Технология квантового распределения ключей - хайп или реальная ценность?

Александр Поздняков

Ключевая проблема

Базовые практические задачи криптографии

1. Генерация качественных случайных чисел
2. Защищенные реализации криптографических алгоритмов
3. Управление ключами - совокупность процедур и процессов, сопровождающих жизненный цикл ключей в (крипто) системе:
   - Генерация
   - Установка или транспортировка
   - Архивирование или восстановление
   - Использование или хранение
   - Смена
   - Вывод из эксплуатации

Тенденции развития телеком сетей и угроз ИБ

- Увеличение объемов и скоростей передачи информации: 10 Гбит/с → 100 Гбит/с
- Развитие распределенных вычислительных систем
- Увеличение доли оптики на «последней миле»
- Быстрая выработка нагрузки на ключ
- Отложенный взлом
- Создание эффективного квантового компьютера
- Компрометация сети администратором

Ключи

«Враг знает систему» © Клод Шеннон

ТЕХНО infotecs 2019 ФЕСТ

То есть:

- Секретность алгоритмов шифрования и аппаратной реализации **не определяют** стойкость криптосистемы
- Стойкость криптосистемы определяется лишь **секретностью ключа**

Откуда взять ключ?

Существующие механизмы

1. Доверенная доставка (предраспределенные ключи)
2. Кодовое зашумление
3. Выработка общего ключа по открытому каналу
4. Защищенный транспорт ключей
5. Предварительное распределение ключей
6. Квантовое распределение ключей

Проблемы всех классических механизмов распределения ключей

- Не обеспечивается безусловная секретность ключей
- Дорогостоящие организационно-технические меры
- Всегда есть «человеческий фактор»
- Создание квантового компьютера приведет к компрометации всех ассиметричных криптографических алгоритмов и протоколов на их основе (DH, RSA, ECDSA TLS/SSL, HTTPS, IPsec, X.509)

Зачем нужна быстрая смена ключей?

Для
- конкретного алгоритма шифрования
- в конкретном режиме работы
- для конкретной реализации СКЗИ

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

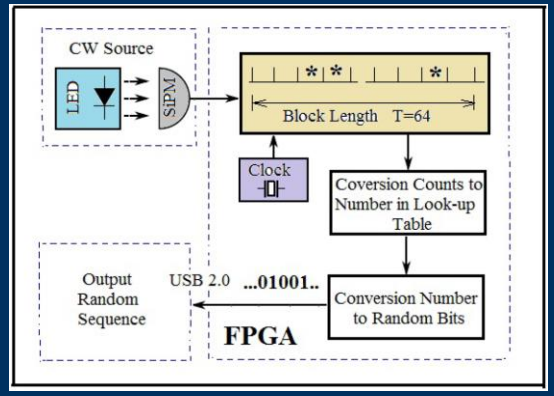
Пример – Алгоритм блочного шифрования по ГОСТ 28147-89
- Размер блока n = 64
- Предельная теоретическая нагрузка $2^{64/2} = 2^{32}$ блоков шифртекста, или 256 Гбит данных
- Шифратор на скорости 10 Гбит/с израсходует ключ за 25 секунд

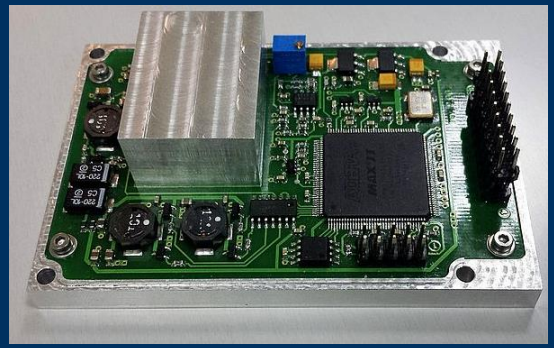
Генерация случайной последовательности

Истинная приватность

Квантовый датчик случайных чисел:

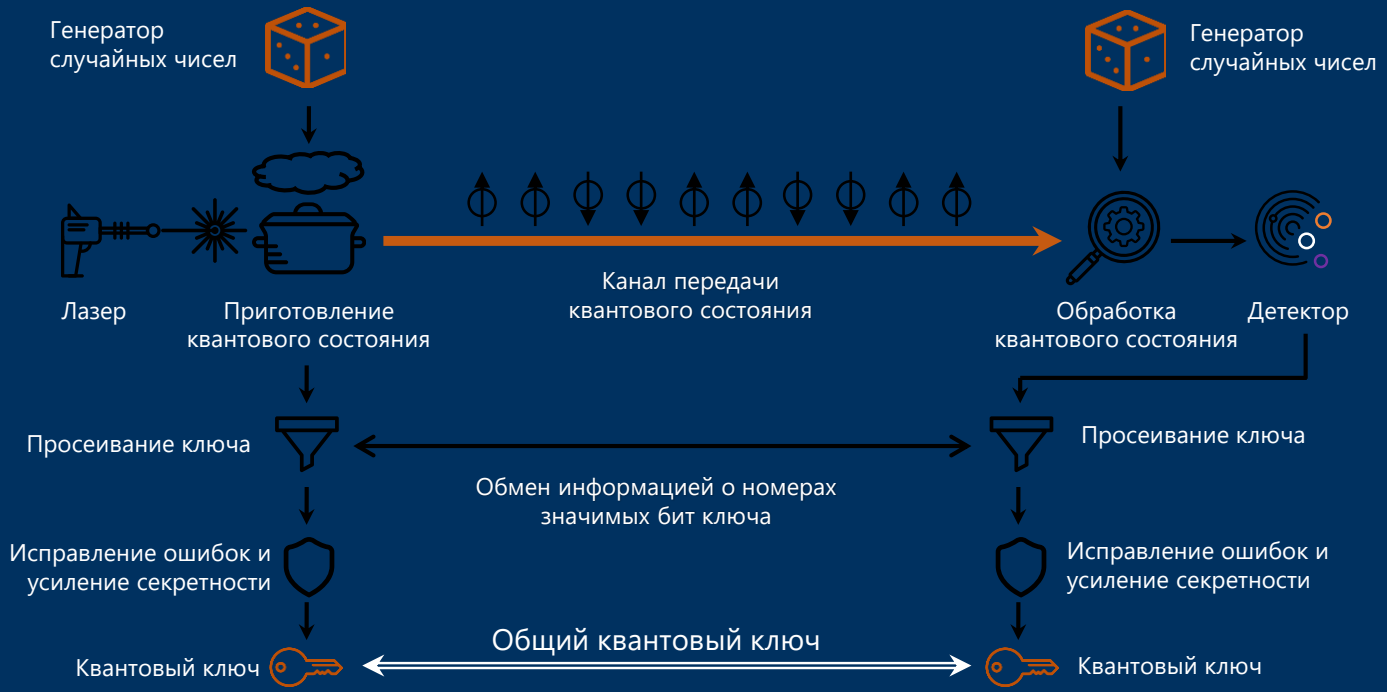
- Скорость генерации:
  200 000 000 квантовых отсчетов –
  400 бит секретного ключа на 100 км
- Источник случайности фотоотсчеты от квазиоднофотонного излучения, регистрируемые матрицей кремниевых лавинных детекторов (SiPM)





Технология квантового распределения ключей

Квантовое распределение ключей
Принцип действия

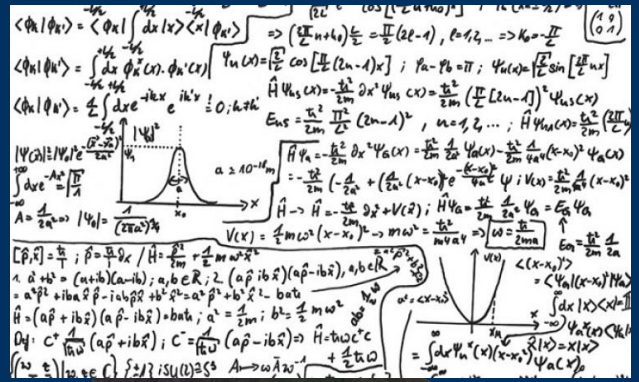


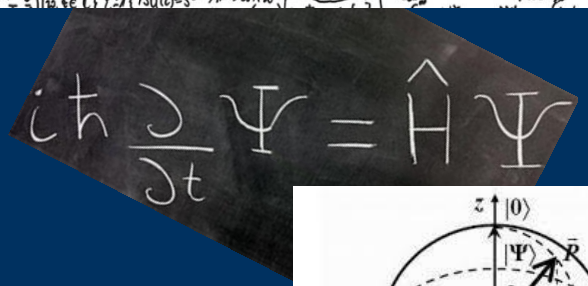
- Передача информации осуществляется с помощью квантовых состояний
- Определение совпадающих битов в независимых случайных последовательностях дает сырой ключ
- Секретность обеспечивается за счет учета уровня ошибок в квантовом канале
- Служебный канал аутентифицируется
- Квантовый ключ распределяется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

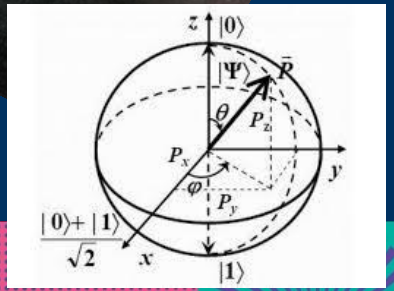
В чем «квантовость»?

