

**КВАНТОВЫЕ КОММУНИКАЦИИ** (Quantum Communication – QC) - коммуникационная сеть, работающая по законам квантовой механики, используя эффект квантовой сцепленности состояний.

## РАСШИРЕННЫЙ ПРОФИЛЬ

### 1. ОПИСАНИЕ

Квантовые коммуникации (Quantum Communication – QC) – это область знаний о передаче неизвестного квантового состояния из одного местоположения (скажем, от Алисы) в другое, удаленное от первого, местоположение (скажем, Бобу). Эта задача не является тривиальной из-за теоремы о невозможности квантового клонирования состояния, которая запрещает делать это так, как делается в классической физике.

В системах рассылки квантового ключа в качестве носителей информационного сигнала используются одиночные фотоны, которые в большинстве случаев генерируются путём предельного ослабления лазерного излучения. Альтернативный подход предлагается в системах квантовой криптографии, основанных на применении боковых (поднесущих) частот в результате фазово-частотной модуляции квантовые сигналы выносятся на соседние частотные компоненты (рис. 1).

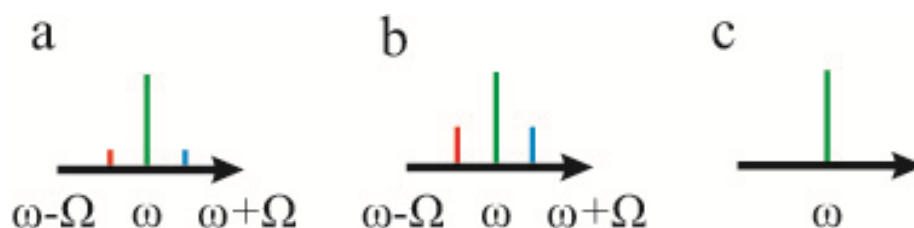


Рис. 1. Спектр оптического сигнала после модуляции в блоке отправителя (a) и получателя в случае конструктивной (b) и деструктивной (c) интерференции

При этом спектральный интервал между несущей и боковыми частотами определяется параметрами модулирующего сигнала и составляет порядка 10-20 пм. Системы на боковых частотах характеризуются более высокой скоростью генерации ключей и низкой вероятностью возникновения ошибок. Однако их главным преимуществом является возможность генерировать сразу несколько боковых частот в окрестности одной центральной, что позволяет размещать до 10 независимых квантовых каналов внутри одного окна мультиплексора.

В комбинации с WDM эта технология позволяет увеличить спектральную эффективность систем квантовой криптографии в оптических сетях с сегодняшних 4% до 40% и более, реализовав квантовые сети со скоростью

передачи данных порядка 400 Мбит/с. Все это делает технологию экономически эффективной – сейчас скорость лучших в мире квантовых систем всего 1-2 Мбит/с (50 км), в то время как пропускная способность канала в сети Ethernet – порядка 1 Гбит/с.

Ниже (рис. 2) приведена упрощённая схема системы. Полупроводниковый лазер генерирует излучение с узким спектром на длине волны 1550 нм. После этого излучение поступает в фазовый модулятор FM1, управляемый электронным блоком управления (electronic control unit). В результате фазовой модуляции в излучении появляются две боковые частоты, отличающиеся от несущей на величину модулирующего радиосигнала 4,4 ГГц.

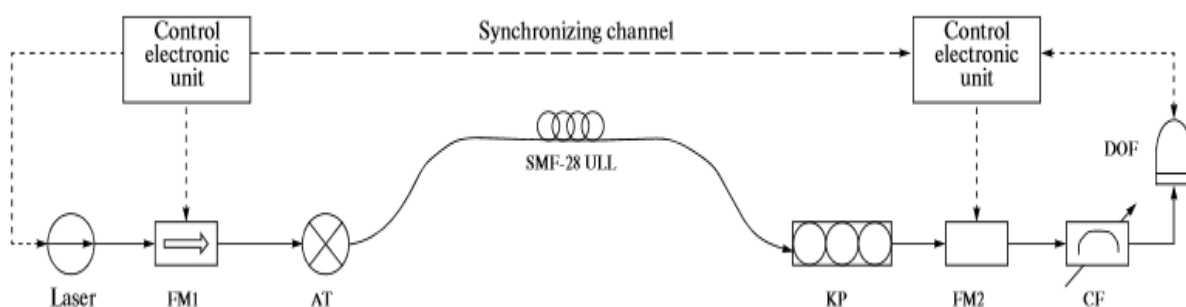


Рис. 2 – Принципиальная схема системы квантовой криптографии, основанной на применении поднесущих частот.

