Internet Research Task Force (IRTF)
Request for Comments: 9583
Category: Informational
ISSN: 2070-1721

C. Wang
InterDigital Communications, LLC
A. Rahman
Ericsson
R. Li
Kanazawa University
M. Aelmans
Juniper Networks
K. Chakraborty
The University of Edinburgh

June 2024

Application Scenarios for the Quantum Internet

Сценарии применения Quantum Internet

Аннотация

Quantum Internet может улучшить функциональность приложений за счёт внедрения квантовой теории информации в инфраструктуру Internet. В этом документе представлен обзор некоторых приложений, которые предположительно будут применяться в Quantum Internet, и дана их классификация. Рассматриваются также некоторые общие требования к Quantum Internet. Целью документа является описание модели для приложений и некоторых вариантов применения Quantum Internet. Документ является результатом работы исследовательской группы Quantum Internet (QIRG).

Оглавление

1. Введение

Классическая (не квантовая) сеть Internet постоянно растёт с момента, когда она стала коммерчески доступной в начале 1990-х годов. По сути, сеть состоит из большого числа конечных узлов (например, ноутбуков, смартфонов,

[1]Internet Research Task Force - комиссия по исследовательским задачам Internet.

серверов), соединённых маршрутизаторами и объединённых в автономные системы (Autonomous System или AS). На конечных узлах могут работать приложения, предоставляющие конечным пользователям такие услуги, как передача голоса, видео или данных. Соединения между узлами Internet включают магистральные каналы (например, оптические), линии доступа (например, оптически, Wi-Fi, сотовые сети, DSL[1]). Биты передаются через Classical Internet в пакетах.

В последние несколько лет активизировались исследования и эксперименты по разработке квантовых сетей (Quantum Internet) [Wehner]. Конечные узлы также будут частью Quantum Internet и в этом случае их называют квантовыми конечными узлами (quantum end node). Эти узлы могут соединяться квантовыми повторителями и маршрутизаторами. На конечных квантовых узлах будут работать добавляющие услуги (value-added) приложения, которые будут рассмотрены ниже.

Квантовые каналы физического уровня между узлами Quantum Internet могут быть волноводами (например, оптическими волокнами) или открытым пространством. Особенно полезны фотонные каналы, поскольку свет (фотоны) очень хорошо подходит для физической реализации кубитов. Quantum Internet будет работать в соответствии с принципами квантовой физики, такими как суперпозиция и запутанность [RFC9340].

Предполагается, что Quantum Internet не заменит, а усовершенствует Classical Internet и/или обеспечит прорывные приложения. Например, квантовое распространение ключей может повысить уровень безопасности Classical Internet, а квантовые вычисления - ускорить и оптимизировать задачи с большим объёмом расчётов. Quantum Internet будет работать в связке с Classical Internet, а процессы интеграции будут похожи на процесс внедрения новых коммуникационных и сетевых парадигм в существующую сеть Internet, но с более серьёзными последствиями.

Назначение этого документа состоит в обеспечении базового понимания и моделей применения Quantum Internet. Отмечается, что в ITU-T SG13-TD158/WP3 [ITUT] кратко описаны 4 вида использования квантовых сетей в дополнение к квантовому распространению ключей. Это квантовая синхронизация часов, квантовые вычисления, квантовые генераторы случайных чисел и квантовые коммуникации (например, квантовые цифровые подписи, квантовая анонимная передача, квантовые деньги). Этот документ сосредоточен на квантовых приложениях, оказывающих важное влияние на работу сетей, таких как организация защищённых коммуникаций, квантовые вычисления вслепую и распределенные квантовые вычисления. Хотя такие приложения упомянуты в [ITUT], этот документ указывает больше деталей и задаёт некоторые требования с точки зрения сети.

Документ был создан исследовательской группой QIRG и обсуждался в почтовой конференции QIRG и на встречах исследовательской группы. Документ был детально рассмотрен членами QIRG, имеющими опыт в квантовой физике и работе Classical Internet. Документ представляет согласованное мнение членов QIRG, являющихся как экспертами в данной области (квантовая физика и сети), так и новичками, которые являются целевой аудиторией. Это не результат работы IETF и не стандарт.

2. Термины и сокращения

В этом документе предполагается знакомство читателя с концепциями и терминами квантовой теории информации, представленными в [RFC9340]. Кроме того, ниже даны определения некоторых терминов и сокращений.

Bell Pairs - пары Белла
: Особый тип квантового состояния двух кубитов. Такие два кубита демонстрируют корреляцию, которую невозможно встретить в классической теории информации. Такую корреляцию называют квантовой запутанностью. Пары Белла демонстрируют максимальную квантовую запутанность. Одним из примеров пары Белла является (|00>+|11>)/(Sqrt(2)). Пары Белла являются фундаментальным ресурсом квантовых коммуникаций.

Bit - бит
: Двоичная цифра (фундаментальная единица информации в классических коммуникациях и вычислениях). Биты применяются в Classical Internet, где состояние бита детерминировано. В Quantum Internet состояние кубита является неопределённым до его измерения.

Classical Internet
: Существующая сеть Internet (около 2020 г.), где биты переносятся в пакетах между узлами для передачи информации. В Classical Internet поддерживаются приложения, которые могут быть усовершенствованы в Quantum Internet. Например, сквозная защита приложений Classical Internet может быть улучшена за счёт защищённой организации коммуникаций с использованием квантовых приложений. Classical Internet - это сеть классических сетевых узлов, не поддерживающих квантовую теорию информации. Quantum Internet состоит из квантовых узлов, основанных на квантовой теории информации.

Entanglement Swapping - обмен запутанностью
: Процесс обобщения (sharing) запутанности между двумя удалёнными одна от другой сторонами через некие промежуточные узлы. Предположим, например, что имеется три стороны (A, B, C) и каждая из сторон имеет общие пары Белла - (A, B) и (B, C). B может использовать кубиты, общие с A и C, для выполнения операций обмена запутанностью и в результате A и C будут иметь одщие пары Белла. Обмен запутанностью, по сути, реализует распространение (распределение) запутанности, где два разнесённых территориально узла могут иметь общую пару Белла.

Fast Byzantine Negotiation - быстрые византийские переговоры (согласование)
: Квантовый метод быстрого согласования в Византийских переговорах[2] [Ben-Or] [Taherkhani].

Local Operations and Classical Communication (LOCC) - локальные операции и классические коммуникации
: Метод, при котором узлы могут взаимодействовать в раундах, где (1) они могут передавать друг другу любую классическую информацию, (2) могут индивидуально выполнять локальные квантовые операции и (3) выполняемые в каждом раунде операции могут зависеть от результатов предыдущих раундов.

Noisy Intermediate-Scale Quantum (NISQ) - зашумлённые квантовые системы промежуточного уровня
: Определение NISQ было дано в [Preskill] для представления ближайшей эры квантовой технологии. Согласно этому определению, компьютеры NISQ имеют две важных особенности: (1) размер компьютеров NISQ варьируется от 50 до нескольких сотен физических кубитов (промежуточный уровень) и (2) кубиты в компьютерах NISQ имеют врожденные ошибки и контроль над ними несовершенен (шум).

[1] Digital Subscriber Line - цифровая абонентская линия.
[2] В русском языке принят термин «задача византийских генералов», см. здесь. *Прим. перев.*

Packet - пакет
Самоидентифицирующееся сообщение со встроенными адресами или иными сведениями, которые могут служить для пересылки сообщения. Сообщение содержит упорядоченный набор битов определённого числа (количества). Биты пакета являются классическими.

Prepare and Measure - подготовка и измерение
Набор сценариев Quantum Internet, в которых квантовые узлы поддерживают лишь простые квантовые функции (подготовка и измерение кубитов). Например, BB84 [BB84] - это протокол квантового распределения ключей с подготовкой и измерением.

Quantum Computer (QC) - квантовый компьютер
Квантовый конечный узел, имеющий квантовую память и возможности квантовых вычислений, считается полноценным квантовым компьютером.

Quantum End Node - квантовый конечный узел
Конечный узел, на котором размещаются приложения и интерфейсы с остальной частью Internet. Обычно конечный узел может служить клиентом, сервером или узлом одноранговой сети в зависимости от приложения. Квантовый конечный узел должен также быть способным взаимодействовать с Classical Internet для целей управления, т. е. принимать, обрабатывать и передавать классические биты и/или пакеты.

