные законы квантовой физики могут способствовать улучшению технологий приема, передачи и обработки информации.

Мотивация:

понять, как фундаментальные законы квантовой физики могут способствовать улучшению технологий приема, передачи и обработки информации

Решение:

использование квантовых технологий

Инструментарий:

квантовые биты и суперпозиции;
квантовый параллелизм,
непрерывные квантовые переменные;
перепутывание как новый ресурс и т.д.

Примеры: кубиты вместо классических битов

$$|\Psi\rangle = c_1|0\rangle + c_2|1\rangle$$

(двухуровневая система)

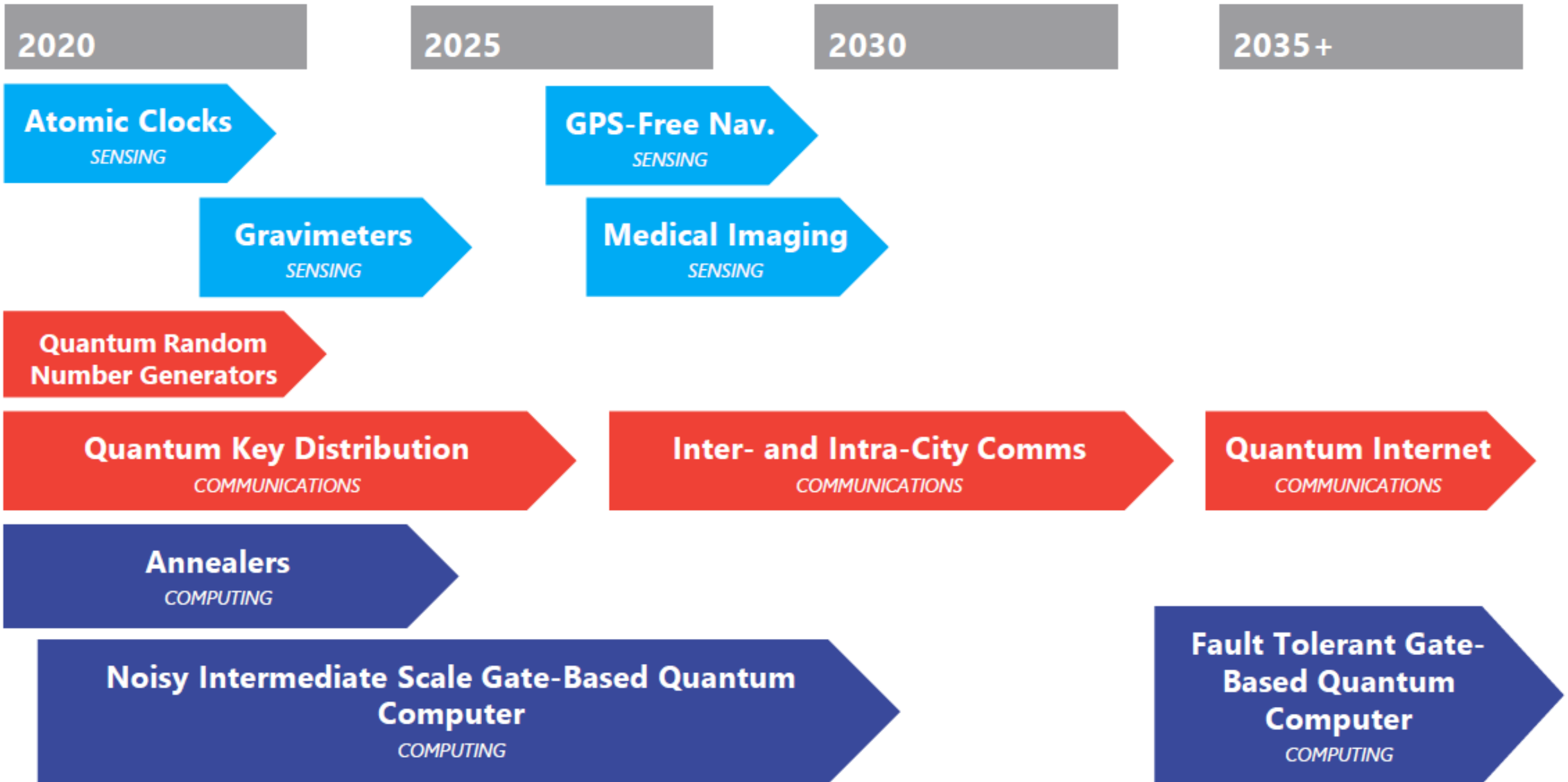
либо "0" либо "1" (trigger)

$$|\Psi_{12}\rangle = \frac{1}{\sqrt{2}} \{ |0_1\rangle |1_2\rangle + |1_1\rangle |0_2\rangle \}$$

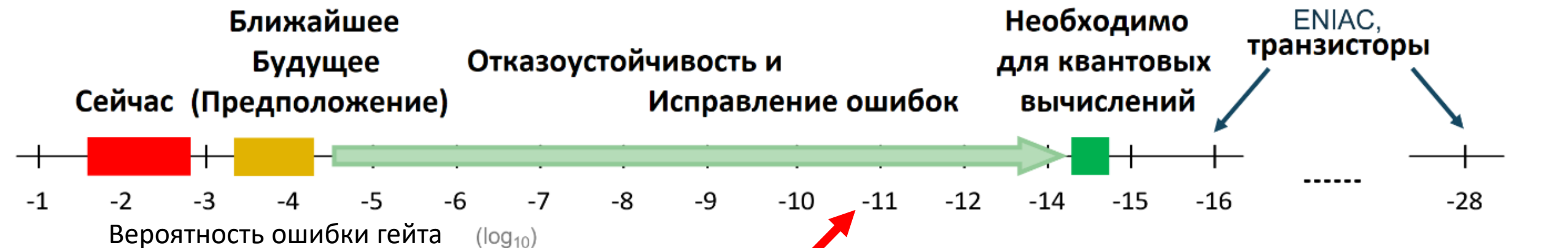
перепутанное состояние

нет аналогов

ПЕРСПЕКТИВЫ ОТРАСЛИ



Предельный уровень ошибок для выполнения полномасштабных квантовых вычислений



Квантовые компьютеры для специальных приложений и ограниченного спектра задач

Квантовые компьютеры широкого применения: общецелевые, масштабируемые, точные

Для поверхностных кодов:

$$P_{\text{logical}} \approx C \left(P_{\text{physical}} / P_{\text{threshold}} \right)^{(d+1)/2}$$

$$d = \sqrt{n}, \quad C \approx 0.1, \quad P_{\text{threshold}} \approx .01$$

Пусть $P_{\text{physical}} = .001, P_{\text{logical}} = 10^{-11} \Rightarrow d = 19, n = 361$ физических кубитов на один логический

Если $P_{\text{physical}} = 10^{-4} \Rightarrow d = 9, n = 81$

John Preskill, US QIS Summer School July 2024

Универсальный квантовый
компьютер



Коды коррекции ошибок
(Quantum Error Correction)

Альтернативы

NISQ
(noisy intermediate-scale quantum)
компьютеры –
рядка сотни кубитов

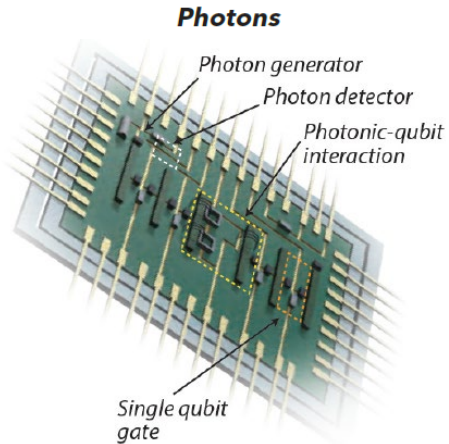
Квантовый отжиг
(quantum annealing)

Сортировка бозонов
(boson sampling)

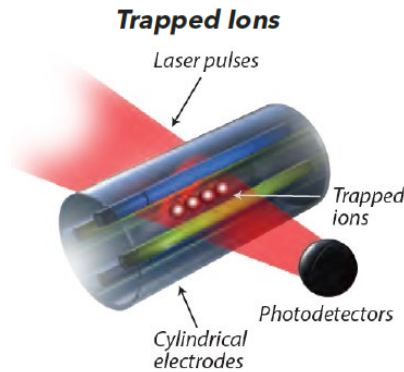
Квантовые симуляторы

Квантовое превосходство может быть достигнуто в два этапа:

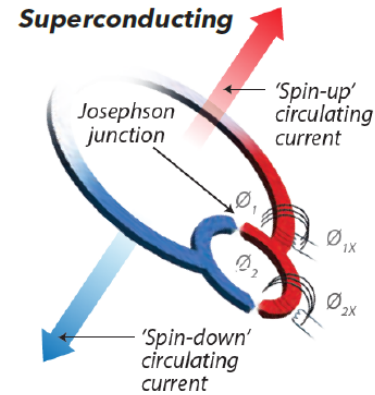
1. демонстрация способности существующих квантовых устройств выполнять точные вычисления на масштабах, выходящих за рамки «грубой» классической симуляции;
2. поиск практически важных задач, использующих преимущества квантовых устройств.



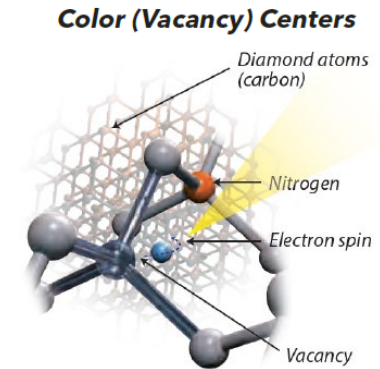
Фотонные чипы



Ионы в ловушках

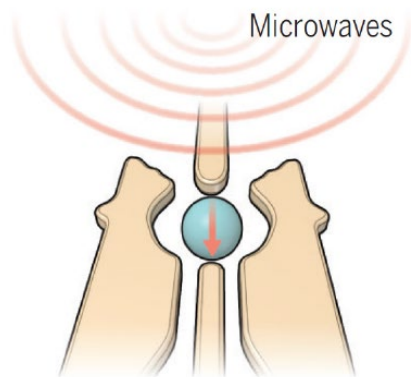


Сверхпроводниковые схемы



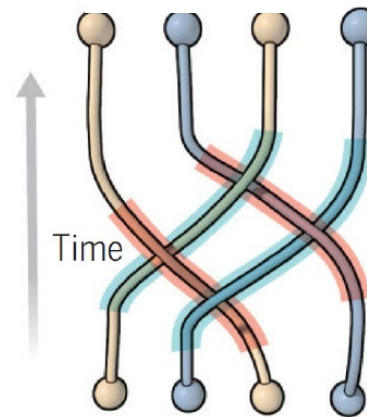
Вакансионные центры в алмазах

Silicon Spins



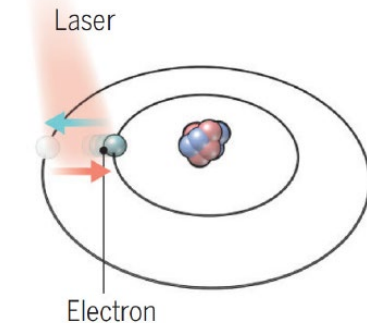
Примеси в полупроводниках

Topological Qubits



Топологические кубиты

Neutral Atoms



Нейтральные атомы

СПЕЦИАЛИЗИРОВАННЫЙ КВАНТОВЫЙ СОПРОЦЕССОР



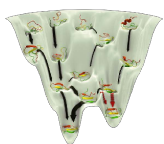
Квантовый отжиг



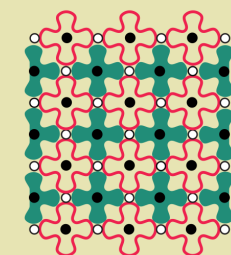
ПРИМЕНЕНИЕ
глобальная оптимизация

УНИВЕРСАЛЬНОСТЬ
ограниченная

ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ
ограниченная



КЛАССИЧЕСКИЙ ВЫЧИСЛИТЕЛЬНЫЙ КЛАСТЕР



КВАНТОВЫЙ СОПРОЦЕССОР

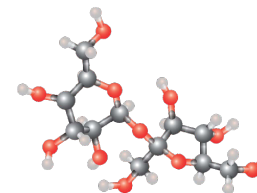
NISQ устройство

ПРИМЕНЕНИЕ
квантовая химия
наука о материалах
глобальная оптимизация
задачи сэмплинга
квантовая динамика



УНИВЕРСАЛЬНОСТЬ
частичная

ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ
высокая?



