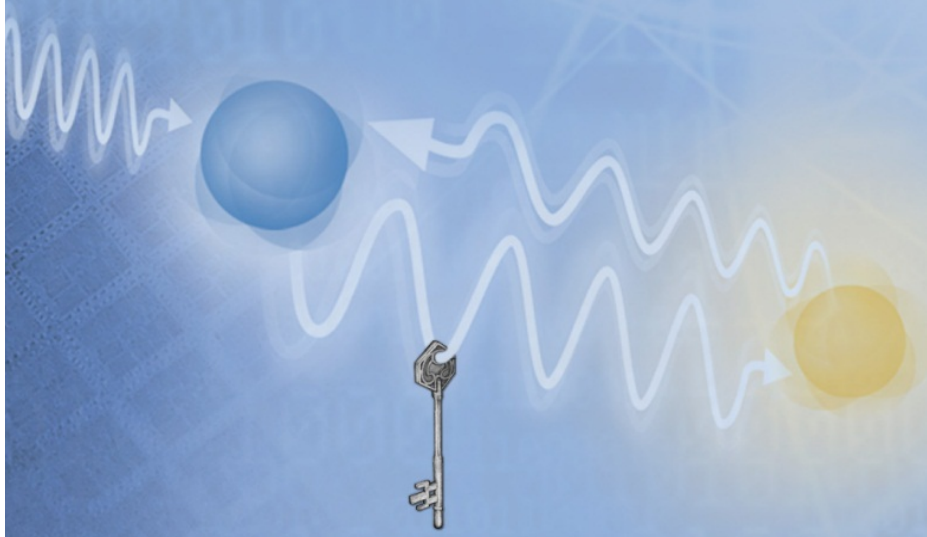
PKI-FORUM 2012

ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

ТТИ ЮФУ

ИБТКС

Квантовая криптография: … вчера, сегодня, завтра …



к.т.н., доцент кафедры
информационной безопасности
телекоммуникационных систем (ЮФУ)

Горбунов Александр Валерьевич

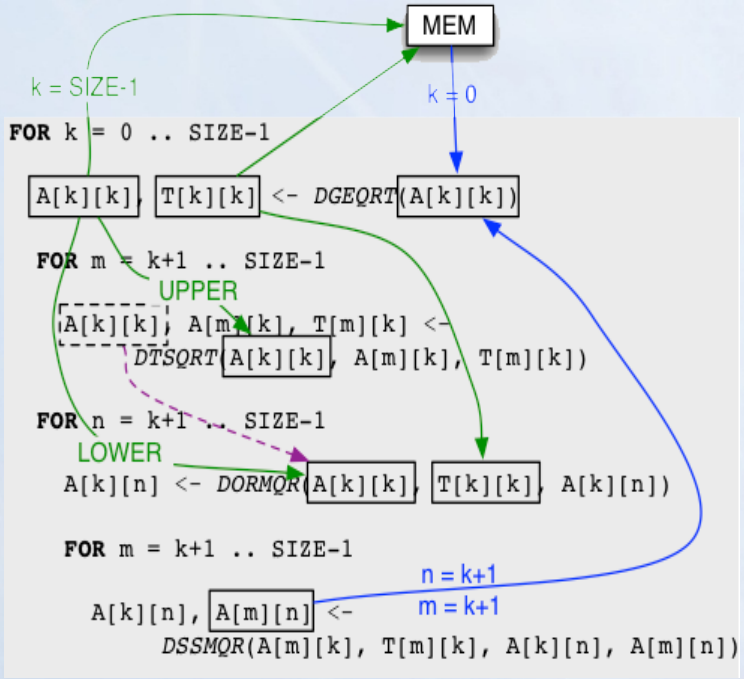
ассистент кафедры
информационной безопасности
телекоммуникационных систем (ЮФУ)

Голубчиков Дмитрий Михайлович

Классическая криптография

Защищённость классической криптографии строится на уверенности в том, что

- **злоумышленник не успеет** за разумное время «взломать» шифр ввиду сложности используемых математических алгоритмов