Quantum Internet
Сеть квантовых сетей. Предполагается слияние Quantum Internet с Classical Internet. Quantum Internet может улучшить классические приложения и создать новые квантовые приложения.

Quantum Key Distribution (QKD) - квантовое распространение ключей
Метод, использующий квантовую механику (например, теорему об отсутствии клонирования), чтобы позволить паре узлов создать один и тот же произвольный классический ключ.

Quantum Network - квантовая сеть
Новый тип сети, создаваемый на основе квантовой теории информации, где квантовые ресурсы, такие как кубиты и запутанность, используются и передаются между квантовыми узлами. Квантовая сеть будет использовать квантовые каналы и классические каналы Classical Internet. Это называется гибридной реализацией.

Quantum Teleportation - квантовая телепортация
Метод доставки квантовой информации с помощью локальных операций и классической связи (LOCC). Если две стороны имеют общую пару Белла, отправитель может передать квантовый бит данных получателю без его передачи по физическому квантовому каналу.

Qubit - кубит
Квантовый бит (фундаментальная единица информации в квантовых коммуникациях и вычислениях). Кубит похож на классический бит в том, что имеет после измерения состояние 0 или 1, обозначаемые как |0> и |1> в нотации Дирака. Однако кубит отличается от классического бита тем, что он до измерения может быть линейной комбинацией обоих состояний, которую называют суперпозицией. Для кодирования кубита может применяться любая из нескольких степеней свободы (Degrees of Freedom или DOF) фотона (например, поляризация, time-bin, частота) или электрона (например, спин).

Teleport a Qubit - телепортация кубита
Операция на двух или более кубитах последовательно для переноса кубита от отправителя к получателю с использованием квантовой телепортации.

Transfer a Qubit - перенос кубита
Операция переноса кубита от отправителя к получателю без указания способа перемещения кубита, каковым может служить передача или телепортаци.

Transmit a Qubit - передача кубита
Операция кодирования кубита в подвижный носитель (обычно, фотон) и его передачи по квантовому каналу от отправителя (передатчик) к получателю.

3. Применение Quantum Internet

Предполагается, что применение Quantum Internet будет полезно для некоторых имеющихся и новых приложений. Приложения Quantum Internet все ещё находятся в стадии разработки, поскольку становление Quantum Internet пока не завершено [Castelvecchi] [Wehner]. Однако начальный (и неполный) список приложений, поддерживаемых в Quantum Internet уже можно определить и классифицировать с использованием двух разных схем. Отметим, что этот документ не рассматривает квантовых вычислений, которые полностью выполняются на локальном узле.

Приложения можно группировать по решаемым задачам (услугам). В частности, можно выделить указанные ниже категории.

Quantum cryptography applications - квантовая криптография
Использование квантовой теории информации для задач криптографии (например, квантового распространения ключей [Renner]).

Quantum sensor applications - квантовые датчики
Использование квантовой теории информации для поддержки распределенных датчиков (например, синхронизации часов [Jozsa2000] [Komar] [Guo]).

Quantum computing applications - квантовые вычисления
Использование квантовой теории информации для поддержки удалённых квантовых вычислительных комплексов (например, распределённые квантовые вычисления [Denchev]).

Эта схема будет понятна технической и нетехнической аудитории. Ниже схема рассматривается более подробно.

3.1. Квантовая криптография

Примеры квантовой криптографии включают организацию защищённой квантовой связи и быстрое византийское согласование.

Secure communication setup - организация защищённых коммуникаций
Защищённое распространение криптографических ключей между двумя (или более) конечными узлами. Наиболее известный метод называется квантовым распространением ключей (QKD) [Renner].

Fast Byzantine negotiation - быстрое византийское согласование
Квантовый мотод быстрого согласования в византийских переговорах [Ben-Or], например, для сокращения числа ожидаемых раундов связи и ускоренного соглашения в классических византийских переговорах. Квантовое

византийское соглашение в сетях квантовых повторителей, предложенное в [Taherkhani], включает методы оптимизации, позволяющие значительно сократить глубину квантовой схемы (устройства) и число кубитов на каждом узле. Квантовые методы бытрого согласования в византийских переговорах можно применять для улучшения протколов согласия (consensus), таких как pBFT[1], а также иных функций распределенного вычисления, использующих византийское согласование.

Quantum money - квантовые деньги

Основным требованием к деньгам является невозможность их подделки. Схема квантовых денег нацелена на использованием свойства невозможности клонирования неизвестных квантовых состояний. Хотя идея квантовых денег возникла ещё в 1970 г., ранние протоколы позволяли проверить подлинность квантовых денег лишь банку-эмитенту. Недавние протоколы, такие как квантовые деньги с открытым ключом [Zhandry] позволяют любому локально проверить подлинность денег.

3.2. Квантовые датчики и метрология

Запутанность, суперпозиция, интерференция и сжатие свойств могут повышать чувствительность квантовых датчиков и в конечном счёте превзойти классические варианты. Примерами применения квантовых датчиков являются синхронизация часов, высокочувствительные датчики и т. п. Эти приложения в основном используют сеть запутанных квантовых датчиков (т. е. сеть квантовых датчиков) для высокоточных измерений множества параметров [Proctor].

Network clock synchronization - синхронизация часов

Общемировой набор часов, подключённых к Quantum Internet для обеспечения сверхточных сигналов часов [Komar] с ограничениями точности, определяемыми квантовой теорией.

High-sensitivity sensing - датчики с высокой чувствительностью

Приложения, использующие квантовые явления для достижения надёжного наноразмерного измерения физических величин. Например, в [Guo] применяется запутанная квантовая сеть для измерения среднего сдвига фазы между множеством распределенных узлов.

Interferometric telescopes using quantum information - интерферометрические телескомы

Интерферометрические методы, применяемые для объединения сигналов от двух и более телескопов с целью получения изображений с более высоким разрешением, нежели может обеспечить отдельный телескоп. Это позволяет исследовать очень мелкие астрономические объекты, если телескопы распределены по большой площади. Однако флуктуации фазы и потери фотонов в каналах связи между телескопами вносят ограничения на размер базы оптических интерферометров. Потенциально это ограничение можно обойти с помощью квантовой телепортации. В общем случае обобщение пар Эйнштейна-Подольского-Розена с использованием квантовых повторителей позволяет оптическим интерферометрам обмениваться фотонами на больших расстояниях, обеспечивая базу произвольного размера [Gottesman2012].

3.3. Квантовые вычисления

В этом параграфе рассматриваются приложения для квантовых вычислений. Предполагается, что квантовые компьютеры в будущем станут доступными как облачные услуги. Иногда для запуска таких приложений в облаке с сохранением приватности клиенту и серверу потребуется обмен кубитами (например, для расчётов вслепую [Fitzsimons], как описано ниже. Поэтому для сохранения приватности в приложениях квантовых вычислений потребуется Quantum Internet.

Примеры квантовых вычислений включают распределенные вычисления и вычисления вслепую, которые могут обеспечить новый тип облачных вычислений.

Distributed quantum computing - распределенные квантовые вычисления

Набор распределенных квантовых компьютеров малой мощности (например, с небольшим числом кубитов), соединённых между собой и работающих согласованно для имитации высокопроизводительного квантового компьютера [Wehner].

Blind quantum computing - квантовые вычисления вслепую

Квантовые расчёты с сохранением приватности, обеспечивающие клиентам возможность передачи вычислительных задач одному или нескольким удалённым квантовым компьютерам без раскрытия источника данных для расчётов [Fitzsimons].

4. Некоторые приложения Quantum Internet

В Quantum Internet будут поддерживаться различные приложения и конфигурации развёртывания. В этом разделе описано несколько ключевых сценариев использования, демонстрирующих преимущества Quantum Internet. В системной инженерии сценарий приложения обычно представляет собой набор возможных последовательностей взаимодействия между узлами и пользователями в определённой серде для достижения конкретной цели. Это определение применяется в данном разделе.