Универсальный квантовый компьютер



ПРИМЕНЕНИЕ
защищенные вычисления
машинное обучение
криптография
квантовая химия
наука о материалах
глобальная оптимизация
задачи сэмплинга
квантовая динамика
задачи поиска

УНИВЕРСАЛЬНОСТЬ
полная, математически обоснованное
ускорение

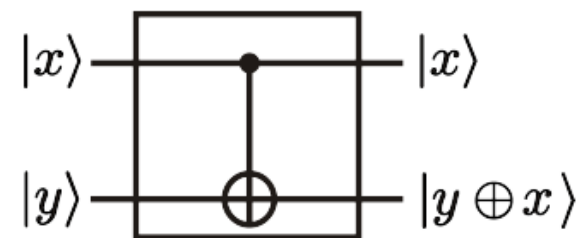
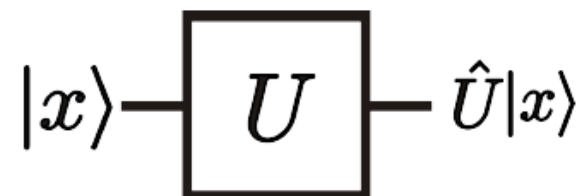
ВЫЧИСЛИТЕЛЬНАЯ МОЩНОСТЬ
очень высокая



Сегодня обозначена возможность
использования квантового компьютера для
решения практически значимых задач

Универсальный набор гейтов¹

- ▶ Arbitrary single qubit gates
(H,S,T set is sufficient)
- ▶ Entangling two-qubit gate - for
example, a CNOT

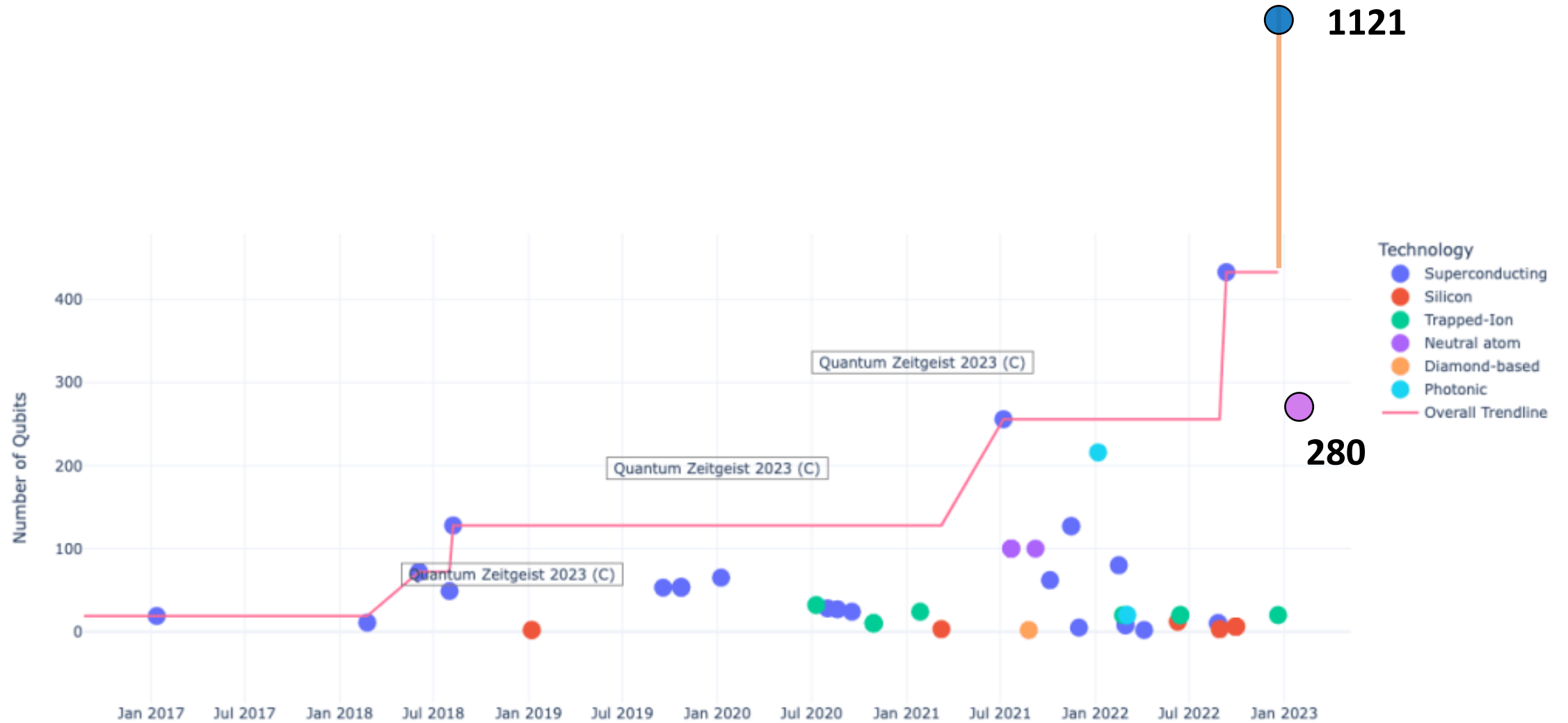


¹A.Barenco, *et al.*, Elementary gates for quantum computation, Phys. Rev. A **52**, 3457 (1995)

Критерии Ди Винченцо:

- масштабируемость;
- надежная инициализация;
- большие времена декогеренции (релаксации)
по сравнению с временем срабатывания
отдельных гейтов;
- возможность манипуляций;
- передача и считывание состояний кубитов,

-



СРАВНЕНИЕ МЕЖДУ РАЗНЫМИ ПЛАТФОРМАМИ



Платформа Параметр	Ионы	Нейтральные атомы	Сверхпроводники	Фотоны*	Центры в алмазах	Примеси /КТ в кремнии
Масштабируемость (число кубитов в регистре)	218	256 (1 167, два массива)	433 (1121, блоки)	>1000	10	2 [кубита (2e ⁻)] 3 [кубита (2ядра+1e ⁻)] /6
Время когерентности, с	5 500	3	0.5	«∞»	60	30 [спин ядра] 0.5 [спин e ⁻] /0.028
Время срабатывания гейта (1 кубит/2 кубита), мкс	5/25	2/0.4	0.02/0.03	<0.001/ 0.01	0.01/0.7	0.0008/0.025
Фиделити (1 кубит/2 кубита)	0.99998 /0.999	0.999 /0.995	0.9998 /0.9987	>0.9999 /0.994	0.99995 /0.992	99.99/99.96
R-фактор (1 кубит/2 кубита) 10 ⁶	1100/220	1.5/7.5	25/16.7	«∞»	6000/85.7	1.12/0.28

В БЛИЖНЕСРОЧНОЙ, СРЕДНЕСРОЧНОЙ И ДОЛГОСРОЧНОЙ ПЕРСПЕКТИВАХ

	«Эра» NISQ 3-5 лет	Всеобщее квантовое превосходство Более 10 лет	Полномасштабный помехоустойчивый квантовый компьютер Более 20 лет
Технические достижения	Устранение ошибок	Исправление ошибок	Модульная архитектура
Пример влияния на бизнес	Симуляторы задач материаловедения	Оценки финансовых рисков в близком к реальному времени (например, для инвестиционных фондов)	Дизайн лекарств, содержащих большие биопрепараты, с минимальными побочными эффектами
Расчетное воздействие (операционная прибыль)	2-5 млрд. долларов	25-50 млрд. долларов	450-850 млрд. долларов

Задача	Полезно для...	Отраслевые приложения
Комбинаторная оптимизация	Минимизация или максимизация целевой функции, например, поиск наиболее эффективных ресурсов или поиск самого короткого расстояния между точками (задача странствующего коммивояжера)	• Оптимизация сети (например, для авиалиний, такси) • Оптимизация цепочек поставок и/или логистики • Оптимизация финансовых сервисов
Решение систем дифференциальных уравнений	Моделирование поведения сложных систем, (например, уравнение Навье-Стокса в гидродинамике)	• Моделирование гидродинамики для дизайна - автомобильной и авиационной техники; • Моделирование медицинских приложений (например, анализ кровотока); • Молекулярное моделирование новых материалов и/или лекарств
Решение систем линейных уравнений	Задачи машинного обучения с использованием матрицы диагонализации (например в задаче кластеризации)	• Управление рисками в финансовой сфере • Классификация последовательностей ДНК • Маркетинг и сегментация клиентов
Задача факторизации	Криптография и компьютерная безопасность, (например, RSA)	• Дешифрование и/или взлом кода

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ : ВЫВОДЫ

- Число кубитов и качество логических операций в квантовых вычислителях стабильно растёт
- Квантовое вычислительное превосходство уже продемонстрировано
- Есть основания полагать, что даже небольшие NISQ устройства могут дать преимущество в практически важных задачах
- Квантовые алгоритмы в целом и в приложении оптимизационным задачам в частности – активно развивающаяся область

Квантовая коммуникация/связь

Вопросы

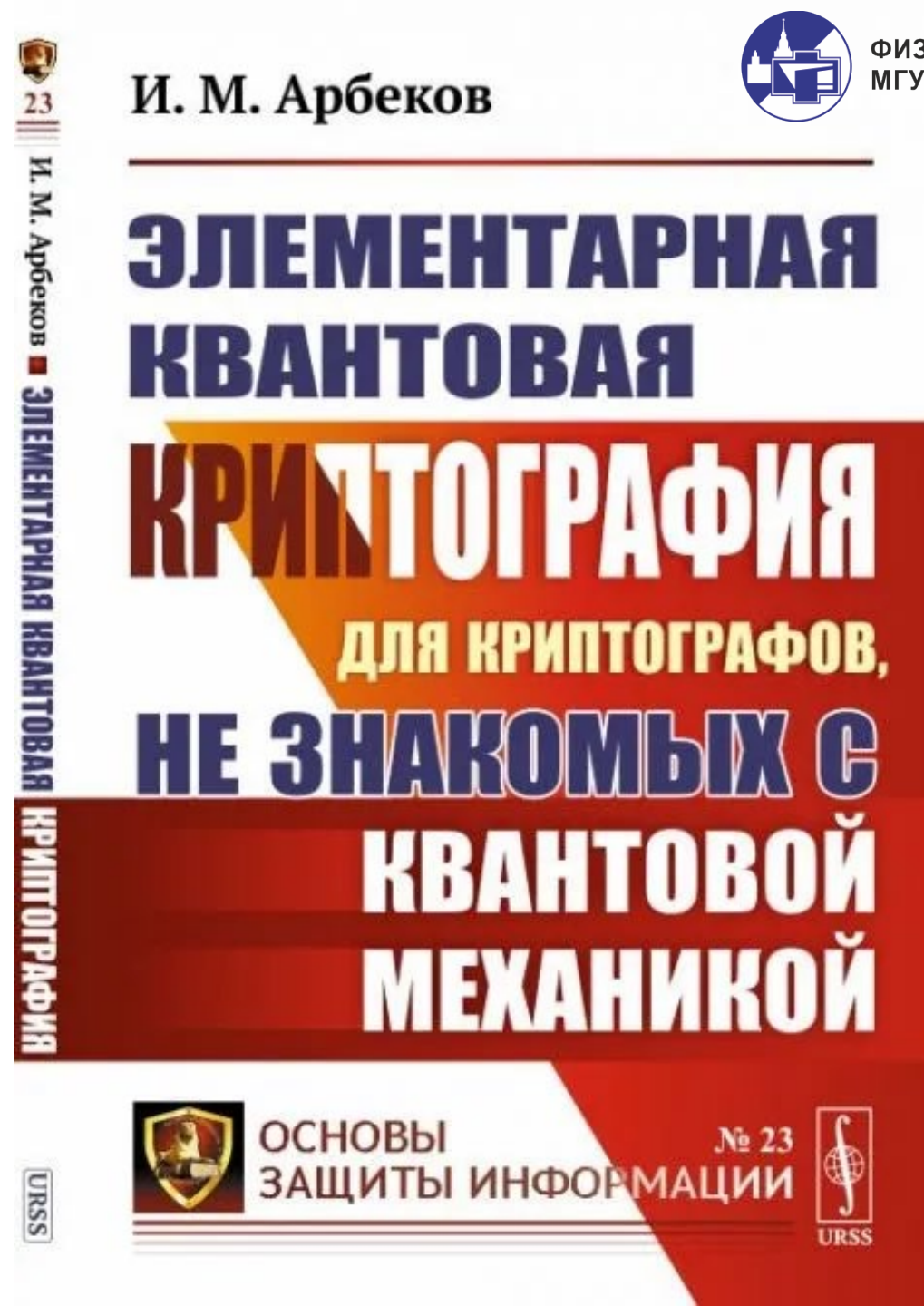
*Вывод защиты
информации на
принципиально иной
уровень!*

одное простран

Квантовые интерфейсы
и память

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

Физики не знают
криптографию, а
криптографы не
знают квантовую
механику



КВАНТОВАЯ СВЯЗЬ: ОСНОВНЫЕ НАПРАВЛЕНИЯ МИРОВЫХ РАЗРАБОТОК



1. Волоконно-оптические линии связи:

- шифрование квантовыми ключами данных, передаваемых 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.

