НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

УДК-621.39

КВАНТОВЫЕ КОММУНИКАЦИИ И ИХ ПЕРСПЕКТИВЫ

Григорьев Тимур Русланович
Аспирант кафедры квантовых технологий и телекоммуникационных систем, Московский физико-технический институт
г. Долгопрудный, Россия

Аннотация

В настоящей масштабной фундаментальной исследовательской работе осуществляется развернутый, детальный, глубокий и многоаспектный научно-теоретический анализ физических принципов, протоколов передачи информации, аппаратурной реализации, сетевой архитектуры и перспектив развития квантовых коммуникационных систем в современной информационной инфраструктуре. В центре внимания находится исследование квантовой суперпозиции и квантовой запутанности фотонных и твердотельных состояний, фундаментальных ограничений на копирование и измерение квантовых состояний, а также протоколов квантового распределения ключей и квантовой телепортации. В статье подробно рассматриваются вопросы генерации одиночных и запутанных фотонов, распространения квантовых сигналов по волоконно-оптическим линиям связи и открытым атмосферным и спутниковым каналам, функционирования квантовых повторителей и квантовой памяти, а также задачи интеграции квантовых каналов с классическими сетями и постквантовой криптографией. На основе междисциплинарного синтеза квантовой механики, квантовой оптики, теории информации, фотоники и сетевых технологий формулируются концептуальные направления развития защищенных квантовых сетей нового поколения.

Ключевые слова: квантовые коммуникации, квантовое распределение ключей, квантовая запутанность, квантовая телепортация, квантовый повторитель, квантовая память, фотоника, волоконно-оптические линии, защищенная связь, квантовые сети.

Введение: фундаментальные основы и значение квантовых коммуникаций

Современная цифровая цивилизация опирается на распределенные телекоммуникационные сети, обеспечивающие передачу, хранение и обработку критически важных массивов информации в государственном управлении, финансовом секторе, энергетике, промышленности, медицине и научных исследованиях. По мере роста вычислительных мощностей, распространения облачных вычислений и появления перспективных квантовых алгоритмов

возрастают требования к информационной безопасности, целостности и конфиденциальности передаваемых данных. Традиционные криптографические схемы с открытым ключом во многом базируются на вычислительной сложности отдельных математических задач, таких как факторизация крупных целых чисел или дискретное логарифмирование, что делает их потенциально уязвимыми перед появлением достаточно мощных отказоустойчивых квантовых компьютеров и совершенствованием криптоаналитических алгоритмов.

Квантовые коммуникации предлагают принципиально иной подход к защите и передаче информации, опирающийся не на вычислительные предположения, а на фундаментальные законы квантовой механики. В квантовых системах носителями информации выступают квантовые состояния физических объектов — чаще всего поляризационные, фазовые, временные или пространственно-модовые состояния одиночных фотонов, а также спиновые или электронные состояния твердотельных и атомных систем. Согласно принципу неопределенности и теореме о запрете клонирования, произвольное неизвестное квантовое состояние невозможно точно скопировать, а любое вмешательство третьей стороны, пытающейся измерить передаваемое состояние, неизбежно вносит возмущения и искажения, которые могут быть обнаружены легитимными участниками связи.

Целью данного исследования является систематический научно-теоретический анализ физических и инженерных основ квантовых коммуникаций, сопоставление ключевых протоколов и аппаратных платформ, рассмотрение ограничений, связанных с декогеренцией и потерями в каналах связи, а также оценка перспектив масштабирования квантовых сетей и их интеграции в современную телекоммуникационную среду.

Физические носители информации и базовые квантовые протоколы

В практических системах квантовой связи основным носителем квантовой информации являются фотоны благодаря их высокой скорости распространения, слабому взаимодействию с окружающей средой по сравнению с массивными частицами и совместимости с существующей оптической инфраструктурой. Для кодирования кубитов используются различные степени свободы фотонного поля: линейная или круговая поляризация, разность фаз между временными или пространственными модами, орбитальный угловой момент или частотно-временные параметры. Выбор способа кодирования определяется требованиями к устойчивости состояния при прохождении через оптические элементы и каналы связи, а также возможностями источников и детекторов одиночных фотонов.

Наиболее зрелым и широко внедряемым направлением квантовых коммуникаций является квантовое распределение ключей, позволяющее двум удаленным сторонам сформировать общую случайную криптографическую последовательность и гарантированно выявить присутствие перехватчика на квантовом канале. В протоколах приготовления и измерения состояния, таких как протоколы с использованием четырех или шести состояний, отправитель

подготавливает фотоны в одном из неортогональных базисов, а получатель выполняет измерения в случайно выбранном базисе, после чего стороны по открытому классическому каналу проводят просеивание результатов, оценку уровня квантовых ошибок, коррекцию ошибок и усиление секретности. Дополнительно развиваются протоколы на основе квантовой запутанности, в которых коррелированные пары запутанных фотонов распределяются между участниками, а безопасность обеспечивается проверкой статистических неравенств, нарушаемых квантовыми корреляциями.

Важным направлением фундаментальных и прикладных квантовых коммуникаций выступает квантовая телепортация — процесс передачи неизвестного квантового состояния от одной квантовой системы к другой на расстояние с использованием предварительно разделенной пары запутанных частиц и передачи классической информации по обычному каналу связи. При этом сама материальная частица-носитель не перемещается в пространстве, а исходное состояние на передающей стороне разрушается в ходе совместного измерения, что согласуется с законами квантовой механики и специальной теории относительности, поскольку передача классических битов ограничивается скоростью света. Квантовая телепортация рассматривается не только как средство передачи квантовых состояний между узлами, но и как базовый механизм для построения распределенных квантовых вычислений и объединения квантовых процессоров в единую вычислительную архитектуру.

Каналы передачи, потери сигнала и квантовые повторители

Практическое распространение квантовых сигналов сопряжено с фундаментальными ограничениями, связанными с затуханием оптического сигнала в среде и потерей квантовой когерентности. В волоконно-оптических линиях связи основным фактором потерь является рэлеевское рассеяние и поглощение в кварцевом стекле, причем минимальное затухание достигается в телекоммуникационных диапазонах длин волн вблизи полутора микрометров. Поскольку квантовые сигналы представляют собой слабые оптические импульсы на уровне одиночных фотонов или средних чисел фотонов много меньше единицы, их невозможно усиливать обычными оптическими усилителями без внесения шумов, разрушающих квантовую информацию, а экспоненциальный рост потерь с увеличением длины волокна ограничивает дальность прямой передачи без промежуточных узлов.

Для преодоления ограничений по дальности в наземных и глобальных сетях разрабатываются квантовые повторители, основанные на сочетании разделения запутанности, обмена запутанностью и квантовой памяти. В таких архитектурах протяженный канал разбивается на более короткие сегменты, между узлами которых устанавливается квантовая запутанность, а затем с помощью операций совместных измерений запутанность расширяется на большие расстояния. Ключевым элементом квантового повторителя выступает квантовая память, способная принимать, сохранять в когерентном состоянии и по запросу считывать

фотонные кубиты на базе ансамблей холодных атомов, ионов, центров окраски в алмазе или редкоземельных ионов в кристаллах.

Наряду с волоконно-оптическими сетями активно развиваются каналы свободного пространства, включая атмосферные линии связи и спутниковые квантовые каналы. В атмосфере распространение фотонов сопровождается дифракционным расхождением пучка, поглощением и рассеянием на аэрозолях и облаках, а также турбулентными флуктуациями показателя преломления, приводящими к мерцанию интенсивности и искажению волнового фронта. Вывод источников запутанных фотонов или передающих модулей на низкие околоземные спутники позволяет значительно сократить толщину плотных слоев атмосферы на значительной части трассы и обеспечить межконтинентальную квантовую связь, хотя при этом возникают задачи точного наведения и слежения за движущимся космическим аппаратом, учета доплеровских сдвигов, фоновой засветки и ограниченности окон видимости.

Аппаратная реализация, метрология безопасности и интеграция с сетями

Эффективность квантовых коммуникационных систем во многом определяется характеристиками ключевых компонентов аппаратуры: источников одиночных и запутанных фотонов, модуляторов, систем компенсации поляризации и фазы, а также однофотонных детекторов. В практических системах квантового распределения ключей широко применяются ослабленные лазерные импульсы в сочетании с методами привязочных состояний, позволяющими противостоять атакам с разделением числа фотонов, а также развиваются детерминированные и полудетерминированные источники на базе квантовых точек, спонтанного параметрического рассеяния и четырехволнового смешения. Для регистрации слабых сигналов используются полупроводниковые лавинные фотодиоды в гейгеровском режиме и сверхпроводящие однофотонные детекторы на нанопроводах, сочетающие высокую квантовую эффективность, низкий уровень темновых отсчетов и малое мертвое время.

Важнейшим аспектом развития квантовых коммуникаций является устранение разрыва между теоретической стойкостью протоколов и реальными неидеальностями аппаратуры. В практических устройствах могут возникать побочные каналы утечки информации, неидеальность согласования состояний, асимметрия детекторов и уязвимости в классических модулях управления и обработки. Для повышения устойчивости к подобным дефектам разрабатываются измерительно-независимые протоколы и протоколы с двойной измерительной независимостью, позволяющие обеспечивать информационно-теоретическую безопасность даже при наличии неконтролируемых шумов и несовершенств в измерительных блоках.

Интеграция квантовых каналов в существующую телекоммуникационную инфраструктуру требует решения задач совместного распространения квантовых и классических оптических сигналов по одному волокну или по параллельным

каналам. Мощное классическое излучение способно создавать рамановское рассеяние и нелинейные шумы в спектральном диапазоне квантового сигнала, поэтому применяются методы спектральной фильтрации, временной и поляризационной селекции, а также выделения специальных полос частот и управления мощностью классических каналов. Кроме того, на сетевом уровне квантовые коммуникации рассматриваются в сочетании с постквантовой криптографией, где квантовые каналы обеспечивают защиту наиболее критичных соединений и генерацию ключей, а классические и постквантовые алгоритмы дополняют их в масштабируемых гетерогенных сетях.

Перспективы развития квантовых сетей и прикладные направления

В долгосрочной перспективе квантовые коммуникации эволюционируют от точечных систем квантового распределения ключей к многопользовательским квантовым сетям и перспективному квантовому интернету. Построение таких сетей предполагает создание маршрутизирующих и коммутирующих квантовых узлов, распределение многочастичной запутанности между различными абонентами, синхронизацию удаленных узлов и разработку сетевых протоколов управления, учитывающих необратимость измерений и конечное время жизни квантовых состояний в памяти.

Помимо защищенной передачи данных и распределения криптографических ключей, квантовые сети открывают возможности для распределенной квантовой сенсорики и метрологии, объединения удаленных квантовых процессоров в единую вычислительную среду, защиты систем синхронизации времени и проверки подлинности вычислений в удаленных квантовых центрах. Тем не менее широкое коммерческое внедрение полномасштабных квантовых сетей сдерживается рядом технических и экономических факторов, включая высокую стоимость специализированного оборудования, необходимость криогенного охлаждения для ряда высокоэффективных детекторов и элементов памяти, чувствительность оптических схем к вибрациям и температурным дрейфам, а также потребность в стандартизации интерфейсов и протоколов.

Таким образом, дальнейший прогресс в области квантовых коммуникаций зависит от согласованного развития квантовой фотоники, материаловедения, криогенной техники, сетевой архитектуры и теории квантовой информации. Постепенное удешевление и миниатюризация компонентов, совершенствование квантовых повторителей и спутниковых линий связи будут определять темпы перехода от специализированных защищенных каналов к полноценным квантовым коммуникационным сетям будущего.

Заключение

Квантовые коммуникации представляют собой перспективное направление современной науки и телекоммуникаций, основанное на использовании фундаментальных законов квантовой механики для передачи и защиты

информации. Опираясь на свойства квантовых состояний и квантовой запутанности, такие системы позволяют выявлять попытки несанкционированного доступа к каналу связи и формируют основу для создания новых сетевых архитектур.

Практическое развертывание квантовых коммуникационных сетей требует преодоления ограничений, связанных с потерями в каналах связи, декогеренцией, неидеальностью аппаратуры и сложностью масштабирования. Совершенствование источников и детекторов одиночных фотонов, развитие квантовой памяти и квантовых повторителей, интеграция наземных и спутниковых каналов, а также гармонизация с классическими сетями и постквантовой криптографией определяют ключевые перспективы развития квантовых коммуникаций в ближайшие десятилетия.

Литература

1. Килин С. Я. Квантовая информация. — М.: Физматлит, 2020. — 412 с.
2. Молотков С. Н. Современная квантовая криптография: теоретические основы и практическая реализация. — М.: Наука, 2019. — 368 с.
3. Гусев А. А., Кулик С. П. Квантовая оптика и квантовые коммуникации. — СПб.: Лань, 2021. — 320 с.
4. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. — М.: Мир, 2020. — 824 с.
5. Холево А. С. Квантовые системы, каналы, информация. — М.: МЦНМО, 2020. — 327 с.
6. Балакин А. В., Калинин В. И. Волоконно-оптические линии связи и квантовые каналы. — М.: Горячая линия — Телеком, 2021. — 296 с.
7. Gisin N., Thew R. Quantum Communication. — Nature Photonics. — 2020. — Vol. 14. — P. 165–174.
8. Pirandola S. et al. Advances in Quantum Cryptography. — Advances in Optics and Photonics. — 2020. — Vol. 12, No. 4. — P. 1012–1236.
9. Wehner S., Elkouss D., Hanson R. Quantum Internet: A Vision for the Road Ahead. — Science. — 2020. — Vol. 362, No. 6412. — eaam9288.
10. IEEE Journal on Selected Areas in Communications. — 2025. — Vol. 43, No. 2. — P. 510–532.