Октябрь 2021 г. *Том 191, № 10*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

ОБЗОРЫ АКТУАЛЬНЫХ ПРОБЛЕМ

Протяжённые квантовые сети

Д.Д. Сукачёв

Квантовые сети, позволяющие генерировать запутанные состояния между удалёнными кубитами, обладают огромным научным и прикладным потенциалом. Их можно использовать для безопасной квантовой криптографии и телепортации квантовых состояний между городами и странами, в астрономии высокого разрешения и распределённых квантовых вычислениях. Рассеяние фотонов в оптоволокне и трудности в создании полноценных квантовых узлов не позволяют пока построить пространственно протяжённые квантовые сети. Проводится обзор текущих подходов к созданию таких сетей, в первую очередь квантовых повторителей, которые призваны "компенсировать" потери в оптоволокне. Обсуждаются методы увеличения радиуса действия систем квантовой криптографии без использования квантовых повторителей.

Ключевые слова: квантовая сеть, квантовая криптография, квантовый повторитель

PACS numbers: 03.65.Ud, **03.67.–a**, 42.50.Ex DOI: https://doi.org/10.3367/UFNr.2020.11.038888

Содержание

1. Введение

За прошедший век квантовая механика, некогда абстрактная физическая теория, стала основой для множества технологий, которыми мы пользуемся каждый день: лазеры, системы спутниковой навигации, магнитно-резонансная томография, полупроводниковая электроника. Тем не менее применение квантовой механики для анализа многих физических, биологических и химических задач часто ограничено невозможностью рассчитать поведение квантовых систем на современной вычислительной технике из-за экспоненциальной зависимости необходимой вычислительной мощности от размера квантовой системы [1].

Для решения таких задач в 1980-х годах Ю.И. Манин и Р. Фейнман предложили использовать квантово-механические системы — *квантовые компьютеры* [2, 3], которые благодаря хранению и обработке информации в квантовом виде могут избежать указанного экспоненциального возрастания. Затем в 1992 г. Дойч и Йожа установили, что квантовые компьютеры могут также ускорить решение некоторых математических задач [4]. Знаковое событие произошло в 1994 г., когда П. Шор разработал квантовый алгоритм, факторизующий простые числа за полиномиальное время, — огромный скачок по сравнению с экспоненциальной зависимостью для лучшего классического алгоритма [5].

Задача факторизации целых чисел имеет особое значение в современном мире — она является основой для алгоритма RSA (аббревиатура от фамилий Rivest, Shamir и Adleman), наиболее распространённой криптографической системы с открытым ключом [6] в интернете (асимметричное шифрование), которая позволяет конфиденциально обмениваться информацией двум пользователям, никогда ранее не встречавшимся и не имевшим возможности договориться об общем ключе шифрования [7]. Для этого первый пользователь (сервер) выбирает два простых числа, q и r, формирует из них *открытый ключ* $p = qr$ и посылает его второму пользователю (клиенту) по незащищённому каналу связи. Клиент шифрует открытым ключом своё сообщение и отправляет его обратно серверу по тому же каналу. Для дешифрования сервер использует известный только ему *секретный ключ*, который строится на основе q и r.

Таким образом, возможность злоумышленника расшифровать сообщение напрямую зависит от его способ-

Д.Д. Сукачёв. University of Calgary, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada
E-mail: sukachev@gmail.com

Статья поступила 9 июня 2020 г., после доработки 26 ноября 2020 г.

ности факторизовать открытый ключ, а значит, когда-нибудь квантовые компьютеры смогут взломать каналы передачи данных. Ввиду огромной сложности создания квантовых компьютеров пока удалось факторизовать только 8-битовое число [8], а для факторизации 2048-битового открытого ключа (стандарт на 2020 г.) может потребоваться больше миллиона кубитов [9]. Существующие универсальные квантовые компьютеры имеют всего 50 – 100 кубитов [10 – 12] и в ближайшее время не смогут взломать алгоритм RSA, однако некоторые данные, переданные сегодня, требуется держать в секрете в течение многих десятилетий [13].

Проблема защищённости телекоммуникационных систем от квантовых атак имеет как минимум два решения. Первое — это постквантовая криптография [14], использующая математические алгоритмы шифрования, для которых не существует аналога алгоритма Шора, однако нет гарантии, что соответствующий квантовый алгоритм дешифрования не будет разработан позднее. Второе решение было найдено в 1984 г., когда Ч. Беннет и Ж. Брассар придумали, как использовать одиночные фотоны для генерации *симметричного* ключа шифрования между двумя пользователями (протокол BB84), причём секретность такого ключа — факт, что этот ключ известен только этим двум пользователям, — гарантирована законами квантовой механики [15]. Само шифрование осуществляется методом *одноразовых блокнотов*, в котором сообщение шифруется побитовой операцией "исключающее или" с ключом шифрования [7]. Такой алгоритм обладает *абсолютной криптографической стойкостью*, т.е. не существует математического алгоритма, позволяющего расшифровать сообщение без знания ключа. Это открытие дало начало новому направлению — *квантовой криптографии* или, более корректно, *квантовому распределению ключей* (КРК) (Quantum Key Distribution — QKD) [16]. Сегодня системы КРК стали коммерчески доступными. В России они выпускаются компаниями QRate, основанной сотрудниками Российского квантового центра, и "Инфотекс" совместно с Центром квантовых технологий Московского государственного университета (МГУ) им. М.В. Ломоносова [17] и применяются некоторыми банками [18].

Основа упомянутого выше алгоритма BB84 [15] состоит в обмене классическими битами информации, закодированными в поляризационные состояния *одиночных фотонов* в двух неортогональных базисах, между двумя пользователями: Алисой и Бобом. Естественно, передача информации состоится, только если посланный одиночный фотон достигнет адресата. Поэтому если злоумышленник перехватил одиночный фотон, то ему необходимо его измерить и отправить точную копию дальше, чтобы себя не выдать, однако этому препятствует *теорема о запрете клонирования* [19] в квантовой механике. В итоге злоумышленник не может с достоверностью узнать, какой фотон (бит) был послан, а секретность созданного ключа шифрования гарантирована физическими законами, а не сложностью вычисления некоторой математической функции [16].

Следующим логическим шагом является создание достаточно протяжённых систем КРК для коммуникации на географических расстояниях. Основной трудностью при этом являются поглощение и рассеяние света, что удобно продемонстрировать на разобранном алгоритме квантовой криптографии (см. [16] для технических подробностей). Если посылать 10^9 фотонов в 1 с через 500 км коммерческого оптоволокна — самый удобный способ передачи, то на другом конце волокна будет зарегистрирован только 1 фотон в 1 с (см. раздел 4). В то же время коммерческие детекторы одиночных фотонов имеют примерно такую же вероятность ложного срабатывания (количество темновых отсчётов), другими словами, половина битов получившегося ключа шифрования окажется неправильной, что делает его бесполезным [13, 16]. Хотя в лабораторных условиях реализовано КРК через 400 км оптоволокна [20], практическое применение существующих систем квантовой криптографии пока ограничено расстоянием порядка 100 км [13].

Для решения указанной проблемы в 1998 г. были предложены *квантовые повторители* [21], способные "компенсировать" потери на поглощение фотонов без нарушения теоремы о запрете клонирования [21, 22]. Квантовые повторители позволят не только реализовать КРК на больших расстояниях, но и создать *квантовый интернет*, *или квантовые сети* [23, 24], в котором квантовые компьютеры — *узлы сети* — связаны между собой квантовыми каналами связи. Основной задачей квантового интернета является распределение квантовой запутанности между узлами сети, что можно использовать для распределённых [24] и защищённых облачных квантовых вычислений, где сервер обрабатывает закодированную информацию [25, 26]; увеличения углового разрешения в астрономии [27, 28]; защищённого распределения сигналов времени и частоты [29]; создания глобальной сети атомных часов с чувствительностью, близкой к квантовому пределу [30 – 32], и метрологии [33 – 35]. Особый интерес представляет реализация метода *аппаратно-независимого КРК* (*device-independent QKD*) [36], в котором узлы сети могут самостоятельно убедиться в полной секретности полученных ключей шифрования посредством измерения квантовых корреляций (неравенства Белла [37]), даже если злоумышленник имеет доступ к квантовой сети. В этом состоит преимущество метода аппаратно-независимого КРК над существующими коммерческими системами КРК, не использующими запутанные состояния.

Целью настоящего обзора является рассмотрение последних экспериментальных результатов в создании крупномасштабных квантовых сетей. В разделе 2 обсуждаются основные компоненты квантовых сетей, раздел 3 посвящён обзору платформ для создания узлов квантовых сетей. Раздел 4 посвящён обзору разных схем квантовых повторителей и экспериментальных результатов. В разделе 5 описывается преобразование фотонов из оптического диапазона в телекоммуникационный, что необходимо для их эффективной передачи по оптоволокну. В разделе 6 обсуждаются методы увеличения радиуса квантовой сети без использования квантовых повторителей.

2. Квантовые сети

Как и классические компьютерные сети, квантовые сети состоят из узлов, каналов связи и конечных пользователей (рис. 1). Основной задачей квантовой сети является генерация запутанных состояний между кубитами, находящимися в разных узлах или у конечных пользователей. Для создания квантовой сети необходимы помимо физических устройств (узлов, однофотонных источни-

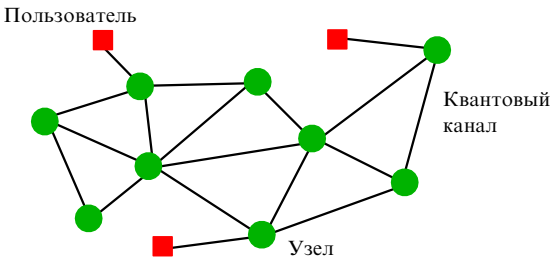

Рис. 1. Квантовая сеть, в которой узлы сети (кружки) и конечные пользователи (квадраты) соединены между собой квантовыми каналами связи. (Рисунок любезно предоставлен Б. Макиелсом (B. Machielse).)

ков) протоколы обмена данных наподобие TCP/IP (Transfer Control Protocol/Internet Protocol), которые позволят подключать к сети разные устройства (например, квантовые компьютеры), не задумываясь о их физической реализации [38]. Ниже перечислены основные физические компоненты квантовой сети.

Квантовый канал. Канал связи должен обладать способностью передавать квантовую информацию между узлами сети и конечными пользователями. Сегодня единственным кандидатом для передачи квантовой информации на макроскопические расстояния является квант света видимого или ближнего инфракрасного диапазона — фотон, распространяющийся в свободном пространстве или по оптоволокну. Чтобы обеспечить информационную безопасность канала связи, необходимо кодировать один бит квантовой информации — *кубит* — одиночным фотоном [16, 19] (или кластерным состоянием) (см. раздел 4.2). Для этого можно использовать разные параметры фотона: его поляризацию, частоту, фазу, время детектирования (time-bin encoding), пространственную моду и др., каждый из которых имеет свои преимущества и недостатки. Стоит отметить, что при создании квантовых сетей в пределах одной лаборатории, например, для соединения нескольких квантовых компьютеров можно использовать также фононы (колебания кристаллической решётки) [39–41] и микроволновые фотоны [42]. Однако они не пригодны для соединения удалённых квантовых узлов — например, для направленного распространения микроволн требуются негибкие металлические волноводы, охлаждённые до температуры порядка 4 К, что абсолютно непрактично.

Источник одиночных фотонов. Одиночные фотоны — важный компонент квантовых сетей. Например, рассмотренный во введении алгоритм BB84 в простейшей форме требует использования именно одиночных фотонов для кодирования информации. Идеальный источник должен испускать одиночный фотон по нажатию кнопки (фотон по желанию). Из множества различных подходов к созданию таких источников [43, 44] наибольший потенциал имеют квантовые точки в двумерных материалах [45] и эпитаксиальные (self-assembled) квантовые точки в микрорезонаторах [46–50].

В 2015 г. был продемонстрирован однофотонный источник на длине волны 1,5 мкм, который использовался для квантовой криптографии на расстоянии до 120 км [51]. Тем не менее надёжного коммерческого источника одиночных фотонов пока не существует. К счастью, во многих протоколах квантовой информации, в том числе протоколе BB84, можно использовать сильно ослабленное когерентное излучение лазеров, в котором вероятность детектирования двух и более фотонов много меньше вероятности детектировать однофотонное состояние. Однако такой лазерный импульс в подавляющем большинстве случаев вообще не будет содержать фотонов, и вероятность получить даже один фотон будет низкой, что существенно замедлит работу квантовой сети. Более того, наличие многофотонной компоненты приводит к возможности прослушивания канала связи, чего, естественно, надо избегать [52, 53]. Таким образом, создание надёжного однофотонного источника остаётся актуальной задачей, решение которой необходимо для создания квантовых сетей.

Фотодетекторы. Наряду с однофотонными источниками существуют детекторы одиночных фотонов. Основными параметрами этих детекторов являются квантовая эффективность, показывающая вероятность срабатывания детектора при попадании в него фотона; темновой ток, равный числу ложных срабатываний в единицу времени, и скорость счёта [54].

Высокая квантовая эффективность необходима не только для увеличения скорости работы квантовой сети (что очевидно), но и для правильной работы многих узлов сети. Действительно, после взаимодействия фотона с кубитом они оказываются запутанными, и только после измерения состояния фотона состояние кубита станет известным. Однако если фотон был потерян или детектор его "пропустил", то состояние кубита останется неизвестным и его надо будет заново инициализировать [55], а поскольку неизвестно, в какой момент детектор не сработал, низкая квантовая эффективность повышает вероятность ошибки квантовых операций (см. раздел 4). Темновой ток тоже увеличивает вероятность ошибки, так как в этом случае создаётся ложное впечатление о получении фотона [16].

До недавнего времени самыми используемыми детекторами одиночных фотонов в квантовой оптике являлись счётчики фотонов на основе лавинных фотодиодов, которые в видимом диапазоне имеют достаточно высокую квантовую эффективность ($> 50\,\%$) и низкий темновой ток (< 100 фотонов в 1 с). Однако такие счётчики намного хуже работают в телекоммуникационном диапазоне (квантовая эффективность $< 20\,\%$, темновой ток > 1000 фотонов в 1 с), который как раз представляет наибольший интерес для квантовых сетей и КРК. Но даже квантовой эффективности около $70\,\%$ часто недостаточно [55]. Недавно появились детекторы на основе сверхпроводящих нанопроволок [56] (в России их производит компания "Сконтел"), которые имеют квантовую эффективность $> 95\,\%$ и темновой ток < 1 фотона в 1 с как в видимом, так и в телекоммуникационном диапазонах [57].

Квантовые узлы. Узлом сети в общем случае является небольшой квантовый компьютер, который может хранить, обрабатывать квантовую информацию и обмениваться ею с другими узлами сети. Подходы к обработке квантовой информации, а следовательно, и к созданию квантовых узлов можно разделить на две большие группы: на основе унитарных обратимых квантовых логических элементов с использованием стационарных кубитов (атомов, ионов, сверхпроводящих кубитов (см. раздел 3)) и на основе необратимых измерений фотонных кластерных состояний [58–60] (см. раздел 4.3). Квантовый узел может выполнять различные функции. Например, он может представлять полноценный квантовый компью-

тер со множеством кубитов или атомные часы, соединённые квантовым каналом с другим узлом, отвечающим за подключение к квантовой сети. В этом обзоре рассматривается только один конкретный тип квантового узла — квантовый повторитель, который необходим для создания протяжённых квантовых сетей.