Мощность боковых частот контролируется путем изменения амплитуды модулирующего сигнала. Модулированный сигнал поступает на аттенуатор АТ, на выходе которого мощность сигнала на боковых частотах соответствует среднему числу фотонов на импульс (порядка единицы). Каждый бит передаваемого сигнала кодируется с помощью фазового сдвига ФА, добавляемого в модулирующий сигнал. Фазовый сдвиг контролируется электронным блоком управления и на каждый бит выбирается случайно из четырёх величин: 0;  $\pi/2$ ;  $\pi$  и  $3\pi/2$ .

Электронные блоки управления в передающем и принимающем модулях синхронизируются с помощью сигнала специальной формы: синусоиды с частотой 10 МГц и стробирующего импульса длительностью 10 нс. Стартовый строб-сигнал инициирует генерацию ключа, а последующие – синхронизируют запись квантовых отсчетов в буферную память передающего и принимающего модулей. Модуляционные генераторы передающего и принимающего модулей синхронизирует синусоидальный сигнал. Синхросигналы передаются по отдельному оптическому волокну.

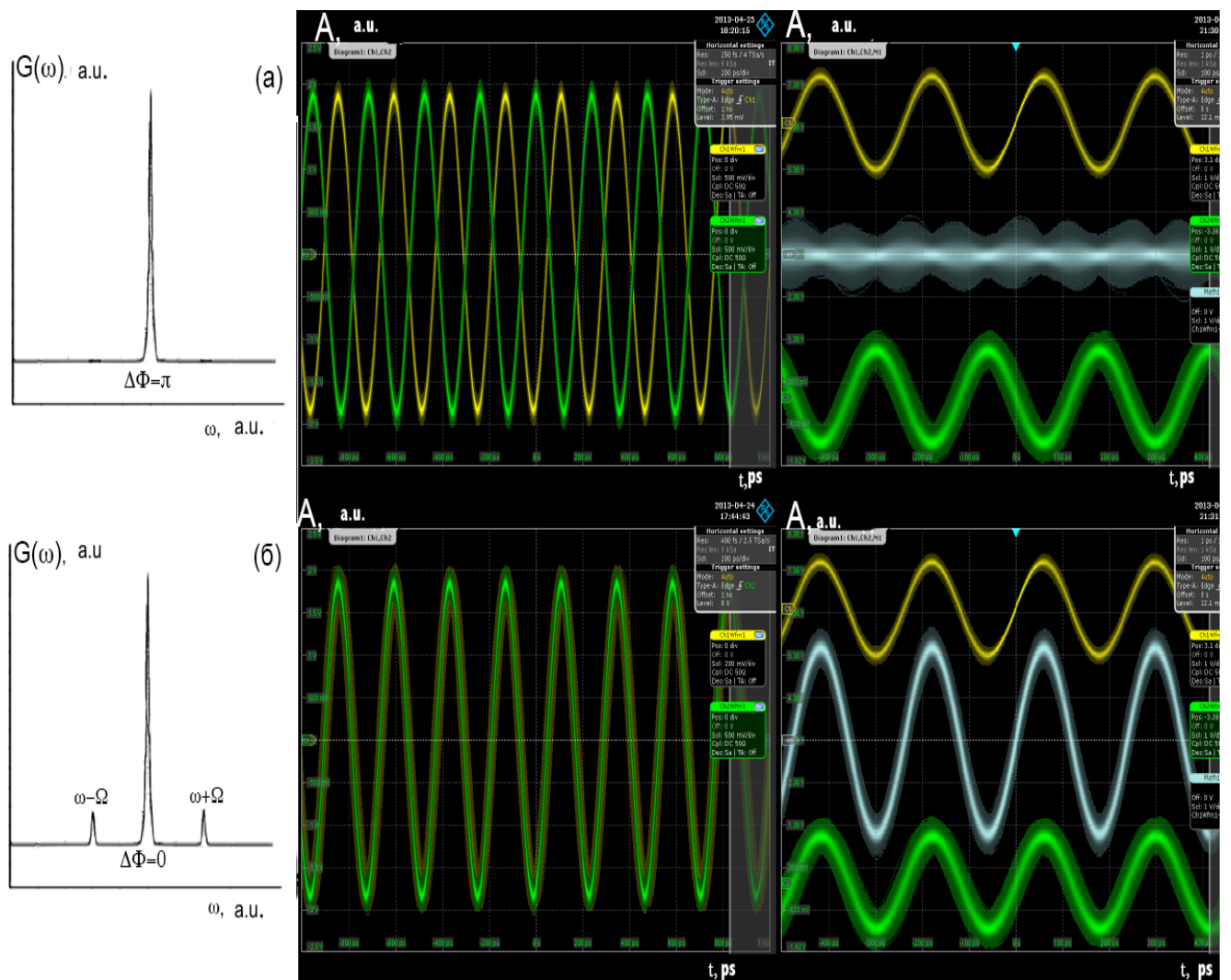


Рис. 3 – Спектр и осциллограмма (а) ослабляющей и (б) усиливающей интерференции

Криптографический ключ генерируется по протоколу BB84 с сильным опорным импульсом. Квантовый сигнал в принимающем модуле возникает в момент прохождения лазером поляризационного контроллера, фазового модулятора FM2 и спектрального фильтра SF, подключенных последовательно.

Спектральный фильтр выделяет сигнал боковых частот, который отслеживается с помощью детектора (счетчика) фотонов DOF. На этом этапе сигнал подвергается повторной фазовой модуляции. Фазовый модулятор FM2 управляется электронным блоком управления, а битовая последовательность кодируется точно так же как в передающем модуле. Частота смены фазы равна 100 МГц. Фазовый модулятор вносит в модулирующий сигнал сдвиг фазы ФВ; каждый битовый сдвиг выбирается случайным образом из четырех возможных величин. Результирующая мощность поднесущей волны зависит от фазовых сдвигов ФА и ФВ. Если  $\Phi_A =$

ФВ, то возникает усиливающая интерференция (рис. 3б), и мощность оптического сигнала оказывается отличной от нуля. Если  $\Phi_A - \Phi_B = \pi$ , то проявляется ослабляющая интерференция (рис. 3а), а мощность оптического сигнала оказывается сопоставимой с шумом темнового тока детектора фотонов. Состояния с разностью фаз  $\pi/2$  отбрасываются. Обмен информацией, необходимой для обработки результатов измерения, выполняется по открытому каналу. При этом «сырой» ключ генерируется одновременно в передающем и принимающем модулях. После этого для «сырого» ключа вычисляется коэффициент ошибок (QBER), по которому легитимные пользователи могут определить, была ли предпринята попытка прослушки. Если прослушки не было, то ошибки корректируются, а в передающем и принимающем модулях генерируется секретный криптографический ключ.

Величина QBER определяется как отношение количества ошибочных битов к общему числу полученных битов:

$$QBER = \frac{N_{wrong}}{N_{right} + N_{wrong}} = \frac{R_{err}}{R_{err} + R_{sift}} \approx \frac{R_{err}}{R_{sift}}$$

где  $R_{sift}$  (длина «просеянного» ключа) равняется количеству совпадений базисов Алисы и Боба (приемника и передатчика), что в свою очередь равняется половине длины «сырого» ключа:

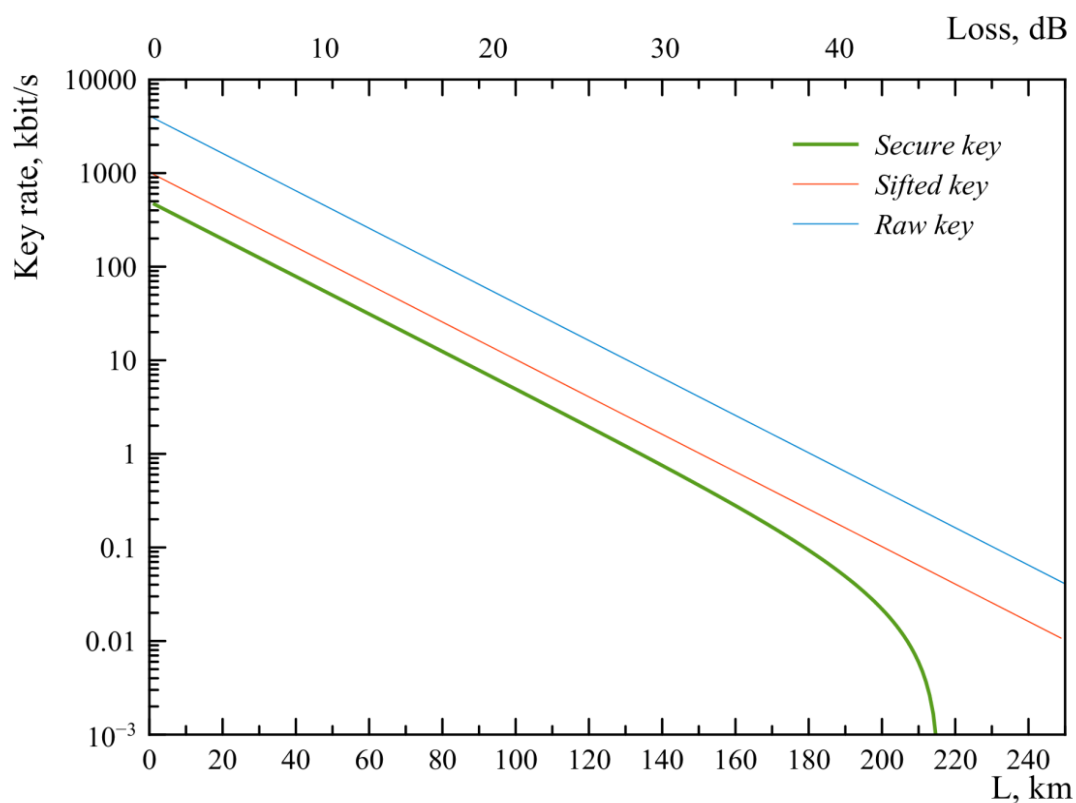
$$R_{sift} = \frac{1}{4} R_{raw} = \frac{1}{4} q f_{rep} \mu t_{link} \eta ,$$

где  $f_{rep}$  – частота повторения импульсов,  $\mu$  – среднее число фотонов за импульс,  $t_{link}$  – коэффициент передачи, то есть вероятность фотона достичь детектора Боба,  $\eta$  – вероятность обнаружения фотона, то есть квантовая эффективность детектора. Фактор  $q \leq 1$  введен для систем с фазовым кодированием, чтобы учесть не интерферирующие фотоны.

Результаты собраны в таблице ниже и представлены на графиках.

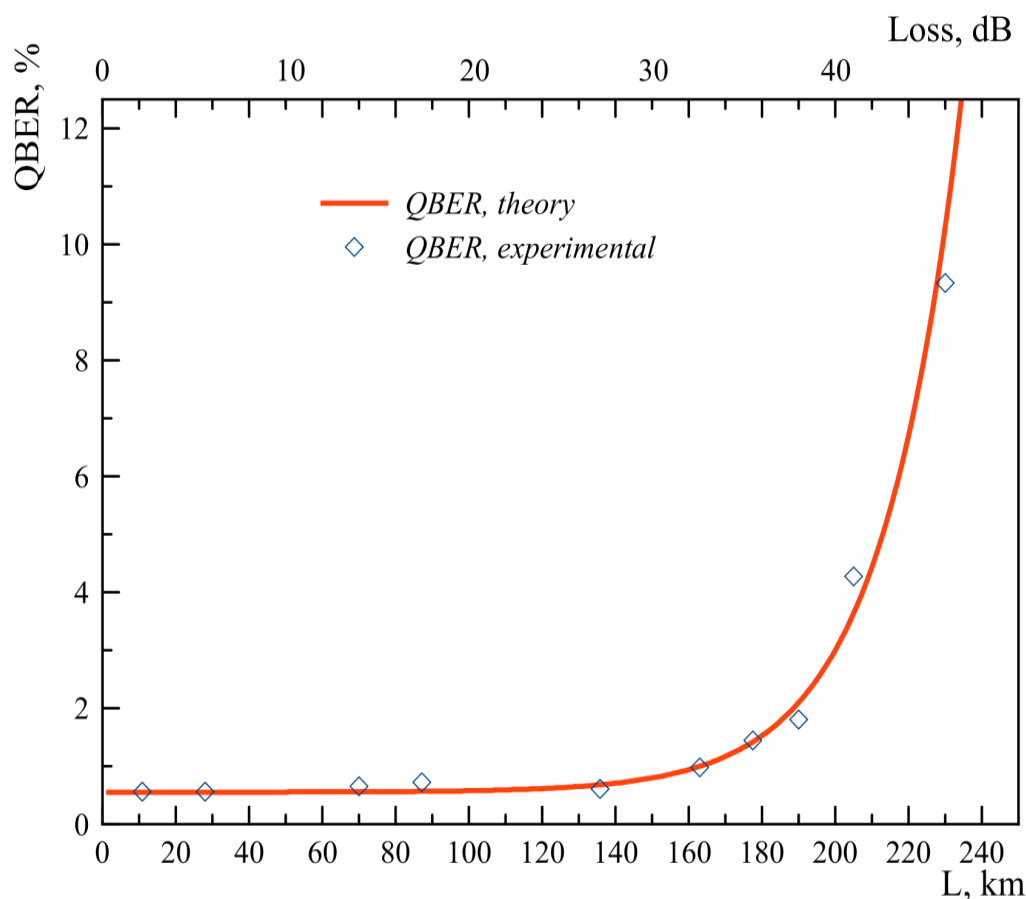
Параметр	Дистанция		
	25 км	100 км	200 км
Скорость генерации сырого ключа, кбит/с	1250	10	0,1
QBER, %	0,55	0,56	2,8
Среднее количество фотонов на импульс	1		

Если расстояние передачи равно 200 м, то скорость генерации «просеянного» ключа составит 200 бит/с, при QBER равном всего 1%. Что примечательно, такие результаты были получены на синхрочастоте в 100 МГц, что значительно упрощает электронную подсистему и оставляет задел для дальнейшего увеличения скорости (в рекордных системах со сравнимыми параметрами используется синхрочастота порядка 1 ГГц).



Это стало возможным благодаря инженерным решениям специалистов ИТМО, которые позволили добиться высокой видимости интерференционной картины ( $V > 98,9\%$ ) в однонаправленном канале за счёт точного контроля

относительных фазовых сдвигов и свойств детектора SNSPD (низкий уровень темновых отсчётов и высокие быстродействие). Для максимального расстояния, на котором проводился эксперимент, скорость рассылки «просеянного» ключа составила 28 бит/с, при QBER равном 9,3%, что по-прежнему допускает безопасную генерацию ключей.



С одной стороны, QC – чудесная вещь, т.к. позволяет нам распространять область запутывания на большие расстояния и, таким образом, устанавливать так называемые нелокальные корреляции, что подтверждается нарушениями неравенств Белла, т.е. такие корреляции, которые невозможно объяснить лишь локальными параметрами, распространяющимися в пространстве непрерывно.

С другой стороны, QC имеют огромный потенциал применения. Лучше всего известна задача о распространении квантового ключа (Quantum Key Distribution – QKD), где использование запутывания гарантирует секретность ключа в криптографических приложениях. Другими примерами возможных приложений являются процессы, случайность которых гарантируется нарушением некоторого неравенства Белла. В самом деле, невозможно доказать случайность данной последовательности битов, но можно доказать,

что некоторые процессы случайны, и известно, что случайные процессы продуцируют случайные последовательности битов. Следовательно, случайность переходит из математики в физику.

В QC необходимо использовать источники фотонов, средства кодирования некоторой квантовой информации (в виде квантовых битов или, кратко, кубитов), каналы передачи фотонов, обеспечивающих сохранение переносимой ими информации (например, поляризации или т.н. time-bin кубитов), с возможностью телепортации информации и/или сохранения ее в квантовой памяти и, вероятно, детектор фотонов после анализатора, который позволяет восстановить квантовую информацию. Кроме того, QC эволюционирует от простой двусторонней связи к сложным сетям. Последнее требует, с фундаментальной точки зрения, лучшего понимания многочастичного запутывания и нелокальности, а с экспериментальной точки зрения глобального системного подхода с совершенной синхронизацией, сетевым управлением, процессами восстановления.

## **2. БИЗНЕС-ПОТЕНЦИАЛ**

Квантовые технологии по-новому работают с информацией. Классические вычисления строятся по принципу двоичной логики и последовательных вычислений. Это значит, что компьютер совершает определенное количество последовательных операций за единицу времени. Соответственно, чем сложнее задача, тем больше операций происходит. Приведу простой пример. Если на пол рассыпались цветные бусы – черные и белые, то обычный ПК начнет перебирать все бусины, пока не найдет белую. Квантовый компьютер просто посмотрит на бусины и скажет: «Вот эта». Такой суперкомпьютер совершает вычисления за один машинный такт – в тысячи раз быстрее обычного ПК.

Новые вычислительные мощности влекут за собой и новые угрозы. По прогнозам, настоящий квантовый компьютер может появиться уже через 10 лет. И его создание обесценит все современные средства шифрования данных. Именно поэтому необходимо заранее предусмотреть средства борьбы с данной угрозой. Суть классической криптографии в следующем. Расшифровка криптографических ключей величиной от 1024 бита и более занимает время, значительно превышающее срок актуальности информации. Вместе с тем, ее безопасность напрямую связана с вычислительными возможностями дешифратора и не является абсолютной – хакерские взломы и кибератаки были всегда. Квантовый компьютер вскрыет все криптографические ключи глобального интернета всего за один год – также быстро, как найдет белую бусину. И это очень серьезная угроза для всего человечества.

Развитие квантовых коммуникаций в целом связано с поиском принципиально новых подходов к архитектуре криптографических систем. Мы

вполне можем говорить о кризисе современной системы информационной безопасности. Дело Эдварда Сноудена, Джулиана Ассанжа, вирусы Stuxnet, Duqu и Flame, используемые как кибероружие, взломы и хакерские атаки на правительственные и частные системы передачи данных, проект создания закрытой внутриевропейской коммуникационной сети – с одной стороны это классическая политическая игра, но с другой – реальные проблемы с сетевой безопасностью. Ожидается, что к концу 2017 на борьбу с интернет-преступлениями потратят уже \$120 млрд. По оценке BCG рынок безопасности киберфизических систем к 2020 г. достигнет 389 млрд, а к 2035 г. – 2,1 трлн с ростом 15% год.

Любая научная идея сталкивается с технологическими и рыночными барьерами. Пока решения не доведены до коммерческого уровня – на это нужно время. Мы меняем бизнес-модели предоставления услуг в самых разных областях – от госсектора до телекома. Появляется новое оборудование, новый софт, новые сценарии применения технологий. Нужно постоянно доказывать конкурентоспособность новых решений – они намного дороже предыдущих. Например, в 2011 году канадская компания D-Wave Systems продала прототип квантового компьютера за 10 миллионов долларов авиастроительному концерну Lockheed Martin. D-Wave еще с 2007 года занимается этими разработками, но назвать созданный прототип полноценным квантовым компьютером никто не может. Еще одна проблема коммерческого внедрения – в отсутствии международных технологических стандартов.

В связи с этим сейчас у игроков мирового рынка квантовых коммуникаций есть отличный шанс первыми освоить новую нишу. Обычно на высокотехнологичных рынках мы работаем в рамках чужих стандартов. Сегодня у российских разработчиков появилась возможность написать свои правила игры. У нас есть материально-технологическая база, научная экспертиза, опыт применений решений, которые позволяют задавать тон если не на глобальном рынке, то на нескольких региональных – на Евразийском пространстве, в странах БРИКС и ШОС. По экспертным оценкам, квантовые технологии сформируют новый большой рынок телекома, который может полностью заменить существующую инфраструктуру. Второй мощный тренд – это региональность. Есть подозрения, что в новой телеком-инфраструктуре, которая сложится в ближайшие 10-15 лет, возникнут новые региональные зоны со своими стандартами. Именно в области стандартов и развернется конкурентная борьба на этих рынках.

В России есть три ключевых центра разработки по квантовым коммуникациям, которые имеют собственные разработки: в Санкт-Петербурге Университет ИТМО и два в Москве – Российский квантовый центр в Сколково



и МГУ. Чтобы сделать из разработки технологию и конечный продукт нужно потратить порядка 40-200 млн рублей. Сегодня на мировом рынке уже продаются коммерческие решения устройств рассылки квантового ключа стоимостью порядка 100 тысяч долларов. Российская компания «Квантовые коммуникации», созданная на базе Университета ИТМО, также продает собственные устройства. Но разрабатывать новые технологии недостаточно — повторю, что нужен российский стандарт. В противном случае к нам просто придут западные корпорации и смогут навязать операторам свое оборудование и свои условия.

Необходимо оплачивать новую инфраструктуру – а это совсем другие деньги. Прокладка оптоволокну, строительство типовых коммуникационных узлов, магистральные узлы доступа, системы управления и пользовательские интерфейсы – все это стоит сотни миллиардов рублей и может строиться десятилетиями. В таком долгосрочном проекте должно участвовать и государство, и крупный бизнес. Понятно, что новая инфраструктура появится не сразу. Создание квантовой сети возможно путем разворачивания пилотных проектов – участков, заменяющих классическую инфраструктуру. Такие проекты может осилить и частный бизнес.



В 2016 году университет ИТМО с компанией «СМАРТС» (прим. российский оператор, преимущественно предлагает услуги фиксированной

связи, штаб-квартира в Самаре) запустили проект разворачивания магистральной квантовой телекоммуникационной сети в европейской части России, а в последствии и на евразийском пространстве. Сегодня это один из самых масштабных проектов в мире, реализация которого потребует несколько миллиардов рублей.

Планируется разворачивание телекоммуникационных узлов и ЦОДов, оснащенных квантовыми технологиями, которые обеспечат новое качество связи и ИТ-инфраструктуры – своего рода квантовый VPN и квантовые облака. В итоге клиент получит беспрецедентное качество услуг связи: гарантированную безопасность и надежность.

Конечно, на начальном этапе такие эксклюзивные услуги стоят дорого. Их потребителями являются государство, спецслужбы и крупные корпорации, например, банки. Они обходятся в несколько раз дороже, чем классические услуги связи. Но со временем появляется эффект масштаба за счет наращивания пользователей на построенной инфраструктуре. Поэтому либо операторы в будущем меняют инфраструктуру, либо арендуют ее у того, кто первый ее построил.



В США развивается масштабный проект прокладки по периметру страны квантовой сети по ЦОДам крупных ИТ-компаний: Google, Amazon, Oracle. Дата-центры используются как точки обмена трафиком, между ними прокладывают квантовую сеть. В будущем эти супер-безопасные каналы связи можно будет продавать или сдавать в аренду. В Китае уже протянута ветка Шанхай-Пекин на 2 тыс. км, в Пекине по периметру города строятся квантовые

хабы – точки входа для квантовой сети. Эту сеть отдали для тестирования и отработки бизнес-моделей коммерческим компаниям.

У квантовых коммуникаций есть более широкие области применения, чем безопасность каналов связи. Существует несколько дополнительных эффектов, которые в будущем могут изменить работу с данными и сам принцип связи. Например, квантовые коммуникации позволяют отследить и физически задать потоки передаваемой информации в заданных периметрах, а также производить синхронизацию разных устройств, что позволит пользователям и операторам более эффективно управлять и отслеживать транзакции, пакеты информации. Квантовые сенсоры позволяют получить более точную и эффективную навигацию и позиционирование. Спутанность и квантовая телепортация в перспективе могут привести к смене парадигмы передачи и хранения информации, заменив терабайты (в виде нулей и единиц) на хранение и передачу состояний вещества.

Сейчас мы говорим о гибридных технологиях, когда на классических сетях достраивается квантовая часть. В итоге получается классическое оптоволокно с классическими услугами, но обладающее новыми свойствами за счет квантовых технологий. Уже есть примеры использования таких сервисов для защищенного ВП-банкинга, на выборах, защиты каналов передачи персональных генетических данных.