Квантовый компьютер →
→ Проблемы классической криптографии

- **алгоритм Дойча-Джоза** (1995 год) – квантовый алгоритм проверки функции на детерминированность и сбалансированность
- **алгоритм Гровера** (1996 год) – квантовый алгоритм решения задачи перебора
- **алгоритм Шора** (1994 год, практическая реализация – 2001 год) – быстрый квантовый алгоритм разложения числа на простые множители (полиномиальная скорость) и **квантовое преобразование Фурье**

Этапы развития квантового компьютера

- 1981 год - предложена **модель квантового компьютера** и созданы теоретические основы построения
- 2000 год – **квантовый компьютер из 1-го кубита**
- 2001 год – квантовый компьютер из **2-х** кубит
- 2003 год – квантовый компьютер из **7-и** кубит
- 2005 год – квантовый компьютер из **10-и** кубит

?

Фирма D-Wave:

- февраль 2007 года – **16** кубит
- ноябрь 2007 года – **28** кубит
- май 2011 года – **128** кубит (коммерческий образец стоимостью $10 млн.)

Надёжность алгоритма RSA

- В 2003 году продемонстрировано разложение числа 15=5×3 на простые множители с помощью квантового компьютера из 7-и кубит.
- Создание квантового компьютера с высокой разрядностью сделает **операцию факторизации чисел сопоставимой по сложности с операцией умножения!**
- По мнению Питера Шора (автора квантового алгоритма факторизации) на создание полнофункционального квантового компьютера **потребуется несколько десятков лет.**

Классическая и квантовая криптография: Разница в подходах

Защищённость квантовой криптографии строится на утверждении, что

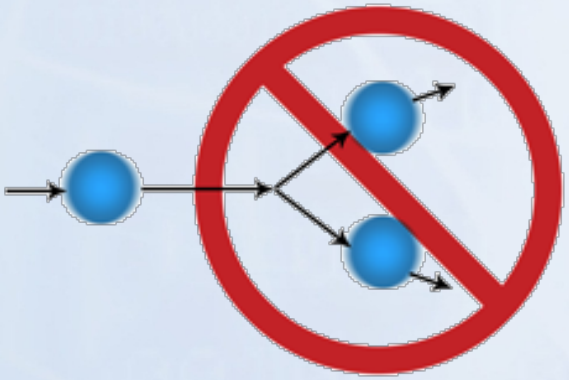
- **никто не сможет** «взломать» шифр, так как это противоречит физическим законам природы (с точки зрения их понимания на текущем этапе развития науки)

Идеи, положенные в основу квантовой криптографии

Передача информации осуществляется с помощью элементарных квантовых объектов – одиночных фотонов.

Системы квантовой криптографии по определению способны обнаруживать подслушивание, так как попытка измерения взаимосвязанных параметров в квантовой системе разрушает исходные состояния.

Теорема о запрете клонирования (1982 год): создание идеальной копии произвольного неизвестного квантового состояния **невозможно !**



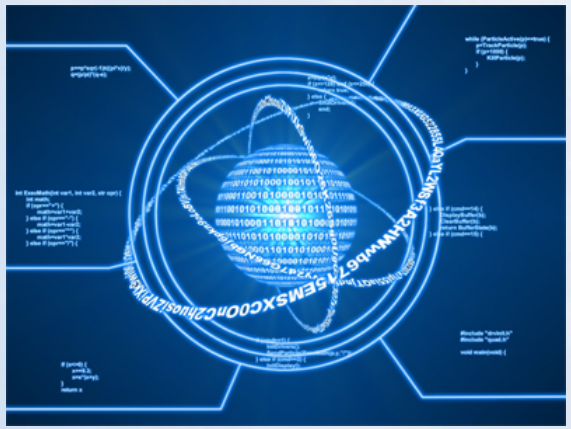
Направления исследований в квантовой криптографической науке

Практическое направление:

- **QKD** – квантовое распределение ключей

Теоретические направления:

- **QSDC** – квантовая защищенная прямая связь
- **QSS** – квантовой разделение состояний
- **QSC** – квантовой поточное шифрование
- **QS** – квантовая стеганография
- **QKI** – инфраструктура квантовых ключей
- **QDC** – квантовая цифровая подпись



Квантовое распределение ключей (QKD)

Цель:

- формирование между двумя пользователями гарантированно секретных ключей

Применение:

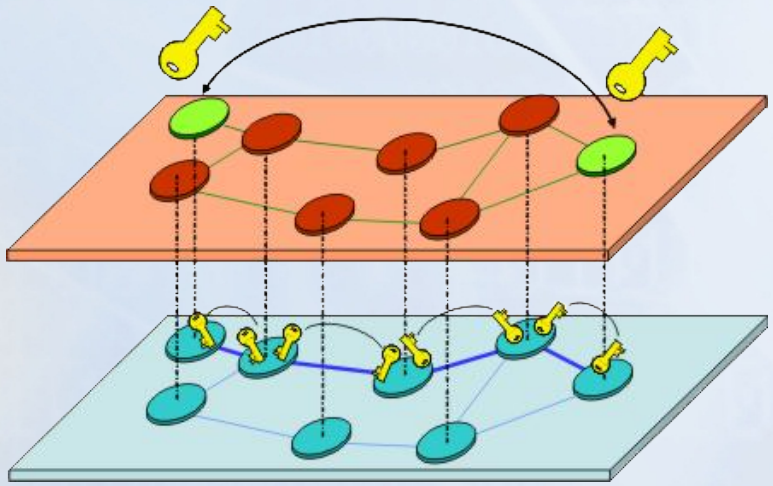
- симметричное шифрование

Защищённость:

- любое «подслушивание» будет замечено

Производительность:

- до мегабита в секунду



История развития QKD

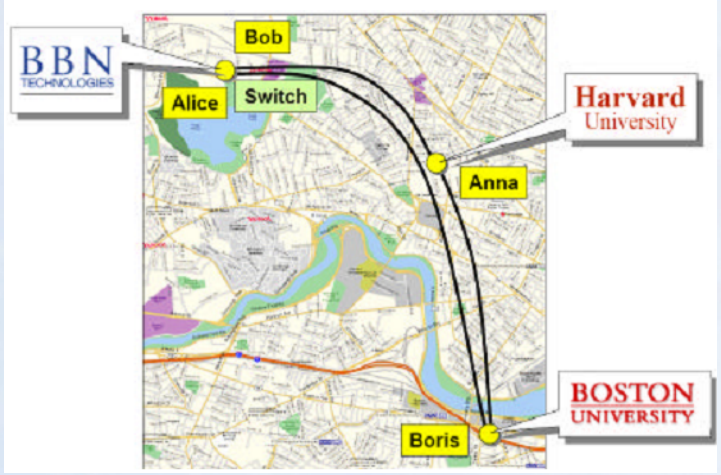
- **1927 год -** принцип неопределённости Гейзенберга
- **1970 год** – идея защиты информации с помощью квантовых объектов (Stephen Wiesner)
- **1984 год** – первый алгоритм (BB84) квантового распределения ключей (Charles Bennett, Gilles Brassard)
- **1989 год** – первая работающая квантово-криптографическая схема на расстояние 32 см (IBM, США)
- **1990-е годы** – алгоритмы E91 и B92, достижение расстояний в 23 км и скоростей в единицы Кбит/с, доказана возможность использования явлений квантовой запутанности
- **2000-е годы** – алгоритмы SARG04, KMB09, COW, DPS, достижение расстояний в 87 км и скоростей в сотни Кбит/с, построение систем по типу «Plug and Play» («Подключай и работай»)