РОССИЙСКИЕ КОМПАНИИ-ВЕНДОРЫ В ОБЛАСТИ КВАНТОВОЙ СВЯЗИ



<https://infotecs.ru/>



<https://goqrate.com/>



СМАРТС
КВАНТТЕЛЕКОМ

<https://quanttelecom.ru/>

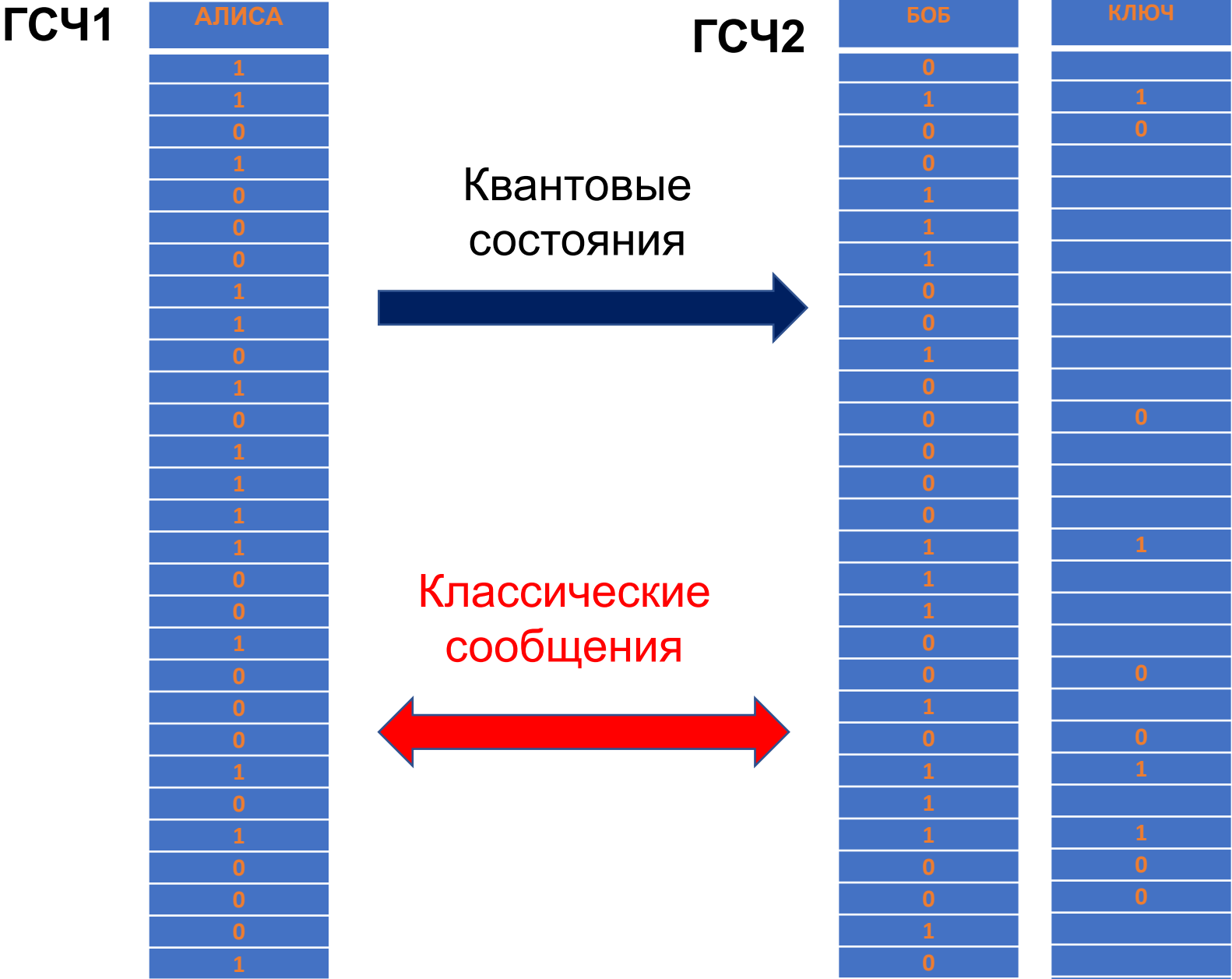


Сертифицированный продукт(ы)



Имеется Заключение Регулятора

ПРИНЦИП ФОРМИРОВАНИЯ КЛЮЧА В КВАНТОВОЙ КРИПТОГРАФИИ

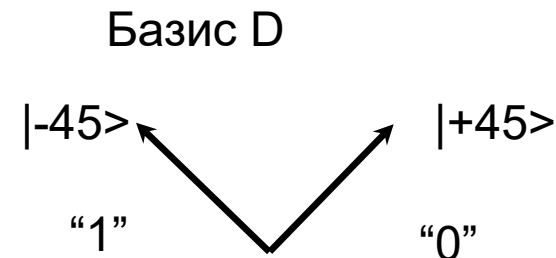
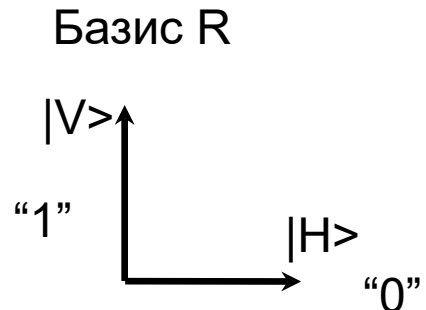


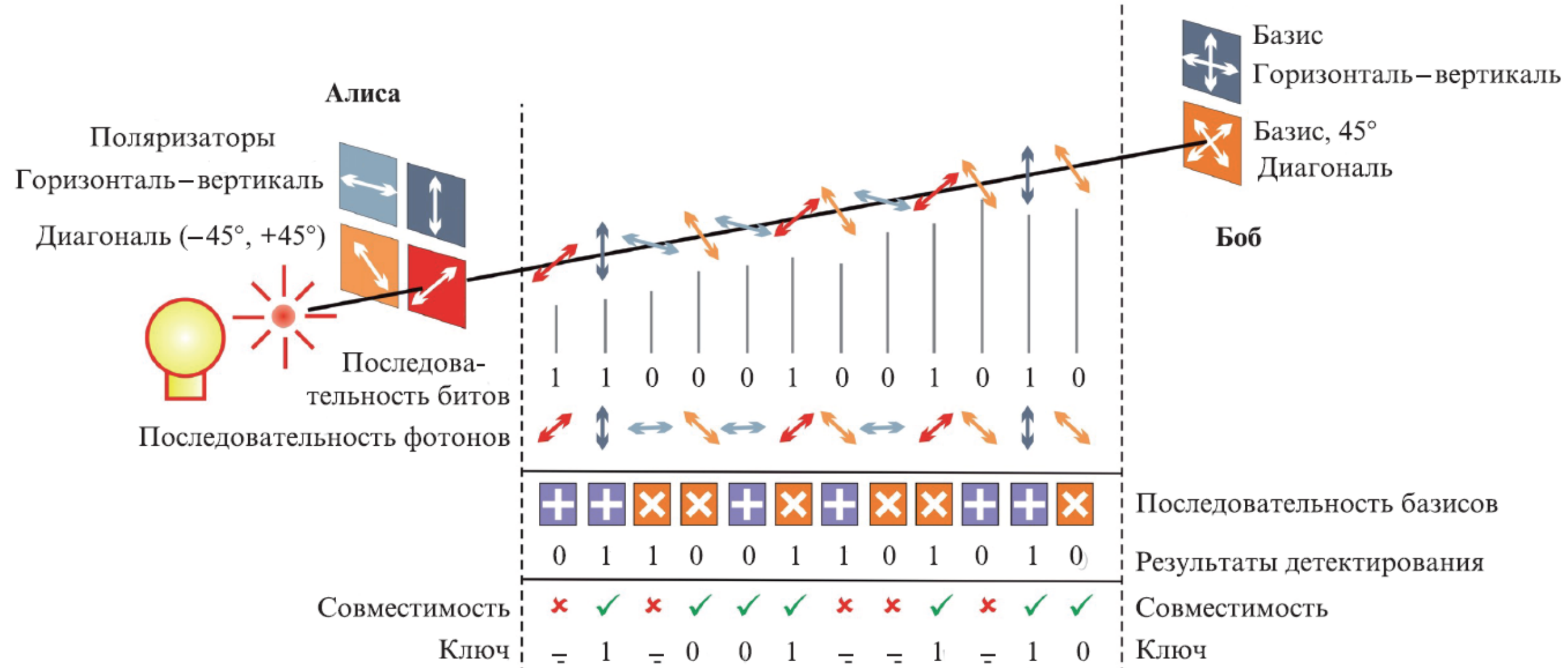
1. Неизвестное квантовое состояние нельзя копировать (no-cloning theorem)
2. Измерение неизвестного состояния вносит возмущение (no-cloning theorem)
3. Случайный выбор из двух неортогональных состояний (базисов)

Взаимно-несмещенные базисы; базис определяется D ортогональными состояниями

$$\left| \langle e_i | e_j \rangle \right|^2 = \begin{cases} 1/D, & \text{если состояния выбраны из разных базисов} \\ 0, & \text{если состояния выбраны из одного базиса} \end{cases}$$

