И.Б. Бобров, кандидат физико-математических наук
Н.А. Борщевская, кандидат физико-математических наук
И.В. Дьяконов
И.В. Кондратьев
Е.В. Ковлаков
С.П. Кулик, доктор физико-математических наук, профессор
С.С. Страупе, кандидат физико-математических наук
Г.И. Стручалин
Н.Н. Сысоев, доктор физико-математических наук, профессор

Квантовая обработка информации: фундаментальные и прикладные аспекты

Краткий обзор основных результатов фундаментальных и прикладных исследований в области квантовых технологий, относящиеся к квантовым вычислениям/моделированию и квантовым коммуникациям, в частности: разработка и создание автоматизированных (без участия оператора) и регенеративных систем квантовой связи на основе волоконно-оптических линий связи и атмосферных каналов с наивысшей степенью защищенности, создание системы мультиплексирования для квантовых каналов связи, изучение физических процессов в сложных квантовых системах, разработка компонентной базы для квантовых компьютеров.

1. Введение

Квантовая обработка информации и квантовая связь (КОИКС) – новая бурно развивающаяся область знаний, которая обладает огромным потенциалом, ведущим к прорыву во многих областях науки и техники. КОИКС использует принципиально новые методы вычисления и связи, базирующиеся на принципах квантовой механики, а не классической физики. Это сулит огромную вычислительную мощность, далеко выходящую за пределы возможностей любого классического компьютера, гарантирует абсолютно безопасную связь, а также стимулирует развитие зарождающихся квантовых технологий.

Развитие технологий квантовых вычислений (КВ) откроет новые перспективы в использовании квантовых алгоритмов, моделировании сложных физических систем, исследовании альтернативных вычислительных архитектур, таких как сетевые квантовые со-процессоры и проч. В свою очередь, это даст толчок к развитию большого числа приложений в научно-технической, экономической и социальной сферах деятельности общества, а также переведет на новый качественный уровень системы связи и управления в том числе в области обороны и безопасности, позволит наиболее полно использовать технологии искусственного интеллекта при создании новых образцов вооружения и военной техники.

Значительный интерес в мире к КОИКС проявляется в увеличении финансирования квантовых информационных технологий по всему миру. В этих разработках участвуют ведущие ученые

в области квантовой физики, математики, вычислительной техники, биологии и др. На физическом факультете МГУ ведутся активные исследования в области КОИКС. Наиболее существенные результаты получены в области создания абсолютно защищенных систем квантовой связи. Были спроектированы и построены устойчивые и управляемые (детерминированные) квантовые устройства для систем мультиплексирования квантовых каналов связи, что позволит значительно увеличить их пропускную способность и для создания автоматизированных (без участия оператора), регенеративных систем квантовой связи на основе как волоконно-оптических линий связи, так и атмосферных каналов с наивысшей степенью защищенности.

Принципиальной особенностью этих разработок является тот факт, что они ведутся на единой оптоэлектронной платформе. Это значит, что общий принцип построения используется в совершенно разных по своему назначению системах: и для дальнодействующих оптоволоконных систем, и для относительно коротких атмосферных линий связи, вне зависимости от функциональных требований потребителей.

Проводимые исследования направлены как на математическое доказательство секретности оригинальных квантовых протоколов, так и на разработку всего комплекса экспериментального оборудования – источников и детекторов *N*-фотонных состояний; систем модуляции и диагностики квантовых состояний; на обеспечение комплекса мер по предотвращению активного несанкционированного зондирования систем квантовой связи. На сегодняшний день сформирован технологический задел для серийного производства систем защищенной связи с квантовым распределением ключей и перехода на новый технологический уровень отечественной компонентной базы таких систем.

Квантовые технологии – это современные технологии, основанные на явлениях квантовой физики, которые не могут быть объяснены в рамках классических теорий, таких как законы движения Ньютона, уравнения термодинамики и уравнения Максвелла для электромагнетизма. Ряд уже существующих технологий (например, микроэлектроника, атомная энергетика, квантовая метрология, полупроводниковые оптические приборы, лазерная техника и т. д.) используют достижения квантовой физики и широко распространены в настоящее время. Хорошо известно, что классическая физика стала основой промышленной революции XIX века. Развитие квантовой физики и квантовых технологий привело к резкому скачку в развитии информационных технологий в XX веке в контексте создания аппаратного обеспечения (hardware), тогда как принципы представления и обработки информации (software) оставались вполне классическими.

Однако в конце XX в. были предложены принципиально новые технологии, основанные на использовании более тонких эффектов квантовой физики, которые можно назвать технологиями «квантовой обработки информации». Эти технологии для представления и обработки информации используют явления и свойства, присущие исключительно квантовым системам, такие, как квантовые корреляции, запутанность и суперпозиция квантовых состояний, квантовый параллелизм, принцип неопределенности (дополнительности) Гейзенберга и запрет клонирования неизвестных квантовых состояний. Отличительной особенностью развития квантовых технологий XXI века, основанной на инструментальных возможностях эксперимента, является возможность манипулирования с одиночными квантовыми объектами – атомами, ионами, молекулами, фотонами. Заметим, что теоретические предпосылки для этой возможности были, в основном, разработаны к середине XX в., когда был сформирован аппарат квантовой механики. Все это создает основу для революционного прорыва в области информационных и телекоммуникационных технологий XXI века.

Сегодня, согласно принятой терминологии, ключевые научно-технические направления, развитие которых позволит обеспечить радикальное изменение ситуации на существующих рынках

технологий, продуктов и услуг или будут способствовать формированию новых рынков, называются сквозными. Одной из сквозных технологий в РФ являются квантовые технологии, куда относятся инструменты хранения, обработки, обеспечения безопасности информации и алгоритмы решения задач посредством квантово-механических систем.

В феврале 2018 года на физическом факультете Московского государственного университета имени М.В. Ломоносова был создан Центр квантовых технологий (ЦКТ) – в качестве поддержки ведущихся здесь широкомасштабных исследований. ЦКТ решает три стратегические задачи:

1) В научно-техническом направлении – создание фундаментального научного задела и образцов аппаратуры в области технологий квантовой обработки информации:

- защищенные квантовые коммуникации и новое поколение аппаратуры с гарантированной криптографической стойкостью через волоконные линии связи, атмосферные каналы, вплоть до низкоорбитальных спутников;
- квантовые вычисления и квантовые компьютеры.