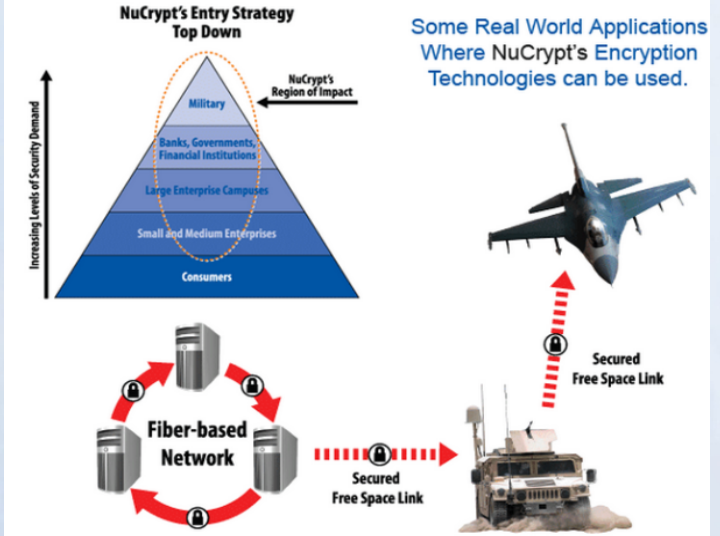
Разновидности реализаций систем QKD

- с **фазовым** и **поляризационным** кодированием состояний фотонов
- с передачей фотонов **по оптическому волокну** и **через атмосферу**
- с использованием **одночастичных состояний** и явлений **квантовой запутанности**
- на основе алгоритмов **BB84**, **E91**, **B92**, **SARG04**, **KMB09**, **COW**, **DPS, Decoy, Y00, CV** и др.

Военные проекты в области QKD и квантовой криптографии

- **Quantum Network Project** (BBN, DARPA)
- **AlphaEta** (NuCrypt)
- **SQ Fiber Shield** (SmartQuantum)





Коммерческие образцы систем QKD

- **id 3100 Clavis2,**
  id 5100 Cerberis
  (Швейцария)

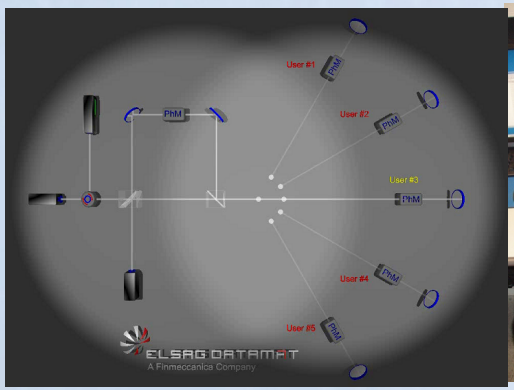
- **Quantum Link Encryptor**
  (Австралия)

- **MagiQ QPN 5505,**
  MagiQ QPN 7505
  MagiQ QPN 8505
  (США)

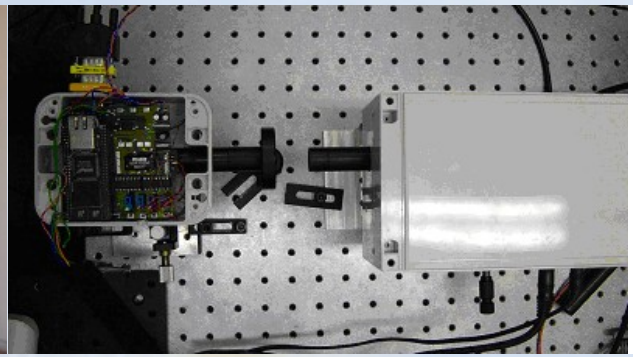
- **SQ Box** (Франция)

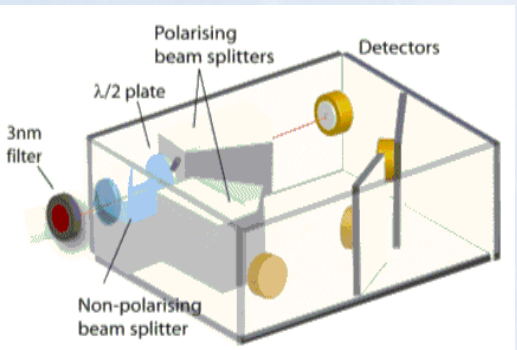
Пользовательские системы QKD

- **Q-KeyMaker**



- **Low cost secure key exchange for consumer protection**





Примеры внедрения систем QKD на муниципальном и государственном уровне

- **2004 год** - проект «DARPA Quantum network» - сеть квантового распределения ключей из 10-и узлов (США)
- **2007 год** – повсеместное использование квантовой криптографии на выборах в Швейцарии
- **2008 год** – первая сеть «SECOQC» (6 узлов с общей протяжённостью линий связи в 200 км), полностью защищённая системами квантовой криптографии (Австрия)
- **2009 год** – построение полномасштабной сети «SwissQuantum» (Женева, Швейцария) для тестирования работоспособности и надёжности систем квантовой криптографии в «полевых» условиях в течение длительного времени
- **2010 год** – проекты «Quantum City» и «Quantum Stadium» (ЮАР, чемпионат мира по футболу 2010)
- **2011 год** – проект «Tokyo QKD Network» для квантового шифрования телекоммуникационных систем