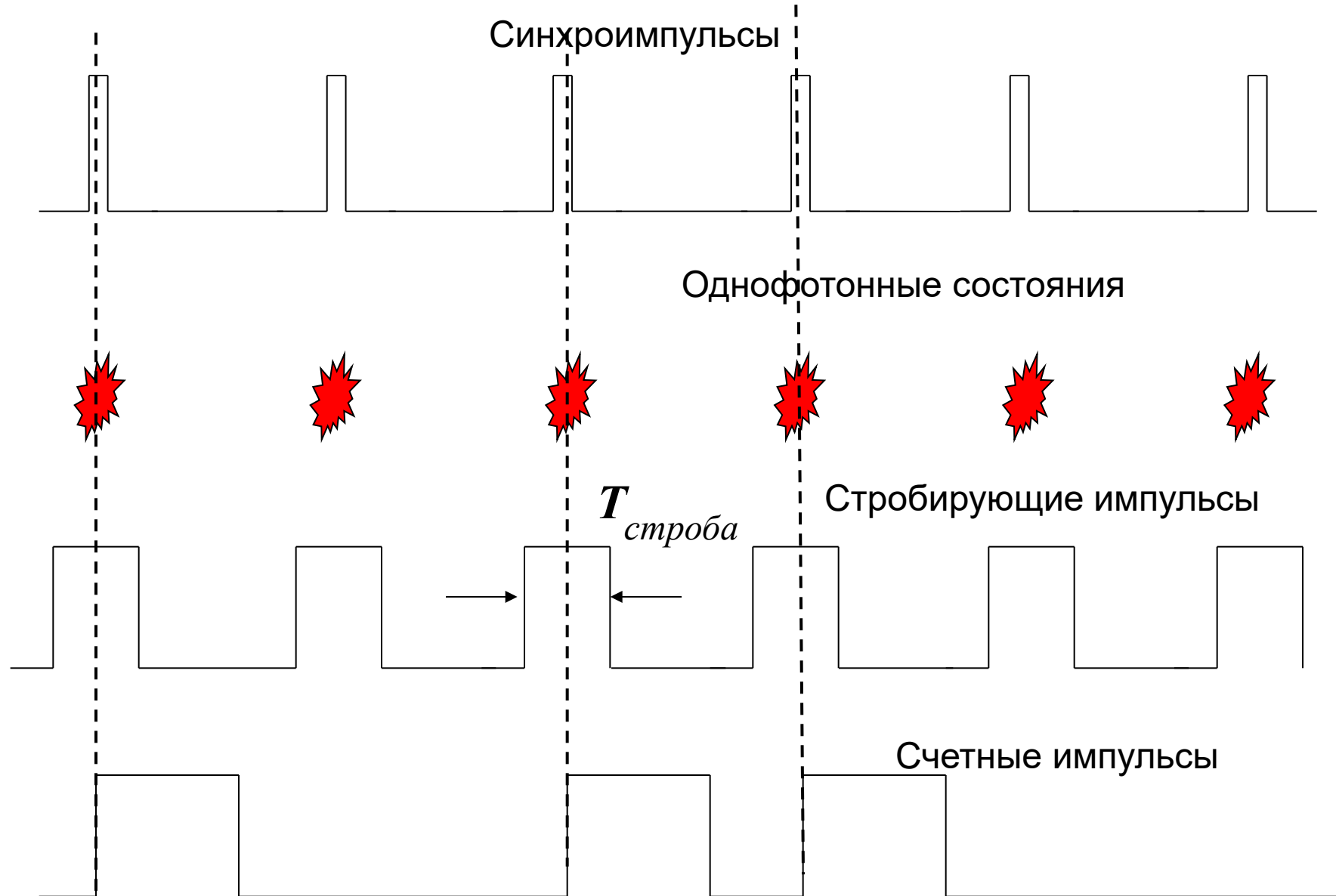
Например, если $D = p^k$, где p простое число, k - целое, то имеется набор $M = D + 1$ взаимно-несмещенных состояний







ИДЕЯ ОДНОФОТОННОЙ РЕГИСТРАЦИИ В КВАНТОВОЙ КРИПТОГРАФИИ



Лазерное излучение соответствует **когерентному состоянию** или **пуассоновской статистике фотонов**.

Вероятность найти n фотонов при среднем значении числа фотонов μ дается распределением Пуассона:

$$P(n, \mu) = \frac{\mu^n}{n!} e^{-\mu}$$

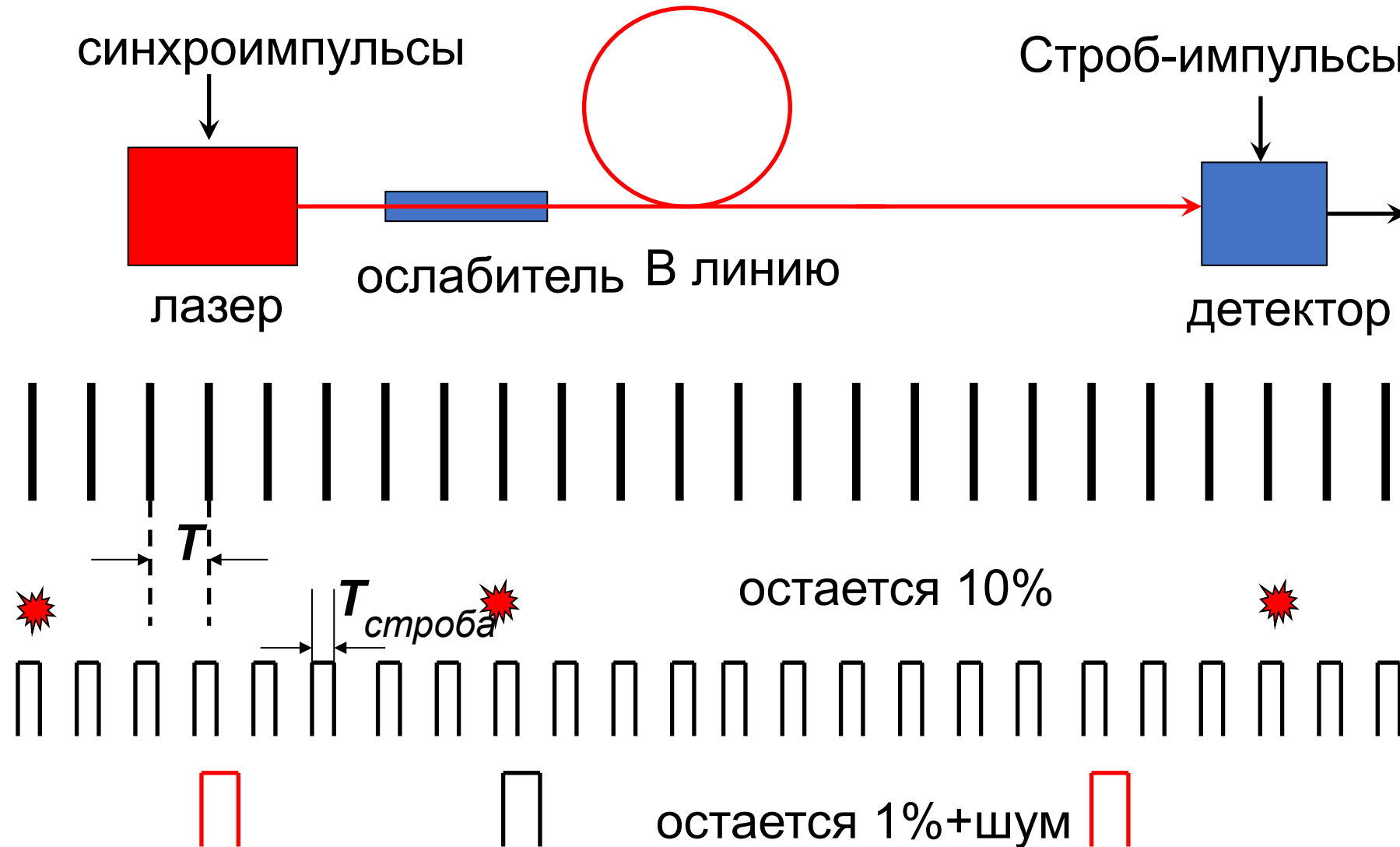
Принято выбирать среднее число фотонов на уровне $\mu = 0.1$, что примерно дает однофотонное состояние на каждый десятый синхроимпульс.

При этом 5% непустых импульсов содержит **> 1 фотона**

Этот уровень оценивается из соотношения:

$$\mu = \frac{W}{\hbar \omega} T_{gate}$$

где W – средняя мощность лазера в непрерывном режиме генерации,
 ω - частота излучения



Проблема – темновые отсчеты однофотонного приемника

Основные типы протоколов

<i>Одиночные фотоны (BB84)</i>	<i>Пары перепутанных фотонов (E91)</i>
Поляризационное кодирование Фазовое кодирование Фазово-временное кодирование	перепутывание «поляризация-угол»
Квантовый канал связи	
Свободное пространство (включая передачу на спутники) 880 нм (Si-детекторы) Волоконные линии связи 1.55 мкм (InGaAs-детекторы)	Свободное пространство (включая передачу на спутники) Волоконные линии связи

ПЕРЕДАЧА КВАНТОВЫХ ДАННЫХ																			
АЛИСА																			
Случайная последовательность битов у Алисы	1	1	1	0	1	1	0	0	1	0	1	1	0	0	1	1	0	1	0
Базис, случайно выбираемый Алисой	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R	D	R	R	D
Состояние, которое посылает Алиса	□	↕	□	↔	↕	↕	↔	↔	□	□	↕	□	□	□	↕	□	↔	↕	□
БОБ																			
Базис, случайно выбираемый Бобом	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R	R	R	D	D
Биты, регистрируемые Бобом (сырой ключ)	1	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	0
Учли технические потери	1	×	1	×	1	1	0	0	×	1	1	1	×	0	1	×	0	0	0
ОТКРЫТОЕ ОБСУЖДЕНИЕ																			
Боб сообщает базис, в котором зарегистрирован бит	R		D		R	D	D	R	×	R	D	D	×	D	R	×	R	D	D
Алиса сообщает, какой базис совпадает с ее базисом	-		Д а		Д а	-	-	Д а	-	-	-	Д а	Д а	Д а	Д а		Д а	-	Д а
Предварительная распределенная информация (подслушивания нет) - просеянный ключ			1		1			0				1		0	1		0		0
КОРРЕКЦИЯ ОШИБОК																			
Боб сообщает случайно выбранные биты					1										1		0		
Алиса сравнивает их с соответствующими своими					Д а										Д а		Д а		
ИТОГ																			
Распределенный ключ			1					0				1		0					0

Таблица 1. Протокол BB84 (нет подслушивания, без усиления секретности)

Простейшая стратегия подслушивания: перехват-пересылка
Ева получает $I_{Eve}=1/2$ кубитов

Вероятность, что Ева неправильно выберет базис $1/2$

**В этом случае ее измерение приводит к
максимальному возмущению: вероятность ошибки Боба $1/2$**

В среднем, уровень ошибок Боба E_B : $1/2 \times 1/2 = 1/4$

Оптимальное подслушивание: $\max I_{Eve}/E_{Bob}$

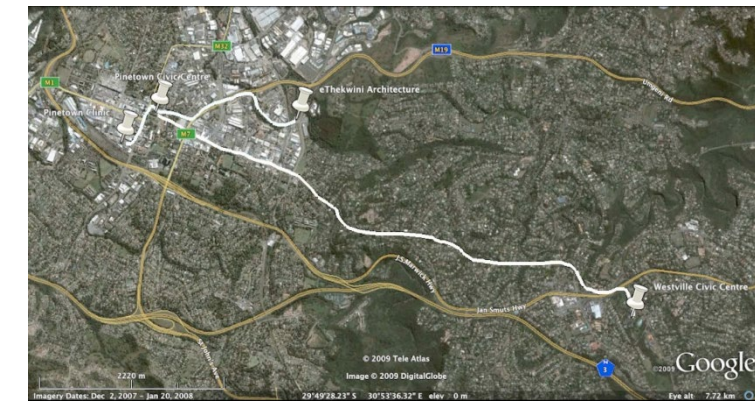
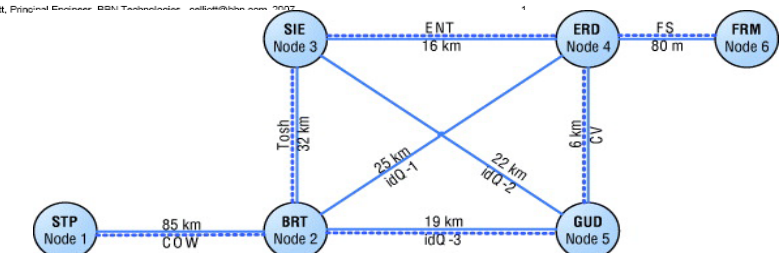
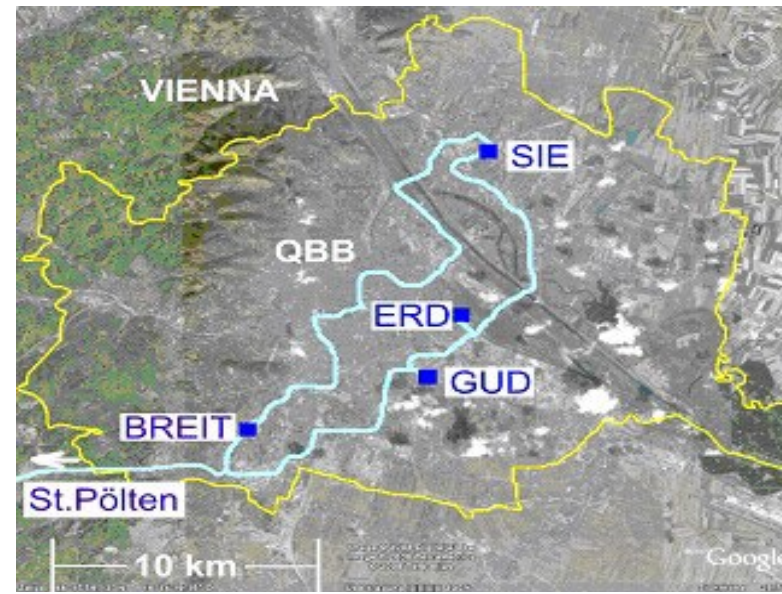
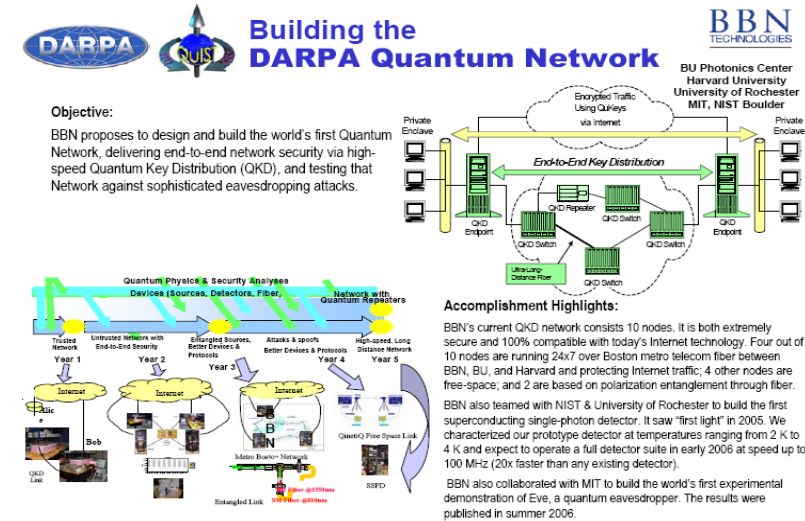
	BB84 ($D = 2$, 2 базиса)	6-state ($D = 2$, 3 базиса)	($D = 3$, 4 базиса)	($D = 4$, 5 базисов)
E_{Bob}/I_{Eve}	$1/2$	1	2	3 (the best!)
e				

1. 2004г. Сеть в Бостоне (BBN Technologies, MIT, Harvard University).
Финансирование DARPA

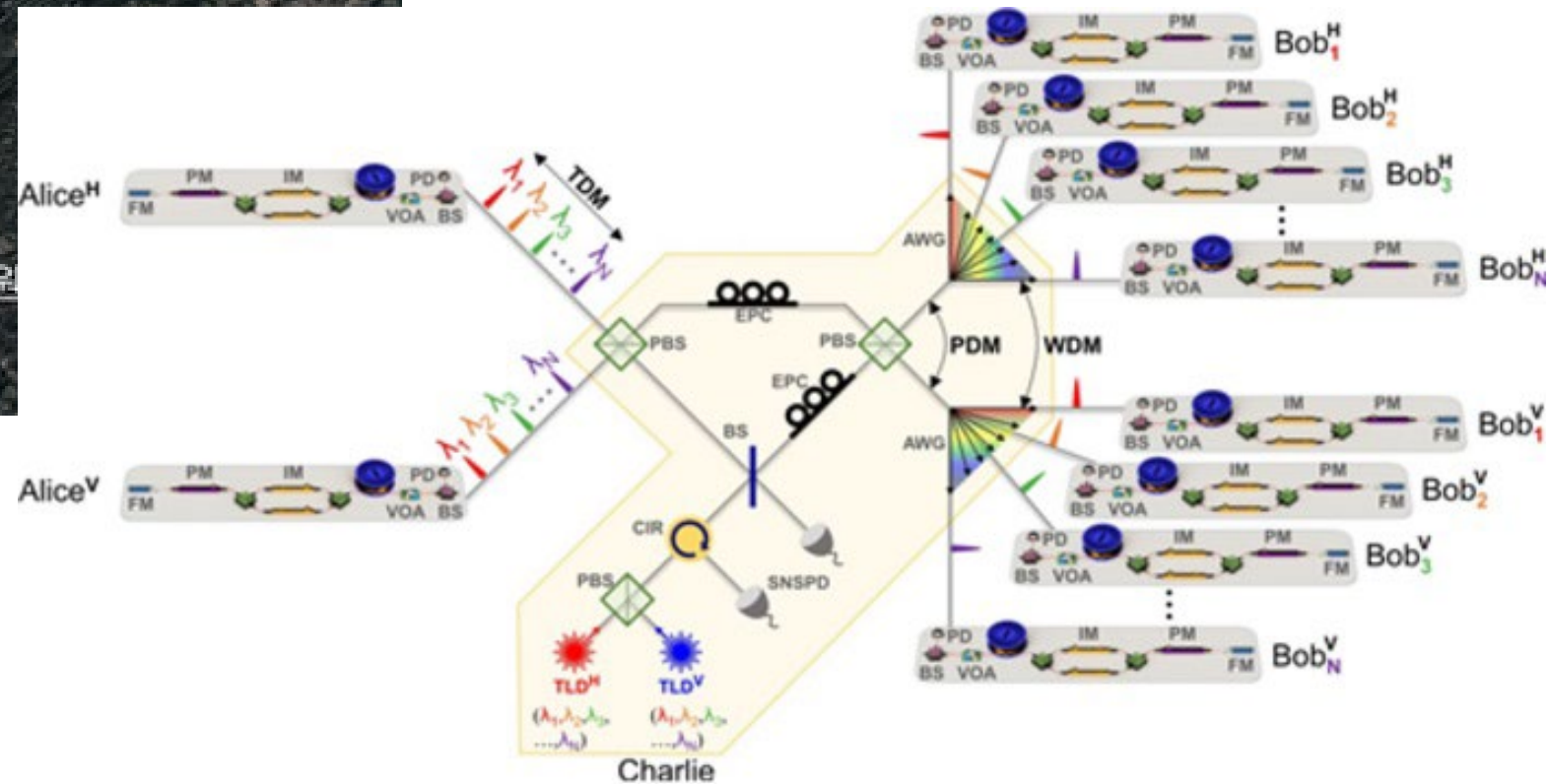
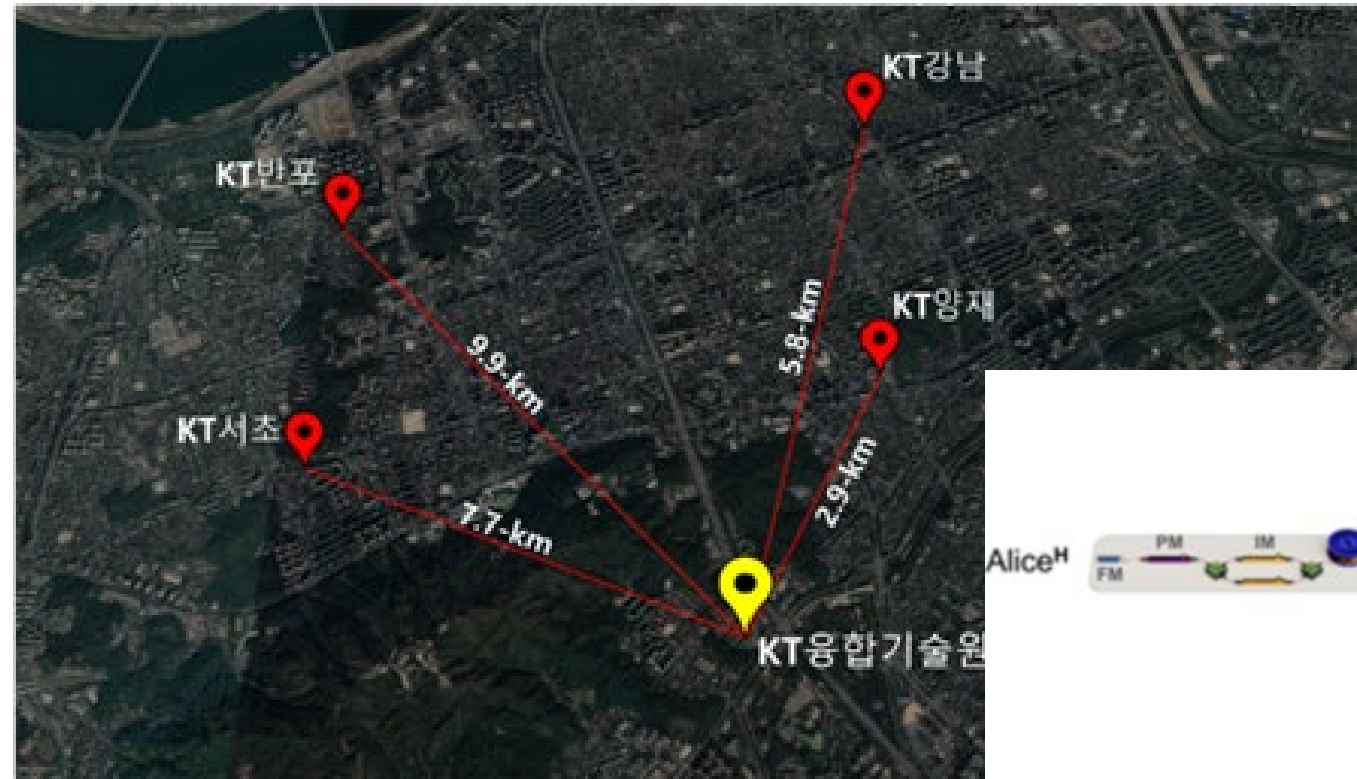
2. Европейский проект **SECOQC** 2004-2008
(<http://www.secoqc.net/>) 40 организаций, 11.3 мил.Евро

3. Проект Chinese Network Company (CNC)
(Китай) 2004-2009

4. Проект **QUANTUMCITY** (ЮАР) 2008-
(<http://quantum.ukzn.ac.za/quantum-city>)



2018년 KIST-KT 1X4 양자암호 네트워크 구축 (서울)



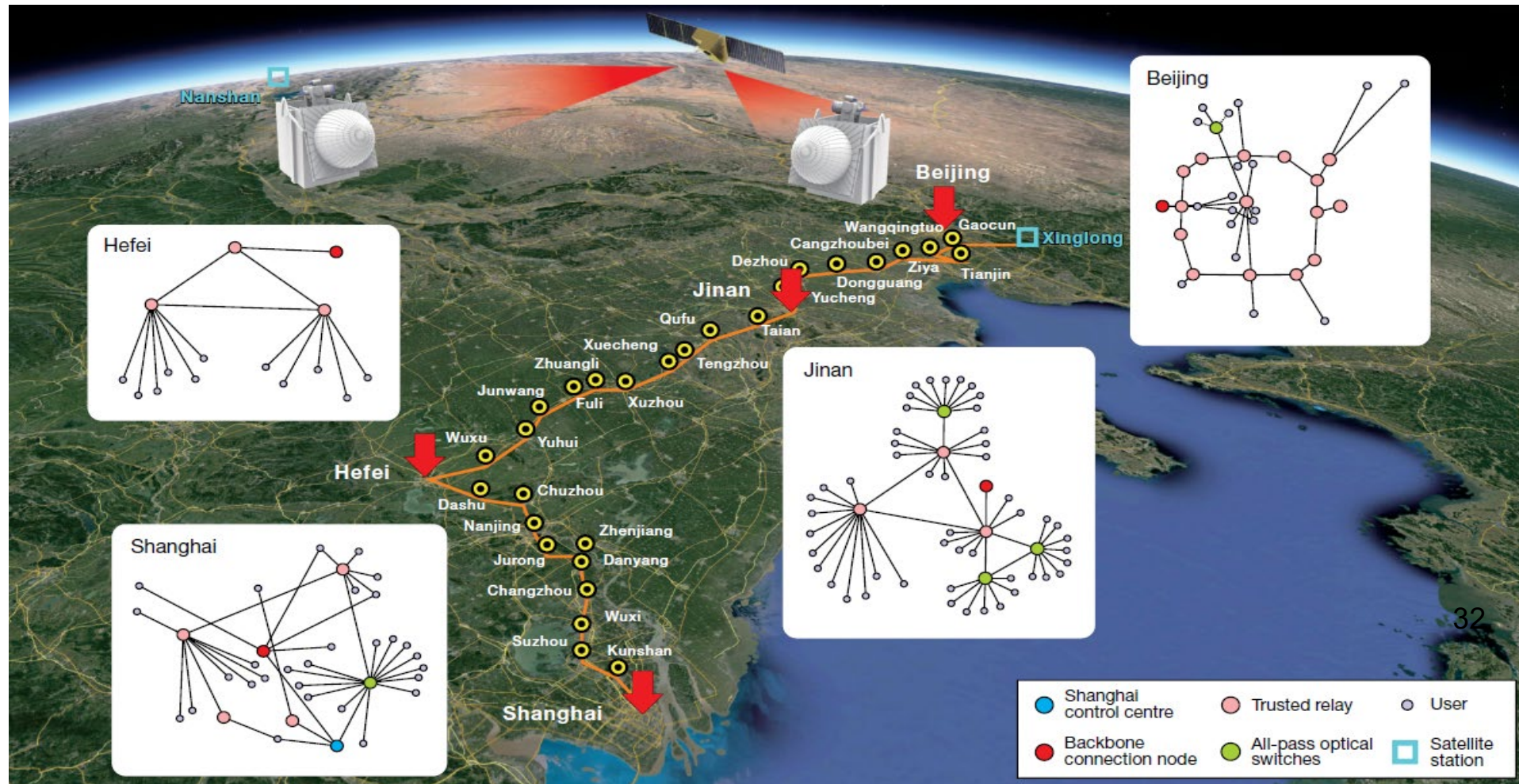
ЗАЩИТА РАСПРЕДЕЛЕННЫХ СЕТЕЙ – МИРОВЫЕ СЦЕНАРИИ

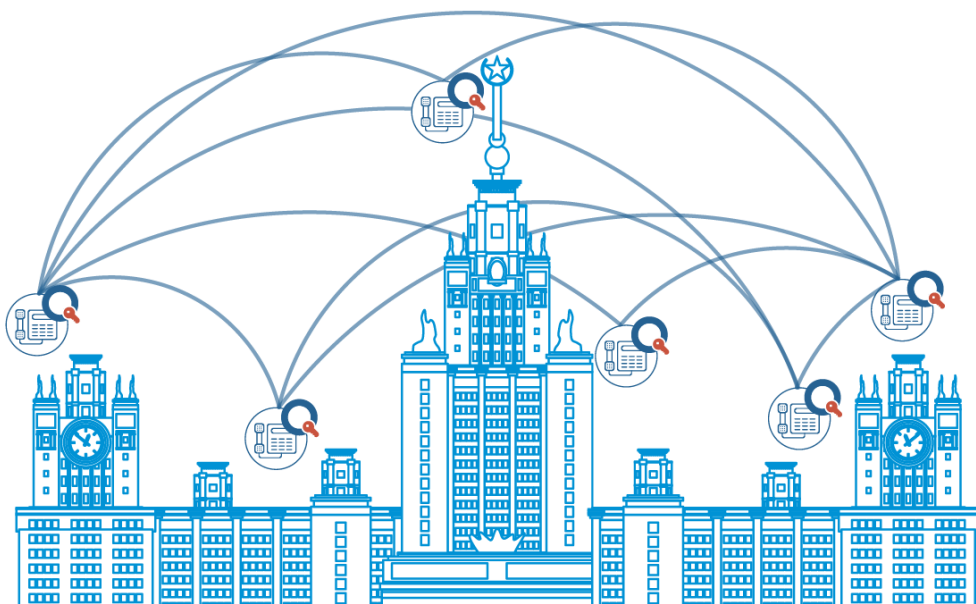
Квантовая сеть Китая

- 22 узла магистральной линии
- 400 сегментов
- 2 спутника

4800 км общая протяженность

157 потребителей





ViPNet QSS — совместная разработка ИнфоТеКС и Центра квантовых технологий физфака МГУ имени М.В.Ломоносова.

Университетская квантовая сеть:

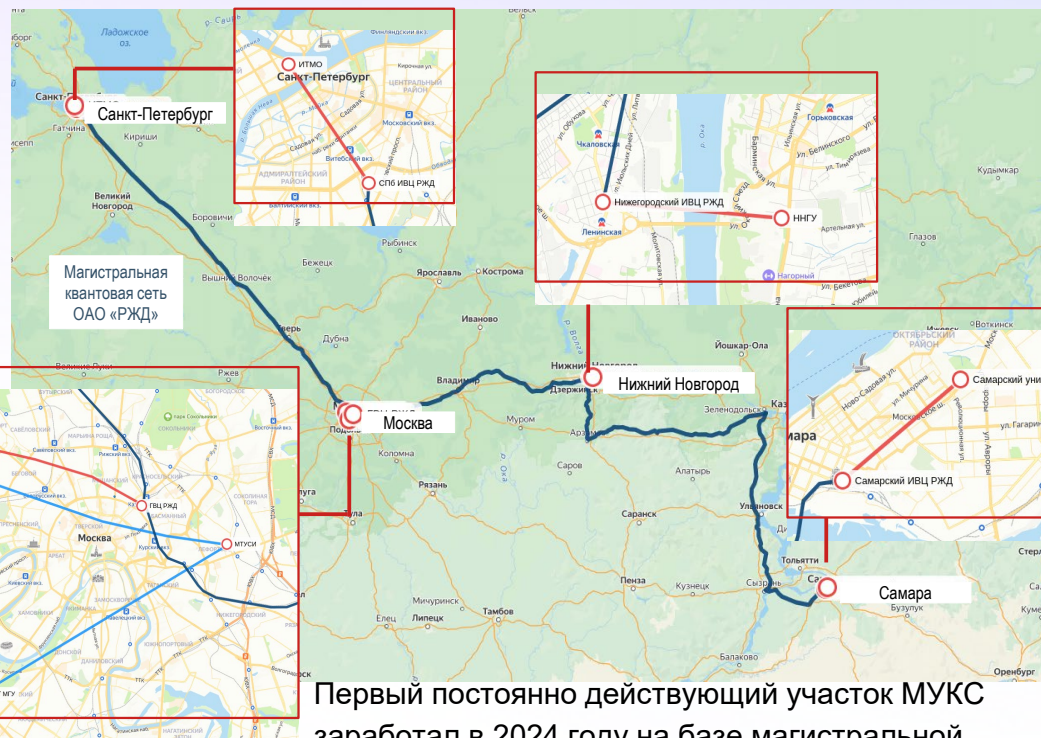
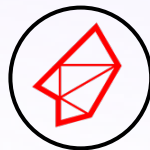
- Пять квантовых устройств
- Двадцать абонентских терминалов
- Длина каналов квантово-защищенной связи в рамках проекта достигла 50 км
- **Серийное оборудование производства ИнфоТеКС**
- Перспектива интеграции с магистральными сетями

Межуниверситетская квантовая

сеть

Межуниверситетская квантовая сеть (МУКС) – специализированная масштабируемая инфраструктурная цифровая платформа с открытой архитектурой для исследования, разработок и образования

СТРАТЕГИЧЕСКИЕ ПАРТНЕРЫ:



Первый постоянно действующий участок МУКС заработал в 2024 году на базе магистральной квантовой сети ОАО «РЖД»



НИЦ «Курчатовский институт»



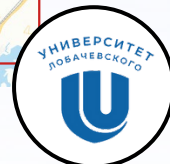
МГУ имени М.В. Ломоносова



Московский технический университет связи и информатики



Национальный исследовательский университет ИТМО



Нижегородский государственный университет им. Н.И. Лобачевского



Самарский национальный исследовательский университет им. С.П. Королева

- ✓ «Дорожная карта» развития высокотехнологичного направления «Квантовые коммуникации»
- ✓ перечень поручений Президента Российской Федерации от 6 апреля 2023 года № Пр-683
- ✓ Указ Президента Российской Федерации от 18 июня 2024 года № 529

МУКС:

- ✓ создана в рамках развития Национальной исследовательской компьютерной сети (НИКС)
- ✓ на базе Магистральной квантовую сеть (МКС) ОАО «РЖД»
- ✓ оператором сетей НИКС и МУКС является НИЦ «Курчатовский институт»

Космическая квантовая связь: планируемый проект РЖД/МГУ

Наземные терминалы

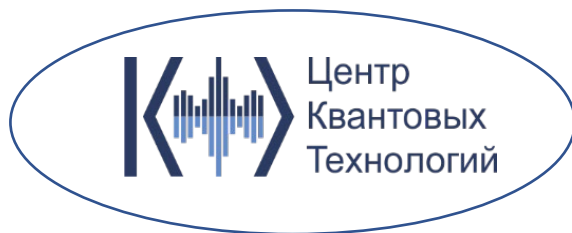


ГАИШ:
наземные терминалы

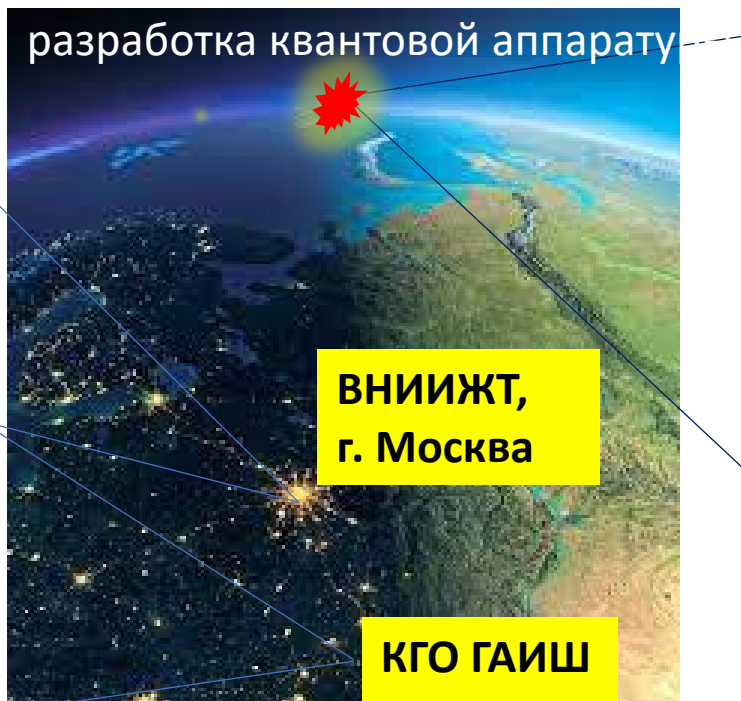


**Кавказская горная
обсерватория
ГАИШ**

Квантовая связь



Центр квантовых технологий МГУ:



разработка квантовой аппаратуры

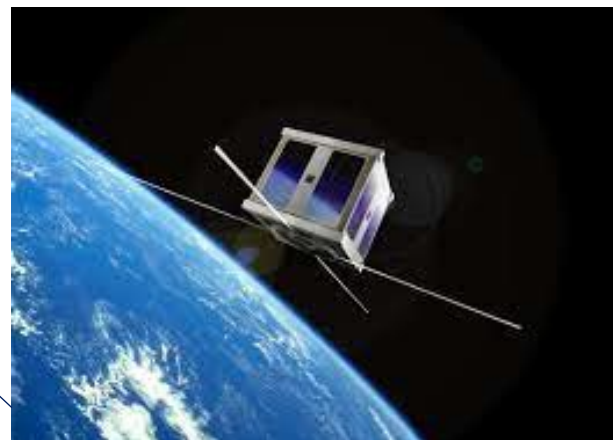
**ВНИИЖТ,
г. Москва**

КГО ГАИШ

Малый спутник



НИИЯФ:
построение малого спутника



АО «Мостком»:
- захват, наведение, сопровождение;
- телеметрия спутника

Специальные исследования



СФБ Лаб:
модель угроз



**Система
слежения**



Технические характеристики	
Наименование параметра	Значение параметра
Длина секретного квантового ключа, сформированного из данных, полученных за один сеанс квантовой связи, не менее	256 бит
Типоразмер космического аппарата класса «Cubesat», не более	16U
<u>Параметры ЭО БТ</u>	
- типоразмер, не более	11U
- масса, не более	17 кг
- энергопотребление, не более	100 Вт
Диаметр апертуры телескопа в составе наземного терминала, не менее	От 1 м до 1,2 м
<u>Расстояние между ЭО НТ и ЭО БТ</u>	
- в случае расположения ЭО НТ в надир по отношению к ЭО БТ	не менее 500 км
- при организации каналов связи на наклонных трассах	до 1000 км и более
Функционирование платформы	солнечно-синхронная орбита, 600±100 км
<u>Параметры квантового канала связи</u>	
- тактовая частота следования импульсов излучения, не менее	10 МГц
- расходимость излучения квантового канала связи, не более	15 мкрад
- квантово-криптографический протокол (в том числе среднее число фотонов в импульсе, длина волны и длительность оптических импульсов)	определяется на этапе проведения специальных исследований
Срок службы КА на орбите, не менее	3 года

