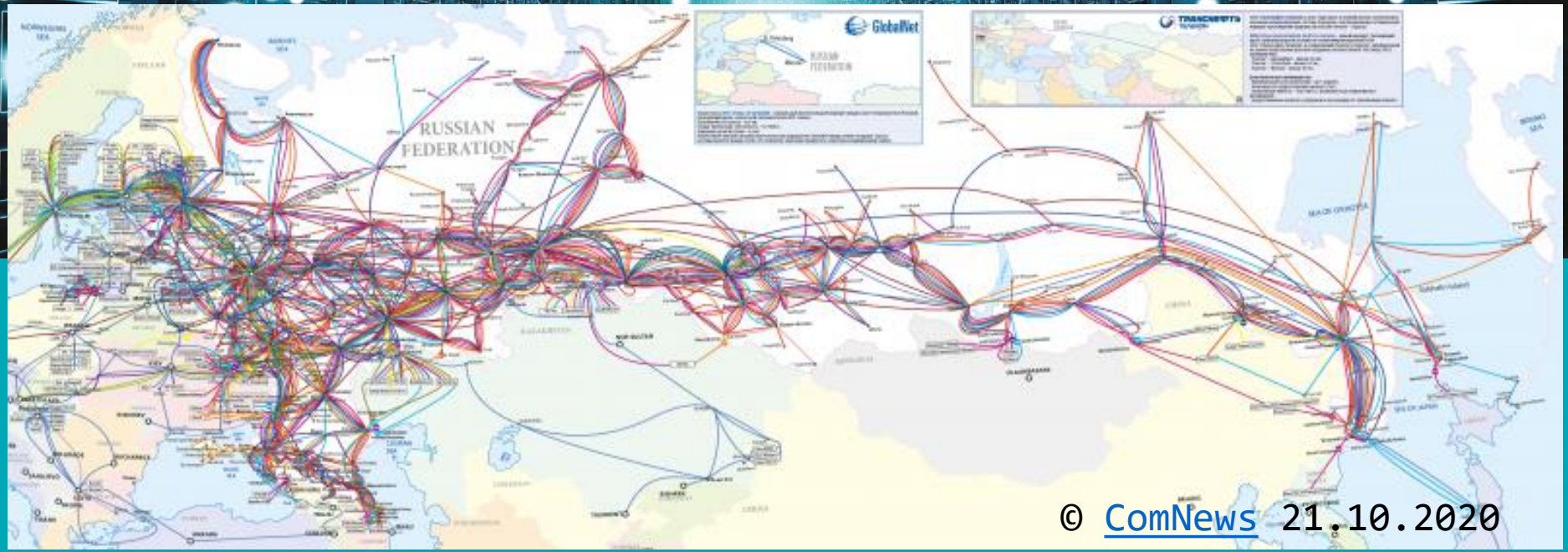
Перспективы развития технологий квантово-криптографической связи в России

Елисеев Владимир
Руководитель Центра научных исследований и перспективных разработок
11.02.2021

Магистральные сети связи в России



© ComNews 21.10.2020

Угрозы при хранении и передаче зашифрованной информации

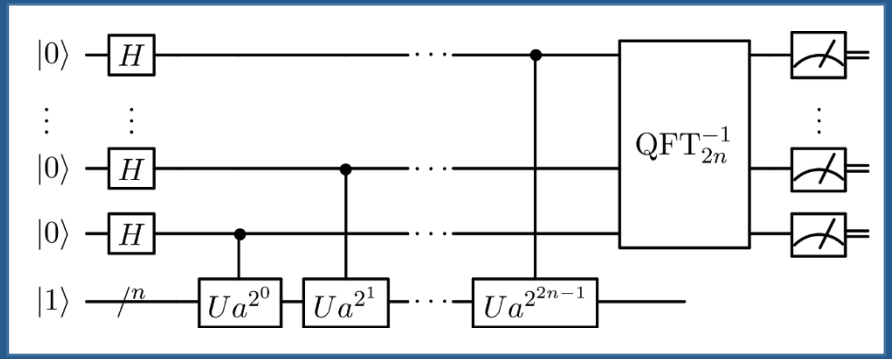
ЧТО ГРОЗИТ ДАННЫМ:

- **Расшифрование (в том числе, в будущем)**
- **Подмена**

ИСТОЧНИКИ УГРОЗ:

- **Вычислительные ресурсы злоумышленника**
  - *Линейный и дифференциальный криптоанализ*
  - *Квантовые алгоритмы Шора и Гровера*
- **Побочные каналы утечки информации о ключах**
- **Разглашение секретных ключей**

Квантовый алгоритм Шора



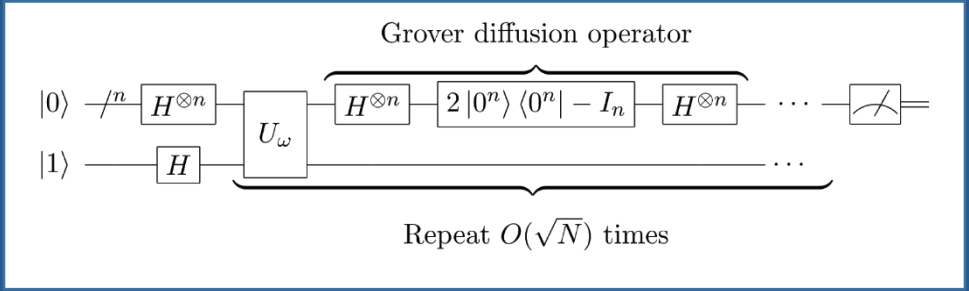
ДЕЙСТВИЕ:

Факторизация – разложение числа M на множители за время $O(Log^3M)$

КОМПРОМЕТАЦИЯ:

- Протокола Диффи-Хеллмана
- Алгоритмов электронной подписи (RSA, эллиптика)

Квантовый алгоритм Гровера



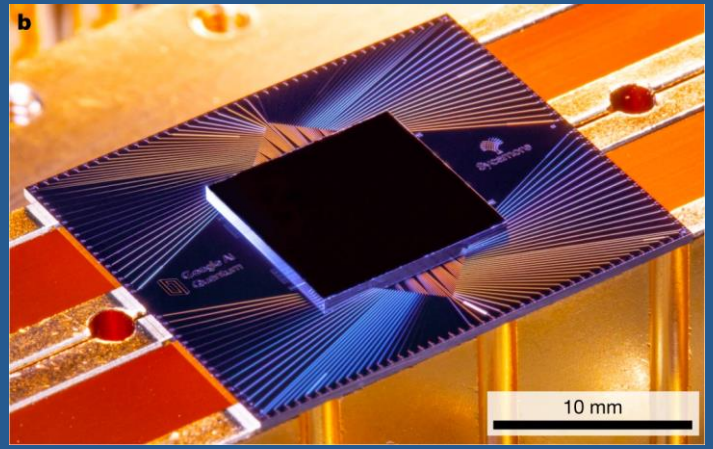
ДЕЙСТВИЕ:

Поиск по таблице за $\sqrt{N}$ попыток

ПОНИЖЕНИЕ СТОЙКОСТИ:

- Симметричных шифров
- Хэш-функций

Квантовый компьютер Google Sycamore



- 53 сверхпроводящих кубита
- Универсально программируется
- Формально показано квантовое превосходство в 2019 году

Квантовый компьютер Jiuzhang 九章算術

- 76 кубитов при комнатной температуре
- Решение узкоспециальной задачи
- Нет сомнений в квантовом превосходстве в 2020 году

Квантовое распределение ключей

- Передача информации осуществляется с помощью квантовых состояний
- Определение совпадающих битов в независимых случайных последовательностях даёт сырой ключ
- Секретность обеспечивается за счет учёта уровня ошибок в квантовом канале
- Служебный канал криптографически аутентифицируется
- Квантовый ключ распределяется на концы квантового канала