В сотовой связи квантовые коммуникации могут также обеспечивать оптический канал между базовыми станциями, ЦОДами и центрами управления. При этом 5G в гибридных сетях – важная часть, обеспечивающая связь с клиентскими устройствами в условиях быстрого развития киберфизической среды (умные устройства, M2M и др.)

Второй способ передачи информации – по открытому пространству через спутники. В августе 2016 Китай запустил на орбиту первый в мире квантовый спутник «Мо-цзы». Как сообщает китайское информагентство, уже установлена устойчивая связь спутника с экспериментальной платформой для квантовой телепортации в Тибете. К 2025 г. планируется запуск коммерческой квантовой связи.

Спутниковая связь позволяет решить главную проблему квантовой связи – это передача сигнала на небольшие расстояния: в среднем 100-150 км в пределах 250-300 км. Поэтому сегодня каждые 250 км необходимо ставить новое устройство, передающее квантовый ключ. Это технологическое ограничение решается двумя способами: улучшение технологии инженерными способами и создание квантового повторителя, который избавит от необходимости переводить оптический сигнал в электрический и дублировать набор

оборудования на этих участках. Этот повторитель может появиться уже в ближайшие 5-7 лет.

Во всем мире в разработку и внедрение квантовых технологий вкладываются большие деньги – как государственные, так и частные. Рынок квантовых коммуникаций должен быть сформирован – в ближайшие полтора технологических цикла.

### 3. БАРЬЕРЫ

Квантовые коммуникации сталкиваются со многими проблемами, которые простираются от индустриализации квантовых технологий до концептуальных вопросов теоретической физики, от оптики до материаловедения.

- 1) Источники: Помимо относительно простого случая двустороннего QKD, все задачи QC требуют источников запутанных фотонов. Сегодня такие источники основаны на спонтанном параметрическом преобразовании с понижением частоты, поэтому являются вероятностными. Следовательно, чтобы исключить генерацию нескольких пар фотонов, вероятность рождения одиночной пары поддерживается достаточно низкой, обычно от 1% до 0.1%. Более того, потери связи между нелинейными кристаллами, в которых рождаются фотоны, и оптоволоконном оказываются критичными. Развитие доступных и детерминистических источников запутанных фотонов является важной задачей.
- 2) Квантовые каналы могут представлять собой либо космический вакуум, либо оптоволоконные кабели. Первый случай наиболее подходит для QC типа Земля-спутник и спутник-спутник; там главные проблемы заключаются в размере и весе телескопов. Для волокон главной проблемой являются потери. Сегодня наилучшие оптоволокна имеют потери до 0.16 дБ/км, т.е. через 20 км более половины фотонов все еще сохраняются.
- 3) Квантовая телепортация: Этот замечательный процесс позволяет передавать квантовые состояния (т.е. квантовую информацию), используя заранее созданное запутывание в качестве канала. Квантовое состояние не передается вдоль какой-либо траектории в пространстве, но “телепортируется” отсюда туда. Кроме передачи запутывания, телепортация требует совместных измерений, еще одно квантовое свойство, не существующее в классической физике. Совместные измерения позволяют измерить относительные свойства двух систем, например выяснить, “являются ли состояния поляризации анти-параллельными?”, не определяя информацию об их индивидуальных. Следовательно, индивидуальные свойства при этом не возмущаются, но

корреляции между свойствами двух систем оказываются “квантово коррелированными”, т.е. запутанными. На практике два фотона смешиваются в светоделителе. Это работает, но требуется высокая стабильность, т.к. оба фотона должны быть неразличимы по всем параметрам. В частности, важна синхронизация, особенно когда фотоны пролетают большие расстояния перед встречей в светоделителе. Более того, этот процесс вероятностный и работает в лучшем случае в половине случаев (при этом известно, когда он работает). Большой проблемой является существенное усовершенствование совместных измерений. Это, вероятно, требует передавать фотонные квантовые состояния с помощью твердотельных носителей (solids), чтобы совместное измерение осуществлялось с помощью степеней свободы, кодирующих квантовое состояние в твердотельных носителях, например, между двумя спинами. Кроме того, с чисто теоретической точки зрения, требуется лучшее понимание сущности совместных измерений, подобно абстрактной формулировке нелокальных корреляций.

