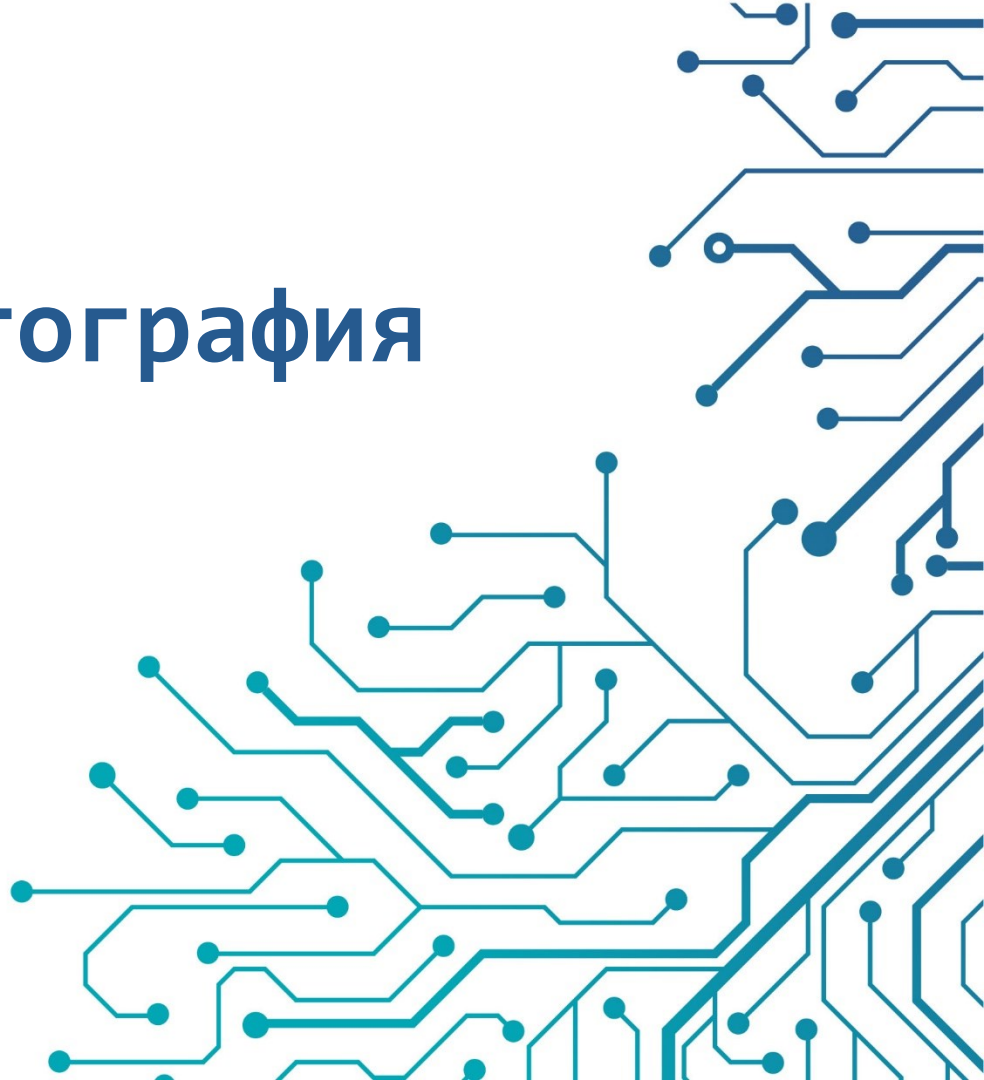
Квантовая криптография

Андрей Жиляев
Старший исследователь
Центра научных исследований
и перспективных разработок

Andrey.Zhilyaev@infotecs.ru



Квантовые технологии

Квантовые технологии: инструменты хранения, обработки и передачи информации и решения задач посредством квантово-механических систем, состоящих из (ансамблей) **одиночных квантовых объектов.**

Квантовые вычисления:

- задачи оптимизации;
- синтез новых материалов;
- криптографические задачи.

Квантовые коммуникации:

- оптоволоконные каналы;
- свободное пространство (атмосфера, космические каналы).