Квантовый повторитель. Во введении обсуждалось, что рассеяние и поглощение света накладывают ограничение на расстояние между двумя узлами, которые можно соединить напрямую с помощью канала связи. Рассмотрим этот вопрос подробнее. Предположим, что требуется послать фотон по оптоволокну — самый важный с прикладной точки зрения метод — для этого разумно использовать фотоны с длиной волны 1550 нм, на которой кварцевое оптоволокно имеет наименьшие потери: $\alpha = 0{,}18$ дБ км$^{-1}$ [61]. Хотя созданы оптоволокна с ещё более низкими потерями — 0,14 дБ км$^{-1}$ [62], их коммерческое производство ещё не налажено. Вероятность того, что фотон не рассеется после прохождения расстояния L в оптоволокне,

$$p_0 = 10^{-\alpha L/10}\,, \tag{1}$$

показана на рис. 2. Экспоненциальная зависимость (1) объясняет, почему коммерческие системы квантовой криптографии ограничены расстоянием порядка 100 км. Чтобы придать этим числам более наглядный смысл, предположим, что Алиса генерирует перепутанные пары фотонов с частотой 10 ГГц (полоса пропускания современных оптоэлектронных устройств [63]). Тогда при $L = 1000$ км среднее время ожидания Бобом одного фотона составит около одного года! Кардинальный способ решения этой проблемы — передача фотона не по волокну, а через атмосферу или даже спутник (см. раздел 6.1), однако это дороже и менее практично.

Существует несколько способов повысить пропускную способность волоконного канала связи. Например, можно использовать спектральное уплотнение каналов, т.е. передавать по одному волокну одновременно несколько импульсов на разных длинах волн, что позволяет увеличить в ~ 100 раз скорость передачи данных, но такое уплотнение не способно устранить экспоненциальную зависимость (1). С другой стороны, широко применяемые оптоволоконные оптические усилители бесполезны для квантовых сетей, так как квантовая механика запрещает клонирование одиночного фотона [19]. В 1998 году Х. Бригель, В. Дюр, И. Цирак и П. Золлер (Briegel – Dür – Cirac – Zoller, BDCZ) предложили схему *квантового повторителя* [21] на основе квантовой телепортации [64] и обмена запутанностью [65, 66] (BDCZ-протокол). Использование квантовых повторителей "компенсирует" потери в оптоволокне и может заменить экспоненциальную зависимость скорости перепутывания удалённых узлов полиномиальной за счёт увеличения необходимого числа квантовых ресурсов. Очевидно, что квантовый повторитель — это частный случай узла квантовой сети. Протокол BDCZ и его практическая реализация рассматриваются в разделе 4.1. Раздел 4.2 посвящён новому типу квантовых повторителей — *однонаправленным повторителям* (*one-way quantum repeaters*), которые дают многократный выигрыш в быстродействии по сравнению с протоколом BDCZ, а в разделе 4.3 кратко описана схема квантового повторителя на основе фотонных кластерных состояний, который не требует стационарной квантовой памяти.

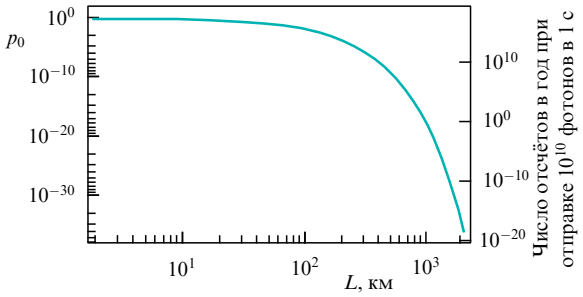

Рис. 2. Влияние рассеяния в оптоволокне на КРК. p_0 — вероятность детектирования фотона на расстоянии L оптоволокна с потерями 0,18 дБ км$^{-1}$. Правая ось ординат показывает количество отсчётов в год при посылке 10^{10} фотонов в 1 с.

Предел прямой передачи. Для сравнения пропускной способности квантовых сетей и демонстрации выигрыша от применения квантовых повторителей удобно использовать КРК, так как оно представляет собой важное приложение таких сетей. В КРК одной из основных характеристик является количество битов ключа шифрования, которые можно получить, посылая один фотон, — *ёмкость канала* (*secret key capacity*). Можно показать, что теоретический верхний предел, который будем называть *пределом прямой передачи*, выражается как [67]

$$r_{\mathrm{DT}} = -\log_2(1 - p_0) \approx 1{,}44\, p_0\,. \tag{2}$$

Очевидно, что для протокола BB84 ёмкость канала

$$r_{\mathrm{BB}} = p_0\,. \tag{3}$$

Использование идеального квантового повторителя уже даёт существенный выигрыш за счёт смены линейной зависимости от p_0 коренной зависимостью [68] (см. раздел 4):

$$r_{\mathrm{QR}} = -\log_2(1 - \sqrt{p_0}\,) \approx 1{,}44\sqrt{p_0}\,, \tag{4}$$

а несколько повторителей могут обеспечить полиномиальную зависимость от расстояния L.

Из-за отсутствия эффективных квантовых повторителей существующие квантовые сети ограничены двумя узлами и расстоянием порядка нескольких метров или километров [71 – 75] (рис. 3), но уже такие относительно простые сети использовались для проверки теории скрытых параметров в квантовой механике [69, 70]. Однако практическое использование этих сетей, например, для аппаратно-независимого КРК пока невозможно из-за относительно низкого качества перепутанных состояний или очень малой скорости их генерации. Также стоит отметить недавно созданную квантовую сеть на основе двух сверхпроводящих квантовых компьютеров, разнесённых на 10 м друг от друга и связанных криогенным каналом для микроволновых фотонов (группа Андреаса Вальрафа (Andreas Wallraff) [42]). Хотя такой сетью невозможно покрыть целый город, она может пригодиться для создания кластера из квантовых компьютеров — квантового суперкомпьютера.

3. Квантовые узлы

Квантовые узлы, фактически являясь квантовыми компьютерами, должны уметь хранить, обрабатывать квантовую информацию и обмениваться ею с другими узлами. Наиболее распространённый и интуитивно

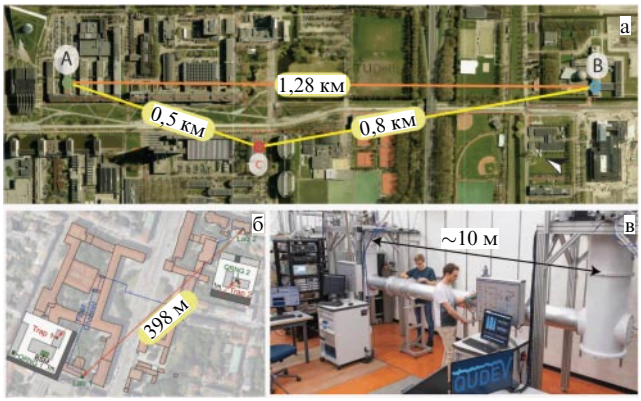

Рис. 3. Примеры квантовых сетей. (а) Аэрофотография кампуса Делфтского технического университета (Нидерланды). Перепутанные кубиты на основе NV-центров в точках A и B, разнесённые на 1,28 км, использовались для проверки неравенств Белла. (Рисунок из работы [69] воспроизводится с разрешения © 2015 Springer Nature.) (б) Карта кампуса Мюнхенского университета Людвига – Максимилиана (Германия); два одиночных атома на расстоянии 398 м использовались для проверки неравенств Белла [70] (рисунок воспроизводится из работы [70], опубликованной под лицензией Creative Commons Attribution 4.0 International). (в) Квантовая сеть из двух сверхпроводящих кубитов, расположенных в разных криостатах (Высшая техническая школа Цюриха (Швейцария)) [42] (рисунок воспроизводится из работы [42] с разрешения © 2021 American Physical Society (APS)).

понятный подход к обработке квантовой информации основан на унитарных квантовых операциях над стационарными кубитами — квантовых логических цепях (квантовые узлы исходя из альтернативной парадигмы, использующей фотонные кластерные состояния, рассмотрены в разделе 4.3). В этом случае для обработки квантовой информации используются одно- и двухкубитовые квантовые операции. Их конкретная реализация зависит от типа кубитов, однако однокубитовые операции в основном осуществляются посредством взаимодействия кубита с внешним электромагнитным полем [76 – 79]. Возможно также применение акустических волн для управления твердотельными кубитами [80, 81], а поскольку такие волны взаимодействуют практически со всеми твердотельными кубитами, их можно использовать для создания гибридных систем [41], которые будут сочетать в себе достоинства разных платформ. Взаимодействие с акустическими волнами также находит применение в квантовых преобразователях длины волны (см. раздел 5). Двухкубитовые операции могут осуществляться за счёт "включения" контролируемого взаимодействия между кубитами [82, 83].

Перечислим в явном виде основные требования к квантовым узлам, необходимые для создания квантового повторителя [84]:

1) наличие кубитов с длительной квантовой памятью и возможностью эффективных инициализации и считывания;

2) наличие нескольких кубитов на узел;

3) возможность проведения двухкубитовых операций;

4) запись фотона в память;

5) испускание фотона в моду оптоволокна;

6) масштабируемость.

Критерий 1 необходим для хранения квантовой информации, а несколько кубитов (пункты 2, 3) необходимо, например, для *дистилляции квантовой запутанности* [85] между узлами сети, позволяющей из нескольких копий запутанных состояний (для их хранения как раз и требуется несколько кубитов) создать одно, имеющее лучшие характеристики, что необходимо для эффективной работы квантовых повторителей (см. раздел 4.1). Взаимодействие с одиночными фотонами (критерии 4, 5) служит для коммуникации с соседними узлами, а масштабируемость (критерий 6) нужна для коммерциализации.

Стоит отметить, что выполнение всех критериев не гарантирует, например, что квантовый повторитель даст практический выигрыш в скорости работы квантовой криптографии (см. раздел 4.1.2). Сегодня существует много платформ, удовлетворяющих некоторым из указанных критериев, но такой системы, которая сочетала бы в себе все эти свойства, пока не создано. Некоторые критерии могут быть ослаблены в случае специализированных квантовых узлов; например, ряд протоколов однонаправленных квантовых повторителей не требует длительной квантовой памяти [86] (см. раздел 4.2).

Основываясь на критериях 4, 5, можно выделить две группы кубитов: когерентно взаимодействующие со светом видимого или инфракрасного диапазона (атомы, ионы) и не взаимодействующие (сверхпроводящие кубиты). Последние нуждаются в квантовых преобразователях (quantum transducers), которые пока ещё далеки от совершенства, несмотря на значительный прогресс в этой области [87, 88] (см. раздел 5). В дальнейшем будут обсуждаться только взаимодействующие со светом кубиты. Их можно разделить на две большие подгруппы: кубиты на атомах и ионах в ловушках [89] и твердотельные кубиты (центры окраски, квантовые точки) [90].

Хотя нейтральные атомы и ионы являются перспективными платформами для квантовых симуляций [91, 92], сложность экспериментальных установок делает их малопригодными для широкого использования [93, 94] (нарушение критерия 5). Однако стоит отметить атомные и ионные ловушки на чипах с интегрированными резонаторами [95, 96], которые имеют практический потенциал для квантовых сетей. Также наличие в атомах узких часовых переходов позволит создать квантовую сеть из оптических часов [30 – 32].

Наибольший практический интерес представляют твердотельные кубиты, которые можно интегрировать на чипе с однофотонными источниками, фотодетекторами и нанофотонными оптическими элементами [97, 98]. Такие системы намного проще и надёжнее атомных ловушек, и они могут в принципе производиться в больших масштабах (критерий 6). В то же время выполнение критериев 1 – 3 зависит от конкретного вида кубита и не имеет универсального решения.

3.1. Оптические резонаторы

Для удовлетворения приведённых выше критериев 4 и 5 необходимо детерминистическое взаимодействие между кубитом и фотоном, однако сечение рассеяния фотона изолированным кубитом слишком мало́. Общепринятым методом решения этой проблемы является помещение кубита в оптический резонатор, в котором благодаря многократному отражению фотона от зеркал вероятность его взаимодействия с кубитом возрастает в $\propto Q/V$ раз (эффект Парселла), где Q — добротность резонатора, V — объём моды резонатора [99 – 101].

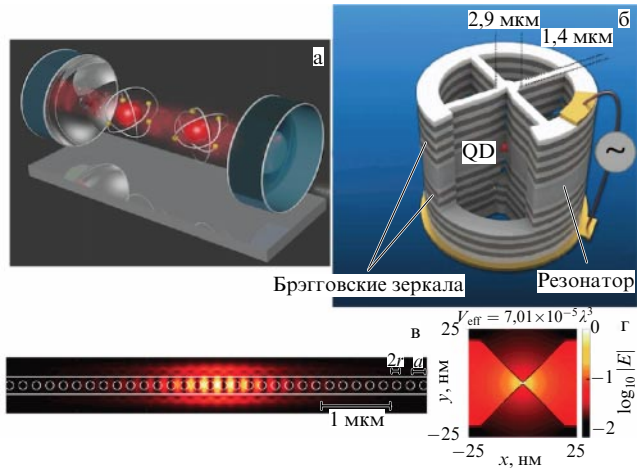

Рис. 4. Оптические резонаторы. (а) Резонатор Фабри – Перо с двумя разнесёнными зеркалами (рисунок воспроизводится с разрешения © St. Welte, Max-Plank Institute for Quantum Optics). (б) Микрорезонатор с брэгговскими зеркалами (рисунок воспроизводится из работы [108], опубликованной под лицензией Creative Commons CC BY). (в) Фотонно-кристаллический резонатор (рисунок воспроизводится из работы [109] с разрешения © 2017 AIP Publishing). (г) Резонатор с экстремально малым объёмом моды (рисунок воспроизводится из работы [106] с разрешения © 2017 American Physical Society).

Таким образом, желательно иметь высокодобротный резонатор с как можно меньшей длиной.

На рисунке 4 приведены разные варианты резонаторов. Резонатор Фабри – Перо с двумя диэлектрическими зеркалами (рис. 4а) используется в экспериментах с нейтральными атомами [95, 102] и центрами окраски в твёрдых телах [103 – 105], и хотя его добротность может быть достаточно высокой, достижение малого объёма моды и стабилизация длины требуют значительных усилий. При работе с твердотельными кубитами появляется возможность изготовить резонаторы на основе брэгговских зеркал или фотонных кристаллов (рис. 4б, в) с интегрированными кубитами и объёмом моды порядка куба длины волны. Фотонно-кристаллические резонаторы теоретически могут иметь объём моды меньше 10^{-3} длины волны в кубе [106, 107] (рис. 4г), однако внедрение кубитов в такие резонаторы пока не удалось осуществить.

Важным параметром системы кубит – резонатор является *кооперативность*, учитывающая спектральное уширение оптического перехода кубита:

$$C = \frac{4g^2}{\kappa\gamma}\,, \tag{5}$$

где $g \propto 1/\sqrt{V}$ — частота Раби для одиночного фотона, $\kappa \propto 1/Q$ и γ — спектральные ширины резонатора и оптического перехода в кубите (с учётом разного рода уширений). Когда $C \gg 1$, кубит когерентно взаимодействует с одиночным фотоном и становится возможным создание высокоэффективных логических операций между ними [110]. Этот режим был достигнут с нейтральными атомами ($C \geqslant 100$ [95]), центрами окраски в алмазах ($C \geqslant 100$ [55]), квантовыми точками ($C \geqslant 100$ [111]) и ионами ($C \approx 10$ [112, 113]).

Существует большое число твердотельных кубитов [114 – 116], в разделах 3.2 – 3.6 кратко рассматриваются самые перспективные из них.

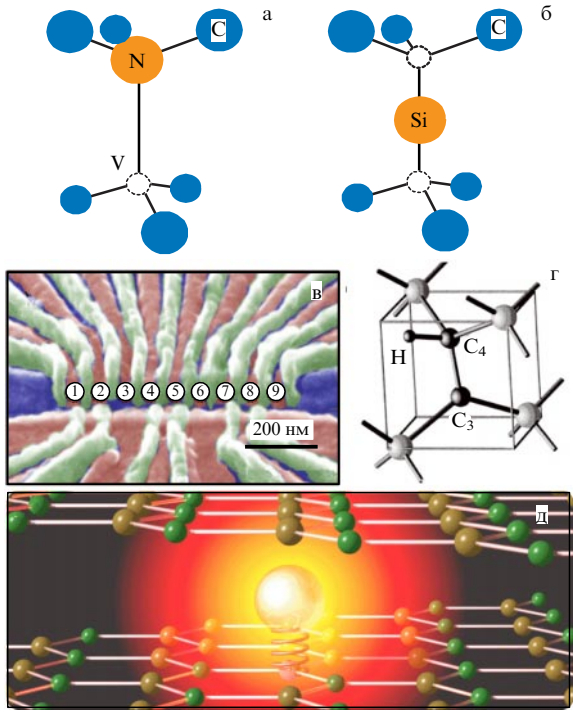

Рис. 5. (В цвете онлайн.) Примеры твердотельных кубитов. (а) NV-центры в алмазе, синие кружки — атомы углерода (C), белые кружки — вакансии (V) в кристаллической решётке, N — примесный атом азота, замещающий один атом C. (б) SiV-центр в алмазе, примесный атом кремния (Si) находится в междоузлии, обеспечивая более высокую степень симметрии, чем NV-центры. (в) Массив электронных квантовых точек в кремнии (рисунок воспроизводится из работы [128], опубликованной под лицензией Creative Commons Attribution 4.0 International License). (г) Структура T-центра в кремнии. Два атома углерода (C_3, C_4) замещают один атом кремния, и атом водорода соединён с C_4 (рисунок воспроизводится из работы [129] с разрешения © 1996 American Physical Society). (д) Примесный атом, находящийся между двумя слоями гексагонального нитрида бора (hBN) [130] (рисунок воспроизводится из работы [131] с разрешения © 2020 American Physical Society).

3.2. Азотно-вакансионные центры в алмазе

Азотно-вакансионные (NV) центры окраски в алмазе образованы атомом азота, замещающим атом углерода, и вакансией в близлежащем узле решётки (рис. 5а). Оптический переход на длине волны ~ 637 нм происходит между электронными энергетическими уровнями, находящимися в запрещённой зоне алмаза, а квантовая память основана на электронном и ядерном спинах. NV-центры после детектирования одиночного NV-центра в 1997 г. [117] стали основой для множества прорывных экспериментов в квантовой оптике [118] и магнитометрии [119]. За последние десятилетия проделана огромная работа по созданию квантового узла на основе NV-центра. Например, продемонстрированы квантовая память с временем когеренции более 1 с и регистр из 10 кубитов на основе ядерных спинов с двухкубитовыми операциями [120, 121]. Кроме того, реализованы квантовая запутанность пространственно разнесённых кубитов и дистилляция запутанности [72, 122]. Таким образом, NV-центры удовлетворяют всем приведённым выше требованиям, кроме критериев 4 – 6, — они слабо взаимодействуют со светом.

Попытки поместить NV-центры в нанорезонаторы приводят к большому неоднородному уширению опти-

ческого перехода (γ в уравнении (5)) [123], что пока не позволило достичь режима $C > 1$, необходимого для эффективного взаимодействия с фотонами. Основной проблемой являются линейный эффект Штарка и электрические шумы в материале нанорезонатора. Линейная восприимчивость NV-центров к электрическому полю объясняется наличием ненулевого статического дипольного электрического момента (~ 1 Д) из-за разной электроотрицательности азота и вакансии [124] (см. рис. 5), которую устранить невозможно. Хотя природа электрических шумов до конца не ясна, скорее всего, они вызваны изменением зарядового состояния дефектов кристаллической решётки под действием лазерного излучения, необходимого для контроля над NV-центром. Эти шумы можно минимизировать путём более щадящей нанофабрикации [125], но перспективы использования NV-центров для квантовых повторителей пока выглядят туманными [126].

Альтернативный подход основан на преобразовании телекоммуникационного фотона в механические колебания (с помощью оптомеханических резонаторов), которые взаимодействуют с электронным спином NV-центра либо непосредственно [40, 80], либо через модуляцию магнитного поля [127]. Это позволит в будущем обойти проблему электрических шумов и создать интерфейс между NV-центром и фотоном, работающий при комнатной температуре.

3.3. Кремний-вакансионные центры в алмазе

Кремний-вакансионные (SiV) центры окраски в алмазе состоят из двух вакансий в соседних узлах кристаллической решётки и атома кремния посредине между ними (рис. 5б). Так же как и в случае NV-центров, оптический переход на длине волны ~ 737 нм происходит между электронными энергетическими уровнями, находящимися в запрещённой зоне алмаза, а квантовая память основана на электронном и ядерном спинах. SiV-центры были открыты в Физическом институте им. П.Н. Лебедева (ФИАН) в 1980 г. [132 – 134], и в течение длительного времени они считались нежелательной примесью в алмазе и служили индикатором искусственного происхождения алмазов. Всё изменилось в 2006 г., когда обнаружили, что SiV-центры являются источниками одиночных фотонов [135], а в 2016 г. впервые были запутаны два твердотельных кубита, находящихся в одной наноструктуре (нановолновод) [136]. В 2019 г. был создан первый твердотельный квантовый узел с временем квантовой когеренции более 1 мс, двумя кубитами и детерминистическим взаимодействием с фотонами [137, 138], тем самым SiV-центры удовлетворяют всем критериям. Более того, квантовый узел имеет полосу пропускания больше 10 ГГц благодаря малому времени жизни возбуждённого уровня в нанорезонаторах. На базе этого узла в 2020 г. продемонстрирован первый повторитель, который преодолел предел прямой передачи (см. раздел 4.1.2).

Термально-возбуждённые акустические фононы в алмазе при температуре 4 К имеют частоту около 100 ГГц, что совпадает с величиной тонкого расщепления основного состояния SiV-центров (50 – 200 ГГц), их резонансное рассеяние ограничивает когерентность SiV-центров при температуре 4 К временем порядка 100 нс [139]. Достижение времени когерентности более 1 мс требует охлаждения до температур $\sim 100 - 500$ мК [139, 140], что в свою очередь требует дорогостоящих криостатов растворения и ограничивает масштабируемость.

Основной причиной успеха SiV-центров является высокая симметрия, а именно наличие центра инверсии [141] (см. рис. 5), который гарантирует отсутствие статического электрического момента и, следовательно, SiV-центры испытывают только квадратичный эффект Штарка. Это приводит к небольшому уширению оптического перехода в нанорезонаторах (на несколько естественных ширин) [142], позволяя достичь режима $C \geqslant 100$ [55]. Понимание этого факта послужило толчком к исследованию других центров окраски, которые имеют центр инверсии [141] или разница дипольных моментов уровней оптического перехода в которых близка к нулю [124]. Например, центры окраски в алмазе на основе других примесных атомов III [143] и IV групп: GeV [134, 144, 145], SnV [146, 147] и PbV [148] — тоже обладают симметрией относительно инверсии и могут работать при более высоких температурах, близких к 4 К, но их изучение находится на начальном этапе.

3.4. Широкозонные полупроводники

Причина наличия большого числа центров окраски в алмазе — это большая ширина запрещённой зоны ($\sim 5{,}5$ эВ), что делает центры окраски, излучающие в видимом и ближнем инфракрасном (ИК) диапазонах, фотостабильными. Конечно, существуют и другие широкозонные полупроводники.

Гексагональный нитрид бора. Этот материал с запрещённой зоной шириной ~ 6 эВ содержит множество центров окраски, которые сейчас активно изучаются [149 – 152]. Однако один центр окраски заслуживает отдельного обсуждения. В отличие от спектральной ширины всех других известных центров окраски, его спектральная ширина практически не зависит от температуры: при температуре 300 К наблюдается фурье-ограниченная линия шириной около 60 МГц [130, 131]! Для сравнения, типичная спектральная ширина остальных центров окраски порядка нескольких нанометров. Хотя природа этого дефекта ещё плохо изучена, как и его структура, считается, что примесный атом находится между слоями hBN (рис. 5д) и слабо взаимодействует с фононами [130, 131]. Пока неизвестно, есть ли у этого центра электронный спин, необходимый для квантовой памяти, но его можно использовать для создания источника одиночных фотонов с фурье-ограниченной спектральной шириной даже при комнатной температуре.

Карбид кремния. Данный полупроводник имеет запрещённую зону 2,3 – 3,3 эВ в зависимости от политипа. Хотя кристаллическая структура SiC не позволяет центрам окраски иметь центр инверсии, важность которого упоминалась выше, тем не менее один центр — кремний – вакансия — обладает одинаковыми статическими электрическими моментами в основном и возбуждённом энергетических уровнях [124], что обеспечивает его эффективную интеграцию в оптические нанорезонаторы.

Большой потенциал имеют также несколько центров окраски, которые обладают квантовой памятью с временем когеренции больше 1 мс при температуре 4 К и излучают в телекоммуникационном диапазоне [153, 154], что делает ненужным преобразование длины волны.

3.5. Т-центры в кремнии

Процессы нанофабрикации перечисленных выше полупроводников очень сложны, что ограничивает их возможности и увеличивает стоимость производства. Наиболее технологичным материалом является кремний, для которого мировая полупроводниковая промышленность разработала методы очистки и нанофабрикации. Поэтому было бы очень удобно построить квантовые сети на основе центров окраски в кремнии, однако малая ширина запрещённой зоны (1,14 эВ) приводит к тому, что большинство центров окраски, излучающих в телекоммуникационном диапазоне, оказываются фотонестабильными из-за двухфотонной ионизации. Однако недавние результаты с Т-центрами (открытыми ещё в 1996 г. [129]) указывают на их фотостабильность [155, 156]. Большое время квантовой памяти (~ 1 мс для электронного и ~ 1 с для ядерного спинов) и длина волны 1,326 нм, попадающая в телекоммуникационный диапазон [155, 156], делают Т-центр перспективным кандидатом для создания квантовых узлов.

3.6. Квантовые точки

Квантовыми точками (КТ) называют полупроводниковые приборы, в которых движение носителей заряда квантовано во всех трёх пространственных направлениях (0-размерные системы) [157]. Кратко рассмотрим два типа КТ, представляющих интерес для квантовых сетей.

Эпитаксиальные (self-assembled) КТ — наноразмерные гетероструктуры (~ 10 нм). В них за счёт сочетания полупроводников с разными ширинами запрещённой зоны становится возможным пространственно локализовать носители заряда, а малый размер приводит к дискретным уровням энергии [158]. Кубитом является спин электрона, захваченного квантовой точкой, а испускание фотона осуществляется возбуждением электрона и переходом его в зону проводимости с последующей излучательной рекомбинацией получившегося экситона (пары электрон–дырка) [159]. Такие КТ после помещения в нанорезонаторы демонстрируют отличные оптические свойства и могут иметь кооперативность $C > 100$ с одиночным фотоном [111, 158]. С другой стороны, подходящие прямозонные полупроводники (например, GaAs) не имеют бесспиновых изотопов. Магнитное диполь-дипольное взаимодействие между этими ядерными спинами и спином захваченного электрона приводит к декогеренции последнего и ограничивает время квантовой памяти несколькими микросекундами [160]. Этого времени когерентности недостаточно для многофункционального квантового узла, но оно подходит для некоторых протоколов квантовых повторителей (см. раздел 4.2) или создания источника одиночных фотонов.

Другой класс составляют *электронные* (*gate-defined*) КТ, в которых двумерный электронный газ, образованный вблизи поверхности полупроводника, захвачен в электростатические ловушки, созданные напылёнными электродами [161]. Длительная квантовая память (более 20 мс [162]) благодаря использованию материалов с бесспиновыми изотопами, детерминированное создание массива КТ, возможность осуществлять квантовые операции между ними [163] делают такие КТ кандидатами для использования в квантовых компьютерах [164]. Однако электронные КТ не являются оптически активными, что затрудняет их применение для создания квантовых узлов.

Интересным и перспективным направлением является создание КТ в полупроводниковых двумерных материалах толщиной в один или два атомных слоя [165]. Например, дихалькогениды переходных металлов [166] обладают прямой запрещённой зоной, большой энергией связи экситона [167, 168] и могут быть изготовлены из бесспиновых изотопов. Это позволяет надеяться на создание КТ, которые одновременно являются оптически активными [169, 170] и имеют длительную квантовую память, что необходимо для конструирования квантового узла.

4. Квантовые повторители

Квантовые повторители — это частный случай узла квантовой сети. Задачи квантового повторителя аналогичны задачам классического волоконного усилителя: "компенсировать" рассеяние света в оптоволокне и обеспечить обмен квантовой информацией между удалёнными узлами сети [21], заменяя экспоненциальную зависимость (1) полиномиальной.

4.1. Протокол BDCZ

Кратко рассмотрим первый протокол квантового повторителя (BDCZ), предложенный в 1998 г. Разделим канал связи длиной L между Алисой и Бобом на $N+1$ равных отрезков, поместив N дополнительных узлов (рис. 6) — квантовых повторителей, каждый из которых имеет два кубита, L_i и R_i, способных долго хранить квантовую информацию. Затем приведём кубиты R_i и L_{i+1} смежных узлов в максимально запутанное состояние [72, 171], используя квантовый канал связи между ними (например, разделив между ними ЭПР-пару (ЭПР — Эйнштейн, Подольский, Розен) фотонов). Потом создаём запутанность между кубитом A и L_1 и между B и R_N. Из-за потерь в оптоволокне генерация делокализованного запутанного состояния — это случайный процесс, и если бы квантовые повторители не обладали длительной квантовой памятью, то полная вероятность *синхронного* попарного перепутывания всех смежных узлов была бы по-прежнему $\exp(-\alpha L/10)$. Однако квантовая память позволяет осуществить этот процесс *асинхронно*, тем самым устраняя экспоненциальную зависимость от расстояния.

Следующим шагом является обмен запутанностью [65, 66]. Например, если узел k измерит два своих кубита

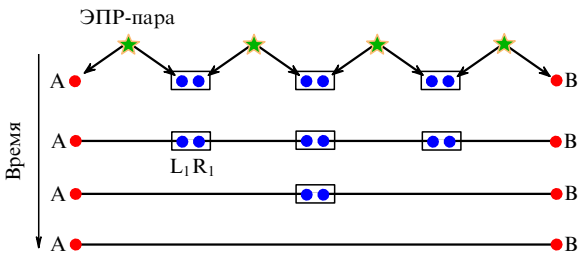

Рис. 6. (В цвете онлайн.) Схема работы квантового повторителя. Требуется перепутать два кубита, находящихся у Алисы (A) и Боба (B). Между ними установлены квантовые повторители (чёрные прямоугольники), содержащие по два кубита, L и R (синие кружки). Источники ЭПР-пар (звёзды) распределяют перепутанные фотоны между соседними узлами.

в базисе состояний Белла [172], то кубиты R_{k-1} и L_{k+1} окажутся запутанными. После повторения этого процесса со всеми N узлами кубиты у Алисы и Боба будут запутаны — искомая цель достигнута. Наглядный пример, как работает асинхронность, рассмотрен в разделе 4.1.1.

Конечно, это рассуждение не учитывает многих физических ограничений существующих систем. Например, частичная декогеренция ЭПР-пары в процессе распространения в оптоволокне и конечная вероятность ошибки локальных квантовых операций над кубитами квантового повторителя приводят к "неидеальности" перепутанного состояния $|\Psi\rangle$ между смежными узлами. Если *точность* этого состояния равна $\langle\Psi|\Psi_0\rangle = 1 - v$, где $|\Psi_0\rangle$ — одно из максимально запутанных двухкубитовых состояний (состояний Белла), то точность конечного запутанного состояния между Алисой и Бобом можно оценить как $P = 1 - Nv \approx \exp(-Nv)$, т.е. она экспоненциально уменьшается с возрастанием числа квантовых повторителей. При этом если $P < 85\,\%$, то такое состояние уже нельзя использовать для КРК [16].

Для повышения точности запутанного состояния необходимо использовать *дистилляцию запутанности* [85, 173, 174], при которой из нескольких копий запутанных состояний создаётся одно, имеющее лучшие характеристики. Вероятность ошибок при локальных квантовых операциях можно также уменьшить *алгоритмами квантовой коррекции ошибок* [175, 176]. Все эти шаги увеличивают необходимое количество ресурсов (кубитов), усложняют создание квантовой сети и понижают скорость её работы. Более подробно проблемы числа необходимых ресурсов и коррекции ошибок рассмотрены в работах [177, 178].

Эффективная имплементация протокола квантового повторителя затруднена отсутствием физической платформы для кубита, который удовлетворял бы всем критериям, перечисленным в разделе 3. Тем не менее за прошедшие два десятилетия была проделана огромная работа: созданы прототипы квантовых узлов на основе атомных ансамблей [71, 179–181] (использующие модифицированный протокол [22, 182, 183]), центров окраски [72, 120, 121, 137], сверхпроводящих кубитов [10, 82, 184, 185], ионов [186–189] и нейтральных атомов [102]. Однако большинство из этих систем не могут увеличить пропускную способность канала связи, что является целью квантового повторителя. Виной тому — кратковременная квантовая память, отсутствие эффективного интерфейса с оптическими фотонами и конечная точность локальных квантовых операций (см. раздел 4.1.2).

4.1.1. Асинхронность. Для наглядной демонстрации того, как именно квантовая память помогает увеличить пропускную способность квантовой сети, рассмотрим модифицированный протокол КРК BB84, не зависящий от измерительной аппаратуры (Measurement-Device-Independent QKD, MDI-QKD) [16, 190]. Для этого Алиса и Боб посылают одиночные фотоны Чарли, который находится посредине между ними (на расстояния $L/2$ от каждого из них) (рис. 7). Чарли производит измерение фотонов, полученных от Алисы и Боба, в базисе состояний Белла $(\{(|00\rangle \pm |11\rangle)/\sqrt{2}, (|01\rangle \pm |10\rangle)/\sqrt{2}\}$, где $|0\rangle$ и $|1\rangle$ — квантовые состояния посланных фотонов), после чего публично сообщает результаты измерений. Такое измерение говорит только о том, передали ли Алиса и

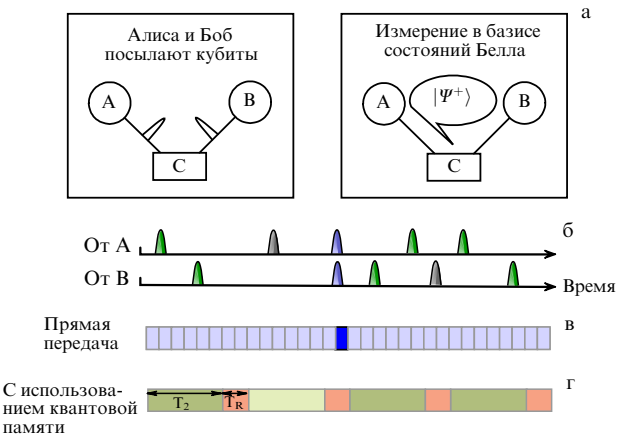

Рис. 7. (В цвете онлайн.) Выигрыш от использования квантовой памяти [55]. (а) Схема MDI-QKD: Алиса (A) и Боб (B) посылают фотоны Чарли (C), который проводит их измерение в базисе состояний Белла. (б) Фотоны, достигшие Чарли. (в) В отсутствие квантовой памяти Чарли может провести измерения, только когда оба фотона от Алисы и Боба долетели до него одновременно (синий прямоугольник). (г) Квантовая память позволяет Чарли проводить измерения асинхронно (тёмно-зелёные прямоугольники), что повышает вероятность успеха. (Рисунок воспроизводится из работы [55] с разрешения © 2000 Springer Nature.)

Боб одинаковые биты или нет, но не раскрывает значения битов. Этого достаточно Алисе и Бобу, чтобы сформировать общий ключ шифрования, но такой информации не хватит злоумышленнику. Очевидно, что если Чарли не имеет квантовой памяти, то фотоны от Алисы и Боба должны достигнуть Чарли синхронно, чтобы измерение было успешным. Так как вероятность того, что фотон от Алисы или Боба достигнет Чарли, равна $\sqrt{p_0}$, то вероятность успеха — оба фотона одновременно достигли Чарли — по-прежнему равна $\sqrt{p_0}\,\sqrt{p_0} = p_0$ (1).

Эта схема имеет два основных преимущества по сравнению с BB84. Во-первых, степень секретности легко определить проверкой нарушения неравенств Белла, даже если злоумышленник контролирует аппаратуру у Чарли. Во-вторых, поскольку канал связи содержит одновременно два фотона (на бит информации), отношение сигнал/шум во время детектирования будет выше, позволяя увеличить скорость генерации ключа шифрования [190].

Пусть теперь Чарли имеет в своём распоряжении простой, состоящий из двух кубитов, C_l и C_r, с временем когерентности T_2, квантовый компьютер, способный записывать состояния одиночных фотонов на эти кубиты. Рассмотрим следующий протокол.

1. Алиса и Боб посылают Чарли одиночные фотоны с частотой f.

2. Если Чарли получил фотон от Алисы (Боба), то он записывает его квантовое состояние в свой кубит C_l (C_r) и игнорирует все последующие фотоны от Алисы (Боба).

3. Шаги 1 и 2 повторяются до тех пор, пока Чарли не получит оба фотона. Если за время T_2 этого не произошло, то всё повторяется сначала.

4. Теперь Чарли, используя локальные операции на своём квантовом компьютере, производит измерение кубитов C_l и C_r в базисе состояний Белла.

За время T_2 Алиса и Боб пошлют по $n = fT_2$ фотонов. Если не использовать квантовую память и если $np_0 \ll 1$,

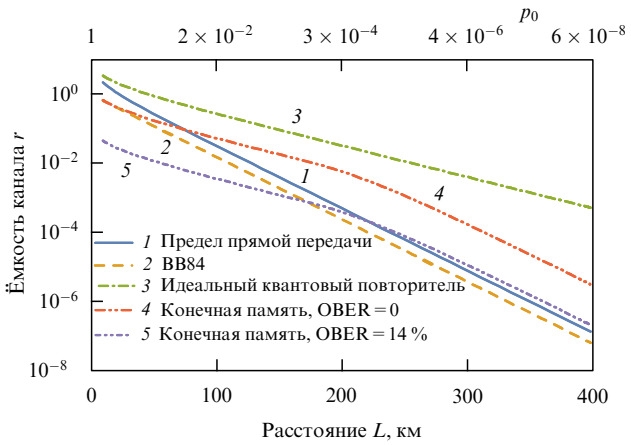

Рис. 8. (В цвете онлайн.) Ёмкость квантового канала для КРК на расстоянии L оптоволокна с потерями 0,18 дБ км$^{-1}$ и идеальным фотодетектором (квантовая эффективность 100 %, нулевой темновой ток). *1* — предел прямой передачи; *2* — идеальный протокол BB84; *3* — идеальный квантовый повторитель; *4* — квантовый повторитель, разобранный в разделе 4.1, с $n = 50$; *5* — квантовый повторитель с $n = 50$ и QBER = 14 %.

то за время T_2 оба фотона хотя бы один раз синхронно достигнут Чарли с вероятностью np_0 или в общем случае:

$$p_{\mathrm{DT}} = 1 - (1 - p_0)^n \approx np_0\,. \tag{6}$$

Однако если использовать квантовую память, то тогда достаточно, чтобы фотоны достигли Чарли асинхронно за время T_2. Вероятность того, что фотон от Алисы или Боба достигнет Чарли за n попыток, равна $n\sqrt{p_0}$. Так как теперь фотоны от Алисы и Боба могут быть зарегистрированы асинхронно, полная вероятность успеха будет n^2p_0 или в общем случае

$$p_{\mathrm{QR}} = \left(1 - (1 - \sqrt{p_0}\,)^n\right)^2 \approx n^2p_0\,. \tag{7}$$

Видно, что квантовая память даёт выигрыш, пропорциональный n — числу попыток послать фотон за время когерентности квантовой памяти. Более точное сравнение требует нахождения ёмкости канала для каждого случая. Для рассматриваемого метода КРК, не зависящего от измерительной аппаратуры, ёмкость канала — это количество бит секретного ключа, которое можно получить, посылая одну *пару* фотонов. Для бесповторительного метода мы, очевидно, имеем

$$r_{\mathrm{DT}} = \max\left(\frac{p_{\mathrm{DT}}}{n}\right) \approx p_0\,, \tag{8}$$

что, естественно, совпадает с пределом прямой передачи (2) (см. раздел 2). Для квантового повторителя

$$r_{\mathrm{QR}} = \max\left(\frac{p_{\mathrm{QR}}}{n}\right) \approx \sqrt{p_0}\,, \tag{9}$$

который достигается при

$$T_2^{\mathrm{opt}} \propto \frac{1}{\sqrt{p_0}}\,. \tag{10}$$

Таким образом, квантовый повторитель действительно может дать существенный выигрыш в скорости работы квантовой сети (рис. 8).

4.1.2. Предел прямой передачи. Основной трудностью в демонстрации квантового повторителя, который мог бы увеличить пропускную способность квантового канала связи по сравнению с пределом прямой передачи, является необходимость создания квантового узла, имеющего одновременно: а) большое время квантовой памяти T_2 и б) высокую точность квантовых операций. Необходимость первого условия (а) следует из (10).

Рисунок 8 показывает, как конечное время квантовой памяти сказывается на производительности квантового повторителя. Неточность квантовых операций приведёт к тому, что Алиса и Боб обнаружат ошибки в полученном ключе шифрования. Такие ошибки могут быть вызваны не только неточностью квантовых операций, но и действиями злоумышленника, поэтому Алисе и Бобу необходимо *дистиллировать* ключ шифрования, чтобы обеспечить его секретность [16]. Это в свою очередь приводит к тому, что конечный ключ шифрования будет содержать только $1-\mathrm{QBER}/15\,\%$ битов изначального ключа, где QBER (Quantum Bit Error Rate) — полная вероятность ошибки. Например, при QBER $\approx 14\,\%$ можно будет использовать только 7 % битов (см. рис. 8), а если QBER $> 15\,\%$, то ключ шифрования создать невозможно.

Лишь недавно удалось разрешить указанные трудности и преодолеть предел прямой передачи, используя квантовый узел, состоящий из SiV-центра в алмазе [137], помещённого в фотонокристаллический резонатор (рис. 9). В работе [55] продемонстрирован простейший метод КРК, который в четыре раза быстрее, чем прямая передача фотона после дистилляции, и в 80 раз быстрее, чем передача без дистилляции (см. рис. 9). Разный наклон красной и зелёных прямых на рис 9в отражает выигрыш за счёт замены линейной зависимости от p_0 коренной зависимостью (см. (2) и (4)).

Более того, полученная QBER $< 11\,\%$ обеспечивает стойкость КРК для любых видов атак [16]. Этого удалось достигнуть благодаря высокой кооперативности, $C > 100$, длительной квантовой памяти (> 100 мкс) и возможности измерить состояние SiV-центра с точностью $F > 0{,}99$. В этом эксперименте эффективные потери между Алисой и Бобом составляли 80 дБ, что соответствует $L = 400$ км оптоволокна на длине волны 1550 нм. Здесь следует заметить, что SiV-центры испускают фотоны на длине волны 737 нм и их необходимо сначала преобразовать в телекоммуникационный диапазон (см. раздел 5).

4.2. Однонаправленные квантовые повторители

Квантовые повторители, рассмотренные выше, обладают рядом существенных недостатков. Так как генерация перепутанности между соседними узлами происходит в случайные моменты времени, такие узлы нуждаются в кубитах с длительной квантовой памятью. Это также приводит к необходимости двустороннего обмена классической информацией между узлами для подтверждения успешности каждой операции (two-way signaling). Всё это ограничивает скорость работы квантовой сети [89, 177]. Для устранения указанных недостатков разработаны схемы, названные *однонаправленными квантовыми повторителями* (*one-way quantum repeaters*), в которых информация распространяется последовательно по всей цепочке квантовых повторителей, напоминая классические компьютерные сети [86, 193–196]. В

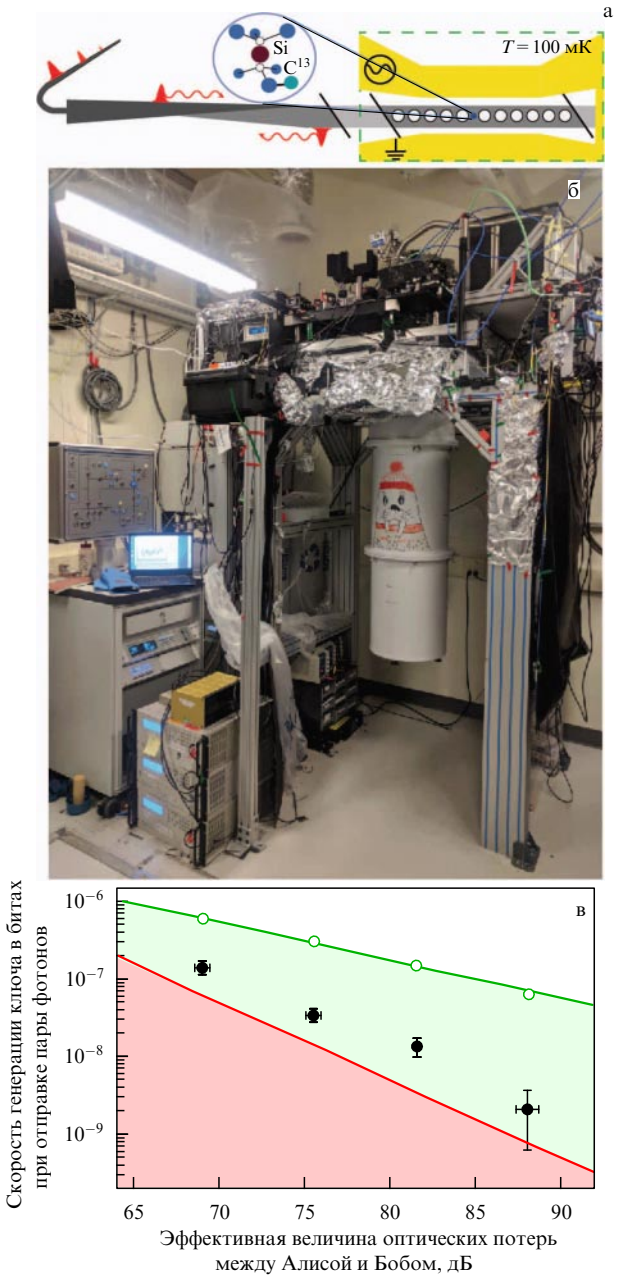

Рис. 9. (В цвете онлайн.) Преодоление предела прямой передачи. (а) Схема квантового узла: SiV-центр находится в центре фотонно-кристаллического резонатора (серый прямоугольник), вокруг него напылён золотой сверхвысокочастотный (СВЧ) волновод (жёлтый), фотонный резонатор адиабатически соединён с одномодовым оптоволокном (слева) (рисунок воспроизводится из работы [191] с разрешения © 2019 American Physical Society). (б) Фотография экспериментальной установки: в центре — криостат растворения, в который помещается алмазный образец. (в) Скорость генерации ключа шифрования в зависимости от эффективной величины оптических потерь между Алисой и Бобом. Красная линия — теоретический предел для MDI-QKD при прямой передаче (2). Зелёные кружки — скорость генерации ключа без дистилляции (sifted key rate) с использованием квантовой памяти. Чёрные кружки — скорость генерации ключа после исправления ошибок (рисунок воспроизводится из работы [55] с разрешения © 2020 Springer Nature).

этих схемах соседние узлы заранее не перепутываются, в отличие от таковых классического квантового повторителя [21], а для передачи квантовой информации между узлами используются специальные многофотонные перепутанные состояния — *древовидные кластерные состояния* (*tree cluster state*) [192, 197] — вместо одиночных фотонов. Такие состояния благодаря своей специальной структуре позволяют успешно передать закодированную в них квантовую информацию даже при значительных потерях в оптоволокне, например, состояние на рис. 10 устойчиво при потерях до 50 % [192] (примерно 15 км в оптоволокне).

Протокол работает следующим образом [86].

1. Алиса создаёт древовидное кластерное состояние, при этом корневой узел (корень) является стационарным кубитом, а все остальные кубиты (листья) — фотоны.

2. Затем Алиса *кодирует* состояние своего кубита (A) квантовой памяти в кластерное состояние, проводя совместное измерение A и корня кластерного состояния в базисе состояний Белла. Так как корневой кубит перепутан с остальными листьями, это фактически является *квантовой телепортацией* кубита A на оставшееся кластерное состояние.

3. Теперь кластерное состояние больше не содержит стационарного корня и отправляется в сторону первого повторителя.

4. Квантовый повторитель проводит измерения фотонов в полученном кластерном состоянии на уровнях 2 и 3, тем самым определяя, какой из фотонов уровня 1 (L_1) не был потерян при передаче. При этом после измерения фотонов 2-го и 3-го уровней фотон L_1 содержит в себе информацию, закодированную Алисой [192].

5. Квантовый повторитель создаёт своё кластерное состояние с корневым стационарным кубитом.

6. Затем квантовый повторитель телепортирует выбранный фотон L_1 на своё кластерное состояние (*перекодирование*) и отправляет его дальше.

7. В конце Боб определяет сохранившийся фотон 1-го уровня полученного кластерного состояния и записывает его на свой стационарный кубит.

Использовать такую схему можно следующим образом: Алиса создаёт перепутанное состояние двух кубитов, один кубит она хранит у себя, а другой кодирует в кластерное состояние и через цепочку квантовых повторителей отправляет Бобу, который записывает полученный кубит в свою память. В результате Алиса и Боб обладают парой перепутанных кубитов. Кластерные состояния можно также использовать и в протоколе BDCZ для ускорения перепутывания соседних узлов сети.

Простейшая реализация этого метода требует одного кубита с эффективным фотонным интерфейсом и двух дополнительных логических кубитов [86]. (Коррекция ошибок и дистилляция запутанности, естественно, приведут к необходимости использования большего числа кубитов.) При этом в данном случае требуется хранить информацию только до тех пор, пока происходят измерение полученного кластера и создание нового, что можно осуществить достаточно быстро ($\leqslant 1$ мкс), тогда как в случае классического квантового повторителя время когерентности должно быть как минимум больше времени, затрачиваемого фотоном на путь между соседними узлами (100 мкс соответствуют примерно 100 км).

На сегодняшний день детерминистическая генерация простого кластерного состояния продемонстрирована с помощью квантовых точек [198, 199]. Также недавно продемонстрированный эффективный фотонный интерфейс, длительная квантовая память и взаимодействие с ядерными спинами делают кремний-вакансии в алмазе

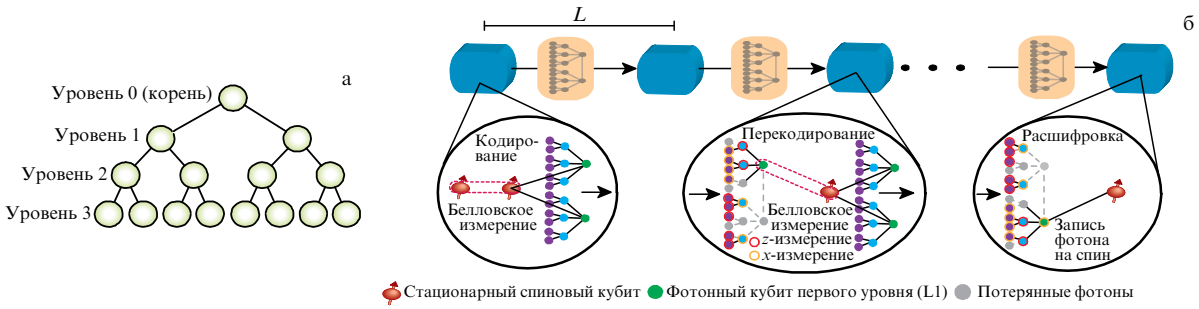

Рис. 10. (В цвете онлайн.) Однонаправленные квантовые повторители. (а) Пример древовидного кластерного состояния. Кружки (вершины графа) — кубиты, а рёбра связывают попарно перепутанные кубиты (рисунок воспроизводится из работы [192] с разрешения © 2006 American Physical Society). (б) Схема повторителя на основе кластерных состояний (см. текст) (рисунок воспроизводится из работы [86], опубликованной под лицензией Creative Commons Attribution 4.0 International).

возможными кандидатами для создания таких квантовых повторителей в обозримом будущем [55, 137, 140].

4.3. Фотонные повторители

Фотонные кластерные состояния можно использовать не только для передачи квантовой информации через канал с потерями, но и для квантовых вычислений на основе разрушающих измерений (measurement-based quantum computing) [197, 200, 201]. В 2015 г. была предложена схема *фотонного квантового повторителя* (*all-photon quantum repeater*), которая использует фотонные кластерные состояния для хранения, обработки и передачи кубитов [202]. Такой квантовый повторитель в принципе вообще не требует квантовой памяти на основе атомов или твердотельных систем, работа с которыми является основной трудностью на пути создания квантовых повторителей, рассмотренных в разделе 4.2. Однако детерминистическое создание нетривиального фотонного кластерного состояния возможно только с использованием однофотонного источника с квантовой памятью [198, 199, 203, 204], что, вероятно, делает такие схемы сравнимыми по сложности с предыдущими. Тем не менее с использованием спонтанного параметрического распада для вероятностной генерации кластерных состояний [59, 205] были проведены первые демонстрации прототипа квантового повторителя без стационарных кубитов [206, 207].

5. Преобразование длины волны

Потери в оптоволокне сильно зависят от длины волны света (рис. 11). Существующие кварцевые оптоволокна имеют наименьшие потери на длинах волн 1300 и 1550 нм, следовательно, для увеличения радиуса квантовых сетей надо использовать фотоны, длина волны которых попадает в эти *телекоммуникационные диапазоны*. Однако большинство кубитов излучает на более коротких длинах волн и требует дополнительного преобразования. Такие преобразователи должны обладать следующими свойствами:

1) высокая квантовая эффективность;
2) сохранение когерентности;
3) низкий добавочный шум.

Самыми важными являются два последних пункта, так как даже 10%-ная эффективность при преобразовании длин волн с 740 нм в 1300 нм увеличивает расстояние, на которое можно послать фотон, с 10 до 100 км. Когерентность требуется для сохранения квантовой перепутанности, например, между фотоном и испустившим его атомом. Низкий добавочный шум необходим, в частности, для сохранения однофотонного характера излучения. Более того, отношение сигнал/шум (SNR) устанавливает нижнюю границу для вероятности ошибки в каждом отдельном бите ключа шифрования для КРК $\mathrm{QBER} \geqslant 0{,}5\,\mathrm{SNR}^{-1}$, так как детектирующая аппаратура не может отличить "хороший фотон" от "плохого", который с вероятностью 50 % приведёт к неправильному результату. В случае, когда $\mathrm{QBER} > 15\,\%$, ключ нельзя использовать для кодирования [16]; таким образом, можно сформулировать критерий практичности преобразователя длины волны для простейшего протокола BB84: $\mathrm{SNR} \geqslant 3{,}5$. Сегодня существуют два основных подхода для преобразования длины волны: нелинейно-оптический и оптомеханический.

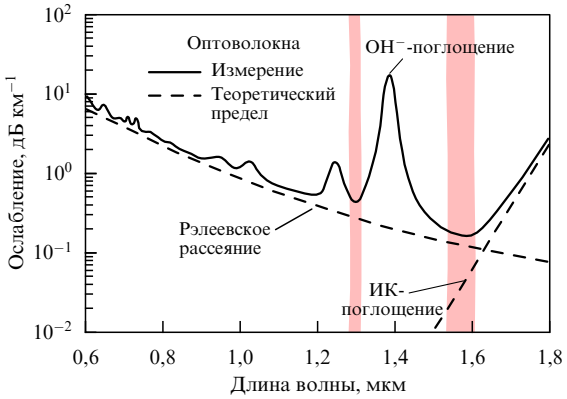

Рис. 11. Зависимость потерь в кварцевом оптоволокне от длины волны. Затемнёнными полосами отмечены основные телекоммуникационные диапазоны, соответствующие минимальным потерям ($\approx$ 1300 и 1550 нм). (Рисунок воспроизводится с любезного разрешения Э.Ф. Шуберта (E.F. Schubert).)

Нелинейно-оптический метод обычно использует вынужденное параметрическое преобразование частоты света [210–212], в котором исходный фотон (с длиной волны λ_s) смешивается с фотоном лазера накачки (λ_p), что приводит к генерации фотона на разностной частоте ($\lambda_0^{-1} = |\lambda_\mathrm{s}^{-1} - \lambda_\mathrm{p}^{-1}|$). Как и все нелинейные процессы, параметрическая генерация требует большой интенсивности света лазера накачки для получения высокой эффективности преобразования [213], чего можно добиться с помощью оптических резонаторов [214]. Однако такие резонаторы требуют аккуратной юстировки и активной стабилизации длины, что делает их малопригодными

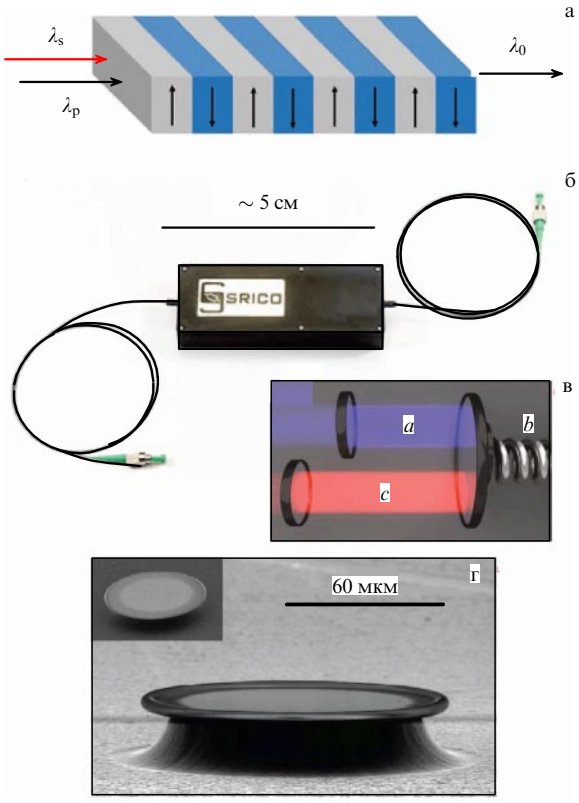

Рис. 12. (В цвете онлайн.) Преобразователи длины волны. (а) Периодически поляризованный нелинейно-оптический кристалл, стрелками показано направление поляризации. (б) Интегрированный периодически поляризованный кристалл, готовый к подключению в оптоволоконную сеть (рисунок воспроизводится с разрешения © Srico Inc.). (в) Схематическое изображение двух оптических мод резонатора (a, c), взаимодействующих с механическим резонатором (b) (рисунок воспроизводится из работы [208], опубликованной под лицензией Creative Commons Attribution 4.0 International License). (г) Пример оптомеханического резонатора — микродиск (рисунок воспроизводится из работы [209] с разрешения © 2003 Springer Nature).

для широкого применения за пределами физических лабораторий.

Более практичным является использование волноводов из периодически поляризованных нелинейных кристаллов, в которых направление одной из главных осей двулучепреломления периодически изменяется на 180° [215] (рис. 12). Во-первых, периодическая структура позволяет использовать фазовый квазисинхронизм для выбора такой ориентации кристалла, при которой отсутствует пространственный снос излучения [216], а во-вторых, малое поперечное сечения волновода увеличивает интенсивность света. Благодаря этому можно применять волноводы из кристаллов, например ниобата лития (PPLN), длиной в несколько сантиметров, что значительно повышает эффективность преобразования длины волны света без использования резонаторов.