Примеры внедрения систем QKD в коммерческих предприятиях

Банки:

- Notenstein Private Bank (Швейцария)
- Swissquote Bank (Швейцария)
- Hyposwiss Private Bank (Швейцария)
- Global Bank (Швейцария)

Коммерческие частные компании:

- Battelle's System Heralds (США)
- Bloombase Extends Enterprise (США)
- Colt (Великобритания)
- Cygate (Швеция, Финляндия)

Кто владеет технологиями QKD ?

Производители:

- id Quantique, Inc. (Швейцария)
- MagiQ Technologies, Inc. (США)
- SmartQuantum, Inc. (Франция)
- QuintessenceLabs, Pty Ltd (Австралия)

Исследователи:

- IBM
- QinetiQ
- MITSUBISHI
- TOSHIBA
- hp
- NEC
- NTT

Открытые отечественные разработки

Молотков Сергей Николаевич

Кулик Сергей Павлович

- Институт физики твердого тела РАН, Черноголовка,
- Факультет вычислительной математики и кибернетики, МГУ им. М. В. Ломоносова, Москва

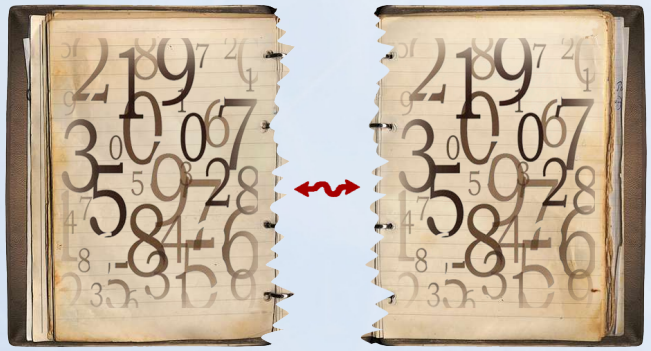
Игорь Рябцев

- Института физики полупроводников им. А.В.Ржанова СО РАН

Защищённость криптографических систем с QKD

Защищённость квантовых каналов связи базируется на использовании фундаментальных физических законов

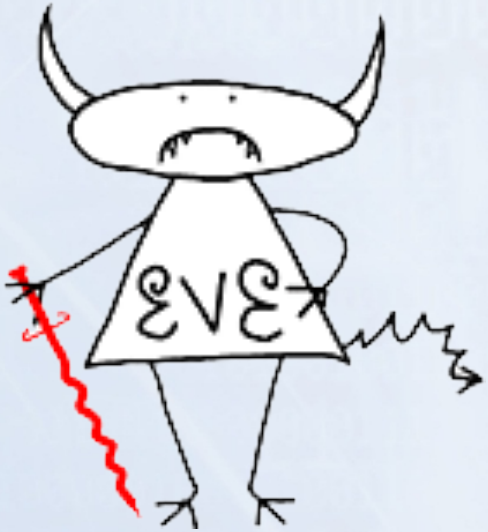
Криптосистемы с использованием квантового распределения ключей позволяют обеспечить **практическую реализацию алгоритма одноразового блокнота**



При соответствующей технической реализации систем квантовой криптографии получение несанкционированного доступа к передаваемой информации **невозможно !**

Виды атак на системы QKD

- **Intercept and resend** – перехват и пересылка новых фотонов (что приводит к повышению на 25% ошибок в основном канале)
- **Man-in-the-middle** – «Человек посередине»
- **Photon number splitting** – при отсутствии идеальных источников одиночных фотонов злоумышленник теоретически может ответвлять часть фотонов из двух- и более фотонных импульсов, оставаясь не замеченным