Квантовая сенсорика:

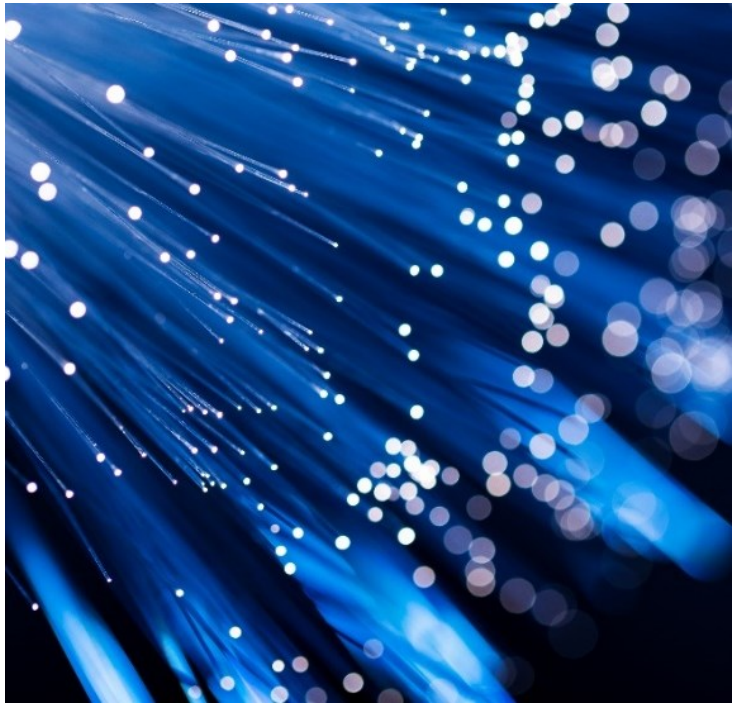
- магнитометры, гравиметры, акселерометры;
- атомные часы, квантовая метрология.

Квантовые коммуникации

Квантовые коммуникации – область знаний/техники о **передаче квантовых состояний** между удаленными объектами:

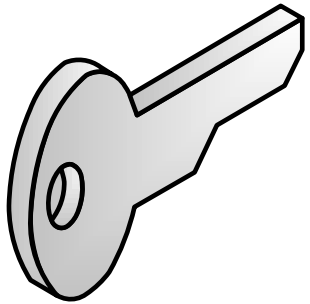
- квантовые репитеры
- квантовая память
- квантовая телепортация
- сверхплотное кодирование
- квантовое распределение ключей

Наибольшее практическое развитие получило **квантовое распределение ключей – КРК.**



Проблемы практической криптографии

- Генерация случайных чисел
- Защищенные реализации криптографических механизмов
- **Управление ключами** – совокупность процедур и процессов, сопровождающих жизненный цикл ключей в (крипто) системе:
  - генерация;
  - **установление/транспортировка;**
  - архивирование/восстановление;
  - использование/хранение;
  - **смена;**
  - вывод из эксплуатации.



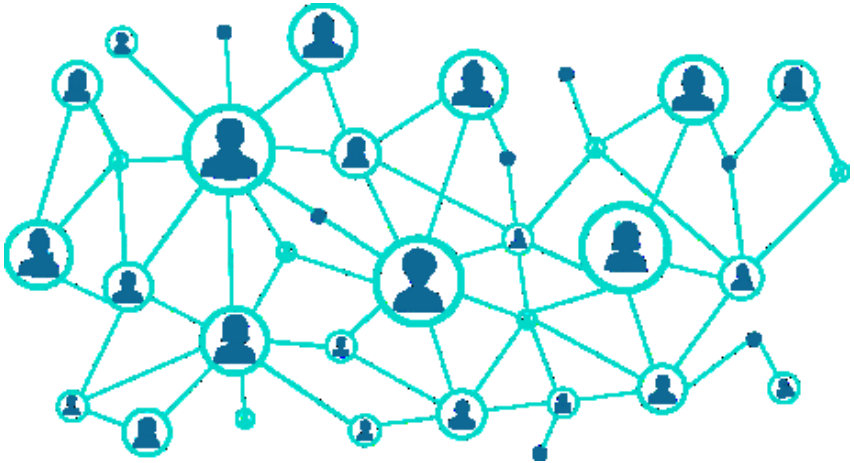
Смена ключей? Зачем?