4.1. Организация защищённых коммуникаций

В этом сценарии двум узлам (например, квантовым узлам A и B) требуется организовать защищённую связь для передачи конфиденциальных сведений (см. рисунок 1). Для этого им сначала нужно защищённым способом организовать общий классический секретный криптографический ключ (последовательность классических битов). Процесс запускает конечный пользователь с защищённым локальным интерфейсом к квантовому узлу A. В результате квантовый узел A защищённо организует классический секретный ключ с квантовым узлом B. Это называется организацией защищённой связи. Отметим, что квантовые узлы A и B могут быть простыми (bare-bone) квантовыми узлами или полноценными квантовыми компьютерами. Это приложение показывает, что Quantum Internet можно использовать для повышения защищенности приложений Classical Internet.

Одним из требований к такому процессу организации защищённой связи является неуязвимость к классическим и квантовым вычислительным атакам. Этого можно добиться с помощью квантового распространения ключей (QKD), которое в принципе не поддаётся взлому. QKD может защищённо организовать секретный ключ между парой квантовых узлов, используя классический канал проверки подлинности и незащищённый квантовый канал без физической передачи ключа через сеть, что обеспечивает требуемую защиту. Однако необходимо позаботиться о

[1]Byzantine Fault Tolerance - византийская отказоустойчивость.

защите системы QKD от атак по побочным физическим каналам, которые могут скомпрометировать систему. Примером атаки по побочному физическому каналу является скрытое введение дополнительного света в оптические устройства, применяемые QKD, чтобы получить сведения о системе, такие как поляризация. Другие специализированные атаки на QKD используют классический канал аутентификации и незащищённый квантовый канал. К таким атакам относятся переотображение фазы (phase-remapping), расщепление числа фотонов, ложное состояние [Zhao2018]. QKD можно применять для разных криптографических коммуникаций, таких как IPsec и защита транспортного уровня (Transport Layer Security или TLS), где участвующие стороны должны организовать общий ключ защиты, хотя это обычно влечёт высокую задержку.

QKD является наиболее развитым свойством квантовой информационной технологии и такое распространение ключей уже реализовано коммерчески в небольших системах и на коротких расстояниях. Варианты применения QKD описаны в документе ETSI [ETSI-QKD-UseCases], а интерфейс между пользователями и устройствами QKD задан в [ETSI-QKD-Interfaces].

В общем случае протоколы QKD с подготовкой и измерением (например, [BB84]) без использования запутанности работают, как описано ниже.

1. Квантовый узел A кодирует классические биты в кубиты. Узел A генерирует две строки случайных классических битов X и Y. Строка X служит для выбора базы, Y - для выбора состояния, соответствующего выбранной базе. Например, при X=0 в случае использования протокола BB84 Алиса готовит состояние в базе {|0>, |1>}, иначе - в базе {|+>, |->}. При Y=0 Алиса готовит кубит как |0> или |+> (в зависимости от X), а при Y =1 - как |1> или |->.

2. Квантовый узел A передаёт кубиты квантовому узлу B по квантовому каналу.

3. Квантовый узел B принимает кубиты и измеряет каждый из них в одной из двух баз, выбранной случайно.

4. Квантовый узел B информирует квантовый узел A о своём выборе базы для каждого кубита.

5. Квантовый узел A сообщает квантовому узлу B, какие из случайно выбранных баз были верны.

6. Оба узла отбрасывают все биты измерений с отличающейся квантовой базой, а оставшиеся биты могут служить секретным ключом. Перед генерацией финального секретного ключа выполняется процедура пост-обработки через аутентифицированные классические каналы. Эта процедура может делиться на 3 этапа - оценка параметров, исправление ошибок и повышение приватности. На этапе оценки параметров Алиса и Боб используют некоторые из битов для оценки канальных ошибок. Если число ошибок превышает некий порог, протокол прерывается, иначе выполняется корректировка ошибок. Если подслушивающий попытается перехватить и прочитать кубиты, переданные от A к B, он будет обнаружен в соответствии с теоремой квантовой механики об энтропийной неопределённости. Как часть процедуры пост-обработки оба узла обычно выполняют сверку (reconciliation) информации [Elkouss] для эффективного исправления ошибок и/или проводят усиление приватности [Tang] для генерации окончательных ключей на основе теории информации.

7. Процедура пост-обработки должна выполняться по аутентифицированному классическому каналу. Иными словами, квантовым узлам A и B нужно убедиться в подлинности классического канала, чтобы быть уверенными в отсутствии на пути подслушивающих или атакующих. Проверка выполняется по протоколам аутентификации, иаким как [Kiktenko]. В соответствии с [Kiktenko] подлинность классического канала проверяется в самом конце процедуры пост-обработки вместо того, чтобы делать это для каждого классического сообщения передаваемого по каналу между квантовыми узлами A и B.

Следует отметить ряд обстоятельств, указанных ниже.

1. Имеются усовершенствованные протоколы QKD, основанные на [BB84]. Например, был обнаружен ряд брешей, связанных с несовершенством измерительных устройств, и имеются решения, учитывающие такие атаки, например, независимое от измерительных устройств решение QKD [Zheng2019]. Эти улучшенные протоколы QKD могут работать иначе, нежели описанные этапы протокола BB84 [BB84].

2. Для крупномасштабных QKD, требуются сети QKD (QKD Network или QKDN), которые можно считать частью Quantum Internet. QKDN может включать прикладной, сетевой и канальный уровень QKD [Qin]. Между квантовыми узлами A и B может находиться один или несколько ретрансляторов QKD [Zhang2018], соединённых через QKDN. Как вариант, QKDN может работать на основе распространения запутанности и основанных на запутанности протоколов QKD. В результате для крупномасштабных QKD будут требоваться квантовые повторители и/или маршрутизаторы вместо доверенных ретрансляторов QKD. Для распределения запутанности может применяться обмен запутанностью.

3. QKD обеспечивает основанные на теории информации общие секретные ключи для двух сторон (передатчик и приёмник) при наличии подслушивания. Однако это верно в теории, которая в значительной мере оторвана от практики. Используя несовершенство детекторов, Ева может получить сведения об общем ключе [Xu]. Для предотвращения таких атак через побочные каналы в [Lo] исследователи предложили протокол QKD, названный независимым от измерительных устройств (Measurement Device-Independent или MDI) QKD, где два пользователя (передатчик Алиса и приёмник Боб) могут безопасно взаимодействовать даже если используемое ими (измерительное) оборудование подменено (захвачено) злоумышленником и перестало быть доверенным. Это достигается путём измерения корреляция между сигналами от Алисы и Боба вместо измерения самих сигналов.

4. Протоколы QKD, основанные на QKD с непрерывной переменной (Continuous Variable QKD или CV-QKD), вызывают в последнее время большой интерес, поскольку для их реализации достаточно легко доступного и широко распространённого телекоммуникационного оборудования. Этот тип технологии потенциально обеспечит высокопроизводительный метод защищённого распространения ключей на ограниченных расстояниях. Недавние демонстрации CV-QKD показали совместимость с классическими схемами когерентного детектирования, которые широко применяются в классических широкополосных системах связи [Grosshans]. Отметим, что до сих пор нет квантовых повторителей для систем с непрерывными переменными, поэтому этот тип QKD пригоден лишь для коротких расстояний или сетей QKD с доверенными ретрансляторами.

5. Распространение секретов может применяться для распределения секретного ключа между множеством узлов, позволяя каждому узлу знать долю или часть секретного ключа, но не предоставляя всего ключа ни одному из узлов. Секретный ключ можно восстановить лишь при совместной работе достаточного числа узлов. Квантовым обменом секретами (Quantum Secret Sharing или QSS) обычно называют сценарий, где секретный ключ обобществляется на основе квантовых состояний, а не классических битов. QSS позволяет разделять (splitting) и обобществлять (sharing) такие квантовые состояния между множеством узлов.

6. Имеются основанные на запутанности протоколы QKD, такие как описано в [Treiber], [E91] и [BBM92], которые работают не так, как описано в предыдущих этапах. Основанные на запутанности схемы, где состояния запутанности подготавливаются вне квантовых узлов A и B, обычно не считают подготовкой и измерением, описанными в [Wehner]. Другие схемы на основе запутанности, где запутанность создаётся внутри квантового узла-источника и служит для вывода ключей, могут считаться подготовкой и измерением. Схемы с передачей и возвратом (Send-and-return) могут считаться подготовкой и измерением, если информационное содержимое, из которого выводятся ключи, подготавливаются в квантовом узле A перед их отправкой квантовому узлу B для измерения.

Quantum Internet на рисунке 1 включает квантовые каналы. Для организации защищённой связи, особенно в больших системах, требуется также генерация и распространение запутанности [QUANTUM-CONNECTION], квантовые повторители и/или маршрутизаторы, доверенные ретрансляторы QKD.