Одна из трудностей параметрической генерации связана с низким отношением сигнал/шум из-за шумовых фотонов, обусловленных неупругим рассеянием излучения мощного лазера накачки. Длина волны рассеянного фотона почти всегда больше длины волны исходного, следовательно, если $\lambda_p > \lambda_0$, то рассеянные фотоны можно легко отфильтровать спектральными методами. Например, в работе [217] продемонстрировано преобразование излучения квантовых точек из $\lambda_s = 711$ нм в $\lambda_0 = 1313$ нм с использованием лазера накачки с $\lambda_p = 1550$ нм, что позволило получить SNR ≈ 50. Напротив, преобразование излучения от NV-центров (640 нм) в телекоммуникационный диапазон $\approx 1300-1500$ нм требует накачки с более короткой длиной волны, что усложняет получение высокого SNR [218].

Также можно использовать процесс генерации суммарной частоты: $\lambda_0^{-1} = \lambda_s^{-1} + \lambda_p^{-1}$. Такой подход позволяет преобразовать фотон из телекоммуникационного диапазона в видимый, что выгодно для схемы BDCZ-повторителя, в котором соседние узлы сети перепутываются путём разделения ЭПР-пары фотонов (см. рис. 6). Такую пару можно генерировать изначально в телекоммуникационном диапазоне, а потом преобразовать уже в квантовом повторителе. Например, для преобразования из $\lambda_s = 1310$ нм в $\lambda_0 = 737$ нм (длина волны излучения SiV-центра в алмазе) используется лазер накачки на длине волны $\lambda_p = 1700$ нм. Так как $\lambda_p \gg \lambda_0, \lambda_s$, лазер накачки практически не добавляет шумов. Однако если $\lambda_p < \lambda_s$, то спектр шумовых фотонов от рассеяния фотонов лазера накачки перекрывается со спектром исходного фотона λ_s, приводя к уменьшению как SNR, так и когерентности преобразования. Уже сегодня нелинейные преобразователи на основе PPLN продаются в интегрированном виде (см. рис. 12), и они могут быть легко встроены в оптоволоконные сети с потерями < 4 дБ.

Оптомеханический метод основан на взаимодействии двух оптических мод посредством механических колебаний резонатора [219–221]. Хотя по эффективности этот подход пока сильно уступает методам нелинейной оптики, он обладает рядом существенных преимуществ. Во-первых, такие микрорезонаторы благодаря своему малому размеру (≈ 100 мкм) могут быть интегрированы на чипе и производиться в большом количестве. Во-вторых, этот метод способен не только преобразовывать свет из видимого диапазона в инфракрасный, но и переводить микроволновые фотоны в инфракрасный свет, что необходимо для подключения сверхпроводящих квантовых компьютеров к квантовым сетям [87, 88]. К недостаткам можно отнести необходимость охлаждения микрорезонаторов до криогенных температур для подавления теплового шума, однако большинство кубитов и так требует температур < 4 К.

Интересным применением оптомеханических резонаторов является создание интерфейса между телекоммуникационными фотонами и кубитами без использования оптического перехода в кубите. Например, это позволит подключить сверхпроводящие квантовые компьютеры к квантовым сетям, преобразовав микроволновые фотоны в инфракрасные [87, 88]. Более того, спиновой степенью свободы большинства твердотельных кубитов, рассмотренных в разделе 3, можно управлять с помощью фононов, следовательно, оптомеханические резонаторы способны связать такие кубиты с телекоммуникационными фотонами даже при слабом или нестабильном оптическом переходе в кубите (например, как в NV-центрах) [127].

6. Бесповторительные методы

Как отмечалось, квантовые повторители позволят развернуть глобальную квантовую сеть, но их создание — очень сложная техническая задача. Однако существует

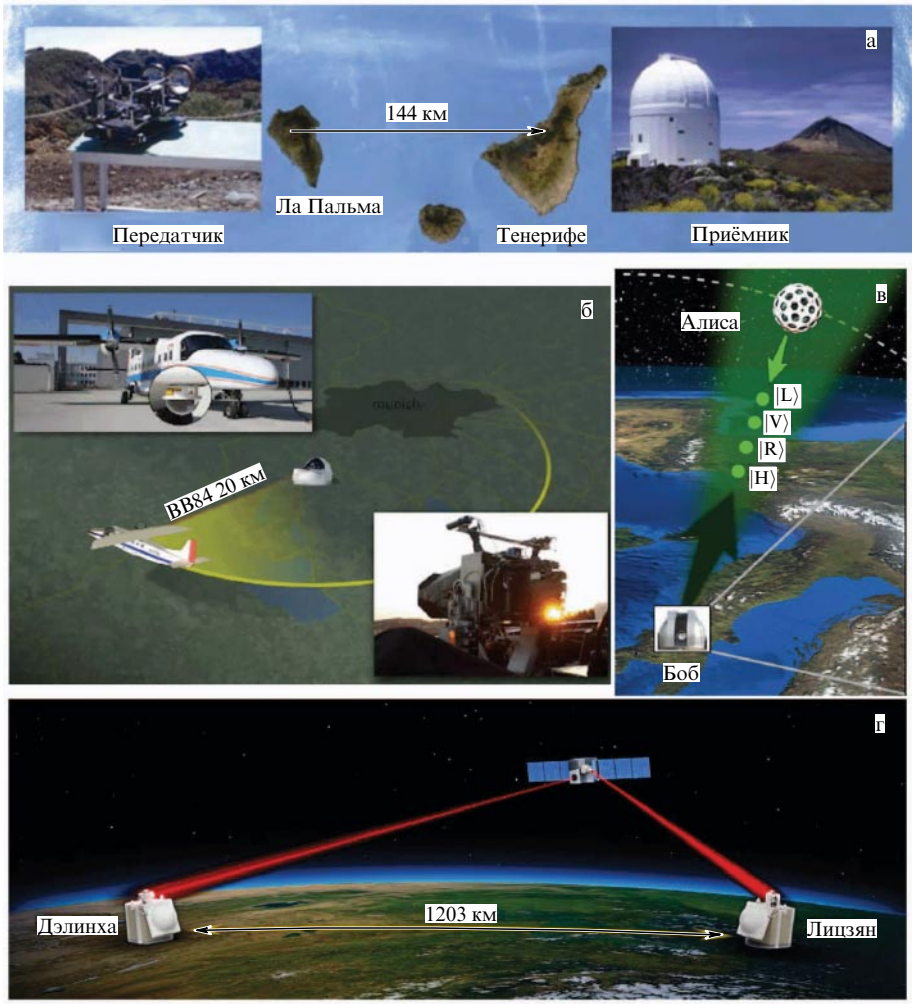

Рис. 13. (В цвете онлайн.) Атмосферная квантовая криптография. (а) КРК между двумя Канарскими островами. Слева изображено передающее устройство, справа — принимающий телескоп (рисунок воспроизводится из работы [223] с разрешения © 2007 Springer Nature). (б) КРК между наземной станцией и самолётом (рисунок воспроизводится из работы [224] с разрешения авторов (H. Weinfurter, F. Moll) и издательства © 2012 Society of Photo-optical Instrumentation Engineers (SPIE)). (в) КРК, использующее спутник в качестве ретрорефлектора (рисунок воспроизводится из работы [225] с разрешения © 2015 American Physical Society). (г) Схема распределения квантовой перепутанности с использованием источника перепутанных фотонов, расположенного на спутнике [226].

несколько компромиссных решений. В разделе 6.1 рассказывается об использовании спутников для распределения запутанных фотонов между двумя удалёнными пользователями на Земле. В разделе 6.2 описан гибридный метод построения сети для КРК с использованием *доверенных узлов*, а в разделе 6.3 обсуждается революционный метод КРК, позволяющий преодолеть предел прямой передачи и увеличить радиус действия КРК в два раза без использования квантовой памяти [222].

6.1. Спутники

Поглощение света в оптоволокне ограничивает практическую дальность квантовой криптографии и масштаб квантовой сети без квантовых повторителей расстоянием примерно 100 км. Рассеяние в атмосфере может быть меньше, чем в оптоволокне, поэтому примерно в 2000 г. были начаты эксперименты по атмосферному КРК [227], но из-за естественной кривизны земной поверхности расстояние прямой видимости сильно ограничено: порядка 10 км для наблюдателей, находящихся на уровне моря.

Для осуществления КРК и распределения запутанности на расстоянии порядка 100 км передающее и принимающие устройства были размещены на возвышенностях [223, 228 – 231] (рис. 13а). Использование спутников позволяет связать квантовым каналом двух пользователей, не находящихся в прямой видимости [232]. Первые эксперименты в этом направлении состояли в реализации КРК между наземной станцией и самолётом [233] (рис. 13б) и использовании спутника в качестве ретрорефлектора [225] (рис. 13в). При этом эффективная величина потерь канала между наземной станцией и спутником на высоте 1000 км может составлять всего 40 дБ, что сравнимо с потерями в 200-километровом оптоволокне [234]!

В 2017 г., используя источник перепутанных фотонов, размещённый на спутнике, удалось распределить эти фотоны между двумя наземными лабораториями, удалёнными друг от друга на расстояние 1200 км [226] (эффективные потери 60 – 80 дБ, $\sim$ 400 км оптоволокна), а в 2020 г. было продемонстрированно первое КРК через спутник [235] (протокол E91 [236], скорость генерации ключа шифрования 0,12 бит в 1 с). Так как при этом наблюдалось нарушение неравенств Белла, такие фотоны можно также использовать для проверки фундаментальных физических теорий [237, 238].

В отличие от портативных спутниковых телефонов, которые используют относительно большие мощности радиоволн, квантовая криптография требует одиночных фотонов. Для их эффективного детектирования и соответственно большей пропускной способности квантового канала необходимы астрономические телескопы, которые непрерывно следят за положением спутника (рис. 13а). Высокая цена спутников и телескопов, скорее всего, не позволит этой технологии прийти в нашу повседневную жизнь.

6.2. Доверенные узлы

Если нет необходимости в полноценной квантовой сети, способной распределять запутанность между узлами, а требуется только увеличить радиус действия систем КРК, то можно использовать *доверенные узлы*, работающие как классические реле (рис. 14). Следующий пример объясняет суть этого подхода. Пусть опять Алиса и Боб хотят генерировать секретный ключ, но расстояние между ними L слишком велико для существующих систем КРК. Поместим Чарли, выступающего в качестве доверенного узла, посредине между Алисой и Бобом. Пусть Алиса и Чарли генерируют ключ a, Боб и Чарли в свою очередь генерируют ключ b, используя любой протокол КРК. Теперь Чарли генерирует новый ключ, используя побитовое "исключающее или" ($\oplus$):

$$c = a \oplus b\,, \tag{11}$$

который посылает, например, Бобу по классическому незащищённому каналу (в принципе можно послать всем участникам сети). Боб вычисляет ключ Алисы a, используя свой секретный ключ b:

$$c \oplus b = a \oplus b \oplus b = a\,, \tag{12}$$

который Алиса и Боб могут применить для шифрования своих сообщений.

Очевидно, что, если злоумышленник перехватил ключ c, то без знания ключа b, который известен только Бобу и Чарли, он не способен определить a. Таким образом, если Чарли изолирован от внешнего мира (защищён от прослушивания), то КРК с использованием доверенных узлов имеет такую же степень секретности, как и обычное КРК.

Благодаря этому методу вместо генерации ключа на расстоянии L с вероятностью успеха p_0 создаются два ключа на расстоянии $L/2$ с вероятностью успеха $\sim \sqrt{p_0}$. Если вспомнить пример из раздела 2, то один такой доверенный узел позволит сократить время, требующееся для генерации одного бита секретного ключа на расстоянии $L = 1000$ км, с 1 года до 1 с!

Сети КРК на основе доверенных узлов уже развёрнуты во многих странах и протянулись на несколько тысяч километров (Китай [239], Япония [240] и Англия [241]). В России разработкой и внедрением таких сетей занимаются Российский квантовый центр, МГУ им. М.В. Ломоносова и другие научные учреждения [242] при поддержке Открытого акционерного общества "Российские железные дороги" (ОАО РЖД) [243]. Также следует упомянуть недавний эксперимент с использованием спутника в качестве доверенного узла [244]. В работе [244] была организована генерация ключа шифрования со скоростью ~ 1 кбит $с^{-1}$ между пользователями в Австрии и Китае, удалёнными друг от друга на 7600 км. При этом нет необходимости, чтобы оба наземных

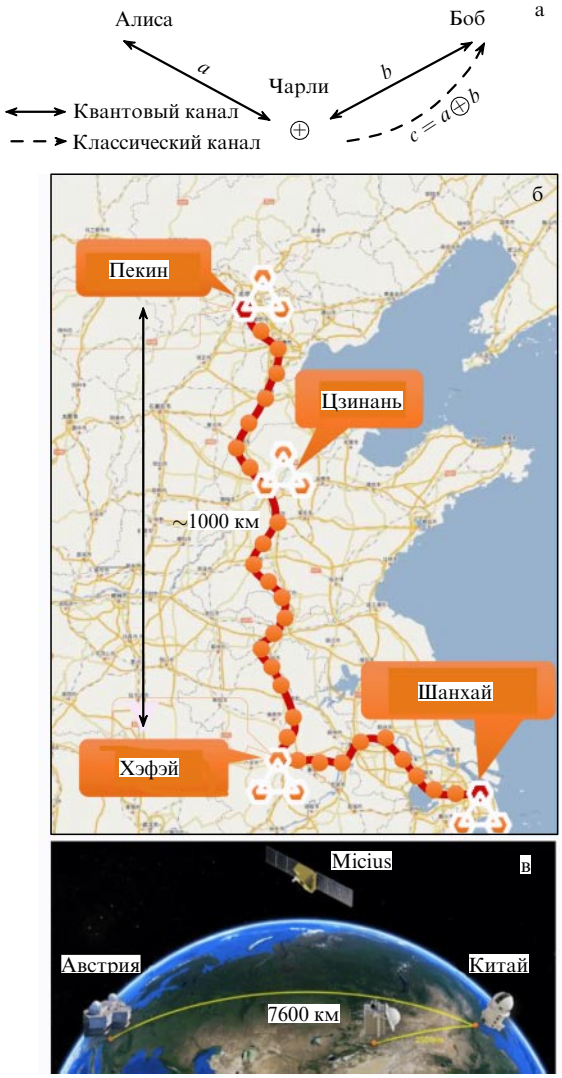

Рис. 14. КРК с доверенными узлами. (а) Принцип работы доверенного узла (см. текст). (б) Квантовая сеть на основе доверенных узлов в Китае между Пекином и Шанхаем [239]. (в) КРК между Китаем и Австрией, использующее спутник Micius в качестве доверенного узла [239]. (Рисунки б и в воспроизводятся из работы [239] с разрешения © 2018 Optical Society of America на условиях OSA Open Access Publishing Agreement.)

пользователя находились одновременно в прямой видимости со спутника: ключи шифрования генерируются асинхронно и хранятся на спутнике.

Основной проблемой такого подхода является защита доверенных узлов от прослушивания, однако та же проблема существует и для "классических" систем КРК, которые хранят сгенерированные ключи на обычных компьютерах, скорее всего, подключённых к публичным сетям обмена данными и подвергающихся риску кражи секретных ключей.

6.3. Квантовое распределение ключей с разделёнными полями

В 2018 г. был предложен новый революционный метод, получивший название *КРК с разделёнными полями* (*Twin-Field QKD*). Этот метод, аналогично квантовому повторителю, позволяет преодолеть предел прямой передачи и удвоить расстояние, доступное для КРК без использования квантовой памяти [222].