Для
- каждого шифра
- в конкретном режиме работы
- для конкретной реализации

имеется предельное количество данных, которые допустимо зашифровать на одном ключе – **нагрузка на ключ**.

- Если больше? Появляется возможность различения (distinguishability) от идеального шифра.
- Если еще больше? Появляются конкретные атаки: восстановление неизвестного открытого текста, ключа и т.д.

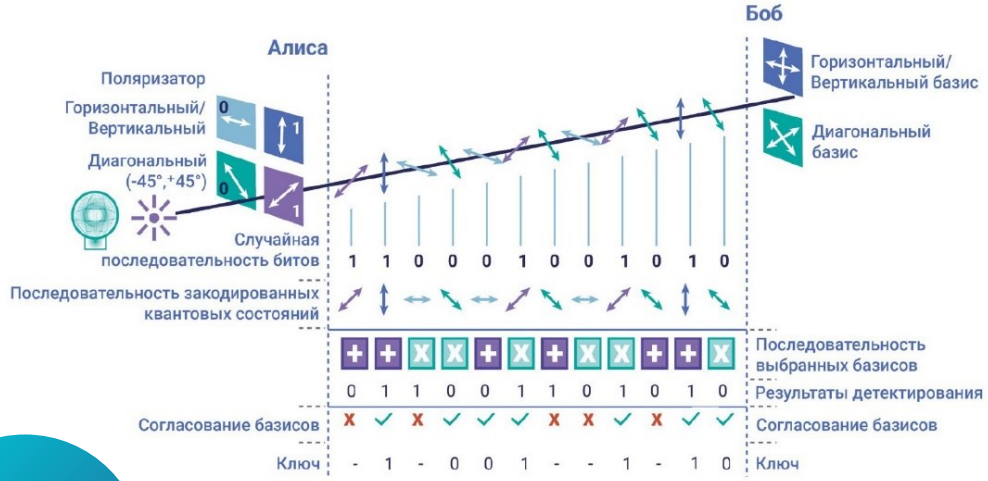
Механизмы выработки и распределения ключей



Задача: получить общий парный секретный ключ (в сети абонентов)

- доверенная доставка (предраспределенные ключи)
- выработка общего ключа по открытому каналу (протокол Диффи-Хеллмана)
- **квантовое распределение ключей**

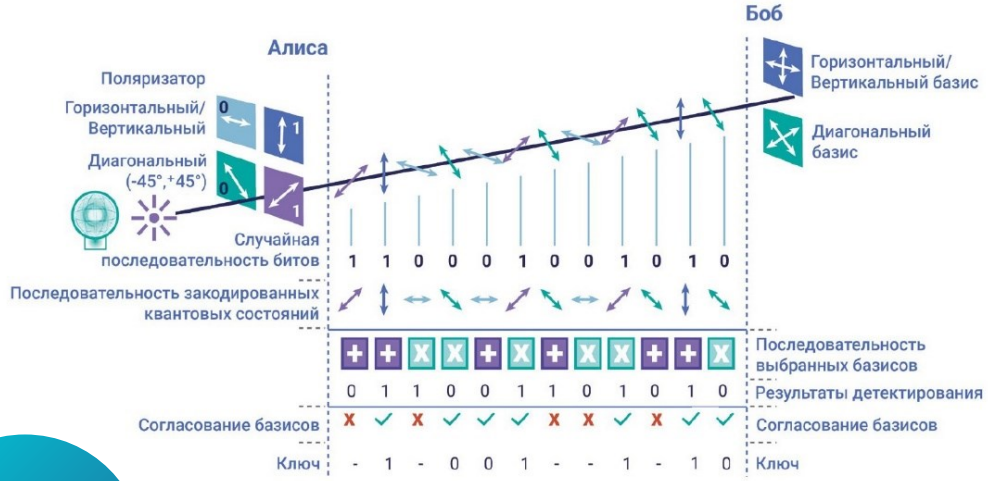
Квантовое распределение ключей



Квантовое распределение ключей (КРК) – криптографический протокол, позволяющий двум удаленным абонентам, использующим независимые энтропийные источники, выработать общий случайный секрет – секретный ключ.