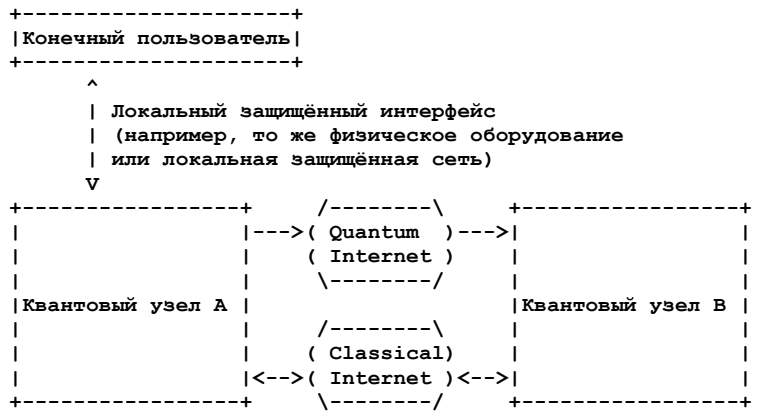

Рисунок 1. Организация защищённой связи.

4.2. Квантовые расчёты вслепую

Квантовыми расчётами вслепую называют описанный ниже сценарий.

1. Клиентский узел с исходными данными передаёт вычисления удалённому расчётному узлу (серверу).

2. Клиентский узел не хочет раскрывать удалённому узлу исходные данные, сохраняя их приватность.

3. Нет каких-либо допущений или гарантий о доверии к удалённому расчётному узлу в части приватности исходных данных.

В примере на рисунке 2 терминальный узел может быть небольшим квантовым компьютером с ограниченными вычислительными возможностями по сравнению с удаленным квантовым расчётным узлом (например, квантовым мэйнфреймом), но терминальному узлу нужно решить задачу с большим объёмом вычислений (например, алгоритм факторизации Шора). Терминальный узел может создать отдельные кубиты и передать их удалённому квантовому расчётному узлу. После этого удалённый квантовый узел может запутать кубиты, выполнить расчёты, провести измерения, оформляя их результаты в классических битах, и вернуть эти результаты терминальному узлу. Следует отметить, что для удалённого квантового расчётного узла эти результаты будут выглядеть просто случайными данными, поскольку начальные состояния кубитов были выбраны криптографически защищённым способом.

Как новая вычислительная модель клиент-сервер, квантовые расчёты вслепую (Blind Quantum Computation или BQC) в целом позволяет выполнить представленный ниже процесс.

1. Клиент делегирует вычислительную функцию серверу.

2. Клиент не передаёт исходные кубиты серверу, но передаёт тому преобразованные кубиты.

3. Сервер применяет вычислительную функцию к преобразованным кубитам для создания промежуточных результатов (кубиты) с помощью квантовых расчётов на основе квантовой схемы (устройства) или квантовых измерений. Сервер передаёт клиенту кубиты промежуточных результатов.

4. Клиент получает кубиты промежуточных результатов и преобразует их в кубиты окончательных результатов.

В этом процессе сервер не может восстановить исходные кубиты из преобразованных. Прямое и обратное (для результатов) преобразование кубитов не требует от клиента значительных усилий. Один из первых протоколов BQC (например, описанный в [Childs]) следует этому процессу, но у клиента требуется наличие некоторого объёма квантовой памяти, подготовка и измерение кубитов, а также их передача. Основанные на измерениях квантовые вычисления выходят за рамки этого документа, а более подробные сведения приведены в [Jozsa2005].

Следует отметить ряд обстоятельств, указанных ниже.

1. Протокол BQC из [Childs] - это основанная на устройстве модель BQC, где клиент реализует лишь простую квантовую схему, а сервер выполняет цепочку квантовых логических операций. Кубиты передаются туда и обратно между клиентом и сервером.

2. Universal BQC (UBQC) из [Broadbent] - это основанная на измерениях модель BQC, где выполняются квантовые измерения с использованием запутанных состояний. Принцип UBQC основан на том, что квантовая трансформация плюс измерение Белла с поворотом (базы) реализуют квантовые вычисления, которые могут

повторяться для реализации расчётной цепочки. В этом случае клиент сначала готовит преобразованные кубиты, затем передаёт их серверу, а тому нужно сначала подготовить запутанные состояния из всех принятых кубитов. Далее между клиентом и сервером выполняется множество раундов взаимодействия и измерения:

i. клиент передаёт серверу новые инструкции по измерению или его адаптации;

ii. сервер выполняет измерения в соответствии с полученными инструкциями для получения результатов (в кубитах или классических битах);

iii. клиент получает результаты измерения и преобразует их в окончательные результаты.

3. В [Zhang2009] предложен гибридный вариант UBQC, где сервер реализует квантовые устройства (схемы), подобно показанным в [Childs], и квантовые измерения, похожие на показанные в [Broadbent], для снижения числа требуемых запутанных состояний [Broadbent]. Клиент в этом случае много проще, нежели в [Childs]. Этот гибридный вариант BQC является сочетанием моделей BQC на основе схемы и измерений.

4. В идеальном случае клиент BQC является чисто классическим и ему требуется лишь взаимодействие с сервером по классическим каналам. В [Huang] продемонстрирован такой подход, где клиент использует два запутанных сервера для выполнения BQC в предположении невозможности взаимодействия между этими серверами (в противном случае расчёты вслепую и приватность клиента не гарантируются). Продемонстрированный в [Huang] сценарий, по сути, является примером BQC с несколькими серверами.

5. Проверка соответствия выполненного сервером запросам и ожиданиям клиента важна для многих протоколов BQC, называемых верифицируемыми. В [Fitzsimons] обсуждается этот вопрос и сравниваются протоколы BQC.

На рисунке 2 Quantum Internet включает квантовые каналы и квантовые повторители и/или квантовые маршрутизаторы для передачи кубитов на большие расстояния [RFC9340].

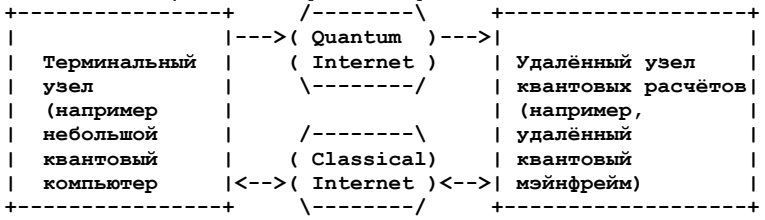

Рисунок 2. Квантовые расчёты вслепую.

4.3. Распределённые квантовые расчёты

Существует два способа распределенных квантовых расчётов [Denchev].

1. Использование квантовой механики для улучшений классических распределенных расчётов. Например, можно использовать запутанные квантовые состояния для улучшения выбора лидера в классических распределенных расчётах путём простого измерения запутанных квантовых состояний на каждой стороне (например, на узле или устройстве) без каких-либо классических коммуникаций между разнесёнными сторонами [Pal]. Обычно сначала нужно организовать между сторонами предварительную запутанность, а затем выполнить операции LOCC на каждой стороне. При этом обычно не нужно передавать кубиты между сторонами.

2. Распределение функций квантовых вычислений между разнесёнными квантовыми компьютерами. Задача или функция квантовых расчётов (например, квантовые вентили) расщепляется и распределяется между множеством физически разделённых квантовых компьютеров. При этом может потребоваться передача кубитов (входных или выходных) между этими распределенными компьютерами. Для поддержки таких распределенных задач требуются и фактически применяются запутанные состояния.

   a. Запутанные состояния можно создавать заранее и хранить или буферизовать.

   b. Скорость создания запутанности будет ограничивать производительность практических приложений Quantum Internet, включая распределенные квантовые расчёты, хотя запутанные состояния можно буферизовать.

   Например, в [Gottesman1999] и [Eisert] показано, что управляемые инверторы (Controlled NOT или CNOT) можно реализовать совместно на нескольких квантовых компьютерах и распределить между ними. Далее в этом параграфе рассматривается в основном этот тип распределенных квантовых вычислений.