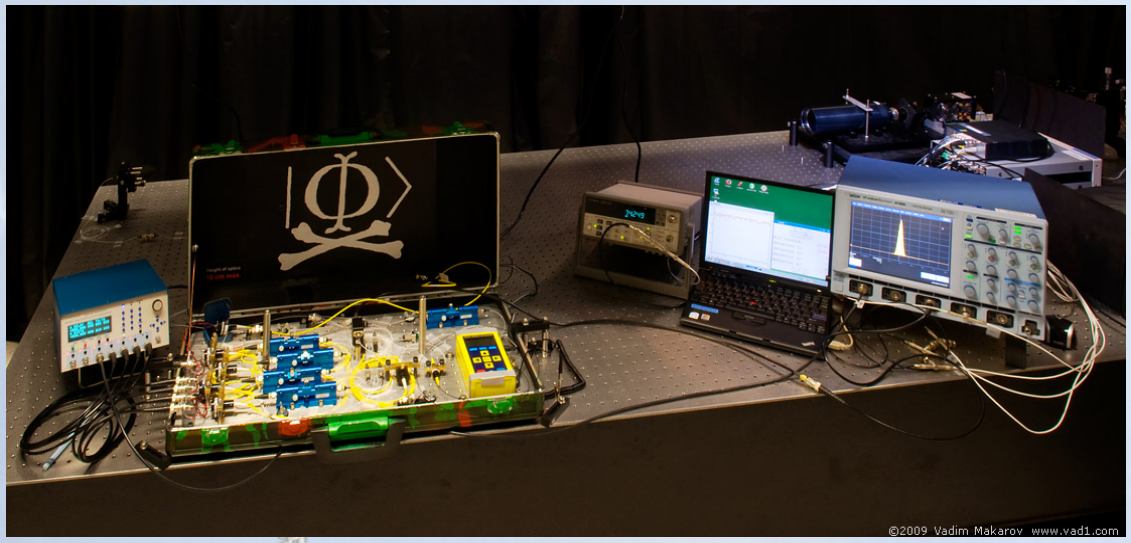


- **Denial of service** – отказ в обслуживании (обрыв линии связи, «ослепление» детекторов и т.п.)

Примеры успешных атак на системы QKD

- **2009-2011 года** – первые примеры практического осуществления успешной атаки на систему квантового распределения ключей, **использующие технические недоработки** конкретных коммерческих реализаций

  Примеры атак показаны **Вадимом Макаровым** и группой «**Quantum Hacking Group**» на базе университетов и исследовательских центров в Норвегии, Германии, Сингапуре и Канаде

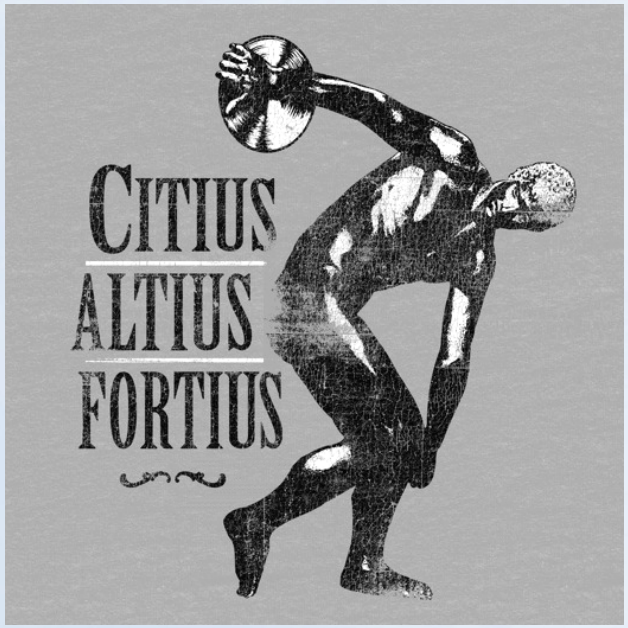


Стандартизация систем QKD (ETSI QKD)

- **ETSI GS 002. QKD**.
  Назначение и примеры использования
- **ETSI GS 003. QKD**.
  Компоненты и внутренние интерфейсы
- **ETSI GS 004. QKD**.
  Интерфейсы приложений
- **ETSI GS 005. QKD**.
  Доказательства безопасности
- **ETSI GS 006. QKD**.
  Интеграция с оптическими сетями (preprint)
- **ETSI GS 007. QKD**.
  Термины и определения (preprint)
- **ETSI GS 008. QKD**.
  Спецификация безопасности модуля QKD