Теорема о запрете клонирования неизвестного квантового состояния позволяет гарантированно детектировать пассивного/активного злоумышленника, пытающегося получить ключ.

Протокол BB84



Два абонента:

- Генерируют по случайной битовой строке
- Обмениваются квантовыми состояниями
- Выбирают совпадающие части переданных и принятых строк – выработка общего секрета

КРК: Типовая схема

КРК: Практические аспекты

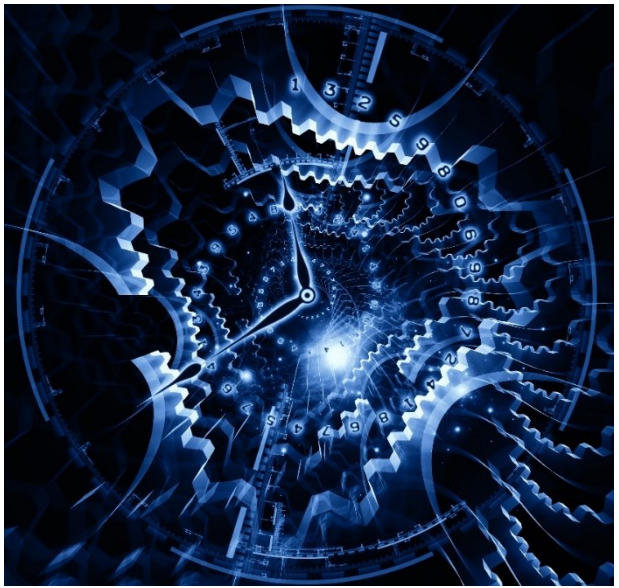
Достоинства:

- **теоретическая абсолютная стойкость**
- **у администратора системы защиты нет доступа к ключам**
- высокая скорость выработки ключей
- полностью автоматическая работа

Ограничения:

- **ограниченная дальность** функционирования
- относительно высокая стоимость оборудования
- топология «точка-точка»

КРК: Текущий уровень и перспективы



Расстояние

- до 100 км – типовое темное волокно, «сухой» детектор;
- до 500 км – спец. волокно, сверхпроводящий детектор.
- 7000 км - спутники

Скорость выработки ключа

типовая – килобиты/с на 50 км волокна;

достижимые:

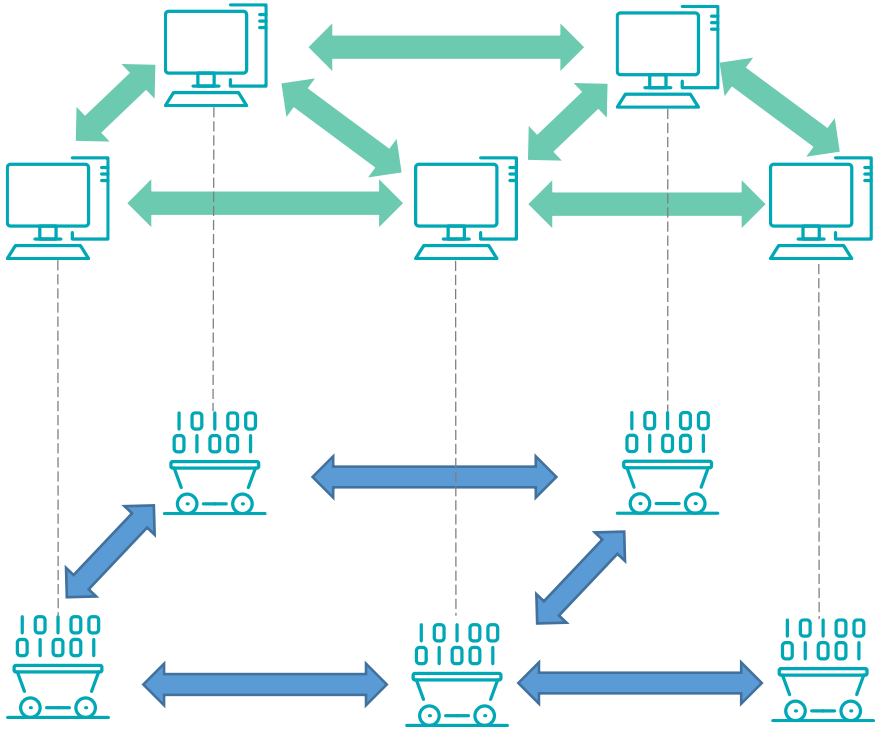
- мегабиты/с в волокне;
- килобиты/с на 1 км воздуха;
- биты/час на низкоорбитальных спутниках.

