Двухканальная система распределения ключа, основанная на квантовой криптографии

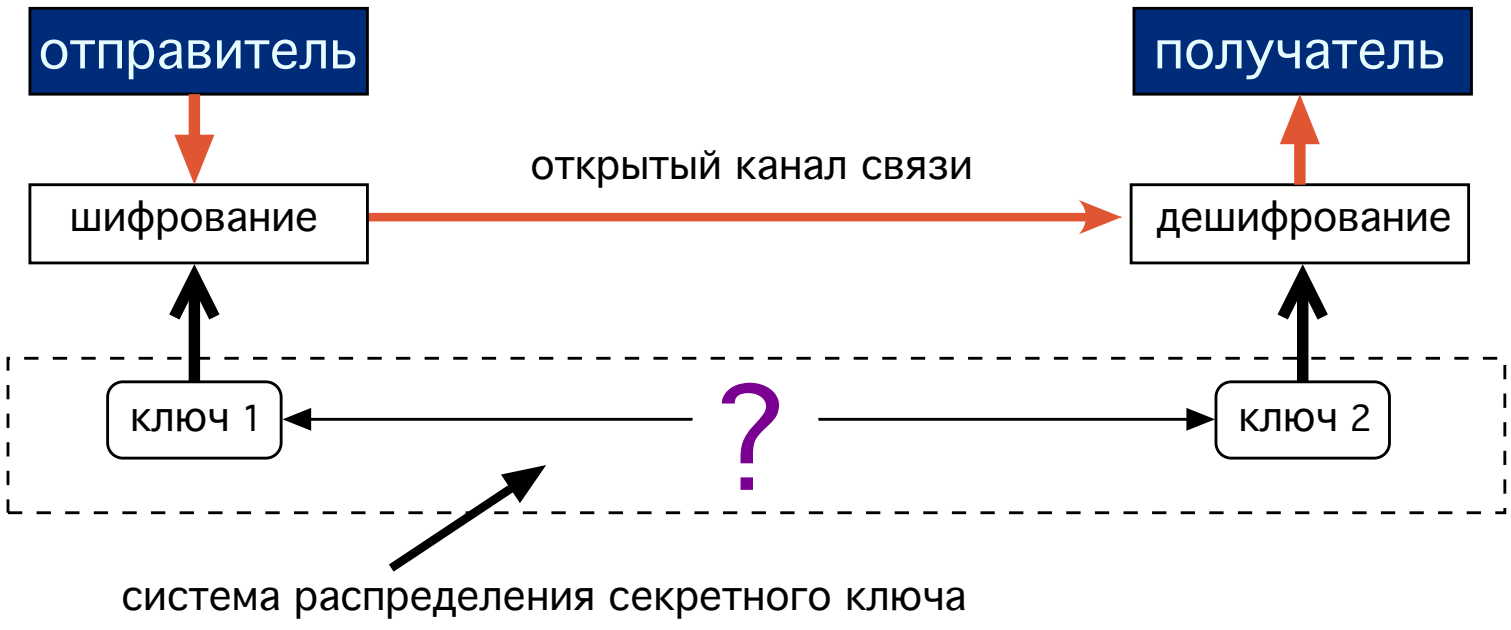
Сайгин Михаил Юрьевич

Международный учебно-научный лазерный центр МГУ им. М.В. Ломоносова,

Физический факульте МГУ им. М.В. Ломоносова

27 февраля, 2012 года

Проблема секретности передачи информации



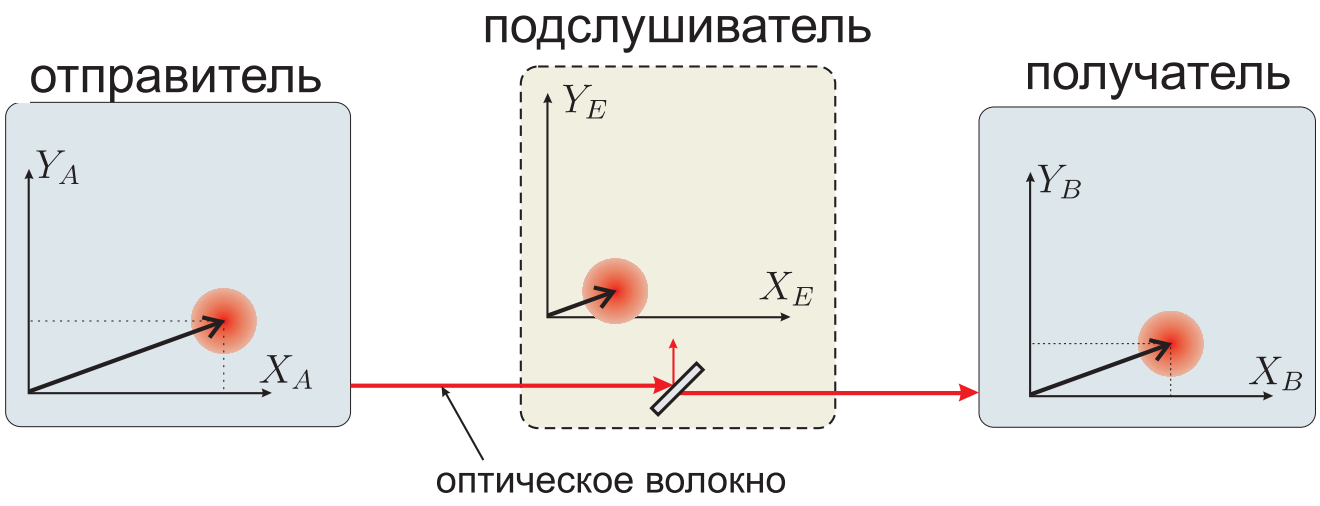
Условия секретности передачи

- ключи известны только отправителю и получателю
- каждому сообщению — новая пара ключей

Недостатки традиционных криптографических систем

Абсолютная секретность не гарантирована.

Квантовая криптография. Как это работает?



Основные особенности

Носители информации — одиночные фотоны или слабые световые импульсы (только так гарантируется секретность).

Воздействие на оптический канал регистрируется авторизованными участниками.

Секретный ключ формируется после передачи импульсов — «испорченные» импульсы не учитываются.

слабые сигналы трудно регистрировать и передавать!

Основные игроки на рынке

Исследования проводят

США	IBM, HP, MagiQ
Япония	NEC, Mitsubishi, AIT, NTT
Англия	QinetiQ, Toshiba Research Europe Ltd.
Швейцария	IdQuantique, GapOptique
Австралия	QuintessensLabs

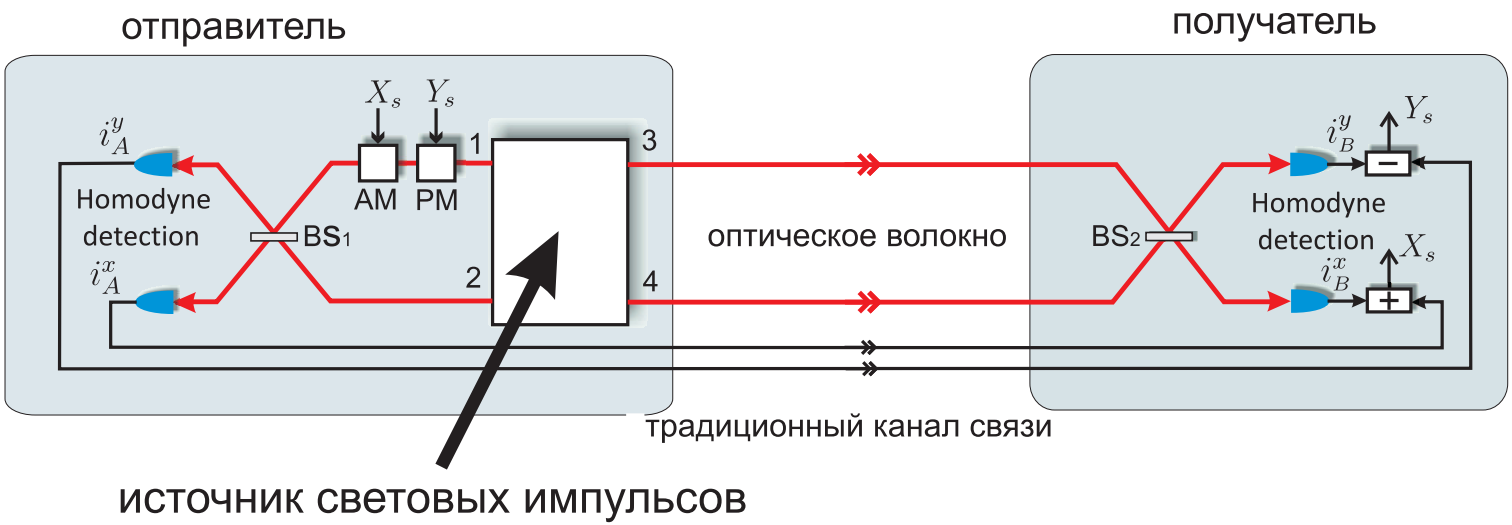
Рынок систем квантовой криптографии

Основные потребители: крупные компании, телекоммуникационные корпорации, банки, военные и государственные ведомства, учебные и научные организации;

Объем: **$ 0.9 млрд.** в перспективе до 2015 года;

Рост рынка за счет внедрения квантовой криптографии в Облачные технологии (Cloud computing) и технологии ближней связи (Near Field Communication).

Предлагаемый проект



Двухканальная система распределения ключей

Преимущества над существующими одноканальными системами

Мощность световых импульсов $\approx$ в 5 раз выше при сохранении уровня секретности $\Longrightarrow$

- увеличение скорости генерации ключей;
- увеличение дистанции передачи;
- использование более дешевой аппаратуры.

Современные коммерческие предложения

Система Cerberis фирмы IdQuantique.
Параметры системы:
дистанция передачи - **100 км**,
скорость генерации ключа - **25 кбит/сек**.

Система Q-Box Workbench фирмы MagiQ.
Параметры системы:
дистанция передачи - **50 км**,
скорость генерации ключа - **1 кбит/сек**.

Сравнение с существующими системами

	у конкурентов	предлагаемая система
дальность передачи	100 км	до 150 км
скорость генерации ключа	25 кбит/с	до 1 Мбит/сек
стоимость	от $ 50 тыс.	от $ 35-40 тыс.

M.Yu. Saygin, A.S. Chirkin, M.I. Kolobov, European Physical Journal D (2012) (в печати)

Планируемые результаты по НИР

- Исследование применения частотного мультиплексирования:
  - увеличение скорости генерации ключа;
  - использование одного оптического волокна для коммуникации.
- Исследование применения временных задержек между световыми импульсами:
  - увеличение «чувствительности» схемы к прослушиванию.
- Сборка макета системы.
- Патентование системы.

Партнеры-экспериментаторы

- Отделение квантовой радиофизики ФИАН им. П.Н. Лебедева;
- Лаборатория квантовой оптики НАН Беларуси.

Спасибо за внимание!

Упрощенная бизнес-модель проекта

Система квантового распределения ключа

Финансовая модель

Структура затрат:

- покупка оборудования
- закупка оптических и электронных компонент
- оплата аренды помещений и оборудования
- зарплата
- прочие затраты

Структура доходов:
продажы систем и дополнительных сервисов (образовательные программы)

Партнеры

ФИАН им. П.Н. Лебедева, Лаборатория квантовой оптики НАН Беларуси.

Клиенты

высшие учебные заведения, банки, крупные коммуникационные компании.

Каналы продаж:
непосредственно Потребителю

Основные риски и пути их решения

- **Проблема:** качество приобритаемой аппаратуры и время её доставки.
  Решение: Все компоненты — стандартные $\Longrightarrow$ поставки диверсифецированы.
- **Проблема:** высокая стоимость иностранных комплектующих - высокая себестоимость продукта.
  Решение: поиск комплектующих с оптимальным отношением цена/качество. Приоритет у отечественных производителей.
- **Проблема:** отсутствие необходимого числа потребителей.
  Решение: участие в выставках; проведение рекламных кампаний; спецпредложения по обслуживанию систем.