Прогноз развития систем QKD на ближайшие годы

- **Создание квантовых каналов с уплотнением по длине волны** (до нескольких десятков каналов в одном волокне)
- **Повышение скорости формирования ключей** (до значений около 50 Мбит/с)
- **Увеличение протяжённости квантовых каналов связи** (устойчивое превышение 100-километровой дальности)
- **Снижение уровня ошибок в «сырых» ключах** (до значений в единицы процентов)
- **Расширение областей практического внедрения** (вплоть до уровня малого бизнеса)



Сравнение QKD и PKI

Квантовое распределение ключей (QKD)	Инфраструктура открытых ключей (PKI)
☹ Требует выделенного оборудования и линий связи	☺ Может быть реализована программно, очень мобильна
☺ Защищённость основана на фундаментальных физических законах и принципах	☹ Требует увеличения длины ключей с ростом производительности компьютеров
☺ Не подвержена проблемам с построением квантового компьютера	☹ С построением квантового компьютера безопасность окажется под угрозой
☹ Высокая стоимость	☺ Низкая стоимость
☹ Требуются только оптические каналы связи	☺ Работает с любыми типами сетей

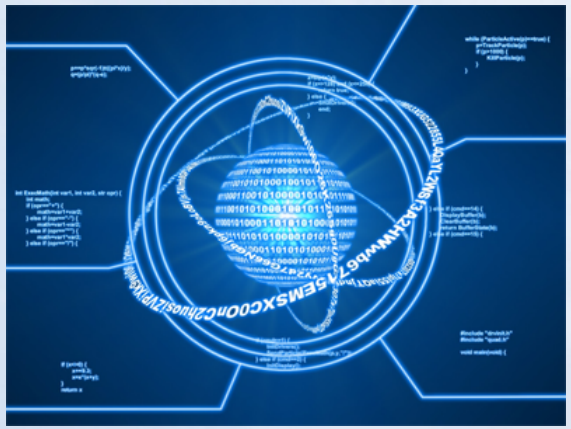
Возможен ли симбиоз имеющихся решений PKI и QKD ?

Да, возможен !

- использование **защищённых каналов** между удостоверяющими центрами, регистрационными центрами
- создание специализированных центров запросов с **защищёнными каналами связи** до удостоверяющих и регистрационных центров
- установка квантово-криптографического оборудования у ряда крупных конечных пользователей, уделяющих **повышенное внимание вопросам безопасности**

Прочие направления исследований в квантовой криптографической науке

- **QSDC** – квантовая защищенная прямая связь
- **QSS** – квантовой разделение состояний
- **QSC** – квантовой поточное шифрование
- **QS** – квантовая стеганография
- **QKI** – инфраструктура квантовых ключей
- **QDS** – квантовая цифровая подпись

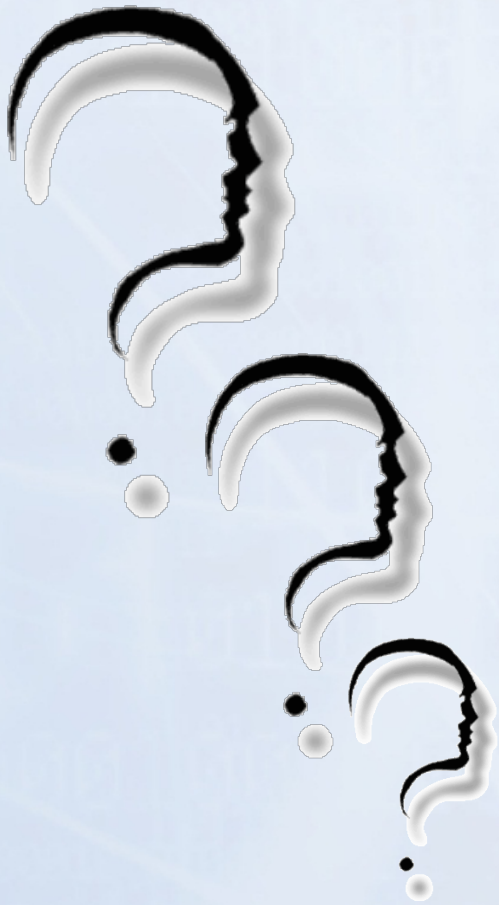


Инфраструктура квантовых ключей (QKI) и квантовая цифровая подпись (QDS)

- По аналогии с классической архитектурой PKI рядом зарубежных исследователей изучается вопрос построения полностью квантовой инфраструктуры открытых ключей – **Quantum Key Infrastructure (QKI)** и, на базе нее, квантовой цифровой подписи – **Quantum Digital Signature (QDS)**
- Работа таких систем (QKI и QDS) основана на использовании односторонних преобразований, но только уже **полностью квантовых односторонних преобразований**
- Будущим системам QKI и QDS не грозят проблемы, прогнозируемые с появлением квантового компьютера – наоборот, **для их построения необходим квантовый компьютер**

Проблемы квантовой криптографии в России

- **Недоверие к новым технологиям**
- **Отсутствие сертификации**
- **Отсутствие стандартов и других регламентирующих документов**
- **Высокая стоимость зарубежных коммерческих решений (около $80..200 тыс.)**
- **Отсутствие российских коммерческих решений**



Направления исследований на кафедре ИБТКС ЮФУ

- **Моделирование систем квантового распределение ключей** с целью поиска путей повышения эффективности
- Создание собственного **прототипа системы квантового распределения ключей**
- **Исследование проблем однофотонного детектирования** как одной из основных проблем эффективной работы систем квантовой криптографии
- **Исследование возможностей использования технологий квантовой связи** для осуществления и противодействия несанкционированного доступа к классическим оптическим системам связи
- **Создание виртуальной сетевой лаборатории** квантовой криптографии с предоставлением удалённого доступа к оборудованию посредством web-интерфейса
- **Анализ современных направлений исследований** в квантовой криптографической науке

Сотрудничество кафедры ИБТКС ЮФУ

- Сотрудники кафедры информационной безопасности телекоммуникационных систем посещали ведущие фирмы-производители систем QKD и участвовали в обучающих семинарах и школах:
  - **MagiQ** (США, 2009 год)
  - **idQuantique** (Швейцария, 2010 год)

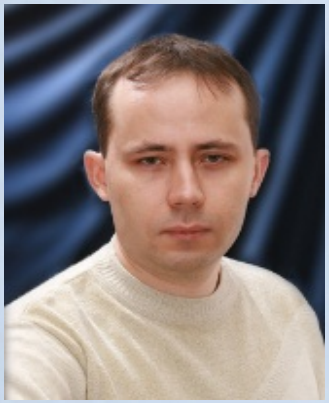
- Сотрудничество с Национальным авиационным университетом (г.Киев, Украина):
  - **Создание виртуальной лаборатории квантовой криптографии**

Заключение

- Классическая криптография столкнётся **с рядом проблем** по мере прогресса в построении квантовых компьютеров
- Квантовая криптография позволяет значительно **повысить уровень защиты**
- Имеющуюся инфраструктуру PKI-систем возможно **дополнительно защитить** уже существующими системами квантового распределения ключей
- В мире активно проводятся исследования по построению полностью квантовых систем PKI **(QKI, QDS)**

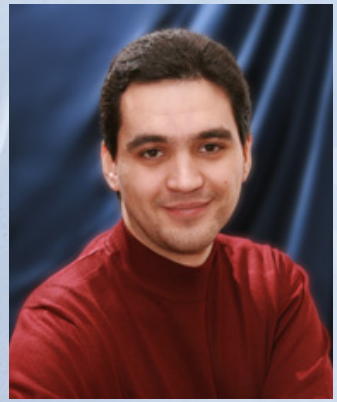
Таким образом,
объединение классических PKI-технологий и принципов квантовой криптографии
возможно !

Спасибо за внимание !



Горбунов Александр Валерьевич
кандидат технических наук,
доцент кафедры
информационной безопасности
телекоммуникационных систем (ИБТКС)
Южного федерального университета (ЮФУ)

al.v.gorbunov@gmail.com



Голубчиков Дмитрий Михайлович
ассистент кафедры
информационной безопасности
телекоммуникационных систем (ИБТКС)
Южного федерального университета (ЮФУ)

dmitriy.golubchikov@gmail.com