2) В коммерческом направлении – вывод на глобальный рынок двух типов продуктов:

- квантовых шифраторов и квантовых телефонов – для использования в магистральных оптоволоконных линиях связи для государственных и коммерческих структур;
- среднемасштабных квантовых компьютеров на основе нейтральных атомов и фотонных чипов с возможностью удаленного сетевого доступа для решения тестовых задач, базирующихся на квантовых алгоритмах.

3) В образовательном направлении – комплексная подготовка как научных, так и инженерных кадров в области квантовых технологий.

Сегодня Центр квантовых технологий физического факультета объединяет более 20 научных, образовательных и коммерческих организаций Российской Федерации в составе Консорциума квантовых технологий. Целью проводимых в ЦКТ научных исследований и практических разработок на их основе является создание фундаментального научного задела и отдельных демонстраторов в области технологий квантовой обработки информации, квантовых вычислений (симуляций) и квантовой связи. Квантовые технологии, являясь сквозной технологией, должны в перспективе привести к практически значимым научно-техническим результатам мирового и опережающего уровня в следующих областях:

- квантовые вычисления и квантовое моделирование;
- квантовые коммуникации и квантовая криптография.

В ряде областей, таких как квантовая криптография, в ЦКТ уже на сегодняшний день получены практически значимые результаты.

2. Квантовые вычисления и квантовое моделирование

Квантовые вычислительные и симулирующие устройства на сегодняшний день рассматриваются как единственный способ удовлетворить растущим нуждам в вычислительных мощностях, продиктованных актуальностью расчетных задач, не поддающихся классическим компьютерам в принципе, например, точный квантово-химический расчет материалов, и вычислительной затратности новых подходов по работе с информацией, способных обеспечить более точный анализ и сократить время выработки решений. Исследованиями и разработкой в направлении создания таких устройств заняты крупные компании и государственные организации. Однако на сегодняшний день квантовых компьютеров и симуляторов, способных решать практически важные задачи, не разработано.

Вычислительные задачи прикладного значения требуют большой вычислительной мощности компьютеров. По этой причине наличие ресурсов для решения вычислительных задач и моделирование сложных систем определяет развитие современной науки и техники – от предсказаний климатических и социальных явлений до создания новых материалов, обладающих уникальными свойствами. Вместе с тем масштабирование классических компьютеров не способно обеспечить надлежащие вычислительные мощности для всего множества таких сложных задач, т. е. имеет место проблема больших вычислительных мощностей. Таким образом, разработка вычислительных устройств на новых принципах является крайне важной задачей. Одно из решений этой проблемы сообщество исследователей видит в создании вычислительных устройств на основе квантовой физики, что обусловило интерес к этой области государственных структур и больших компаний по всему миру.

Например, неподдающиеся для классических компьютеров расчетные задачи встречаются при оптимизации в нейробиологических системах, теории сетей и др. Эти задачи решаются перебором и имеют экспоненциальную сложность, т. е. объем и число требуемых операций растет по экспоненциальному закону с ростом размерности задачи. Важной областью является разработка химических веществ, лекарственных средств (вплоть до индивидуальных) и специальных материалов с улучшенными характеристиками, полагающаяся на затратное компьютерное моделирование, которое на сегодняшний день сильно ограничено по точности и широте спектра учитываемых параметров, все по той же причине вычислительной сложности. Помимо этого, широкое внедрение всевозможных сенсоров в повседневную жизнь и в узкоспециализированные изделия и считывающих информацию из среды, требует как быструю обработку этой информации и принятия управленческих решений, так и соответствующие вычислительные ресурсы, которые могут предоставить только квантовые устройства.

Необходимо различать понятия квантового компьютера и квантового симулятора, которые отличаются своими задачами. *Квантовый компьютер* – устройство, способное решать определенный круг математических задач с существенно большей вычислительной скоростью, чем классический аналог. Обычно, как наглядный пример, выделяют проблему факторизации больших чисел для решения некоторых криптографических задач или вычисление собственных значений и собственных векторов оператора Гамильтона для расчета структуры энергетических уровней сложных молекул или веществ.

Квантовый симулятор – устройство, преследующее цель смоделировать сложный физический процесс, динамика которого описывается гамильтонианом более или менее воспроизводимым в другой доступной для экспериментального контроля и манипуляций физической системе (квантовом симуляторе).

Радикальное ускорение при выполнении квантовых вычислений и моделирования достигается за счет квантового параллелизма и использования принципиально новых (по сравнению с классическими вычислениями) ресурсов:

- информационные биты заменяются принципиально более емкими квантовыми битами – кубитами – двухуровневыми системами, состояния которых в общем случае не сводятся только к 0 или 1, как для классических битов, а являются произвольной суперпозицией этих двух значений (это обеспечивает радикальный рост информационной емкости для реализации промежуточных стадий вычислений);
- используются качественно более сильные, специфически квантовые корреляции между кубитами, встречающиеся, например, в так называемых запутанных состояниях, что приводит к возможности одновременного контролируемого изменения состояний всех элементов регистра из N запутанных между собой кубитов при воздействии на любой единичный кубит из

этого регистра (это обеспечивает радикальный рост скорости выполнения промежуточных стадий вычислений).

Идея квантового симулятора впервые была предложена в 1982 году [1]. В 1996 году была предложена схема универсального квантового симулятора [2], что позволило развить экспериментальные подходы к решению данной задачи. Первые экспериментальные демонстрации возможности точного измерения энергетической структуры молекул были выполнены в 2010 году с помощью двухкубитного оптического квантового симулятора [3] и квантового симулятора на основе ядерного магнитного резонанса (ЯМР) [4]. К настоящему времени удалось разработать прототипы квантовых симуляторов на основе линейно-оптических систем, ЯМР, систем холодных атомов или ионов и сверхпроводящих цепей [3-7]. Максимальное число кубитов, участвующих в реализованных на данный момент алгоритмах квантовой симуляции, составляет 6 [7].

В то же время параллельно развивалась идея универсального квантового компьютера [8-10]. Архитектура универсального квантового компьютера позволяет разработать эффективную физическую реализацию любого из существующих алгоритмов квантовых вычислений. Ученые в ведущих лабораториях США, Европы, Японии, Китая и других стран ведут работу по разработке универсального квантового компьютера на основе различных физических систем – линейно-оптической, холодных атомов и ионов, сверхпроводников, дефектов и центров окраски в кристаллах и др. [11-18].

3. Квантовые коммуникации и квантовая криптография

Технологии квантовых коммуникаций и, в частности, квантовой криптографии, основаны на использовании в качестве носителей информации состояний таких квантово-механических объектов, как фотоны (например, поляризация, фазовая модуляция, запутанность и др.). Преимуществом оптических реализаций физических систем является тот факт, что у электромагнитного поля имеется несколько степеней свободы, на основе которых можно конструировать квантовые состояния фотонов. В частности, комбинируя частотные, пространственные, поляризационные и временные степени свободы, можно задействовать небольшое число фотонов для реализации многокубитовых состояний и операций над ними. Использование фотонов в качестве носителей связано, прежде всего, с такими факторами как максимально возможная скорость распространения в данной среде, а также возможность использования доступных и хорошо разработанных на сегодняшний день инструментов генерации, преобразования и детектирования светового излучения. Кроме того, принимается во внимание, что фотоны слабо взаимодействуют между собой. Это связано с малостью соответствующих коэффициентов в разложении поляризации по степеням поля (восприимчивостей высших порядков). Использование в качестве носителей информации состояний фотонов позволяет задействовать в качестве среды-канала для передачи данных как оптическое волокно, так и «атмосферный канал» в пределах прямой видимости. Такое деление – на волоконно-оптические и атмосферные каналы – обусловливает наличие двух соответствующих направлений в современной квантовой коммуникации – волоконно-оптическое и в свободном пространстве (вплоть до космического).

В случае корректной реализации протоколов квантовой коммуникации обеспечивается гарантированное обнаружение легитимными пользователями любых попыток несанкционированного доступа к каналу передачи информации, поскольку любая попытка измерения состояния квантово-механического объекта приводит к его возмущению и впоследствии обнаруживается по изменениям статистики измеренного сигнала.

Конечной целью разработок в области квантовой коммуникации является создание единой защищенной глобальной сети квантового распределения ключей, включающей распределение ключей через спутники и волоконно-оптические линии связи.

Квантовая криптография – синоним квантовое распределение секретных ключей – неотъемлемая и наиболее развитая в практическом плане часть (технология) квантовых коммуникаций. Эта технология позволяет распределять секретные ключи по открытым волоконным линиям связи или через атмосферу с гарантией их секретности. Целью является постоянная смена секретных ключей в автоматическом режиме без участия операторов, что исключает человеческий фактор. Данные ключи предназначены для дальнейшего использования в системах симметричного шифрования. Высшая степень секретности достигается при использовании ключей в режиме одноразового блокнота – на каждое сообщение свой отдельный ключ, в этом случае достигается наивысшая степень защищенности.

Из общих тенденций по развитию квантовой криптографии можно выделить следующие:

1) Интегрирование систем квантовой криптографии в существующую структуру волоконных телекоммуникационных сетей и передачу ключей вместе с классическим телекоммуникационным сигналом.

2) Увеличение скорости генерации ключей – переход в область гигагерц, а также использование систем с разделением по частоте и времени.

3) Усовершенствование элементной базы. Переход на интегральную платформу для данных систем – создание интегрально оптической платформы для приемо-передающей аппаратуры.

4) Создание реконфигурируемых сетей с квантовым распределением ключей, интегрированных со средствами классического шифрования, которые бы позволяли иметь линейку технических решений для наращивания различного типа сетей в рамках единой идеологии.

5) Продолжение фундаментальных исследований в области квантовых коммуникаций, которые бы обеспечивали поиск новых физических систем, квантовых криптографических протоколов, математических методов, которые бы позволили достичь целей, обозначенных пп. 1-4.

6) Происходит процесс выработки единых международных стандартов для сертификации систем квантовой криптографии. При этом различные страны предлагают свои подходы, лоббируя свои интересы и научно-технические решения. Пока единой точки зрения не выработано.

4. Проектирование устойчивых и управляемых (детерминированных) квантовых устройств.

Одним из направлений деятельности ЦКТ является проектирование устойчивых и управляемых (детерминированных) квантовых устройств. Цель исследований – разработка конкретных устройств для задач квантовой обработки информации. К ним относятся:

- разработка и создание автоматизированных (без участия оператора) и регенеративных систем квантовой связи на основе волоконно-оптических линий связи и атмосферных каналов с наивысшей степенью защищенности;
- создание системы мультиплексирования для квантовых каналов связи, что позволит значительно увеличить их пропускную способность.

Остановимся подробнее на описании основных задач, решаемых в этих направлениях.

4.1. Разработка и создание автоматизированных (без участия оператора) и регенеративных систем квантовой связи на основе волоконно-оптических линий связи и атмосферных каналов с наивысшей степенью защищенности

Говоря о задачах квантовой коммуникации и, в частности, о реализации, связанной с атмосферными каналами, остановимся подробнее на протоколе, который был предложен и обоснован сотрудниками ЦКТ, а впоследствии продемонстрирован на разработанном оборудовании.

Протокол получил название релятивистского, а соответствующее направление – *релятивистская квантовая криптография*.

Квантовая криптография получила широкую известность благодаря обещаниям об абсолютной защищенности от подслушивания. Под «абсолютной» понимается секретность, обеспеченная фундаментальными законами физики, а не текущими технологическими возможностями. Однако реализованные на практике системы квантового распределения ключей не до конца соответствуют тем теоретическим моделям, по которым они были построены. Двумя основными отличиями являются отсутствие строго однофотонных источников и наличие потерь в квантовых каналах связи. Ни от одной из них нельзя избавиться окончательно. На самом деле, существующие протоколы обеспечивают секретность полученных ключей только если потери не превышают определенный порог, зависящий от конкретной реализации. Релятивистская квантовая криптография [19-22] изначально разработана с учетом описанных неидеальностей, работая с сильно ослабленными когерентными импульсами при любых уровнях потерь. Ограничением служит лишь уровень темновых шумов в используемом однофотонном детекторе. Как известно, специальная теория относительности не допускает распространение информации со скоростями, большими скорости света. В описываемом протоколе важным становится не только квантовая природа переносчика информации, но и то, что он обязан быть безмассовой частицей (например, фотоном), которая движется со скоростью света. Заметим, что в остальных системах КРК, где переносчиками информации также являются фотоны, последнее условие не является обязательным.

В протоколе используется фазово-временное кодирование квантовых состояний, при котором фотон распределен между двумя временными окнами, разнесенными на время ΔT. Информация кодируется в относительной фазе между состояниями в каждом временном окне. Классической аналогией являются два следующих друг за другом когерентных импульса света. Такие состояния приготавливаются с помощью единичного лазерного импульса, прошедшего через интерферометр Маха-Цандера с различной длиной плеч.

Чтобы закодировать такое состояние, используется оптический фазовращатель, который накладывает дополнительную фазу ровно на одно из двух временных окон. Если требуется передать «0», то дополнительная фаза не накладывается, если «1», то во втором временном окне осуществляется сдвиг фазы на ϕ. Сначала Алиса кодирует свой бит во втором временном окне и передает его Бобу, который кодирует свой бит на первое, после чего производит измерение результирующего квантового состояния.

Для детектирования используется интерферометр Маха-Цандера с теми же длинами плеч, что при генерации. При повторном прохождении сигнала через интерферометр на выходе вместо двух временных окон будет уже три, и измерение происходит только в определенном временном окне – среднем. Из-за разности хода на втором светоделителе интерферируют передняя, пришедшая из длинного плеча, и задняя, из короткого плеча, половинки пришедшего сигнала. Если Алиса и Боб наложили каждый на свою половинку одинаковую дополнительную фазу (0 или ϕ), то произойдет деструктивная интерференция, и отсчета в фотодетекторе не возникнет, а если разные, то интерференция окажется конструктивной и будет отсчет. Таким образом, по отсчету детектора Боб знает, какой бит выбрала Алиса. Отметим, что Алиса и Боб не должны следить за средним числом долетевших посылок. Потери в канале связи не входят в критерий секретности ключей.

Задержка распространения сигнала играет ключевую роль в данном протоколе, поэтому он пригоден только для связи по прямой видимости в открытом пространстве, когда не существует дополнительных путей распространения. Таким образом, длина линии связи является ключевым априорным параметром протокола. Вторым требованием является распространение сигнала со

скоростью света. Но, важно отметить, что наличие воздуха в канале, который лишь незначительно уменьшает скорость распространения света, не является препятствием для использования протокола, и может быть легко скомпенсировано подбором величины задержки ΔT между временными окнами. С одной стороны, увеличивая это время, мы снижаем допуски к точности измерения длины линии связи и скорости распространения, но с другой, очевидно, понижаем скорость работы системы, т. к. увеличивается время передачи каждого бита.

Существует две реализации данного протокола: одно- и двухпроходная. Каждая из них имеет свои преимущества и недостатки. Исторически первой была реализована двухпроходная конфигурация (рисунок 1).

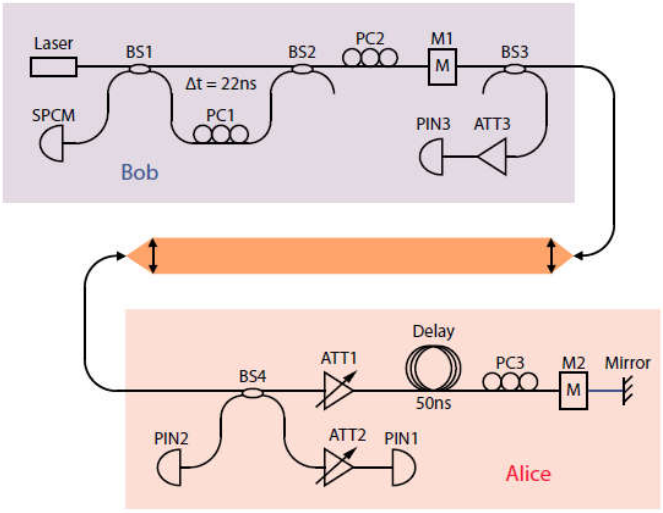

Рисунок 1 – Схема, иллюстрирующая работу двухпроходного варианта протокола релятивистской квантовой криптографии. Выделены станции Боба и Алисы, а также атмосферный канал связи между ними. Laser – импульсный лазер, SPCM – счетчик фотонов, BS1-4 – светоделители, PC1,2 – поляризационные контроллеры, M1,2 – фазовые модуляторы, ATT1-3 – аттенюаторы, Mirror – зеркало, Delay – линия задержки, PIN1,2 – классические детекторы

Сначала Боб генерирует классические оптические импульсы и передает их Алисе [23]. Аппаратура Алисы работает в ждущем режиме. При помощи быстрого классического детектора (PIN1) она фиксирует момент прихода сигналов Боба, после чего ослабляет их до квантового уровня, когда в среднем на один импульс приходится меньше одного фотона, и кодирует их случайными битами. Далее квантовые сигналы отправляются обратно Бобу, где он, зная полную задержку канала связи, в точно рассчитанные моменты времени дополнительно модулирует их уже своими случайными битами, после чего измеряет. Название «двухпроходная схема» следует из того, что свету требуется два раза пройти по каналу связи. Заметим, что если бы Боб посылал импульсы всегда в строго определенные моменты времени, то Ева могла бы посылать свой сигнал непосредственно перед сигналом Боба, тем самым узнавая секретные биты Алисы. Чтобы избежать этого, Боб посылает импульсы апериодично: на каждой итерации он случайным образом выбирает одно из двух времен начала передачи, а после отстрела серии Алиса и Боб сравнивают относительные времена прихода посылок. Стратегия Евы в этом случае уже не работает, поскольку посылка Евой состояния к Алисе в неправильный момент времени непременно приведет к ее обнаружению.

В однопроходной схеме отсутствует первичная передача классического состояния от Боба к Алисе, и происходит только передача квантового состояния в одну сторону. В данной реализации требуется, чтобы и у каждой стороны был свой интерферометр, и они были бы синхронизированы между собой. Эта проблема решается использованием дополнительного лазерного пучка на другой длине волны, по которому происходит как наведение системы, так и стабилизация интерферометров. В противовес этому двухпроходная конфигурация позволяет использовать лишь один интерферометр, установленный у Боба, как для генерации, так и для детектирования, не требуя его стабилизации.

В нерелятивистской квантовой криптографии возможны атаки «прием-перепосыл», когда Ева в каждой посылке измеряет состояния, затем в зависимости от исхода измерения посылает свои состояния, и коллективная атака, когда Ева готовит в каждой посылке свое состояние, запутанное с передаваемым, и оставляет его в квантовой памяти для дальнейших коллективных измерений сразу над всей последовательностью, а модифицированное состояние направляется к Бобу. В релятивистском случае обе атаки приводят к задержкам и к вероятности ошибки 50% в каждой посылке. Это связано с тем, что для получения информации о ключе необходим одновременный доступ к обеим разделенным в пространстве-времени половинкам состояний, для чего их нужно свести вместе, преобразовать и растянуть обратно. А все эти действия, из-за конечной скорости распространения света, которую никак нельзя превысить, будут вносить дополнительные задержки, из-за чего Боб, который детектирует только в определенном временном окне, будет наблюдать уже другой результат.

Таким образом, мы получаем протокол, в котором полностью разделены оптические потери и ошибки, создаваемые подслушивателем. Таким образом, даже при сколь угодно больших потерях в канале и неограниченных ресурсах Евы, любой прирост информации о секретном ключе на стороне Евы обязательно будет сопровождаться ростом числа ошибок, наблюдаемых Бобом, и, соответственно, обнаружением подслушивателя.

В рамках этого же направления ЦКТ совместно с компанией ОАО «ИнфоТеКС» – членом консорциума по квантовым технологиям – также выполняет работы по созданию высокотехнологичного производства комплекса квантовой и криптографической автоматической аппаратуры защиты информации, передаваемой по открытым каналам связи.

Основными задачами этого проекта являются:

- разработка автоматической аппаратуры для квантового распределения ключей, передаваемых по оптическим линиям связи;
- разработка средств криптографической защиты информации, передаваемой по открытым каналам связи и использующих ключи, формируемые с помощью аппаратуры квантового распределения;
- подготовка производства аппаратуры квантового распределения ключей и шифраторов, использующих квантовые ключи;
- производство нескольких комплектов аппаратуры квантового распределения ключей, средств криптографической защиты информации.

В результате реализации проекта будет создана высокотехнологичная квантово-криптографическая аппаратура защиты информации.

Используемые технологии в части создания устройства квантового распределения ключей уникальны. Они основаны на оригинальных протоколах и схемах приемно-передающих модулей (рисунок 2), адаптивном программном обеспечении и процедурах квантовой коррекции ошибок и усиления секретности.

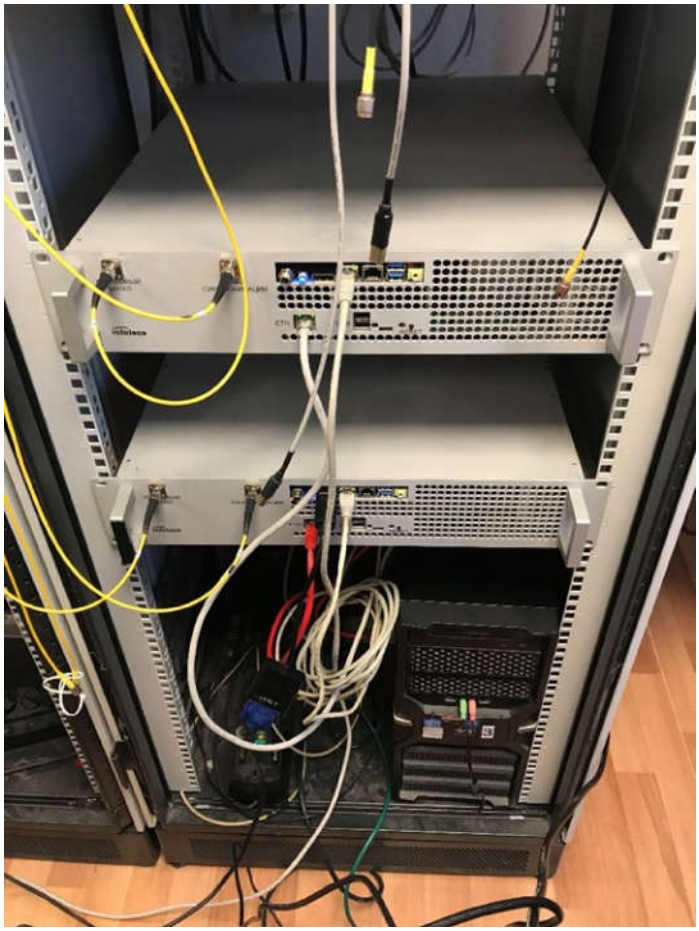

Рисунок 2 – Комплекс квантовой криптографической аппаратуры: высокоскоростные криптографические шифраторы 10G

Скоростные шифраторы канального уровня являются высокотехнологичными устройствами, разработка и производство которых требует наличия квалифицированных специалистов по программированию, цифровой электронике и схемотехнике, криптографии, параллельным вычислениям и многим другим узким специальностям.

Предлагаемая в проекте квантово-криптографическая аппаратура защиты информации, в минимальной комплектации состоящая из пары скоростных шифраторов, интегрированных с аппаратурой квантового распределения ключей, относится одновременно к двум сегментам рынка. Рынок аппаратных шифраторов является уже зрелым сегментом и обладает устойчивыми тенденциями развития. Рынок средств квантового распределения ключей, в свою очередь, только формируется, на нем пока нет ни устойчивого спроса, ни сложившихся моделей потребления.

Целевыми потребителями квантово-криптографической аппаратуры защиты информации являются средние и крупные корпоративные заказчики, органы государственной власти, операторы связи, операторы облачных сервисов, перед которыми стоит задача по обеспечению повышенного уровня защиты высокоскоростных каналов связи.

Типовой ситуацией применения шифраторов с поддержкой квантового протокола распределения ключей на основе волоконно-оптических квантовых каналов является организация канала связи между двумя корпоративными географическими локациями, например, между центром обработки данных (ЦОД) и его резервной копией, разнесенных на расстояние не более 100 км. При этом для целевого применения, например, синхронизации основной и резервной базы данных в ЦОДе, актуальной является как высокая скорость, так и низкие задержки при обработке трафика.

4.2. Создание системы мультиплексирования для квантовых каналов связи

Для развития направления «Квантовые технологии» по приказу ректора МГУ в Программу развития Московского университета включено создание первой в России университетской квантовой сети. Цель работы – разработка и создание аппаратуры шифрования электронного документооборота на основе квантовых оптических технологий.

Проект призван создать в МГУ локальную сеть на базе квантового распределения секретных ключей для реализации защищенного документооборота и шифрованных телефонных соединений между легитимными абонентами (клиентами), в частности, между кабинетом ректора и выделенными подразделениями (деканы факультетов, бухгалтерия, канцелярия и проч.). Такая связь реализуется путем распределения секретных ключей посредством квантовых технологий между доверенным Сервером и несколькими Клиентами с последующей синхронизацией ключей. Легитимные пользователи могут обмениваться секретными сообщениями либо в виде текстовых файлов, либо по телефону. На первом этапе в сети их имеется два, в ближайшей перспективе сеть будет расширена до 32 и более абонентов. На последнем этапе планируется реализовать такую защищенную линию между комплексом зданий МГУ на Ленинских горах и на Моховой улице. В перспективе такими «квантовыми телефонами» предполагается оснастить и другие научные, образовательные и коммерческие организации, расположенные в пределах Москвы, что потребует, в частности, проведения работ, связанных с сертификацией такого оборудования.

Основным партнером ЦКТ физического факультета при реализации этого проекта выступает компания (ОАО «ИнфоТеКС»). Огромную помощь в прокладке оптоволоконных линий связи оказывает компания ООО «ЮлКом Медиа».

На рисунке 3 показана схема, иллюстрирующая один из вариантов топологии защищенной сети, в которой между приемо-передатчиком – Сервером квантово-криптографической системы (ККС) и подключенными клиентами последовательно создаются и синхронно меняются одинаковые секретные ключи, используемые для шифрования файлов или речи при интернет-соединении двух любых абонентов между собой. После каждого телефонного соединения или переданного документа использованный ключ меняется на новый, что значительно увеличивает криптостойкость передаваемой информации.

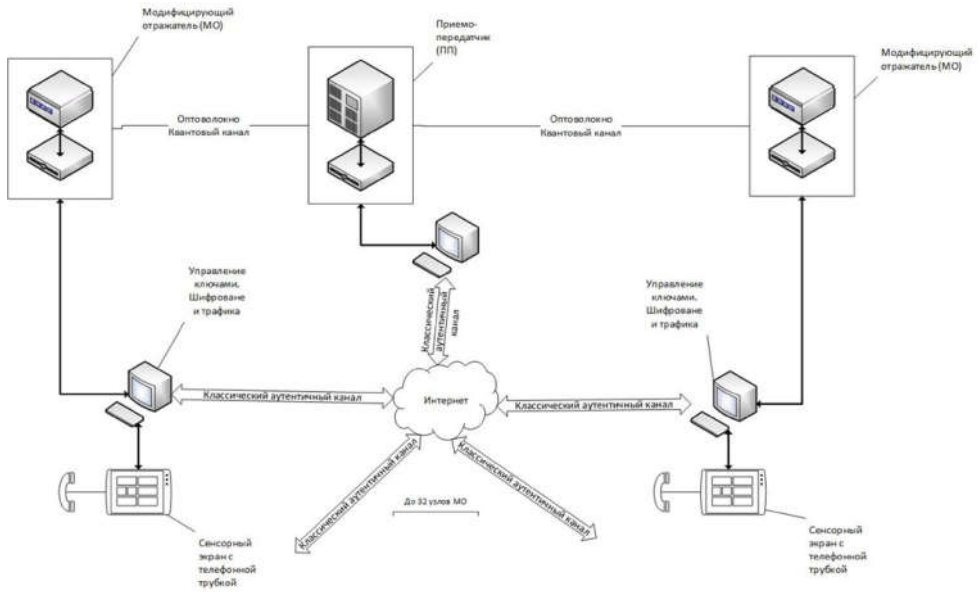

Рисунок 3 – Схема защищенной локальной сети МГУ

Сервер ККС – наиболее сложный и дорогой элемент сети расположен так, чтобы оптимальным образом использовать существующие и специально проложенные оптические линки, которые можно дотянуть до мест расположения абонентской аппаратуры Клиентов. Сервер является объединением ПП узла МГУ (оптико-электрическая часть МГУ, ПО выработки ключей МГУ) и аппаратуры «ИнфоТеКС» для обеспечения защищенного соединения с узлами и аутентичного канала. На модулях Клиентов установлено специально модифицированное программное обеспечение компании «ИнфоТеКС» ViPNet Client и ViPNet Connect, которое обеспечивает шифрование трафика сети ViPNet ключами, получаемыми из ККС. Клиентское программное обеспечение ViPNet Client и ViPNet Connect обеспечивает функции защищенного обмена данными, текстовыми сообщениями (чат) и телефонной связи по IP-каналу (SIP).

Основные пользовательские функции перечислены ниже. В их число входят:

1) индикация защиты коммуникаций ключом из ККС;
2) выбор абонента из адресной книги защищенной сети;
3) проверка связи с абонентом;
4) голосовой вызов абонента;
5) обмен мгновенными текстовыми сообщениями с абонентом;
6) обмен файлами (стандартными средствами операционной системы).

Кроме упомянутых выше направлений, ЦКТ физического факультета ведет исследования и разработки еще в нескольких областях квантовых технологий.

Вид рабочего места квантового телефона приведен на рисунке 4.

Рисунок 4 – Вид рабочего места квантового телефона
(сверху – версия 2018 года, снизу – версия 2019 года)

(*продолжение статьи – в следующем выпуске журнала*)

Список использованных источников

1. Feynman R. Simulating Physics with Computers // Int. J. Theor. Phys. 21, 467 (1982).
2. Lloyd S. Universal Quantum Simulators // Science, 273(5278), 1073 (1996).
3. Lanyon B.P., Whitfield J.D., Gillett G.G., Goggin M.E., Almeida M.P., Kassal I., Biamonte J.D., Mohseni M., Powell B.J., Barbieri M., Aspuru-Guzik A., White A.G. Towards quantum chemistry on a quantum computer // Nat. Chem. 2, 106 (2010).

4. Jiangfeng Du, Nanyang Xu, Xinhua Peng, Pengfei Wang, Sanfeng Wu, Dawei Lu. NMR Implementation of a Molecular Hydrogen Quantum Simulation with Adiabatic State Preparation // Phys. Rev. Lett. 104, 030502 (2010).

5. Bloch I., Dalibard J., Nascimbene S. Quantum simulations with ultracold quantum gases // Nature Phys. 8, 267–276 (2012).

6. Lanyon B.P., Hempel C., Nigg D., Müller M., Gerritsma R., Zähringer F., Schindler P., Barreiro J.T., Rambach M., Kirchmair G., Hennrich M., Zoller P., Blatt R., Roos C.F. Universal digital quantum simulation with trapped ions // Science, 334(6052), 57 (2011).

7. Kandala A., Mezzacapo A., Temme K., Takita M., Brink M., Chow J.M., Gambetta J.M. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets // Nat. Lett. 549, 242 (2017).

8. DiVincenzo D.P. Quantum Computation // Science, 270(5234), 255 (1995).

9. DiVincenzo D.P., Bacon D., Kempe J., Burkard G., Whaley K.B. Universal quantum computation with the exchange interaction // Nature 408, 339 (2000).

10. Briegel H.J., Browne D.E., Dür W., Raussendorf R., Van den Nest M. Measurement-based quantum computation // Nat. Phys. 5, 19-26 (2009).

11. O'Brien J.L., Pryde G.J., White A.G., Ralph T.C., Branning D. Demonstration of an all-optical quantum controlled-NOT gate // Nature 426, 264 (2003).

12. Martin-Lopez E., Laing A., Lawson T., Alvarez R., Zhou Xiao-Qi, O'Brien J.L. Experimental realisation of Shor's quantum factoring algorithm using qubit recycling // Nat. Photon.6, 773 (2012).

13. Harris N.C., Bunandar D., Pant M., Steinbrecher G.R., Mower J., Prabhu M., Baehr-Jones T., Hochberg M., Englund D. Large-scale quantum photonic circuits in silicon // Nanophotonics 5(3), 456 (2016).

14. Ballance C.J., Harty T.P., Linke N.M., Sepiol M.A., Lucas D.M. High-Fidelity Quantum Logic Gates Using Trapped-Ion Hyperfine Qubits // Phys. Rev. Lett. 117, 060504 (2016).

15. Debnath S., Linke N.M., Figgatt C., Landsman K.A., Wright K., Monroe C. Demonstration of a small programmable quantum computer with atomic qubits // Nature 536, 63 (2016).

16. Hanneke D., Home J.P., Jost J.D., Amini J.M., Leibfried D., Wineland D.J. Realization of a programmable two-qubit quantum processor // Nat. Phys. 6, 13 (2010).

17. Mariantoni M., Wang H., Yamamoto T., Neeley M., Bialczak R.C., Chen Y., Lenander M., Lucero E., O'Connell A.D., Sank D., Weides M., Wenner J., Yin Y., Zhao J., Korotkov A.N., Cleland A.N., Martinis J.M. Implementing the quantum von Neumann architecture with superconducting circuits // Science 334(6052), 61 (2011).

18. Xing Rong, Jianpei Geng, Fazhan Shi, Ying Liu, Kebiao Xu, Wenchao Ma, Fei Kong, Zhen Jiang, Yang Wu, Jiangfeng Du. Experimental fault-tolerant universal quantum gates with solid-state spins under ambient conditions // Nature Commun. 6, 8748 (2015).

19. Молотков С.Н. Релятивистская квантовая криптография на «остановленных» фотонах // Письма в ЖЭТФ, т. 76, выпуск 1, 79 (2002).

20. Молотков С.Н. Релятивистская квантовая криптография для открытого пространства без синхронизации часов на приемной и передающей стороне // Письма в ЖЭТФ, т. 94, выпуск 6, 504 (2011).

21. Молотков С.Н. О стойкости релятивистской квантовой криптографии в открытом пространстве при конечных ресурсах // Письма в ЖЭТФ, т. 96, выпуск 5, 374 (2012).

22. Radchenko I.V., Kravtsov K.S., Molotkov S.N., Kulik S. Relativistic quantum cryptography. Relativistic quantum cryptography // Laser Phys. Lett., 11, 065203 (2014).

23. Kravtsov K., Radchenko I., Kulik S., Molotkov S. Relativistic quantum key distribution system with one-way quantum communication // Scientific Reports volume 8, 6102 (2018).

24. Řeháček J., Hradil Z., Knill E., Lvovsky A.I. Diluted maximum-likelihood algorithm for quantum tomography // Phys. Rev. A. – 2007. – Vol. 75 – P. 042108.

25. Shang J., Zhang Z., Hui Khoon Ng. Superfast maximum-likelihood reconstruction for quantum tomography // Phys. Rev. A. – 2017. – Vol. 95 – P. 062336.

26. Struchalin G.I., Pogorelov I.A., Straupe S.S. Experimental adaptive quantum tomography of two-qubit states // Phys. Rev. A. – 2016. – Vol. 93, no. 1. – P. 012103.

27. Gill R.D., Massar S. State estimation for large ensembles // Phys. Rev. A. – 2000. – Vol. 61. – P. 042312.

28. Mahler D.H., Rozema L.A., Darabi A. Adaptive Quantum State Tomography Improves Accuracy Quadratically // Phys. Rev. Lett. – 2013. – Vol. 18 – P. 183601

29. Богданов Ю.И. Унифицированный метод статистического восстановления квантовых состояний, основанный на процедуре очищения // ЖЭТФ. – 2009. – Т. 135. – С. 1068.

30. Kovlakov E.V., Bobrov I.B., Straupe S.S., Kulik S.P. Spatial Bell-State Generation without Transverse Mode Subspace Postselection // Phys. Rev. Lett. – 2017. – Jan. – Vol. 118. – P. 030503.

31. Bolduc E., Bent N., Santamato E. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram / // Opt. Lett. – 2013. – Sep. – Vol. 38, no. 18. – P. 3546-3549.

32. Walborn S.P., Pimentel A.H. Generalized Hermite-Gauss decomposition of the two-photon state produced by spontaneous parametric down conversion // J. Phys. B: At. Mol. Opt. Phys. – 2012. – Vol. 45, no. 16. – P. 165502.

33. Barredo D., de Léséleuc S., Lienhard V., Lahayet T., Browaeys A. An atom-by-atom assembler of defect-free arbitrary two-dimensional atomic arrays // Science 354(6315), 1021 (2016).

34. Endres M., Bernien H., Keesling A., Levine H., Anschuetz E.R., Krajenbrink A., Senko C., Vuletic V., Greiner M., Lukin M.D. Atom-by-atom assembly of defect-free one-dimensional cold atom arrays // Science 354(6315), 1024 (2016).

35. Saffman M.J. Quantum computing with atomic qubits and Rydberg interactions: progress and challenges // Phys. B 49, 202001 (2016).

36. Labuhn H., Barredo D., Ravets S., de Léséleuc S., Macrì T., Lahaye T., Browaeys A. Tunable two-dimensional arrays of single Rydberg atoms for realizing quantum Ising models // Nature 534, 667 (2016).

37. Bernien H., Schwartz S., Keesling A., Levine H., Omran A., Pichler H., Soonwon Choi, Zibrov A.S., Endres M., Greiner M., Vuletić V., Lukin M.D. Probing many-body dynamics on a 51-atom quantum simulator // Nature 551, 579-584 (2017).

38. Fushman I., Englund D., Faraon A., Stoltz N., Petroff P., Vučković J. Controlled Phase Shifts with a Single Quantum Dot // Science 320(5877), 769 (2008).

39. Peyronel T., Firstenberg O., Qi-Yu Liang, Hofferberth S., Gorshkov A.V., Pohl T., Lukin M.D., Vuletić V. Quantum nonlinear optics with single photons enabled by strongly interacting atoms // Nature 488, 57 (2012).

40. Gullans M., Chang D.E., Koppens F.H.L., García de Abajo F.J., Lukin M.D. Single-Photon Nonlinear Optics with Graphene Plasmons // Phys. Rev. Lett. 111, 247401 (2013).

41. Gimeno-Segovia M., Shadbolt P., Browne D.E., Rudolph T. From Three-Photon Greenberger-Horne-Zeilinger States to Ballistic Universal Quantum Computation // Phys Rev. Lett. 115, 020502 (2014).

42. Li Y., Humphreys P.C., Mendoza G.J., Benjamin S.C. Resource Costs for Fault-Tolerant Linear Optical Quantum Computing // Phys. Rev. X 5, 041007 (2015).

43. Abrams D.S., Lloyd Sю Quantum Algorithm Providing Exponential Speed Increase for Finding Eigenvalues and Eigenvectors // Phys. Rev. Lett. 83, 5162 (1999).

44. Peruzzo A., McClean J., Shadbolt P., Man-Hong Yung, Xiao-Qi Zhou, Love PJ., Aspuru-Guzik A., O'Brien J.L. A variational eigenvalue solver on a photonic quantum processor // Nat. Comm. 5, 4213 (2014).

45. Xiao-song Ma, Dakić B., Naylor W., Zeilinger A., Walther P. Quantum simulation of the wavefunction to probe frustrated Heisenberg spin systems // Nature Physics. 7, 399 (2011).

46. Xiao-song Ma, Dakić B., Kropatschek S., Naylor W., Yang-hao Chan, Zhe-xuan Gong, Lu-ming Duan, Zeilinger A., Walther P. Towards photonic quantum simulation of ground states of frustrated Heisenberg spin systems // Nat. Photon. 7, 399 (2011).

47. Barz S., Dakić B., Lipp Y.O., Verstraete F., Whitfield J.D., Walther P. Linear-Optical Generation of Eigenstates of the Two-Site XY Model // Physical Review X, 5, ARTN 021010 (2015).

48. Marandi A., Zhe Wang, Takata K., Byer R.L., Yamamoto Y. Network of time-multiplexed optical parametric oscillators as a coherent Ising machine // Nat. Photon. 8, 937-942 (2014).

49. Aaronson S., Arkhipov A. The Computational Complexity of Linear Optics // arXiv:1011.3245v1 (2010).

50. Tillmann M., Dakić B., Heilmann R., Nolte S., Szameit A., Walther P. Experimental Boson Sampling // Nat. Photon.7, 540 (2013).

51. Crespi A., Osellame R., Ramponi R., Brod D.J., Galvão E.F., Spagnolo N., Vitelli C., Maiorino E., Mataloni P., Sciarrino F. Integrated multimode interferometers with arbitrary designs for photonic boson sampling // Nat. Photon.7, 545 (2013).

52. Spring J.B., Metcalf B.J., Humphreys P.C., Kolthammer W.S., Jin X.M., Barbieri M., Datta A., Thomas-Peter N., Langford N.K., Kundys D., Gates J.C., Smith B.J., Smith P.G., Walmsley I.A. Boson sampling on a photonic chip // Science 339(6121), 798 (2013).

53. Broome M.A., Fedrizzi A., Rahimi-Keshari S., Dove J., Aaronson S., Ralph T.C., White A.G., Photonic boson sampling in a tunable circuit // Science 339(6121), 794 (2013).

54. Spagnolo N., Vitelli C., Bentivegna M., Brod D.J., Crespi A., Flamini F., Giacomini S., Milani G., Ramponi R., Mataloni P., Osellame R., Galvao E.F., Sciarrino F. Efficient experimental validation of photonic boson sampling against the uniform distribution // Nat. Photon. 8, 615 (2014).

55. Dyakonov I.V., Saygin M.Yu., Kondratyev I.V., Kalinkin A.A., Straupe S.S., Kulik S.P. Laser-written polarizing directional coupler with reduced interaction length // Optics Letters, Vol 42, № 20, 4231-4234 (2017).

56. Minnegaliev M.M., Dyakonov I.V., Gerasimov K.I., Kalinkin A.A., Kulik S.P., Moiseev S.A., Saygin M.Yu., Urmancheev R.V. Observation and investigation of narrow optical transitions of 167Er3+ ions in femtosecond laser printed waveguides in 7LiYF4 crystal // Laser Physics Letters, 15, 045207 (6pp) (2018).

57. Skryabin N., Kalinkin A., Dyakonov I., Kulik S. Femtosecond laser written depressed-cladding waveguide 1×2, 2×2 and 3×3 directional couplers in Tm3+:YAG crystal // Micromachines D: Materials and Processing. 11, 1, 1-12, (2020).