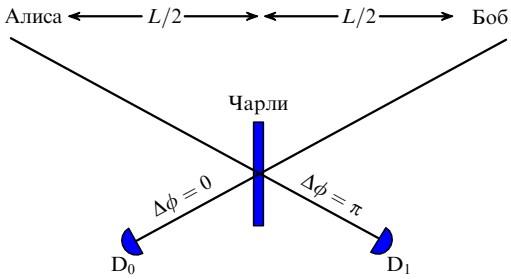

Рис. 15. Схема КРК с разделёнными полями (см. текст).

Для объяснения данного метода рассмотрим следующий эксперимент (рис. 15). Пусть Алиса и Боб имеют по лазеру, которые между собой фазово-когерентны. Каждый из них приготовляет слабый лазерный импульс (среднее число фотонов < 1) и отправляет его Чарли, находящемуся от них на расстоянии $L/2$. При этом Алиса (Боб) кодирует значение посылаемого бита $b_{\mathrm{A}}(b_{\mathrm{B}}) = 0, 1$ через фазу своего лазерного импульса: $\phi_{\mathrm{A(B)}} = \pi b_{\mathrm{A(B)}}$. Фотоны интерферируют на светоделителе, и в зависимости от относительной фазы $\Delta\phi = \phi_{\mathrm{A}} - \phi_{\mathrm{B}}$ между этими импульсами сработает или детектор D_0 (если $\Delta\phi = 0, 2\pi$), или детектор D_1 (если $\Delta\phi = \pi$), о чём публично сообщает Чарли. Используя информацию от Чарли, Алиса и Боб узнают, послали ли они одинаковые биты или нет. В любом случае они могут договориться о секретном ключе, но злоумышленнику этого не хватит для компрометации секретного ключа.

Главная особенность рассматриваемого метода состоит в том, что такая интерференция сохраняется даже тогда, когда только один лазерный импульс достигает Чарли. Это объясняется тем, что светоделитель стирает информацию о том, с какой стороны (от Алисы или Боба) прилетел фотон [245]. Таким образом, этот метод заменяет *двухфотонную интерференцию*, как в схеме MDI-QKD [190], *однофотонной* [246], а так как теперь только одному фотону надо достичь Чарли, то и зависимость скорости генерации ключа от расстояния будет $r \propto \sqrt{p_0}$, точно так же, как и при использовании квантового повторителя.

Проблема рассмотренного метода — необходимость стабилизировать разность длин плечей интерферометра (которые могут быть более 100 км) с точностью, превосходящей длину волны света ($\ll 1$ мкм), — не помешала первым лабораторным экспериментам [247, 248]. Позднее был предложен и реализован другой вариант этого метода, не требующий стабилизации интерферометра [249, 250], а в 2020 г. удалось экспериментально реализовать КРК, которое перешагнуло предел прямой передачи [251].

Стоит также заметить, что похожая однофотонная интерференция использовалась в недавнем эксперименте по перепутыванию двух NV-центров [72].

7. Заключение

Мы живём в эпоху, когда квантовые технологии входят в нашу повседневную жизнь и создание глобального квантового интернета откроет огромный горизонт новых научных и практических приложений. Основным препятствием выступают поглощение и рассеяние фотонов, накладывающие ограничение на расстояние, которое можно покрыть квантовой сетью.

В настоящем обзоре рассмотрены разные подходы к решению этой проблемы: квантовые повторители, доверенные узлы, спутниковая коммуникация — и описан текущий прогресс в их экспериментальной реализации. И хотя все эти подходы могут найти свою область применения, самым практически важным представляется разработка квантового повторителя на основе твердотельных систем, что позволит развернуть квантовые сети сначала в масштабе городов, а потом стран и континентов. Последние результаты вселяют надежду, что полноценный работающий квантовый повторитель будет создан в ближайшее десятилетие.

Благодарности. Хотел бы поблагодарить Н.Н. Колачевского, П. Барклая (P. Barclay), моих коллег М. Бхаскара (M. Bhaskar), Р. Редингера (R. Riedinger), Э. Берзина (E. Bersin), Ю.А. Сукачёва, С.А. Фёдорова и О.В. Беляеву за помощь в написании обзора.

Список литературы

1. Поплавский Р П *УФН* **115** 465 (1975); Poplavskii R P *Sov. Phys. Usp.* **18** 222 (1975)
2. Манин Ю И *Вычислимое и невычислимое* (М.: Советское радио, 1980)
3. Feynman R P *Int. J. Theor. Phys.* **21** 467 (1982)
4. Deutsch D, Jozsa R *Proc. R. Soc. Lond. A* **439** 553 (1992)
5. Shor P W, in *Proc. of the 35th Annual Symp. on Foundations of Computer Science, 20–22 November 1994, Santa Fe, NM, USA* (Los Alamitos, CA: IEEE Computer Soc., 1994) p. 124
6. Rivest R L, Shamir A, Adleman L *Commun. ACM* **21** 120 (1978)
7. Молдовян Н А *Введение в криптосистемы с открытым ключом* (М.: BHV, 2014) p. 228
8. Xu N et al. *Phys. Rev. Lett.* **108** 130501 (2012)
9. Gidney C, Ekerå M *Quantum* **5** 433 (2021); arXiv:1905.09749
10. Arute F et al. *Nature* **574** 505 (2019); arXiv:1910.11333
11. Bernien H et al. *Nature* **551** 579 (2017); arXiv:1707.04344
12. Zhang J et al. *Nature* **551** 601 (2017); arXiv:1708.01044
13. Diamanti E et al. *npj Quantum Inf.* **2** 16025 (2016); arXiv:1606.05853
14. Bernstein D J, Buchmann J, Dahmen E (Eds) *Post-Quantum Cryptography* (Berlin: Springer, 2009)
15. Bennett C H, Brassard G, in *Proc. of IEEE Intern. Conf. on Computers, Systems and Signal Processing* (New York: IEEE, 1984) p. 8
16. Gisin N et al. *Rev. Mod. Phys.* **74** 145 (2002); quant-ph/0101098
17. "Продемонстрирована работа предсерийного образца первого в России квантового телефона", Пресс-служба МГУ им. М.В. Ломоносова. 29.05.2019, https://www.msu.ru/science/main_themes/prodemonstrirovana-rabota-predseriynogo-obraztsa-pervogo-v-rossii-kvantovogo-telefona.html
18. Duplinskiy A V et al. *J. Russ. Laser Res.* **39** 113 (2018); arXiv:1712.09831
19. Wootters W K, Zurek W H *Nature* **299** 802 (1982)
20. Yin H-L et al. *Phys. Rev. Lett.* **117** 190501 (2016)
21. Briegel H-J et al. *Phys. Rev. Lett.* **81** 5932 (1998)
22. Duan L-M et al. *Nature* **414** 413 (2001); quant-ph/0105105
23. Kimble H J *Nature* **453** 1023 (2008); arXiv:0806.4195
24. Monroe C et al. *Phys. Rev. A* **89** 022317 (2014); arXiv:1208.0391
25. Fitzsimons J F *npj Quantum Inf.* **3** 23 (2017); arXiv:1611.10107
26. Barz S et al. *Science* **335** 303 (2012); arXiv:1110.1381
27. Gottesman D, Jennewein T, Croke S *Phys. Rev. Lett.* **109** 070503 (2012); arXiv:1107.2939
28. Khabiboulline E T et al. *Phys. Rev. Lett.* **123** 070504 (2019); arXiv:1809.01659
29. Dai H et al. *Nat. Phys.* **16** 848 (2020)
30. Kómár P et al. *Nat. Phys.* **10** 582 (2014); arXiv:1310.6045
31. Ilo-Okeke E O et al. *npj Quantum Inf.* **4** 40 (2018); arXiv:1709.08423
32. Krutyanskiy V et al. *npj Quantum Inf.* **5** 72 (2019); arXiv:1901.06317
33. Pirandola S et al. *Nat. Photon.* **12** 724 (2018); arXiv:1811.01969
34. Giovannetti V, Lloyd S, MacCone L *Phys. Rev. Lett.* **96** 010401 (2006); quant-ph/0509179

35. Degen C L, Reinhard F, Cappellaro P *Rev. Mod. Phys.* **89** 035002 (2017); arXiv:1611.02427
36. Vazirani U, Vidick T *Phys. Rev. Lett.* **113** 140501 (2014); arXiv:1210.1810
37. Белинский А В, Клышко Д Н *УФН* **163** (8) 1 (1993); Belinskii A V, Klyshko D N *Phys. Usp.* **36** 653 (1993)
38. Wehner S, Elkouss D, Hanson R *Science* **362** eaam9288 (2018)
39. Lemonde M-A et al. *Phys. Rev. Lett.* **120** 213603 (2018)
40. Wang H, Lekavicius I *Appl. Phys. Lett.* **117** 230501 (2020); arXiv:2011.09990
41. Neuman T et al., arXiv:2003.08383
42. Magnard P et al. *Phys. Rev. Lett.* **125** 260502 (2020)
43. Aharonovich I, Englund D, Toth M *Nat. Photon.* **10** 631 (2016)
44. Eisaman M D et al. *Rev. Sci. Instrum.* **82** 071101 (2011)
45. Wang X et al. *Chem. Soc. Rev.* **45** 2239 (2016)
46. Senellart P, Solomon G, White A *Nat. Nanotechnol.* **12** 1026 (2017)
47. Wang H et al. *Nat. Photon.* **13** 770 (2019)
48. Zaske S et al. *Phys. Rev. Lett.* **109** 147404 (2012); arXiv:1204.6253
49. Ates S et al. *Phys. Rev. Lett.* **109** 147405 (2012); arXiv:1207.4226
50. Pelc J S et al. *Opt. Express* **20** 27510 (2012)
51. Takemoto K et al. *Sci. Rep.* **5** 14383 (2015)
52. Pirandola S et al. *Adv. Opt. Photon.* **12** 1012 (2020); arXiv:1906.01645
53. Scarani V et al. *Rev. Mod. Phys.* **81** 1301 (2009); arXiv:0802.4155
54. Hadfield R H *Nat. Photon.* **3** 696 (2009)
55. Bhaskar M K et al. *Nature* **580** 60 (2020)
56. Gol'tsman G N et al. *Appl. Phys. Lett.* **79** 705 (2001)
57. Marsili F et al. *Nat. Photon.* **7** 210 (2013); arXiv:1209.5774
58. Raussendorf R, Briegel H J *Phys. Rev. Lett.* **86** 5188 (2001)
59. Walther P et al. *Nature* **434** 169 (2005)
60. Chen K et al. *Phys. Rev. Lett.* **99** 120503 (2007); arXiv:0705.0174
61. CorningM SMF-28M Ultra Optical Fiber. Product Information, https://www.corning.com/media/worldwide/coc/documents/Fiber/SMF-28%20Ultra.pdf
62. Tamura Y et al. *J. Lightwave Technol.* **36** 44 (2018)
63. Takesue H et al. *Nat. Photon.* **1** 343 (2007)
64. Bennett C H et al. *Phys. Rev. Lett.* **70** 1895 (1993)
65. Żukowski M et al. *Phys. Rev. Lett.* **71** 4287 (1993)
66. Bose S, Vedral V, Knight P L *Phys. Rev. A* **57** 822 (1998); quant-ph/9708004
67. Pirandola S et al. *Nat. Commun.* **8** 15043 (2017); arXiv:1510.08863
68. Pirandola S *Commun. Phys.* **2** 51 (2019)
69. Hensen B et al. *Nature* **526** 682 (2015)
70. Rosenfeld W et al. *Phys. Rev. Lett.* **119** 010402 (2017); arXiv:1611.04604
71. Chou C-W et al. *Science* **316** 1316 (2007); quant-ph/0702057
72. Humphreys P C et al. *Nature* **558** 268 (2018); arXiv:1712.07567
73. Hofmann J et al. *Science* **337** 72 (2012)
74. Delteil A et al. *Nat. Phys.* **12** 218 (2016); arXiv:1507.00465
75. Yu Y et al. *Nature* **578** 240 (2020)
76. Monroe C, Kim J *Science* **339** 1164 (2013)
77. Devoret M H, Schoelkopf R J *Science* **339** 1169 (2013)
78. Awschalom D D et al. *Nat. Photon.* **12** 516 (2018)
79. Stern L et al. *Optica* **4** 1 (2017)
80. MacQuarrie E R et al. *Phys. Rev. Lett.* **111** 227602 (2013); arXiv:1306.6356
81. Arrangoiz-Arriola P et al. *Phys. Rev. X* **8** 031007 (2018)
82. DiCarlo L et al. *Nature* **460** 240 (2009); arXiv:0903.2030
83. Abobeih M H et al. *Nat. Commun.* **9** 2552 (2018)
84. DiVincenzo D P *Fortsch. Phys.* **48** 771 (2000)
85. Bennett C H et al. *Phys. Rev. Lett.* **76** 722 (1996); quant-ph/9511027
86. Borregaard J et al. *Phys. Rev. X* **10** 021071 (2020)
87. Lauk N et al. *Quantum Sci. Technol.* **5** 020501 (2020)
88. Mirhosseini M et al. *Nature* **588** 599 (2020); arXiv:2004.04838
89. Sangouard N et al. *Rev. Mod. Phys.* **83** 33 (2011); arXiv:0906.2699
90. Simon C et al. *Eur. Phys. J. D* **58** 1 (2010)
91. Blatt R, Roos C F *Nat. Phys.* **8** 277 (2012)
92. Gross C, Bloch I *Science* **357** 995 (2017)
93. Lekitsch B et al. *Sci. Adv.* **3** e1601540 (2017); arXiv:1508.00420
94. Duan L-M, Monroe C *Rev. Mod. Phys.* **82** 1209 (2010)
95. Colombe Y et al. *Nature* **450** 272 (2007)
96. Reichel J, Vuletić V (Eds) *Atom Chips* (Weinheim: Wiley-VCH, 2011)
97. Wang J et al. *Nat. Photon.* **14** 273 (2020)
98. Elshaari A W et al. *Nat. Photon.* **14** 285 (2020)
99. Purcell E M, Torrey H C, Pound R V *Phys. Rev.* **69** 37 (1946)
100. Быков В П *Квантовая электроника* **1** 1557 (1974); Bykov V P *Sov. J. Quantum Electron.* **4** 861 (1975)
101. Reiserer A, Rempe G *Rev. Mod. Phys.* **87** 1379 (2015); arXiv:1412.2889
102. Brekenfeld M et al. *Nat. Phys.* **16** 647 (2020)
103. Albrecht R et al. *Phys. Rev. Lett.* **110** 243602 (2013)
104. Ruf M et al. *Phys. Rev. Appl.* **15** 024049 (2021); arXiv:2009.08204
105. Riedel D et al. *Phys. Rev. X* **7** 031040 (2017)
106. Choi H, Heuck M, Englund D *Phys. Rev. Lett.* **118** 223605 (2017)
107. Robinson J T et al. *Phys. Rev. Lett.* **95** 143901 (2005)
108. Giesz V et al. *Nat. Commun.* **7** 11986 (2016)
109. Mouradian S et al. *Appl. Phys. Lett.* **111** 021103 (2017)
110. Duan L-M, Kimble H J *Phys. Rev. Lett.* **92** 127902 (2004); arXiv:0309187
111. Najer D et al. *Nature* **575** 622 (2019)
112. Takahashi H et al. *Phys. Rev. Lett.* **124** 013602 (2020); arXiv:1808.04031
113. Stute A et al. *Nature* **485** 482 (2012)
114. Atatüre M et al. *Nat. Rev. Mater.* **3** 38 (2018)
115. Awschalom D D et al. *Nat. Photon.* **12** 516 (2018)
116. Zhang G et al., arXiv:2008.06458
117. Gruber A et al. *Science* **276** 2012 (1997)
118. Chu Y, Lukin M D, arXiv:1504.05990
119. Barry J F et al. *Rev. Mod. Phys.* **92** 015004 (2020); arXiv:1903.08176
120. Abobeih M H et al. *Nat. Commun.* **9** 2552 (2018); arXiv:1801.01196
121. Bradley C E et al. *Phys. Rev. X* **9** 031045 (2019); arXiv:1905.02094
122. Kalb N et al. *Science* **356** 928 (2017); arXiv:1703.03244
123. Faraon A et al. *Phys. Rev. Lett.* **109** 033604 (2012); arXiv:1202.0806
124. Udvarhelyi P et al. *Phys. Rev. Appl.* **11** 044022 (2019)
125. Ruf M et al. *Nano Lett.* **19** 3987 (2019)
126. Rozpedek F et al. *Phys. Rev. A* **99** 052330 (2019); arXiv:1809.00364
127. Ghobadi R et al. *Phys. Rev. A* **99** 053825 (2019)
128. Mills A R et al. *Nat. Commun.* **10** 1063 (2019); arXiv:1809.03976
129. Safonov A N et al. *Phys. Rev. Lett.* **77** 4812 (1996)
130. Hoese M et al. *Sci. Adv.* **6** eaba6038 (2020)
131. Dietrich A et al. *Phys. Rev. B* **101** 081401 (2020); arXiv:1903.02931
132. Вавилов В С и др. *ФТП* **14** 1811 (1980); Vavilov V S et al. *Sov. Phys. Semicond.* **14** 1078 (1980)
133. Зайцев А М, Вавилов В С, Гиппиус А А *Краткие сообщения по физике ФИАН* (10) 20 (1981)
134. Екимов Е А, Кондрин М В *УФН* **187** 577 (2017); Ekimov E A, Kondrin M V *Phys. Usp.* **60** 539 (2017)
135. Wang C et al. *J. Phys. B* **39** 37 (2005)
136. Sipahigil A et al. *Science* **354** 847 (2016)
137. Nguyen C T et al. *Phys. Rev. Lett.* **123** 183602 (2019); arXiv:1907.13199
138. Evans R E et al. *Science* **362** 662 (2018); arXiv:1807.04265
139. Jahnke K D et al. *New J. Phys.* **17** 043011 (2015)
140. Sukachev D D et al. *Phys. Rev. Lett.* **119** 223602 (2017); arXiv:1708.08852
141. Goss J P et al. *Phys. Rev. B* **72** 035214 (2005)
142. Evans R E et al. *Phys. Rev. Appl.* **5** 044010 (2016); arXiv:1512.03820
143. Harris I et al. *Phys. Rev. B* **102** 195206 (2020); arXiv:1907.12548
144. Palyanov Yu N et al. *Sci. Rep.* **5** 14789 (2015)
145. Iwasaki T et al. *Sci. Rep.* **5** 12882 (2015)
146. Iwasaki T et al. *Phys. Rev. Lett.* **119** 253601 (2017); arXiv:1708.03576
147. Trusheim M E et al. *Phys. Rev. Lett.* **124** 023602 (2020)
148. Trusheim M E et al. *Phys. Rev. B* **99** 075430 (2019); arXiv:1805.12202
149. Kim S et al. *Nat. Commun.* **9** 2623 (2018); arXiv:1801.04399
150. Gottscholl A et al. *Nat. Mater.* **19** 540 (2020)
151. Jungwirth N R, Fuchs G D *Phys. Rev. Lett.* **119** 057401 (2017)
152. Tran T T et al. *Nat. Nanotechnol.* **11** 37 (2016)
153. Zargaleh S A et al. *Phys. Rev. B* **98** 165203 (2018)
154. Christle D J et al. *Phys. Rev. X* **7** 021046 (2017)
155. Bergeron L et al. *PRX Quantum* **1** 020301 (2020)
156. Bergeron L, Ph.D. Thesis (Burnaby, BC: Simon Fraser Univ., 2019)
157. Екимов А И, Онушенко А А *Письма в ЖЭТФ* **34** 363 (1981); Ekimov A I, Onushenko A A *JETP Lett.* **34** 345 (1981)
158. Lodahl P, Mahmoodian S, Stobbe S *Rev. Mod. Phys.* **87** 347 (2015); arXiv:1312.1079
159. Гросс Е Ф *УФН* **76** 433 (1962); Gross E F *Sov. Phys. Usp.* **5** 195 (1962)
160. Press D et al. *Nat. Photon.* **4** 367 (2010)

161. Deng G-W et al., *Quantum Dot Optoelectronic Devices* (Lecture Notes in Nanoscale Science and Technology, Vol. 27, Eds P Yu, Z M Wang) (Cham: Springer Intern. Publ., 2020) p. 107
162. Veldhorst M et al. *Nat. Nanotechnol.* **9** 981 (2014); arXiv:1407.1950
163. Zajac D M et al. *Science* **359** 439 (2018)
164. Loss D, DiVincenzo D P *Phys. Rev. A* **57** 120 (1998); cond-mat/9701055
165. Novoselov K S et al. *Science* **353** aac9439 (2016)
166. Wang Q H et al. *Nat. Nanotechnol.* **7** 699 (2012)
167. Mak K F, Shan J *Nat. Photon.* **10** 216 (2016)
168. Келдыш Л В *Письма в ЖЭТФ* **29** 716 (1979); Keldysh L V *JETP Lett.* **29** 658 (1979)
169. Srivastava A et al. *Nat. Nanotechnol.* **10** 491 (2015)
170. Plechinger G et al. *Phys. Status Solidi Rapid Res. Lett.* **9** 457 (2015); arXiv:1507.01342
171. Childress L et al. *Phys. Rev. Lett.* **96** 070504 (2006)
172. Гриб А А *УФН* **142** 619 (1984); Grib A A *Sov. Phys. Usp.* **27** 284 (1984)
173. Bennett C H et al. *Phys. Rev. A* **53** 2046 (1996); quant-ph/9511030
174. Bennett C H et al. *Phys. Rev. A* **54** 3824 (1996); quant-ph/9604024
175. Shor P W *Phys. Rev. A* **52** R2493 (1995)
176. Terhal B M *Rev. Mod. Phys.* **87** 307 (2015); arXiv:1302.3428
177. Muralidharan S et al. *Sci. Rep.* **6** 20463 (2016)
178. Guha S et al. *Phys. Rev. A* **92** 022357 (2015); arXiv:1404.7183
179. Van der Wal C H et al. *Science* **301** 196 (2003)
180. Kuzmich A et al. *Nature* **423** 731 (2003); quant-ph/0305162
181. Yuan Z-S et al. *Nature* **454** 1098 (2008); arXiv:0803.1810
182. Zhao B et al. *Phys. Rev. Lett.* **98** 240502 (2007)
183. Jiang L, Taylor J M, Lukin M D *Phys. Rev. A* **76** 012301 (2007)
184. Wallraff A et al. *Nature* **431** 162 (2004)
185. Blais A et al. *Phys. Rev. A* **69** 062320 (2004); cond-mat/0402216
186. Häffner H et al. *Nature* **438** 643 (2005); quant-ph/0603217
187. Moehring D L et al. *Nature* **449** 68 (2007)
188. Monroe C et al. *Phys. Rev. Lett.* **75** 4714 (1995)
189. Meraner M et al. *Phys. Rev. A* **102** 052614 (2020); arXiv:1912.09259
190. Lo H-K, Curty M, Qi B *Phys. Rev. Lett.* **108** 130503 (2012); arXiv:1109.1473
191. Nguyen C T et al. *Phys. Rev. B* **100** 165428 (2019); arXiv:1907.13200
192. Varnava M, Browne D E, Rudolph T *Phys. Rev. Lett.* **97** 120501 (2006); quant-ph/0507036
193. Munro W J et al. *Nat. Photon.* **6** 777 (2012); arXiv:1306.4137
194. Fowler A G et al. *Phys. Rev. Lett.* **104** 180503 (2010); arXiv:0910.4074
195. Muralidharan S et al. *Phys. Rev. Lett.* **112** 250501 (2014); arXiv:1310.5291
196. Glaudell A N, Waks E, Taylor J M *New J. Phys.* **18** 093008 (2016)
197. Briegel H J, Raussendorf R *Phys. Rev. Lett.* **86** 910 (2001); quant-ph/0004051
198. Schwartz I et al. *Science* **354** 434 (2016); arXiv:1606.07492
199. Gimeno-Segovia M, Rudolph T, Economou S E *Phys. Rev. Lett.* **123** 070501 (2019); arXiv:1801.02599
200. Nielsen M A *Rep. Math. Phys.* **57** 147 (2006); quant-ph/0504097
201. Raussendorf R, Briegel H J *Phys. Rev. Lett.* **86** 5188 (2001)
202. Azuma K, Tamaki K, Lo H-K *Nat. Commun.* **6** 6787 (2015); arXiv:1309.7207
203. Lindner N H, Rudolph T *Phys. Rev. Lett.* **103** 113602 (2009)
204. He Y-M et al. *Nat. Nanotechnol.* **8** 213 (2013); arXiv:1303.4058
205. Lu C-Y et al. *Nat. Phys.* **3** 91 (2007)
206. Li Z-D et al. *Nat. Photon.* **13** 644 (2019); arXiv:1908.05351
207. Hasegawa Y et al. *Nat. Commun.* **10** 13480 (2020)
208. Lake D P et al. *Nat. Commun.* **11** 2208 (2020)
209. Armani D K et al. *Nature* **421** 925 (2003)
210. Ахманов С А, Хохлов Р В *ЖЭТФ* **43** 351 (1962); Akhmanov S A, Khokhlov R V *Sov. Phys. JETP* **16** 252 (1963)
211. Kroll H *Phys. Rev.* **127** 1207 (1962)
212. Kingston R H *Proc. IRE* **50** 472 (1962)
213. Boyd R *Nonlinear Optics* (New York: Academic Press, 2008) p. 640
214. Ashkin A, Boyd G, Dziedzic J *IEEE J. Quantum Electron.* **2** 109 (1966)
215. Houe M, Townsend P D *J. Phys. D* **28** 1747 (1995)
216. Tanzilli S et al. *Eur. Phys. J. D* **18** 155 (2002)
217. Zaske S et al. *Phys. Rev. Lett.* **109** 147404 (2012); arXiv:1204.6253
218. Dréau A et al. *Phys. Rev. Appl.* **9** 064031 (2018)
219. Hill J T et al. *Nat. Commun.* **3** 1196 (2012); arXiv:1206.0704
220. Dong C et al. *Science* **338** 1609 (2012)
221. Mitchell M, Lake D P, Barclay P E *Optica* **6** 832 (2019); arXiv:1902.07763
222. Lucamarini M et al. *Nature* **557** 400 (2018); arXiv:1811.06826
223. Ursin R et al. *Nat. Phys.* **3** 481 (2007)
224. Nauerth S et al. *Proc. SPIE* **8518** 85180D (2012)
225. Vallone G et al. *Phys. Rev. Lett.* **115** 040502 (2015); arXiv:1406.4051
226. Yin J et al. *Science* **356** 1140 (2017); arXiv:1707.01339
227. Buttler W T et al. *Phys. Rev. Lett.* **84** 5652 (2000); quant-ph/0001088
228. Schmitt-Manderbach T et al. *Phys. Rev. Lett.* **98** 010504 (2007)
229. Liao S-K et al. *Nat. Photon.* **11** 509 (2017)
230. Fedrizzi A et al. *Nat. Phys.* **5** 389 (2009)
231. Yin J et al. *Nature* **488** 185 (2012); arXiv:1205.2024
232. Bedington R, Arrazola J M, Ling A *npj Quantum Inf.* **3** 30 (2017); arXiv:1707.03613
233. Nauerth S et al. *Nat. Photon.* **7** 382 (2013)
234. Boone K et al. *Phys. Rev. A* **91** 052325 (2015); arXiv:1410.5384
235. Yin J et al. *Nature* **582** 501 (2020)
236. Ekert A K *Phys. Rev. Lett.* **67** 661 (1991)
237. Joshi S K et al. *New J. Phys.* **20** 063016 (2018)
238. Rideout D et al. *Class. Quantum Grav.* **29** 224011 (2012)
239. Zhang Q et al. *Opt. Express* **26** 24260 (2018)
240. Sasaki M et al. *Opt. Express* **19** 10387 (2011)
241. Dynes J F et al. *npj Quantum Inf.* **5** 101 (2019)
242. Киктенко Е О и др. *Квантовая электроника* **47** 798 (2017); Kiktenko E O et al. *Quantum Electron.* **47** 798 (2017); arXiv:1705.07154
243. Степанова Ю "Кванты ставят на рельсы. В ОАО РЖД оценили создание новой сети передачи данных", Коммерсантъ 13.01.2020; https://www.kommersant.ru/doc/4219027
244. Liao S-K et al. *Phys. Rev. Lett.* **120** 030501 (2018); arXiv:1801.04418
245. Aharonov Y, Zubairy M S *Science* **307** 875 (2005)
246. Pfleegor R L, Mandel L *Phys. Rev.* **159** 1084 (1967)
247. Minder M et al. *Nat. Photon.* **13** 334 (2019); arXiv:1910.01951
248. Zhong X et al. *Phys. Rev. Lett.* **123** 100506 (2019); arXiv:1902.10209
249. Wang X-B, Yu Z-W, Hu X-L *Phys. Rev. A* **98** 062323 (2018)
250. Liu Y et al. *Phys. Rev. Lett.* **123** 100505 (2019); arXiv:1902.06268
251. Fang X-T et al. *Nat. Photon.* **14** 422 (2020)

Large quantum networks

D.D. Sukachev
University of Calgary, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada
E-mail: sukachev@gmail.com

Quantum networks that allow generating entangled states between distant qubits have enormous scientific and applied potential. They can be used for secure quantum cryptography and the teleportation of quantum states between cities and countries, in high-resolution astronomy, and in distributed quantum computing. The scattering of photons in an optical fiber and the difficulties in creating full-fledged quantum nodes impede the construction of large quantum networks. We review current approaches to the creation of such networks, with the emphasis on quantum repeaters intended for 'compensating' losses in optical fibers. We also discuss methods for increasing the range of quantum cryptography systems without using quantum repeaters.

Keywords: quantum network, quantum cryptography, quantum repeater

PACS numbers: 03.65.Ud, **03.67.–a**, 42.50.Ex

Bibliography — 251 references
Uspekhi Fizicheskikh Nauk **191** (10) 1077–1094 (2021)
DOI: https://doi.org/10.3367/UFNr.2020.11.038888

Received 9 June 2020, revised 26 November 2020
Physics–Uspekhi **64** (10) (2021)
DOI: https://doi.org/10.3367/UFNe.2020.11.038888