- 4) Сигнальный (heralded) вероятностный усилитель кубитов также должен быть упомянут. Соответствующий процесс, восходящий к телепортации, позволяет увеличить вероятность присутствия фотона без возмущения кодируемого им кубита. Проблема состоит в создании такого усилителя для больших расстояний ( $>10$  км).
- 5) Детекторы: QC в основном осуществляются с использованием единичных фотонов, следовательно, требуются отличные детекторы единичных фотонов. Хотя следует сказать, что можно также использовать так называемые непрерывные параметры, например, импульсы сжатого света и гомодинные системы детектирования. Недавно детекторы единичных фотонов получили значительное развитие, их растущая эффективность за пару лет от 20% достигла 80-90% благодаря сверхпроводящим системам детектирования. В то же время нестабильность снизилась ниже чем до 100 пс. Однако еще остались некоторые значительные проблемы:
  - упрощение/удешевление (в частности, при более высоких температурах, как минимум при 3 К, возможно, с применением высокотемпературной сверхпроводимости).
  - повышение чувствительности детекторов к числу фотонов вплоть до нескольких десятков фотонов. Эта замечательная перспектива имеет, однако, смысл, только если эффективность детектирования равна не менее 95%.
  - достижение 99-100% эффективности. Это кажется достижимым.
- 6) Устройства квантовой памяти позволяют обратимым образом и в нужный момент преобразовать фотонные квантовые состояния в некоторые атомные системы (и обратно) с большими временами когерентности. Они нужны для

синхронизации сложных квантовых сетей. Они могут также переключать вероятностные источники в режим квази-детерминированности, обеспечивая их достаточно высокую эффективность. Сегодня устройства квантовой памяти все еще являются лабораторными устройствами. Хотя все параметры – объем памяти, эффективность, надежность, полоса пропускания и возможность работы в мультимодовом режиме – были удовлетворительно продемонстрированы, каждая такая демонстрация использовала свою особенную систему. Следовательно, большой проблемой является разработка системы, способной хранить 100 фотонных кубитов (например, 100 временных мод) в течение 1 секунды с эффективностью 90% и надежностью около 95%. Это огромная проблема. Неясно, окажется ли лучшим решением использовать один естественный или искусственный атом в резонаторе или комплекс атомов (газ или легированные оптические кристаллы). Это требует совместного привлечения материаловедения и химии (в случае кристаллов), криогеники (низкие температуры представляются необходимыми для длительных времен хранения), спектроскопии и радиоволновой спин-эхотехники, оптики и электроники.

- 7) Многочастичное запутывание и нелокальность: будущие сложные квантовые сети будут рутинным образом продуцировать запутанные многочастичные состояния, чьи полные возможности еще должны быть прояснены. В случае 2-частичных, нелокальных корреляций это оказывается мощным ресурсом для некоторых замечательных процессов, называемых независимыми от устройства квантово-информационными процессами (Device Independent Quantum Information Processes (DIQIP)). Аналогично, можно ожидать квантовых корреляций в сложных сетях, чтобы открыть новые возможности, которые еще предстоит создать.
- 8) QKD: Задача распространения квантового ключа является наиболее продвинутым приложением квантовых коммуникаций. Остальные задачи являются по большей части промышленными и коммерческими. Для промышленности задача QKD должна стать менее дорогой и использовать большие скорости (один Гб/с кажется недостижимым). Для коммерческих приложений должны быть переподготовлены специалисты по классической безопасности и криптографии, они должны понять потенциал квантовой физики и то, что их знания являются не устаревшими, но требующими дополнений: кванты не решают всех проблем, но обеспечивают гарантированную случайность и секретность. Следовательно, всегда надо будет сочетать их с классическими системами безопасности и криптографии.

#### **4. ЗНАЧИМОСТЬ ДЛЯ РАЗВИТИЯ БИЗНЕСА**

На рынках Европы, Азии и США квантовые технологии активно развиваются последние 10 лет, постепенно выходя из лабораторий в прикладную сферу. Речь идет не только о создании квантового компьютера, о котором много говорят в СМИ, но о совершенно новой инфраструктуре телекоммуникаций и информационной безопасности. Крупные технологические брокеры на новых рынках давно работают с этим направлением – как с основой для создания перспективных бизнес-моделей. В мире есть 8 глобальных кластеров, которые концентрируют ресурсы по разработке и внедрению квантовых технологий: на западном и восточном побережье США, в Европе, Великобритании, Китае, Японии, Австралии и России. Ключевые свойства квантовых технологий научно доказаны и даже экспериментально подтверждены: квантовая телепортация, высокий уровень безопасности передачи данных, новые вычислительные мощности, сверхскорость передачи данных, суперчувствительность квантовых сенсоров и др. Поэтому они могут найти применение в самых разных отраслях: транспортных системах, инфраструктуре умного города и интернета вещей, робототехнике, телеком-инфраструктуре, спутниковых системах связи.

#### **5. ИСТОЧНИКИ**

1. <http://quope.eu>
2. <http://www.sviaz-expo.ru/ru/articles/2016/kvantovaya-set-tehnologiya-budushhego/>
3. <http://www.sviaz-expo.ru/ru/articles/2016/kvantovaya-set-tehnologiya-budushhego/>
4. <https://www.billing.ru/blog/kvantovyy-kompyuter-poyavitsya-uzhe-v-2025-godu>