Массогабариты

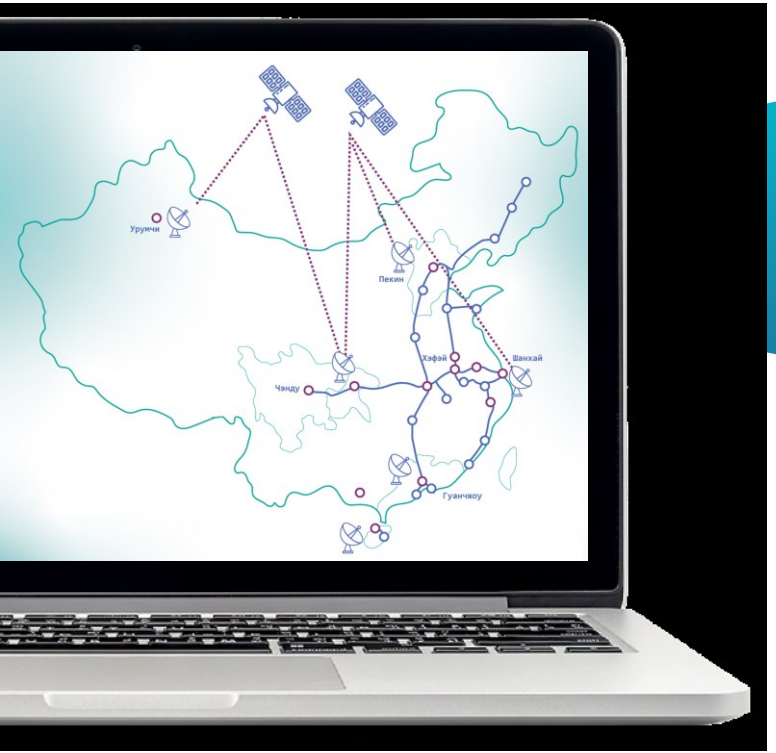
- типовые – сервер 1U-4U;
- достижимые – 5’-CD-ROM;
- перспектива – кредитная карта.

Сети квантового распределения ключей

- Некоторые узлы сети связаны квантовыми каналами
- Сеть полносвязная на классическом уровне
- Создание общего ключа на основе квантовых ключей последовательных сегментов



Современный уровень систем КРК



Достигнутый в России международный уровень:

- Серийная аппаратура КРК
- Квантовые сети масштаба государства
- Научные центры и образовательные программы
- Технические стандарты

Актуальные задачи:

- КРК через спутники
- Элементная база технологии КРК
- Массовые сервисы на основе технологии КРК

Мифы и факты

- **Квантовый шифратор лучше обычного?!**
  Шифраторы сегодня классические,
  но ключи получены из квантового протокола.
- **Квантовый ключ лучше обычного?!**
  Ключ – бинарная строка.
  Источник ключа может быть разного качества.
- **Квантовое распределение ключей абсолютно стойкое?!**
  В теории – да,
  конкретные технические реализации могут иметь недостатки.
- **Постквантовые криптомеханизмы решают проблему появления квантового компьютера?!**
  Неизвестно! Есть ли алгоритмы взлома на квантовом компьютере - неизвестно, но и не доказано, что их не будет.
- **КРК позволяет реализовать одноразовый шифрблокнот (абсолютно стойкий шифр)?!**
  Возможно, для небольших скоростей.
  Для 1 бита квантового ключа
  необходимо 1000000 исходных бит в протоколе КРК.

Ответы на вопросы

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363