Секретность выработки квантовых ключей основана на следующих квантовых принципах:

1. Фотон неделим
2. Невозможно клонировать неизвестное квантовое состояние
3. Невозможно измерить квантовое состояние без его изменения (редукция волновой функции)
4. Невозможно различить два неортогональных квантовых состояния

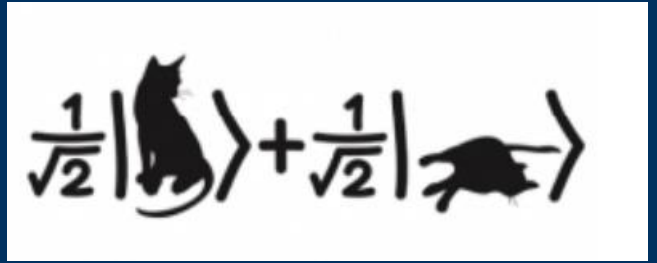


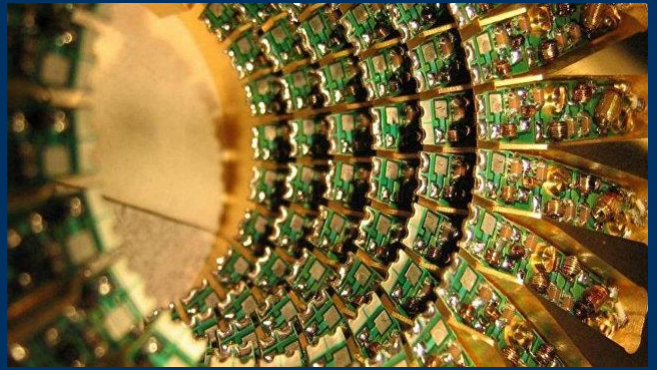




Преимущества КРК

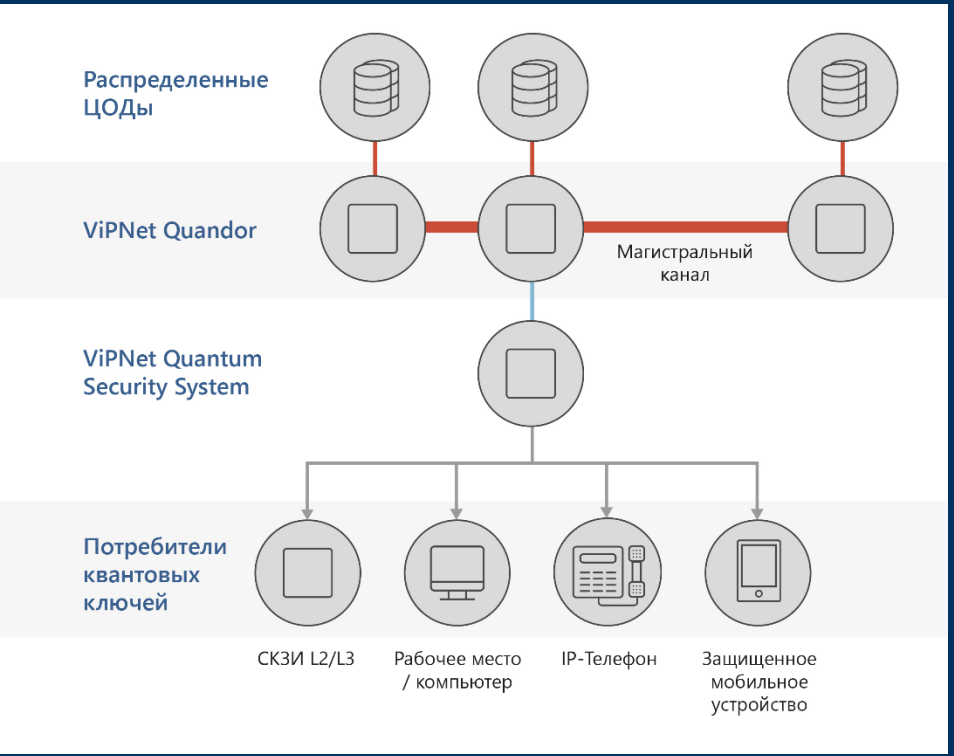
1. Секретность квантовых ключей доказана математически
2. Выработка ключей происходит автоматически без участия администратора
3. Устойчив к квантовому компьютеру
4. Высокая скорость генерации





Квантовые продукты ИнфоТеКС

Концепция развития технологии квантового распределения ключей в компании



- Квантовая сеть произвольной топологии
- Ключи с доказательством секретности
- Не используется ни одного асимметричного криптографического механизма
- Ключи защищены от компрометации администратором сети
- Компрометация возможна только в период развертывания системы
- Автоматическая смена ключей шифрования 1 раз в минуту

Первые промышленные образцы

ТЕХНО infotecs ФЕСТ 2019

ViPNet Quantum Security System

ViPNet Quandor

ViPNet QSS Phone

ViPNet QSS Server

ViPNet QSS Point

ViPNet QSS Switch

Спасибо!

ТЕХНО 2019 infotecs Фест

Александр Поздняков
Менеджер продуктов
Aleksandr.Pozdnyakov@infotecs.ru
ОАО «ИнфоТеКС»