Оборудование КРК в мире и в России

IDQuantique Clavis3

Квантателеком / Системы Практической Безопасности

ИнфоТеКС ViPNet Quandor

Toshiba

QRate

Основные характеристики аппаратуры квантового распределения ключей

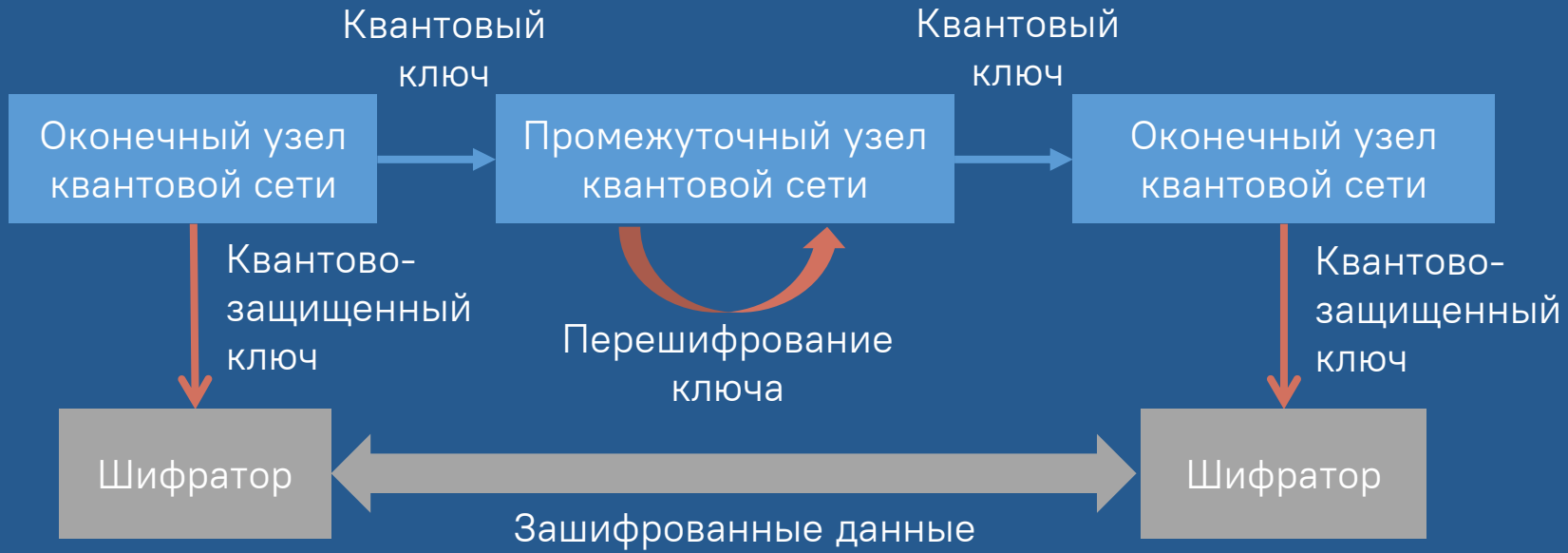
ЧИСЛОВЫЕ:

- Дальность/предельное затухание: ~100 км / ~20 дБ
- Скорость выработки квантовых ключей: 10бит/с – 1Мбит/с
- Рабочие длины волн: 1300-1600 нм

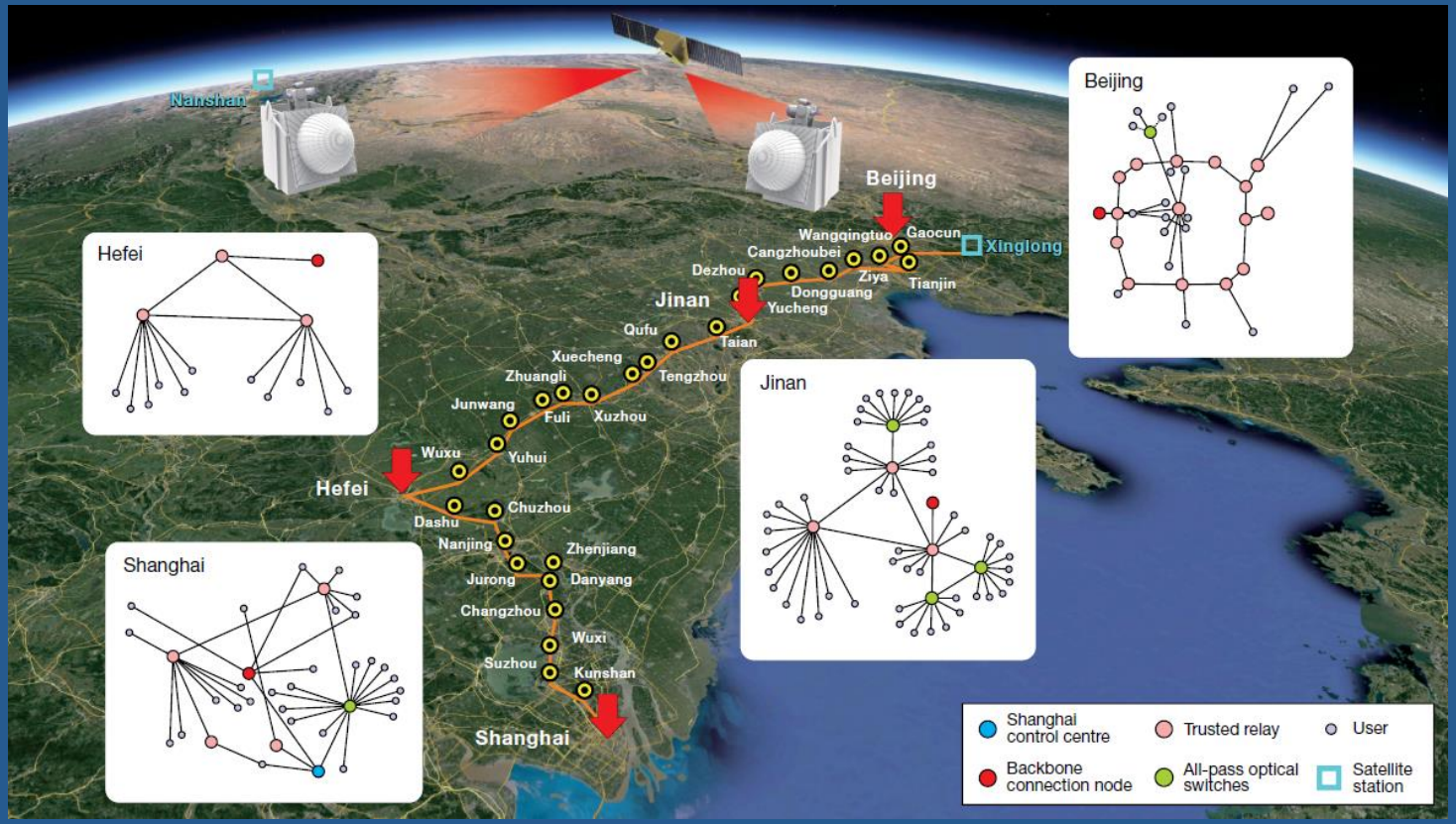
КАЧЕСТВЕННЫЕ:

- Вид датчика случайных чисел: программный, физический
- Доказуемая стойкость квантового протокола
- Следование правилам разработки и исследования СКЗИ
- Стойкость к атакам на квантовую аппаратуру
- Сопряжение с шифраторами

Принцип работы многосегментной сети КРК с доверенными узлами



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



Квантовая сеть Китая

400 сегментов + 2 спутника

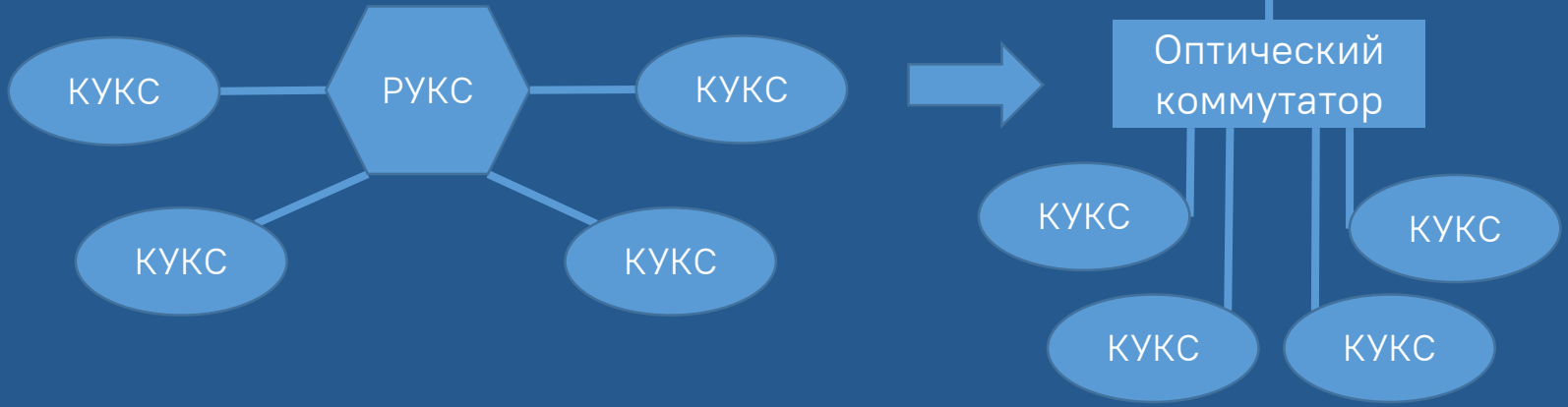
4800 км общая протяженность

157 потребителей

Базовые элементы квантовых сетей

- Магистральный узел квантовой сети (МУКС)

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



Стандартизация технологий КРК

ОБЪЕКТЫ СТАНДАРТИЗАЦИИ:

- Квантовые протоколы – пока неактуально
- Интерфейс и протоколы взаимодействия с СКЗИ
- Методология изучения и оценки свойств аппаратуры

ОРГАНИЗАЦИИ ПО СТАНДАРТИЗАЦИИ:

- ETSI – наиболее многочисленные проекты стандартов по КРК
- ITU-T – аспекты совмещения сетей и сетей КРК
- ISO – требования по безопасности, методы проверки и аттестации
- Росстандарт (рабочая группа ТК-26 по квантовой криптографии):
  - Разработка методических рекомендаций по интерфейсу между СКЗИ и КРК
  - Разработка МР по ключевой системе квантовой сети топологии «звезда»
  - Разработка МР по ключевой системе квантовой сети топологии «граф»

Разработка методических рекомендаций в ТК-26

Разработка методических рекомендаций по интерфейсу между СКЗИ и КРК

Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации (**ProtoQa**)

Разработка МР по ключевой системе квантовой сети топологии «звезда»

Разработка МР по ключевой системе квантовой сети топологии «граф»

Выигран конкурс РЖД на выполнение работ по стандартизации

Аппаратура криптографической защиты информации с КРК

ViPNet Quandor

Два шифратора L2-10G

- 10Гбит/с, полный дуплекс
- ГОСТ 34.12-2018 «Кузнечик»
- Задержка <50 мкс

Аппаратура КРК

- Дальность >100 км (>20дБ)
- Скорость выработки КК >256бит/мин
- Длина волны 1520 нм
- Прошла испытания:
  - ✓ Механические
  - ✓ Климатические
  - ✓ ЭМ-совместимость
  - ✓ Тематические

Аппаратура криптографической защиты информации с КРК

ViPNet Quantum Security System

Оптический коммутатор – ViPNet QSS Switch

Сервер квантового распределения ключей – ViPNet QSS Server

Потребители ключей. IP-телефоны – ViPNet QSS Phone

Клиент квантового распределения ключей – ViPNet QSS Point (до 800 шт к одному серверу)

Спасибо за внимание!

Владимир Елисеев

Руководитель Центра научных исследований и перспективных разработок

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow

11.02.2021