В качестве варианта распределенных квантовых вычислений второго типа можно рассматривать зашумлённые квантовые компьютеры среднего масштаба (NISQ), размещённые в разных местах, доступных для обобществления. В соответствии с определением [Preskill] компьютер NISQ может реализовать лишь небольшое число кубитов и имеет ограниченные возможности корректировки квантовых ошибок. Этот вариант называют распределёнными квантовыми расчётами [Caleffi] [Cacciapuoti2020] [Cacciapuoti2019]. Он отражает значительный рост вычислительной мощности, которые квантовые компьютеры могут обеспечить в составе Quantum Internet по сравнению с классическими компьютерами Classical Internet в контексте экосистемы распределенных квантовых вычислений [Cuomo]. Согласно [Cuomo], квантовая телепортация позволяет применять новую парадигму связи, называемую «теледанными» (teledata) [VanMeter2006-01], где квантовые состояния переносятся между кубитами разнесённых квантовых компьютеров. Для распределенных квантовых расчётов требуется возможность удалённо выполнять квантовые вычисления на кубитах распределённых квантовых компьютеров, например, методом «телевентилей» (telegate) [VanMeter2006-02].

Например, пользователь может применить соединённые компьютеры NISQ для выполнения сложных научных расчётов, таких как анализ химических взаимодействий для разработки медицинских препаратов [Cao] (см. рисунок 3). В этом случае кубиты передаются между квантовыми компьютерами по квантовым каналам, а запросы пользователя для координации и управления - по классическим. Другим примером являются многосторонние защищённые квантовые расчёты (Multi-Party Quantum Computation или MPQC) [Crepeau], которые можно считать квантовым вариантом классических многосторонних защищённых расчётов (Multi-Party Computation или MPC). В защищённом протоколе MPQC множество участников совместно выполняют квантовые расчёты с набором входных квантовых состояний,

подготавливаемых и предоставляемых разными участниками. Одной из целей защищённого MPQC является гарантия того, что ни один из участников не будет знать квантовых состояний, предоставленных другими. Защищённые расчёты MPQC полагаются на верифицированный квантовый обмен секретами [Lipinska].

В примере на рисунке 3 нужно перенести кубиты с одного компьютера NISQ на другой. Для этого можно применить квантовую телепортацию для переноса с квантового компьютера (A) на квантовый компьютер (B). Отметим, что на рисунке 3 не рассматриваются распределенный квантовый расчёт на основе измерений, где телепортация может не требоваться. При реализации квантовой телепортации между узлами A и B выполняются указанные ниже действия. Фактически на обоих компьютерах выполняются операции LOCC [Chitambar] для выполнения квантовой телепортации.

1. Квантовый компьютер A генерирует некие кубиты конфиденциальных данных для телепортирования в B.
2. Организуется общая запутанность A и B (т. е. имеется два запутанных кубита - q1 на A и q2 на B). Например, квантовый компьютер A может создать два запутанных кубита (q1 и q2) и передать q2 квантовому компьютеру B, используя квантовую связь.
3. Компьютер A выполняет измерение Белла для запутанного кубита q1 и кубита конфиденциальных данных.
4. Результат измерения Белла кодируется в 2 классических бита, которые передаются по классическому каналу квантовому компьютеру B.
5. На основе полученных 2 классических битов компьютер B меняет состояние запутанного кубита q2, чтобы создать кубит, идентичный кубиту конфиденциальных данных в компьютере A.

На рисунке Quantum Internet включает квантовые каналы и квантовые повторители и/или маршрутизаторы [RFC9340]. Этот вариант приложения должен поддерживать создание и распространение запутанности (или квантовое соединение) [QUANTUM-CONNECTION] для выполнения квантовой телепортации.

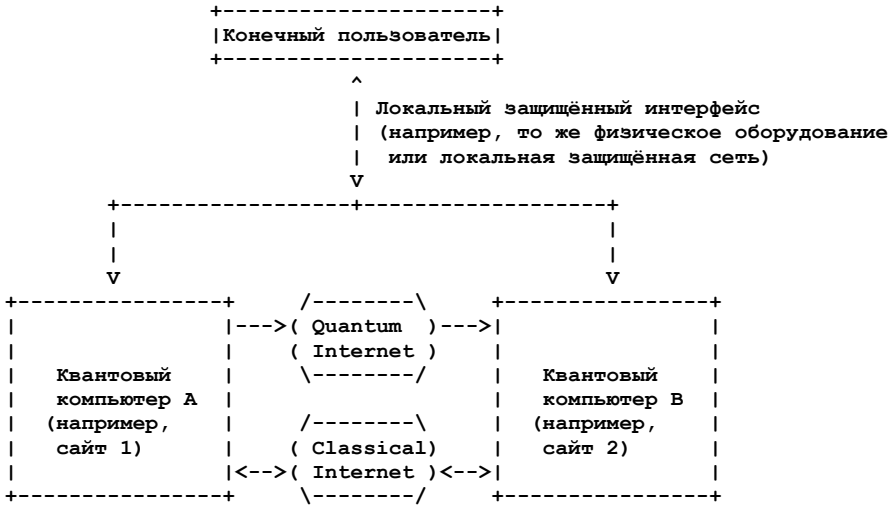

Рисунок 3. Распределённые квантовые вычисления.

5. Общие требования

Квантовые технологии постоянно развиваются и совершенствуются, поэтому сложно предсказать сроки и этапы будущего квантовых технологий, как отмечено в [Grumbling]. В настоящее время компьютер NISQ может поддерживать от 50 до нескольких сотен кубитов с определённой долей ошибок.

В работе [Wehner] описаны 6 этапов развития Quantum Internet на сетевом уровне.

1. Сети доверенных повторителей (Этап 1).
2. Сети с подготовкой и измерением (Этап 2).
3. Сети распределения запутанности (Этап 3).
4. Сети квантовой памяти (Этап 4).
5. Устойчивые к отказам сети из нескольких кубитов (Этап 5).
6. Сети квантовых вычислений (Этап 6).

Первый этап - это простые сети доверенных повторителей, а на последнем возникают сети квантовых вычислений, образующие Quantum Internet. Каждый промежуточный этап добавляет функции, приложения и характеристики. В таблице 1 показаны сценарии применения Quantum Internet, описанные в разделах 3 и 4, с отображением на этапы Quantum Internet из [Wehner]. Например, организация защищённой связи может поддерживаться на этапе 1, 2 или 3, но с применением разных решений QKD.

- На этапе 1 возможны базовые решения QKD для поддержки организации защищённой связи, но для сквозной защиты нужны доверенные узлы. Их наличие является основным требованием.
- На этапе 2 конечные пользователи могут подготавливать и измерять кубиты. Доступна проверка классических паролей без их раскрытия.
- На этапе 3 может обеспечиваться сквозная защита на основе квантовых повторителей и распределения запутанности для поддержки одного и того же приложения организации защищённой связи. Основным требованием является распространение запутанности для использования QKD на длинных дистанциях.
- На этапе 4 квантовые повторители получат возможность хранения кубитов и манипуляций ими в квантовой памяти. В этих квантовых сетях можно выполнять расчёты вслепую, выбор лидера, обобществление секретов.

- На этапе 5 квантовые повторители смогут исправлять ошибки, что позволит выполнять отказоустойчивые квантовые расчёты по полученным данным. Эти повторители позволят выполнять распределенные квантовые расчёты и приложения с квантовыми датчиками на небольшом числе кубитов.

- На этапе 6 станут возможны распределенные между большим числом кубитов квантовые расчёты.

Таблица 1. Примеры приложений на разных этапах Quantum Internet.

Этап	***Примеры приложений Quantum Internet***	***Характеристики***
1	Организация защищённой связи с базовыми QKD	Доверенные узлы
2	Организация сквозной защиты связи с применением QKD	Подготовка и измерение
3	Организация защищённой связи с применением QKD с запутанностью	Распространение запутанности
4	Квантовые вычисления вслепую	Квантовая память
5	Высокоточная синхронизация часов	Отказоустойчивость
6	Распределенные квантовые вычисления	Множество кубитов

Некоторые общие и функциональные требования к Quantum Internet с точки зрения сетей, основанные на указанных выше вариантах применения и планах развития технологий Quantum Internet [Wehner] кратко описаны в последующих параграфах.