ЗАЩИТА РАСПРЕДЕЛЕННЫХ СЕТЕЙ – РОССИЙСКИЕ ПРОДУКТОВЫЕ РЕШЕНИЯ: совместные разработки ЦКТ и ИнфоТеКС



Магистральный узел квантовой сети (ViPNet МУКС)

- Алиса и Боб в одном корпусе
- Подключение шифраторов



Распределительный узел квантовой сети (ViPNet РУКС) – центр «звезды»

- Управление оптическим коммутатором
- Подключение к ViPNet МУКС
- Подключение ViPNet КУКС

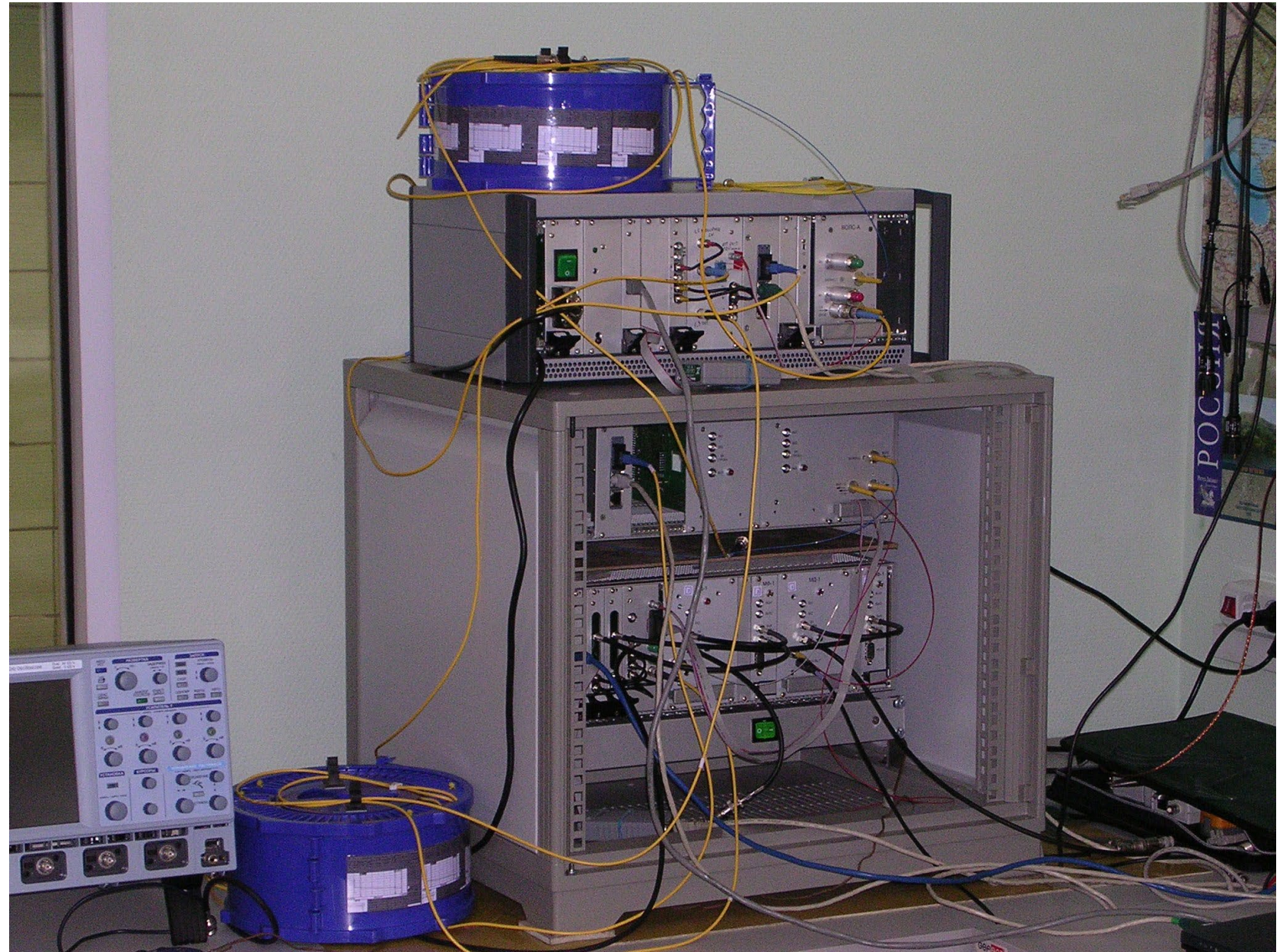
Клиентский узел квантовой сети (ViPNet КУКС)

- Подключение к ViPNet РУКС
- Подключение шифраторов



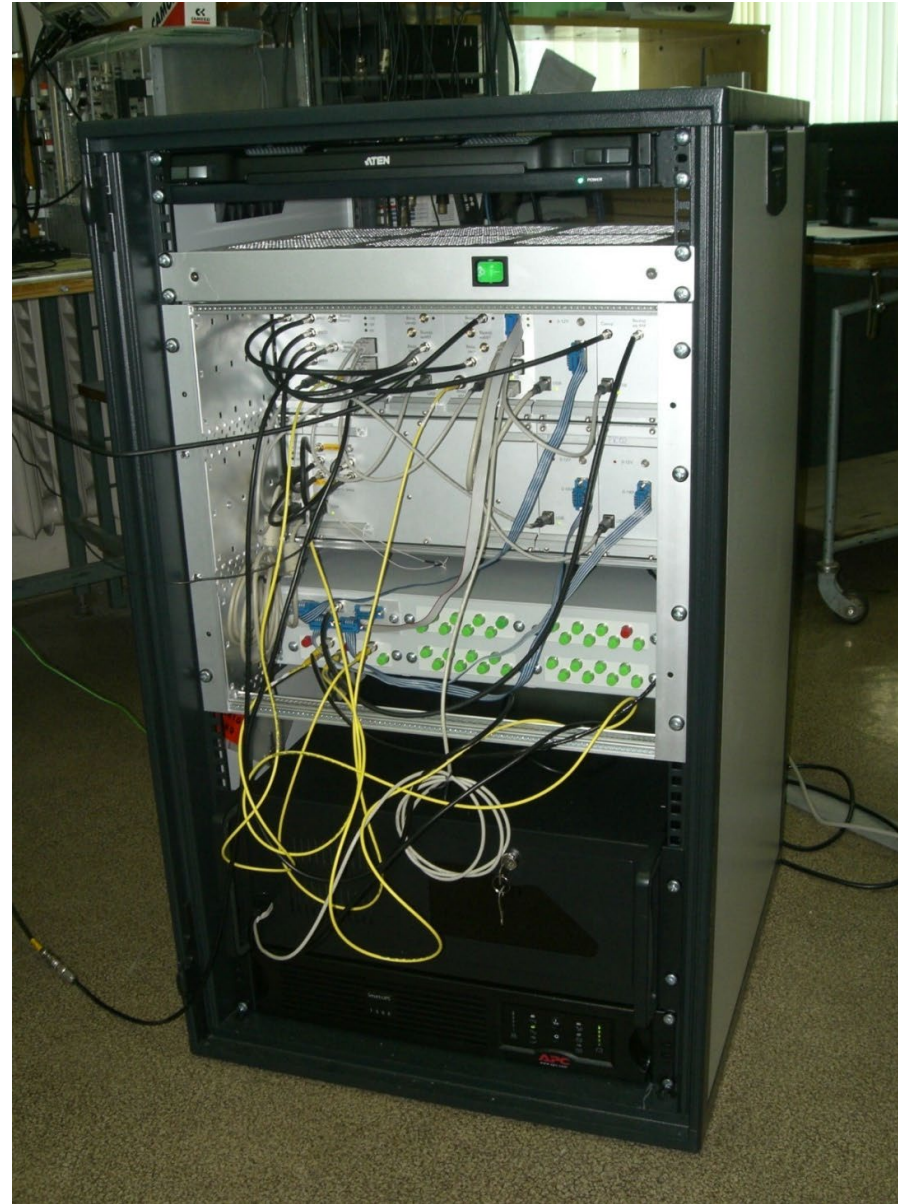
ЦКТ МГУ: опыт разработок систем квантовой связи

2007г.
Проект Минобрнауки



Космическая квантовая связь: планируемый проект РЖД/МГУ

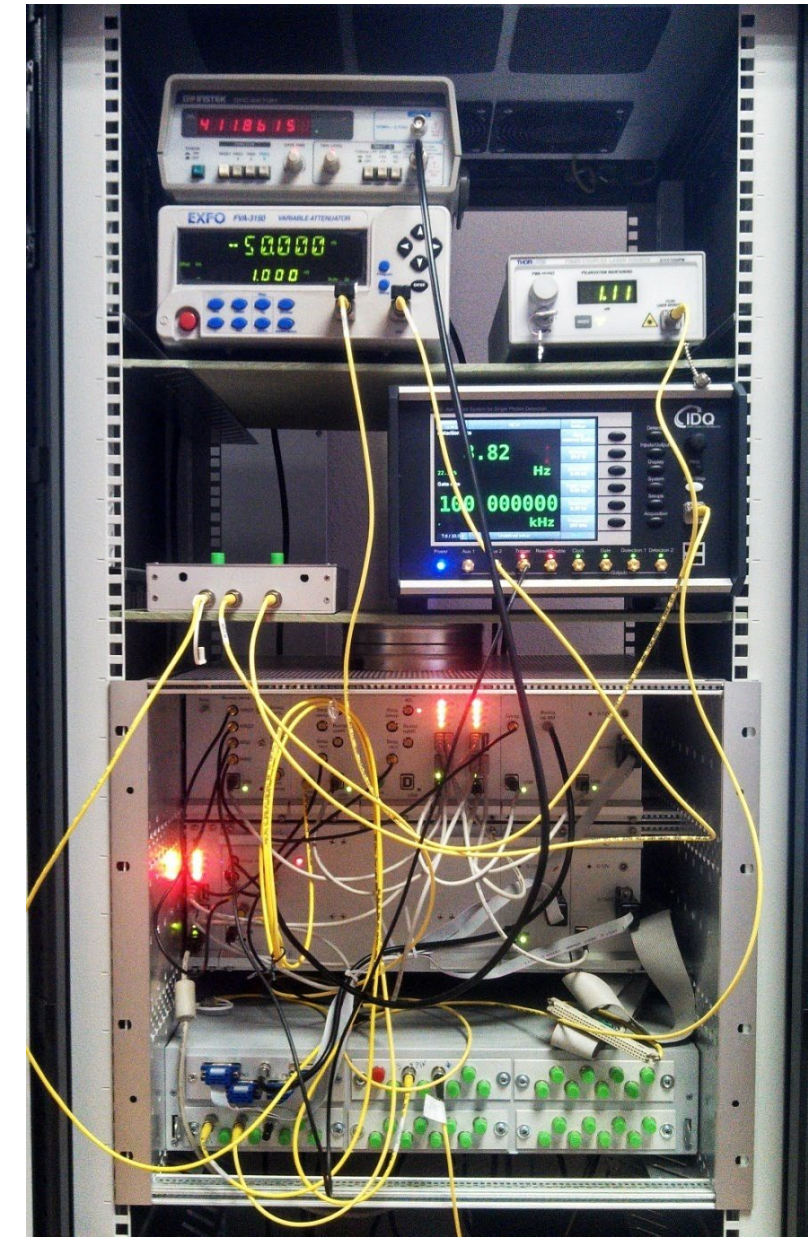
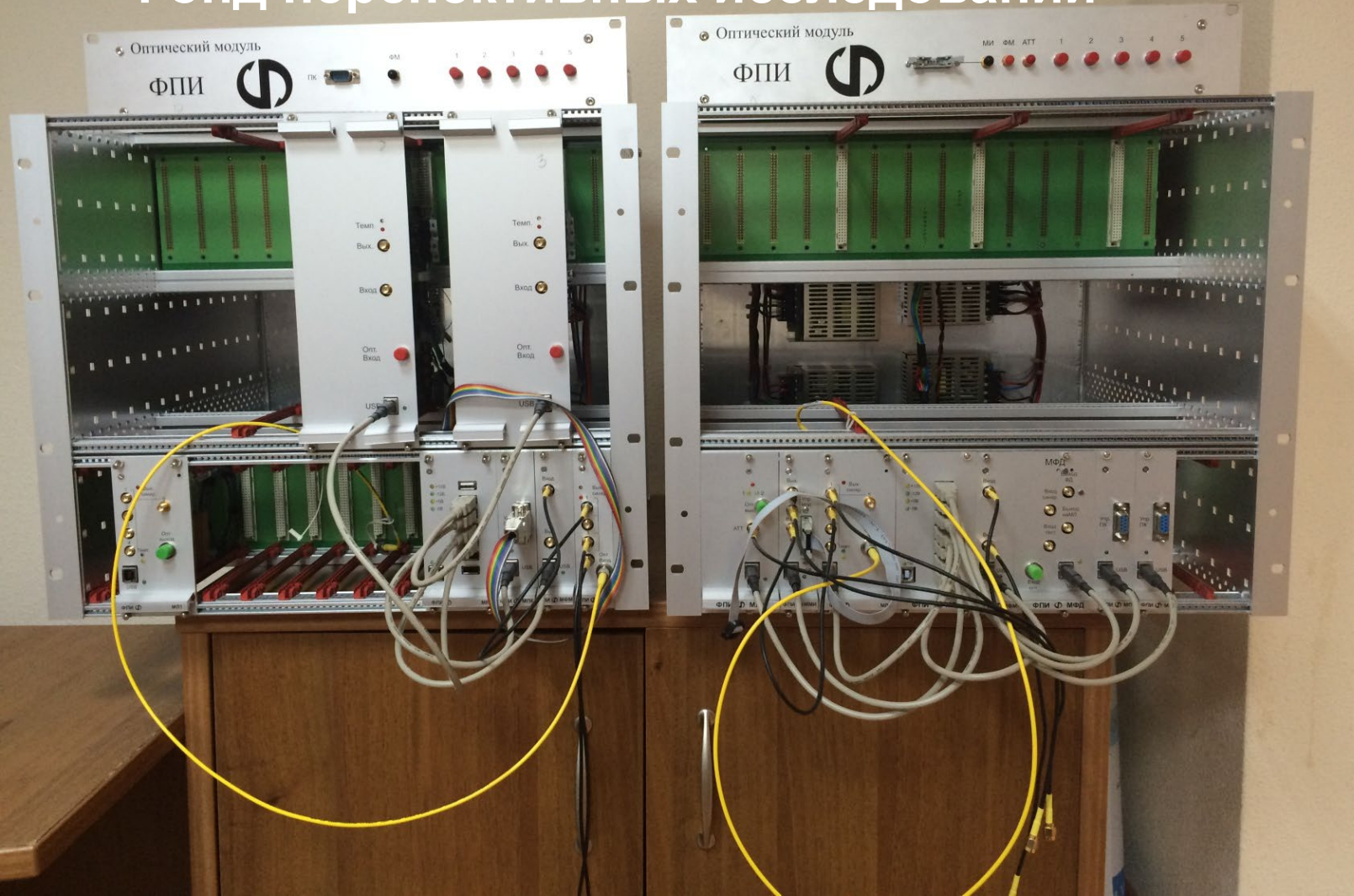
**2013г.
Закрытый проект**



ЦКТ МГУ: опыт разработок систем квантовой связи

2015г.

Фонд перспективных исследований



**2024г.
МУКС**



2023г.

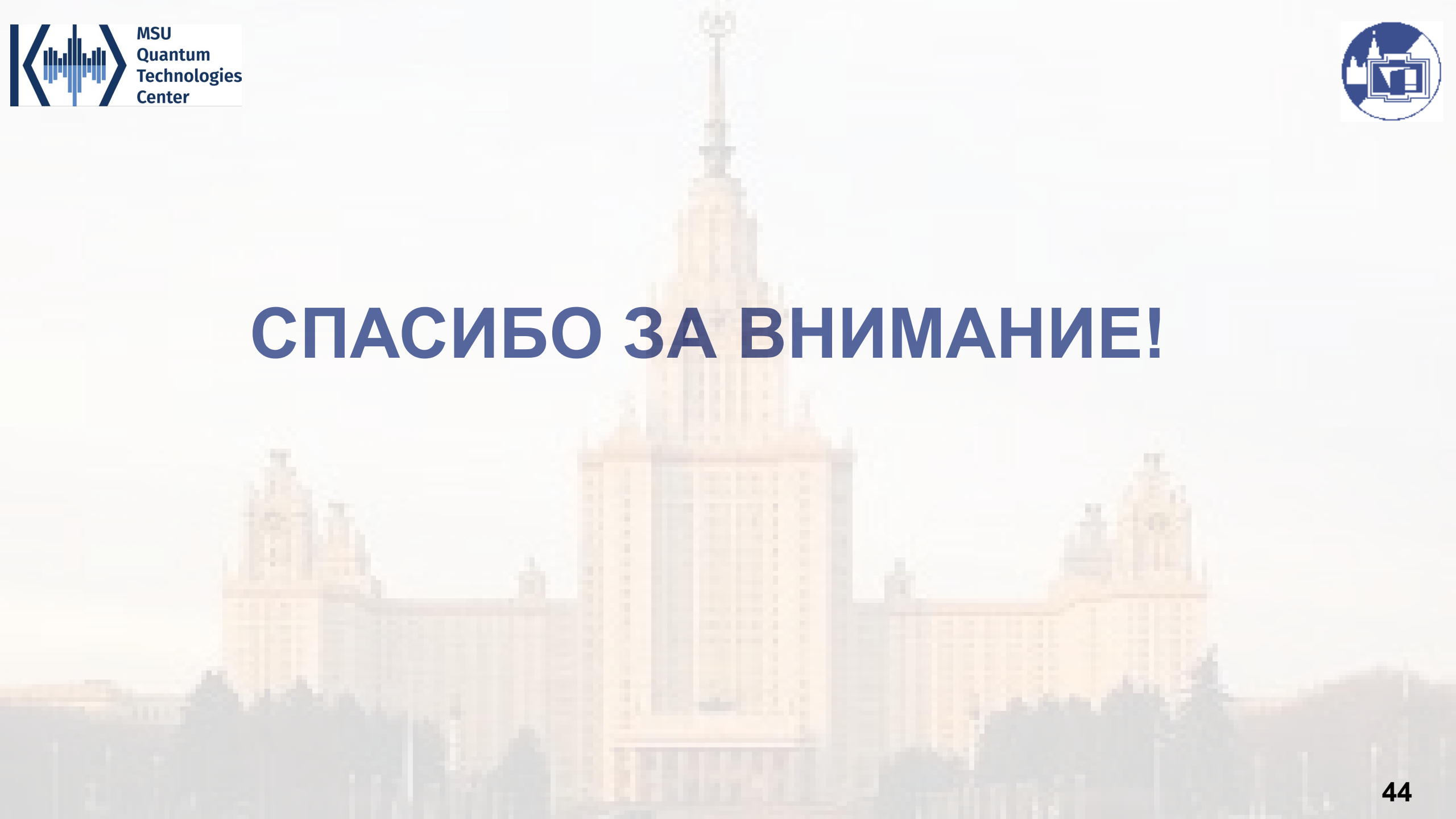


**2018-2020г.
Университетская квантовая
сеть**

Выводы, проблемы, перспективы

1. Квантовая криптография решает «маленькую проблему» классической криптологии – распределение ключа. Отсутствует «человеческий фактор».
2. Генерируемый ключ можно легко менять, достигая режима «одноразового блокнота». При этом осуществляется безусловно секретное шифрование (если длина сообщения не превышает длины ключа, и ключ используется один раз)
3. Подслушивание в квантовом канале связи детектируется статистическими методами. В этом случае сеанс связи прекращается.
4. Поскольку ошибки в канале связи обязаны восприниматься как попытка вторжения в канал, существует предельная длина квантового канала. Она определяется - затуханием оптического сигнала ($0,2 \text{ dB/км}$ для $\lambda = 1,55 \text{ мкм}$) и - допустимым уровнем ошибок, которые могут быть исправлены. Для протокола BB84 это 150 км (11% ошибок)!
5. **Проблемы:** снижение потерь $\longrightarrow$ увеличение дальности, увеличение критической ошибки. Интегрирование в локальные сети.
6. **Перспективы:** новые протоколы, развитие ВОЛС технологий интегрирование в квантовые сети

- 1. В области квантовых вычислений**, речь идет о создании в ближайшие 5 лет среднемасштабных вычислителей, способных продемонстрировать «квантовое преимущество» перед классическими суперкомпьютерами в ряде задач.
- 2. В области квантовых коммуникаций**, речь идет о создании разветвленных сетевых структур управления потоками информации, космической квантовой связи и предоставлении операторами целого спектра услуг по защите информации.
- 3. В области квантовой сенсорики**, речь идет о разработке и внедрении чувствительных малогабаритных устройств для использования в навигации, геологоразведке, медицине и др.
- 4. В организационном плане** имеются существенные заделы в нескольких коллективах: - именно здесь должны концентрироваться передовые научные разработки в области квантовых технологий



СПАСИБО ЗА ВНИМАНИЕ!

МЕЖУНИВЕРСИТЕТСКАЯ КВАНТОВАЯ СЕТЬ (МУКС)

Курчатовский научный Центр, Иннопрактика, Министерство образования и науки: Консорциум



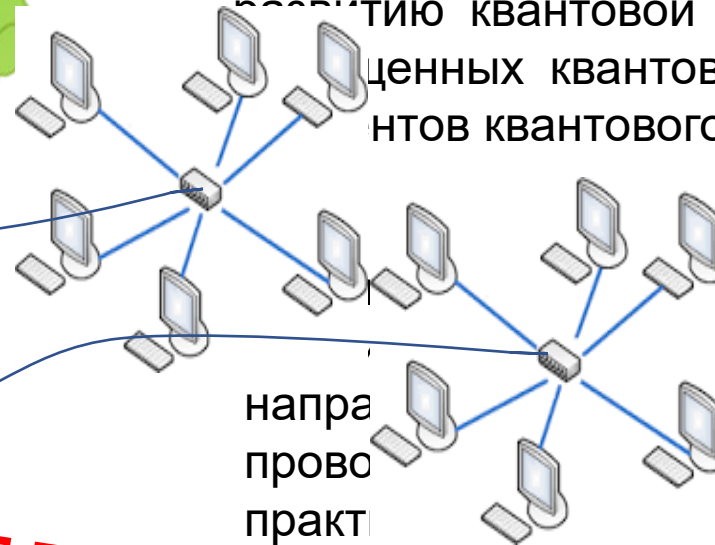
Иннопрактика



МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ И ЭКСПЛУАТАЦИИ МУКС:

- образовательные и научные проекты по развитию квантовой сети для передачи данных, ценных квантовыми ключами и разработке протоколов квантового интернета;



- пилотных проектов - инструмент апробации перспективных технологий квантовых коммуникаций, являющихся в рамках подготовки к запуску оборудования КРК и продвижения концепции квантового интернета;

- стартапы в рамках программы технологического предпринимательства.