5.1. Операции на запутанных кубитах

Требуются методы, позволяющие квантовым приложениям эффективно взаимодействовать с запутанными кубитами, чтобы можно было инициировать распространение выбранных запутанных кубитов потенциально любому квантовому узлу Quantum Internet. Для этого нужно выполнить на запутанных кубитах определённые операции (например, обмен запутанностью или её очистка). Квантовые узлы могут быть конечными узлами, повторителями, маршрутизаторами, квантовыми компьютерами.

5.2. Распределение запутанности

Квантовым повторителям и маршрутизаторам следует поддерживать отказоустойчивое и эффективное распределение запутанности для организации и расширения высокоточной связи между двумя квантовыми узлами. Для этого нужно сначала создать запутанную пару на каждом этапе (hop) пути между двумя узлами, а затем выполнить обмен запутанностью на каждом из промежуточных узлов.

5.3. Необходимость классических каналов

Квантовые конечные узлы должны передавать дополнительную информацию по классическим каналам, чтобы помочь в передаче и распознании кубитов через квантовые повторители и/или маршрутизаторы. Примеры такой дополнительной информации включают измерения кубитов при организации защищённой связи (параграф 4.1) и измерения Белла в распределенных квантовых вычислениях (параграф 4.3). Кроме того, кубиты передаются индивидуально и с ними не связано заголовков пакетов, которые могли бы помочь при передаче. Любые сведения, способствующие маршрутизации, идентификации кубитов и т. п., должны передаваться по классическим каналам.

5.4. Управление Quantum Internet

Для Quantum Internet нужны методы управления и контроля на уровне квантовых узлов и их квантовых ресурсов. Ресурсы квантового узла могут включать квантовую память, квантовые каналы, кубиты, организованные квантовые соединения и т. п. Методы управления могут применяться для отслеживания состояния Quantum Internet, диагностики и обнаружения возможных проблем (например, в квантовых соединениях), а также настройки на квантовых узлах новых действий и/или правил (например, новых операций обмена запутанностью). Может потребоваться разработка новой информационной модели для Quantum Internet.

6. Заключение

В этом документе приведён обзор некоторых ожидаемых категорий приложений Quantum Internet, а также описаны детали некоторых вариантов применения. Приложения сгруппированы по их использованию для упрощения понимания схемы классификации. Набор приложений, разумеется, может расширяться по мере развития Quantum Internet. Приведены также некоторые базовые требования к Quantum Internet.

Документ может служить введением для читателей, заинтересованных в изучении практического применения Quantum Internet. Авторы надеются, что документ поможет направить дальнейшие исследования и разработки функциональности Quantum Internet, требуемой для реализации описанных здесь вариантов применения.

7. Взаимодействие с IANA

Этот документ не требует действия IANA.

8. Вопросы безопасности

Этот документ не задаёт архитектуру или конкретные протоколы для Quantum Internet и посвящён лишь вариантам применения, требованиям и описанию типичных приложений Quantum Internet. Тем не менее можно сделать несколько важных замечаний в части безопасности Quantum Internet.

В [NISTIR8240] отмечено, что реализация крупномасштабных квантовых вычислений позволит взломать множество систем с открытым ключом (асимметричных), используемых сегодня. Это связано с ростом вычислительных возможностей квантовых компьютеров для некоторых классов задач (например, факторизации и оптимизации простых чисел). Это негативно повлияет на многие механизмы защиты, применяемые в Classical Internet и основанные на шифровании с открытым ключом (Diffie-Hellman (DH)). Это стало мощным стимулом для разработки новых криптографических систем, устойчивых в атакам с использованием квантовых вычислений [NISTIR8240]. Развитие Quantum смягчит угрозы, вносимые атаками на криптосистемы на основе открытых ключей DH. В частности, организация защищённых коммуникаций Quantum (параграф 4.1) будет устойчива к квантовым и классическим атакам на криптосистемы с открытыми ключами Diffie-Hellman.

В [RFC7258] рассмотрена важная для Quantum Internet угроза и отмечена опасность внедрения повсеместного мониторинга как широкой атаки на приватность. Повсеместный мониторинг определён как широко распространённое и обычно скрытое наблюдение путём сбора содержимого приложений или метаданных протокола, таких как заголовки. Это может быть реализовано путём пассивного или активного прослушивания, анализа трафика или подмены криптографических ключей, применяемых для защиты коммуникаций.

Организация защищённой связи в Quantum Internet (параграф 4.1) устойчива к повсеместному мониторингу, основанному на прямых атаках на ключи шифрования (Diffie-Hellman). Кроме того, в параграфе 4.2 описан метод распределенных квантовых расчётов с сохранением приватности исходных данных. Присущее кубитам свойство распада при наблюдении (даже скрытном) теоретически позволит обнаружить нежелательное наблюдение в некоторых будущих решениях.

Современные сети основаны на принципах отсутствия доверия (zero trust), где классическая криптография служит для защиты конфиденциальности и целостности, а также для аутентификации на разных логических уровнях сетевого стека, зачастую на всем пути от устройства до программ в облаке [NISTSP800-207]. Используемые сегодня криптографические решения основаны на хорошо известных примитивах, заведомо безопасных протоколах и современных реализациях, защищённых от множества атак через побочные каналы.

В отличие от традиционной и постквантовой криптографии (Post-Quantum Cryptography или PQC), защита QKD неотъемлемо связана с физическим уровнем, что делает фронты атаки на QKD и традиционную криптографию совершенно разными. Реализации QKD уже подвергались известным атакам [Zhao2008] и Агентство национальной безопасности (National Security Agency или NSA) США отмечает, что профиль рисков традиционной криптографии известен лучше [NSA]. Реализация традиционной криптографии и PQC на более высоких уровнях, чем физический, означает, что PQC можно использовать для передачи защищённой информации через недоверенные ретрансляторы. Это контрастирует с QKD, где основой является сквозная защита путём передачи через доверенные промежуточные узлы. PQC лучше подходит для современных технологий, где все больше приложение переходит к принципам сквозной защиты и отсутствия доверия. Важно отметить, что PQC можно внедрить путём обновления программ, а для QKD требуется новое оборудование. В IETF имеется рабочая группа по использованию постквантовой криптографии в протоколах (Post-Quantum Use In Protocols или PQUIP), изучающая вопросы перехода на PQC.

В плане реализации QKD АНБ (NSA) утверждает, что в QKD требования к защите и связи имеют физические противоречия, а инженерные решения для их балансировки крайне неустойчивы к ошибкам. Традиционная криптография может быть реализована аппаратно для повышения производительности или по иным причинам, а QKD по своей природе является аппаратным решением. АНБ отмечает, что это делает подход QKD менее гибким в части обновления или защитных исправлений. Поскольку QKD является протоколом «точка-точка» (point-to-point), АНБ также отмечает, что сети QKD часто требуют использования доверенных ретрансляторов, что повышает риск, связанный с внутренними угрозами.

Национальный центр кибербезопасности Великобритании (UK National Cyber Security Centre) предостерегает от применения QKD, особенно в критически важных секторах национальной инфраструктуры, и предлагает использовать криптографию PQC, стандартизованную NIST, как лучшее решение [NCSC]. Национальное агентство кибербезопасности Франции (National Cybersecurity Agency of France) считает возможным применять QKD в качестве средства глубокой защиты, дополняющего традиционную криптографию, если связанные с этим затраты не окажут негативного влияния на защиту от текущих угроз инфраструктуре систем IT [ANNSI].

9. Литература

[ANNSI] French Cybersecurity Agency (ANSSI), "Should Quantum Key Distribution be Used for Secure Communications?", May 2020, <https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/>.

[BB84] Bennett, C. H. and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", DOI 10.1016/j.tcs.2014.05.025, December 2014, <https://doi.org/10.1016/j.tcs.2014.05.025>.

[BBM92] Bennett, C. H., Brassard, G., and N. D. Mermin, "Quantum cryptography without Bell's theorem", Physical Review Letters, American Physical Society, DOI 10.1103/PhysRevLett.68.557, February 1992, <https://link.aps.org/doi/10.1103/PhysRevLett.68.557>.

[Ben-Or] Ben-Or, M. and A. Hassidim, "Fast quantum byzantine agreement", STOC '05, Association for Computing Machinery, DOI 10.1145/1060590.1060662, May 2005, <https://dl.acm.org/doi/10.1145/1060590.1060662>.

[Broadbent] Broadbent, A., Fitzsimons, J., and E. Kashefi, "Universal Blind Quantum Computation", 50th Annual IEEE Symposium on Foundations of Computer Science, IEEE, DOI 10.1109/FOCS.2009.36, December 2009, <https://arxiv.org/pdf/0807.4154.pdf>.

[Cacciapuoti2019] Cacciapuoti, A. S., Caleffi, M., Van Meter, R., and L. Hanzo, "When Entanglement meets Classical Communications: Quantum Teleportation for the Quantum Internet (Invited Paper)", DOI 10.48550/arXiv.1907.06197, July 2019, <https://arxiv.org/abs/1907.06197>.

[Cacciapuoti2020] Cacciapuoti, A. S., Caleffi, M., Tafuri, F., Cataliotti, F. S., Gherardini, S., and G. Bianchi, "Quantum Internet: Networking Challenges in Distributed Quantum Computing", IEEE Network, DOI 10.1109/MNET.001.1900092, February 2020, <https://ieeexplore.ieee.org/document/8910635>.

[Caleffi] Caleffi, M., Cacciapuoti, A. S., and G. Bianchi, "Quantum internet: from communication to distributed computing!", NANOCOM '18, Association for Computing Machinery, DOI 10.1145/3233188.3233224, September 2018, <https://dl.acm.org/doi/10.1145/3233188.3233224>.

[Cao] Cao, Y., Romero, J., and A. Aspuru-Guzik, "Potential of quantum computing for drug discovery", IBM Journal of Research and Development, DOI 10.1147/JRD.2018.2888987, December 2018, <https://doi.org/10.1147/JRD.2018.2888987>.

[Castelvecchi] Castelvecchi, D., "The quantum internet has arrived (and it hasn't)", Nature 554, 289-292, DOI 10.1038/d41586-018-01835-3, February 2018, <https://www.nature.com/articles/d41586-018-01835-3>.

[Childs] Childs, A. M., "Secure assisted quantum computation", DOI 10.26421/QIC5.6, July 2005, <https://arxiv.org/pdf/quant-ph/0111046.pdf>.

[Chitambar] Chitambar, E., Leung, D., Mančinska, L., Ozols, M., and A. Winter, "Everything You Always Wanted to Know About LOCC (But Were Afraid to Ask)", Communications in Mathematical Physics, Springer, DOI 10.1007/s00220-014-1953-9, March 2014, <https://link.springer.com/article/10.1007/s00220-014-1953-9>.

[Crepeau] Crépeau, C., Gottesman, D., and A. Smith, "Secure multi-party quantum computation", STOC '02, Association for Computing Machinery, DOI 10.1145/509907.510000, May 2002, <https://doi.org/10.1145/509907.510000>.

[Cuomo] Cuomo, D., Caleffi, M., and A. S. Cacciapuoti, "Towards a distributed quantum computing ecosystem", IET Quantum Communication, DOI 10.1049/iet-qtc.2020.0002, July 2020, <http://dx.doi.org/10.1049/iet-qtc.2020.0002>.

[Denchev] Denchev, V. S. and G. Pandurangan, "Distributed quantum computing: a new frontier in distributed systems or science fiction?", ACM SIGACT News, DOI 10.1145/1412700.1412718, September 2008, <https://doi.org/10.1145/1412700.1412718>.

[E91] Ekert, A. K., "Quantum cryptography based on Bell's theorem", Physical Review Letters, American Physical Society, DOI 10.1103/PhysRevLett.67.661, August 1991, <https://link.aps.org/doi/10.1103/PhysRevLett.67.661>.

[Eisert] Eisert, J., Jacobs, K., Papadopoulos, P., and M. B. Plenio, "Optimal local implementation of nonlocal quantum gates", Physical Review A, American Physical Society, DOI 10.1103/PhysRevA.62.052317, October 2000, <https://doi.org/10.1103/PhysRevA.62.052317>.

[Elkouss] Elkouss, D., Martinez-Mateo, J., and V. Martin, "Information Reconciliation for Quantum Key Distribution", DOI 10.48550/arXiv.1007.1616, April 2011, <https://arxiv.org/pdf/1007.1616.pdf>.

[ETSI-QKD-Interfaces] ETSI, "Quantum Key Distribution (QKD); Components and Internal Interfaces", V2.1.1, ETSI GR QKD 003, March 2018, <https://www.etsi.org/deliver/etsi_gr/QKD/001_099/003/02.01.01_60/gr_QKD003v020101p.pdf>.

[ETSI-QKD-UseCases] ETSI, "Quantum Key Distribution; Use Cases", V1.1.1, ETSI GS QKD 002, June 2010, <https://www.etsi.org/deliver/etsi_gs/qkd/001_099/002/01.01.01_60/gs_qkd002v010101p.pdf>.

[Fitzsimons] Fitzsimons, J. F., "Private quantum computation: an introduction to blind quantum computing and related protocols", DOI 10.1038/s41534-017-0025-3, June 2017, <https://www.nature.com/articles/s41534-017-0025-3.pdf>.

[Gottesman1999] Gottesman, D. and I. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations", Nature 402, 390-393, DOI 10.1038/46503, November 1999, <https://doi.org/10.1038/46503>.

[Gottesman2012] Gottesman, D., Jennewein, T., and S. Croke, "Longer-Baseline Telescopes Using Quantum Repeaters", Physical Review Letters, American Physical Society, DOI 10.1103/PhysRevLett.109.070503, August 2012, <https://link.aps.org/doi/10.1103/PhysRevLett.109.070503>.

[Grosshans] Grosshans, F. and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States", Physical Review Letters, American Physical Society, DOI 10.1103/PhysRevLett.88.057902, January 2002, <https://doi.org/10.1103/PhysRevLett.88.057902>.

[Grumbling] Grumbling, E., Ed. and M. Horowitz, Ed., "Quantum Computing: Progress and Prospects", National Academies of Sciences, Engineering, and Medicine, The National Academies Press, DOI 10.17226/25196, 2019, <https://doi.org/10.17226/25196>.

[Guo] Guo, X., Breum, C. R., Borregaard, J., Izumi, S., Larsen, M. V., Gehring, T., Christandl, M., Neergaard-Nielsen, J. S., and U. L. Andersen, "Distributed quantum sensing in a continuous-variable entangled network", Nature Physics, DOI 10.1038/s41567-019-0743-x, December 20219, <https://www.nature.com/articles/s41567-019-0743-x>.

[Huang] Huang, H-L., Zhao, Q., Ma, X., Liu, C., Su, Z-E., Wang, X-L., Li, L., Liu, N-L., Sanders, B. C., Lu, C-Y., and J-W. Pan, "Experimental Blind Quantum Computing for a Classical Client", DOI 10.48550/arXiv.1707.00400, July 2017, <https://arxiv.org/pdf/1707.00400.pdf>.

[ITUT] ITU-T, "Draft new Technical Report ITU-T TR.QN-UC: 'Use cases of quantum networks beyond QKDN'", ITU-T SG 13, November 2022, <https://www.itu.int/md/T22-SG13-221125-TD-WP3-0158/en>.

[Jozsa2000] Josza, R., Abrams, D. S., Dowling, J. P., and C. P. Williams, "Quantum Clock Synchronization Based on Shared Prior Entanglement", Physical Review Letters, American Physical Society, DOI 10.1103/PhysRevLett.85.2010, August 2000, <https://link.aps.org/doi/10.1103/PhysRevLett.85.2010>.

[Jozsa2005] Josza, R., "An introduction to measurement based quantum computation", DOI 10.48550/arXiv.quant-ph/0508124, September 2005, <https://arxiv.org/pdf/quant-ph/0508124.pdf>.

[Kiktenko] Kiktenko, E. O., Malyshev, A. O., Gavreev, M. A., Bozhedarov, A. A., Pozhar, N. O., Anufriev, M. N., and A. K. Fedorov, "Lightweight authentication for quantum key distribution", DOI 10.1109/TIT.2020.2989459, September 2020, <https://arxiv.org/pdf/1903.10237.pdf>.

[Komar] Kómár, P., Kessler, E. M., Bishof, M., Jiang, L., Sørensen, A. S., Ye, J., and M. D. Lukin, "A quantum network of clocks", DOI 10.1038/nphys3000, October 2013, <https://arxiv.org/pdf/1310.6045.pdf>.

[Lipinska] Lipinska, V., Murta, G., Ribeiro, J., and S. Wehner, "Verifiable hybrid secret sharing with few qubits", Physical Review A, American Physical Society, DOI 10.1103/PhysRevA.101.032332, March 2020, <https://doi.org/10.1103/PhysRevA.101.032332>.

[Lo] Lo, H-K., Curty, M., and B. Qi, "Measurement-Device-Independent Quantum Key Distribution", Physical Review Letters, American Physical Society, DOI 10.1103/PhysRevLett.108.130503, March 2012, <https://doi.org/10.1103/PhysRevLett.108.130503>.

[NCSC] National Cyber Security Centre (NCSC), "Quantum security technologies", Whitepaper, March 2020, <https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies>.

[NISTIR8240] Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., and D. Smith-Tone, "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process", DOI 10.6028/NIST.IR.8240, NISTIR 8240, January 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8240.pdf>.

[NISTSP800-207] Rose, S., Borchert, O., Mitchell, S., and S. Connelly, "Zero Trust Architecture", NIST SP 800-207, DOI 10.6028/NIST.SP.800-207, August 2020, <https://doi.org/10.6028/NIST.SP.800-207>.

[NSA] National Security Agency (NSA), "Post-Quantum Cybersecurity Resources", <https://www.nsa.gov/Cybersecurity/Post-Quantum-Cybersecurity-Resources/>.

[Pal] Pal, S. P., Singh, S. K., and S. Kumar, "Multi-partite Quantum Entanglement versus Randomization: Fair and Unbiased Leader Election in Networks", DOI 10.48550/arXiv.quant-ph/0306195, June 2003, <https://arxiv.org/pdf/quant-ph/0306195.pdf>.

[Preskill] Preskill, J., "Quantum Computing in the NISQ era and beyond", DOI 10.22331/q-2018-08-06-79, July 2018, <https://arxiv.org/pdf/1801.00862>.

[Proctor] Proctor, T. J., Knott, P. A., and J. A. Dunningham, "Multiparameter Estimation in Networked Quantum Sensors", Physical Review Letters, American Physical Society, DOI 10.1103/PhysRevLett.120.080501, February 2018, <https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.080501>.

[Qin] Qin, H., "Towards large-scale quantum key distribution network and its applications", June 2019, <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Hao_Qin_Presentation.pdf>.

[QUANTUM-CONNECTION] Van Meter, R. and T. Matsuo, "Connection Setup in a Quantum Network", Work in Progress, Internet-Draft, draft-van-meter-qirg-quantum-connection-setup-01, 11 September 2019, <https://datatracker.ietf.org/doc/html/draft-van-meter-qirg-quantum-connection-setup-01>.

[Renner] Renner, R., "Security of Quantum Key Distribution", DOI 10.48550/arXiv.quant-ph/0512258, September 2005, <https://arxiv.org/pdf/quant-ph/0512258.pdf>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC9340] Kozlowski, W., Wehner, S., Van Meter, R., Rijsman, B., Cacciapuoti, A. S., Caleffi, M., and S. Nagayama, "Architectural Principles for a Quantum Internet", RFC 9340, DOI 10.17487/RFC9340, March 2023, <https://www.rfc-editor.org/info/rfc9340>.

[Taherkhani] Taherkhani, M. A., Navi, K., and R. Van Meter, "Resource-aware System Architecture Model for Implementation of Quantum aided Byzantine Agreement on Quantum Repeater Networks", DOI 10.1088/2058-9565/aa9bb1, January 2017, <https://arxiv.org/abs/1701.04588>.

[Tang] Tang, B-Y., Liu, B., Zhai, Y-P., Wu, C-Q., and W-R. Yu, "High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution", Scientific Reports, DOI 10.1038/s41598-019-50290-1, October 2019, <https://doi.org/10.1038/s41598-019-50290-1>.

[Treiber] Treiber, A., Poppe, A., Hentschel, M., Ferrini, D., Lorünser, T., Querasser, E., Matyus, T., Hübel, H., and A. Zeilinger, "A fully automated entanglement-based quantum cryptography system for telecom fiber networks", New Journal of Physics 11 045013, DOI 10.1088/1367-2630/11/4/045013, April 2009, <https://iopscience.iop.org/article/10.1088/1367-2630/11/4/045013>.

[VanMeter2006-01] Van Meter, R., Nemoto, K., Munro, W. J., and K. M. Itoh, "Distributed Arithmetic on a Quantum Multicomputer", 33rd International Symposium on Computer Architecture (ISCA '06), DOI 10.1109/ISCA.2006.19, June 2006, <https://doi.org/10.1109/ISCA.2006.19>.

[VanMeter2006-02] Van Meter, R. D., "Architecture of a Quantum Multicomputer Optimized for Shor's Factoring Algorithm", DOI 10.48550/arXiv.quant-ph/0607065, February 2008, <https://arxiv.org/pdf/quant-ph/0607065.pdf>.

[Wehner] Wehner, S., Elkouss, D., and R. Hanson, "Quantum internet: A vision for the road ahead", Science 362, DOI 10.1126/science.aam9288, October 2018, <http://science.sciencemag.org/content/362/6412/eaam9288.full>.

[Xu] Xu, F., Qi, B., and H-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system", New Journal of Physics 12 113026, DOI 10.1088/1367-2630/12/11/113026, November 2010, <https://iopscience.iop.org/article/10.1088/1367-2630/12/11/113026>.

[Zhandry] Zhandry, M., "Quantum Lightning Never Strikes the Same State Twice", Advances in Cryptology - EUROCRYPT 2019, DOI 10.1007/978-3-030-17659-4_14, April 2019, <http://doi.org/10.1007/978-3-030-17659-4_14>.

[Zhang2009] Zhang, X., Luo, W., Zeng, G., Weng, J., Yang, Y., Chen, M., and X. Tan, "A hybrid universal blind quantum computation", DOI 10.1016/j.ins.2019.05.057, September 2019, <https://www.sciencedirect.com/science/article/abs/pii/S002002551930458X>.

[Zhang2018] Zhang, Q., Xu, F., Chen, Y-A., Peng, C-Z., and J-W. Pan, "Large scale quantum key distribution: challenges and solutions [Invited]", Optics Express, DOI 10.1364/OE.26.024260, August 2018, <https://doi.org/10.1364/OE.26.024260>.

[Zhao2008] Zhao, Y., Fred Fung, C-H., Qi, B., Chen, C., and H-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems", Physical Review A, American Physical Society, DOI 10.1103/PhysRevA.78.042333, October 2008, <https://link.aps.org/doi/10.1103/PhysRevA.78.042333>.

[Zhao2018] Zhao, Y., "Development of Quantum Key Distribution and Attacks against It", Journal of Physics: Conference Series, DOI 10.1088/1742-6596/1087/4/042028, 2018, <https://iopscience.iop.org/article/10.1088/1742-6596/1087/4/042028>.

[Zheng2019] Zheng, X., Zhang, P., Ge, R., Lu, L., He, G., Chen, Q., Qu, F., Zhang, L., Cai, X., Lu, Y., Zhu, S., Wu, P., and X-S. Ma, "Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution", DOI 10.1117/1.AP.3.5.055002, December 2019, <https://arxiv.org/abs/1912.09642>.

Благодарности

Авторы благодарны Michele Amoretti, Mathias Van Den Bossche, Xavier de Foy, Patrick Gelard, Álvaro Gómez Iñesta, Mallory Knodel, Wojciech Kozlowski, John Preuß Mattsson, Rodney Van Meter, Colin Perkins, Joey Salazar, Joseph Touch, Brian Trammell и сообществу QIRG в целом за полезные рецензии и комментарии к документу.

Адреса авторов

Chonggang Wang
InterDigital Communications, LLC
1001 E Hector St
Conshohocken, PA 19428
United States of America
Email: Chonggang.Wang@InterDigital.com

Akbar Rahman
Ericsson
349 Terry Fox Drive
Ottawa Ontario K2K 2V6
Canada
Email: Akbar.Rahman@Ericsson.Com

Ruidong Li
Kanazawa University
Kakumamachi, Kanazawa, Ishikawa
920-1192
Japan
Email: lrd@se.kanazawa-u.ac.jp

Melchior Aelmans
Juniper Networks
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Netherlands
Email: maelmans@juniper.net

Kaushik Chakraborty
The University of Edinburgh
10 Crichton Street
Edinburgh, Scotland
EH8 9AB
United Kingdom
Email: kaushik.chakraborty9@gmail.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru