УДК 004.056.5 doi: 10.15827/0236-235X.142.695-702 2023. Т. 36. № 4. С. 695–702

О проекте межуниверситетской квантовой сети

А.П. Овсянников
Б.М. Шабанов

Ссылка для цитирования
Овсянников А.П., Шабанов Б.М. О проекте межуниверситетской квантовой сети // Программные продукты и системы. 2023. Т. 36. № 4. С. 695–702. doi: 10.15827/0236-235X.142.695-702
Информация о статье
Поступила в редакцию: 21.08.2023 После доработки: 18.09.2023 Принята к публикации: 13.10.2023

Аннотация. Работа посвящена вопросам создания межуниверситетской квантовой сети – инфраструктурного полигона для проверки решений построения сетей с квантовым распределением ключей и расширения возможностей подготовки кадров в области квантовых коммуникаций. В настоящее время интерес к созданию сетей с квантовым распределением ключей проявляют все передовые страны. В России разработано собственное оборудование квантового распределения ключей и строится магистральная квантовая сеть. Для ускорения практического внедрения квантовых коммуникаций и решения связанных с ним множества научных, технических, нормативных и кадровых вопросов разработана Концепция создания, развития и эксплуатации межуниверситетской квантовой сети национальной исследовательской компьютерной сети. В рамках реализации Концепции создан пилотный проект межуниверситетской квантовой сети, которая объединяет ряд университетов и научных организаций, имеющих собственную инфраструктуру квантовых коммуникаций, обладающих компетенциями в области квантовых технологий, ведущих исследования и разработки в этой области и осуществляющих подготовку специалистов данного направления. Описана топология межуниверситетской квантовой сети, приведены схемы распространения ключа и обмена данными. При рассмотрении различных схем распределения ключей предпочтение отдается схемам с минимальными требованиями к защите доверенных промежуточных узлов. Предложено исследовать применение в межуниверситетской сети протокола MDI квантового распределения ключей через недоверенные узлы. Приведено краткое описание российского оборудования квантового распределения ключей, планируемого для применения в межуниверситетской квантовой сети. Использование в этой сети оборудования всех трех российских производителей квантового распределения ключа позволит продемонстрировать возможности масштабирования квантовых сетей на каждом типе оборудования, исследовать возможности совместной работы оборудования разных производителей и адаптировать его к совместному использованию. Пилотный проект создания межуниверситетской квантовой сети рассчитан на реализацию в 2023–2024 гг.

Ключевые слова: квантовая сеть, квантовое распределение ключей, КРК, квантовые коммуникации, информационная безопасность, национальная исследовательская компьютерная сеть

Введение. Шифрование данных необходимо для безопасности всех современных телекоммуникаций, используемых для банковских операций, управления производственными процессами, применения беспилотных автомобилей, имплантированных медицинских устройств и т.д. Для многих широко используемых криптографических систем серьезную угрозу представляет развитие квантовых компьютеров: доказано, например, что алгоритм Шора [1, 2] на квантовом компьютере позволяет в течение нескольких часов или суток подобрать ключи шифрования для асимметричных шифров, таких, например, как схема Диффи–Хелмана. В [3] показано, что симметричные шифры остаются устойчивыми к взлому квантовым компьютером, хотя и требуют увеличения длины ключа. Однако использование симметричных шифров требует наличия у удаленных абонентов одинакового секретного ключа. Перспективным подходом к замене доверенной доставки ключей курьером является применение систем *квантового распределения ключа* (КРК). Это позволит обеспечить достаточную скорость создания ключей (хотя значительно медленнее, чем уязвимые схемы Диффи–Хелмана) и исключит человеческий фактор из процесса их распределения.

Технология КРК уже вышла из стен лабораторий, в мире активно растет число пилотных квантовых сетей, создаются инфраструктуры КРК разного масштаба. В Китае с 2017 года разрабатывается защищенная сеть передачи данных в интересах государственных и финансовых организаций. В 2021 году была создана сеть КРК, соединившая абонентов на расстоянии 4 600 км с помощью как волоконно-оптических, так и спутниковых каналов КРК [4]. К 2025 году планируется увеличить их протяженность до 35 000 км [5]. При этом наряду с волоконно-оптическими линиями связи реализуются атмосферные и спутниковые каналы распределения ключа шифрования. К сети подключено свыше 200 организаций – государственных, научных, финансовых. В Южной Корее строительство квантово-защищенной инфраструктуры ведется с 2020 года, первая очередь включала 800 км для подключения

около 50 государственных учреждений, вторая – свыше 1 000 км.

В рамках Евросоюза реализуется проект европейской квантовой инфраструктуры EuroQCI [6]. Проект предполагает переход от создания экспериментальных научных квантовых сетей к национальным квантовым инфраструктурам отдельных стран и их объединению в общеевропейскую квантовую инфраструктуру. В проекте предусматриваются использование серийного оборудования разных производителей, развитие наряду с волоконно-оптическими линиями связи спутниковых каналов КРК, разработка сценариев использования квантовых ключей как для передачи данных, так и для защиты сохраняемой информации, а также интеграции в квантовую инфраструктуру квантовых вычислителей и квантовых сенсоров. В значительной мере сеть передачи данных проекта использует инфраструктуру научно-образовательной телекоммуникационной сети GÉANT. Проект планируется завершить к 2027 году, фаза создания национальных квантовых сетей начата в 2023 году, с 2024 года начнется объединение национальных квантовых сетей в единую европейскую квантовую сеть.

Отдельные пилотные проекты по созданию сетей КРК реализованы и в США, однако программа исследований направлена на создание квантовых сетей передачи данных, в которых квантовые линии связи используются не для генерации и передачи ключей, а непосредственно для передачи данных. Это существенно более сложная задача, чем КРК, и технологии для ее решения еще далеки от готовности. В рамках программы создания квантовой инфраструктуры в США планируется квантовая сеть между национальными лабораториями.

Проекты создания сетей с КРК реализуются в России с 2019 года. В МГУ им. М.В. Ломоносова (Москва) и в ТУСУР (Томск) создана университетская квантовая сеть на оборудовании компании «ИнфоТеКС», на оборудовании компании «КуРэйт» реализована университетская сеть между МИСИС и МТУСИ. В университете ИТМО (Санкт-Петербург) создана университетская сеть на оборудовании КРК компании «СМАРС-Кванттелеком».

В соответствии с дорожной картой по развитию высокотехнологичной отрасли «Квантовые коммуникации» компания РЖД создает магистральную сеть с КРК. Создан участок между Санкт-Петербургом, Москвой и Нижним Новгородом. До конца 2023 года будут введены в строй участки Нижний Новгород–Арзамас–Казань и Москва–Тула–Воронеж–Ростов-на-Дону, общая протяженность *магистральной квантовой сети* (МКС) РЖД составит 2 500 км. В 2024 году планируется охватить сетью Краснодар, Сочи, Ульяновск, Самару, Саратов, Волгоград, Ижевск, Пермь, Уфу, Екатеринбург, Челябинск. Некоторые участки этой сети строятся на оборудовании «СМАРТС-Кванттелеком», какие-то – на оборудовании «ИнфоТеКС».

В России разработано оборудование для создания отечественных систем КРК, проведены тестовые испытания этих систем, строится МКС, идет сертификация оборудования КРК (часть линейки оборудования «ИнфоТеКС» уже сертифицирована). На повестке дня – переход к внедрению и широкому применению действующей квантовой коммуникационной инфраструктуры.

Проект межуниверситетской квантовой сети

Основой инфраструктуры КРК страны должна стать МКС РЖД. При этом задачу «последней мили» предоставления доступа пользователям к услугам шифрования квантовым ключом должны решать операторы связи (например, «Ростелеком», «МТС» и др.), создавая в городах присутствия МКС РЖД городские сети с КРК на основе собственной волоконно-оптической инфраструктуры. Таким образом, для практического применения КРК необходима мультидоменная сеть, образованная совокупностью взаимодействующих друг с другом сетей КРК: магистральной сети РЖД и городских сетей «последней мили». Конечные пользователи, которым нужен защищенный обмен информацией, могут быть клиентами разных операторов защищенной квантовой связи, в свою очередь, взаимодействующих между собой через цепочку других операторов. Полноценное функционирование мультидоменной сети с КРК требует решения множества научных, технических, нормативных, кадровых вопросов. Необходима проверка предлагаемых решений на практике, а значит, нужен инфраструктурный полигон, в качестве которого предлагается использовать *межуниверситетскую квантовую сеть* (МУКС).

Создание межуниверситетской сети с КРК предусмотрено дорожной картой по развитию высокотехнологичного направления «Квантовые коммуникации». Рабочей группой, в которую вошли представители университетов и

организаций – разработчиков систем КРК, разработана Концепция создания, развития и эксплуатации МУКС *национальной исследовательской компьютерной сети* (НИКС) на 2023–2030 гг.

Согласно Концепции, целью создания МУКС в составе НИКС является предоставление научным и образовательным организациям Российской Федерации дополнительных возможностей для выполнения исследований и разработок по приоритетным направлениям научно-технологического развития на основе квантовых технологий, а также участия в крупных российских и международных научных и образовательных проектах, базирующихся на использовании отвечающей современным требованиям квантовой сети, интегрированной в инфраструктуру НИКС.

Концепция предполагает использование МУКС для решения следующих задач:

– подготовка инженерных и научных кадров для развития и эксплуатации квантовых сетей: как сетей КРК, так и квантовых сетей передачи данных;

– проведение НИР и ОКР для разработки и совершенствования оборудования для создания квантовых сетей: как для дальнейшего развития технологии КРК, так и для создания научных и инженерных заделов для реализации квантового Интернета;

– создание возможностей для появления и развития технологических компаний-стартапов в области квантовых коммуникаций, квантовых вычислений и квантовых сенсоров;

– создание условий для реализации пилотных проектов компаниями, занимающимися внедрением квантовых коммуникаций.

Возможные направления НИР и ОКР на базе МУКС:

– взаимодействие внутригородских, корпоративных сетей и магистральных сетей с КРК;

– сценарии интеграции квантовой сети с сетью передачи данных;

– управление ключами и мониторинг квантовой сети;

– возможность использования оборудования, в том числе квантового, от разных производителей;

– увеличение дистанции и скорости распределения ключей;

– мультиплексированное распределение ключей в волоконно-оптических линиях связи;

– разработка доверенных и недоверенных узлов (квантовых репитеров);

– распределение ключей в атмосфере, между объектами в космическом пространстве и на поверхности Земли;

– разработка и испытание различных стандартов для квантовых коммуникаций в рамках комитета по стандартизации ТК-26;

– разработка моделей угроз для сетей КРК.

В соответствии с Концепцией МУКС на начальном этапе (2023–2024 гг.) будет создаваться как «надстроенная» на НИКС (сеть передачи данных) сеть КРК.

НИКС – национальная сеть науки и образования (NREN), единственная в России научно-образовательная телекоммуникационная сеть федерального масштаба, обладающая протяженной высокоскоростной магистральной инфраструктурой и международными каналами, обеспечивающими интеграцию с зарубежными NREN и Интернетом [7]. Одной из важнейших функций НИКС является предоставление своим пользователям – организациям науки и образования страны устойчивой и отвечающей современным требованиям (в том числе в части информационной безопасности [8]) телекоммуникационной сети для выполнения исследований и разработок. Как всякая сеть науки и образования, НИКС – не только сеть передачи данных, но и полигон для тестирования и распространения новых информационных технологий. Развертывание МУКС в составе НИКС и на ее основе представляется логичным шагом, обеспечивающим наибольшие возможности для ее функционирования в режиме как научной сети, так и продуктовой, обеспечивающей защиту передаваемых данных в соответствии со всеми требованиями законодательства.

В рамках реализации Концепции разработан пилотный проект МУКС. Предусматривается объединение университетов, имеющих собственную инфраструктуру квантовых коммуникаций (университетские квантовые сети, лабораторные стенды), обладающих компетенциями в области квантовых технологий, ведущих в ней исследования и разработки и осуществляющих подготовку специалистов данного направления. Участники проекта: университет ИТМО (Санкт-Петербург), МГУ им. М.В. Ломоносова, квантовая сеть МИСИС–МТУСИ, МСЦ РАН (Москва), ННГУ им. Н.И. Лобачевского (Нижний Новгород), ИКТИБ ЮФУ (Таганрог), КНИТУ КАИ им. А.Н. Туполева и КФТИ КазНЦ (Казань), Самарский университет им. С.П. Королева и ПГУТИ (Самара).

Схема МУКС в рамках пилотного проекта 2023–2024 гг. приведена на рисунке 1.

Базовой конфигурацией системы КРК является сегмент «точка-точка», ключ создается оборудованием, устанавливаемым на концах волоконно-оптической линии связи, – распределяется между связываемыми ею узлами. Длины сегментов КРК имеют практические ограничения: скорость выработки ключей зависит от оптических потерь [9, 10], необходимо отсутствие активных оптических и электрооптических компонентов, в том числе усилителей сигнала, необратимо разрушающих передаваемые квантовые состояния. Так как защищенный обмен данными требует наличия общего ключа между любой парой узлов, возникает необходимость передачи квантового ключа через несколько сегментов (промежуточных доверенных узлов) [11, 12]. Китайская национальная квантовая сеть также построена на основе доверенных промежуточных узлов [10].

Передача квантового ключа между городами реализуется с использованием МКС РЖД. В городах присутствия МКС создаются узлы МУКС на базе узлов связи НИКС в университетах и научных организациях. Узлы МУКС непосредственно подключаются к узлам МКС, остальные участники пилотного проекта подключаются к узлам МУКС. Генерация квантовых ключей осуществляется на оборудовании КРК, устанавливаемом на концах волоконно-оптических линий связи, обмен данными реализуется по каналам связи НИКС с использованием совместимых с оборудованием КРК *средств криптографической защиты информации* (СКЗИ), получающих квантовые ключи от оборудования КРК. МКС рассматривается как некий единый сегмент – закрытый от МУКС доверенный сервис передачи квантовых ключей между СКЗИ МУКС, размещаемыми в защищенных зонах доверенных узлов МКС РЖД.

Типовая схема сегмента между двумя университетами приведена на рисунке 2, между университетом и узлом МКС РЖД – на рисунке 3. Различие схем обусловлено тем, что зашифрованные квантовыми ключами данные и передаваемые конечным абонентам ключи шифрования в МУКС используют разные пути передачи.

Существенным недостатком доверенных узлов является появление ключа в открытом виде на каждом доверенном узле, что делает необходимой защиту аппаратуры от нарушителя, поскольку на доверенном узле имеются квантовые ключи от соседних сегментов сети, соединенных с данным узлом. Если для МКС РЖД требование защиты доверенных узлов выполняется безусловно, то для узлов МУКС в университетах этого хотелось бы избежать как для снижения стоимости ее создания и эксплуатации, так и для обеспечения максимальной гибкости ее использования в качестве экспериментального стенда для исследовательских работ и подготовки специалистов. Поэтому при рассмотрении различных схем распределения ключей [13] предпочтение отдается схемам с минимальными требованиями к защите доверенных промежуточных узлов. Рассматривается также применение в МУКС протокола MDI (Measurement-Device-Independent) КРК через недоверенные узлы, доказательства стойкости которого приведены в [14].

МУКС использует оборудование всех российских разработчиков оборудования КРК. Для сегментов в Санкт-Петербурге, Нижнем Новгороде, Казани, Самаре используются оборудование КРК от «СМАРТС-Кванттелеком» и СКЗИ «ФПСУ-IP» от «Амикон». Сегменты между ИКТИБ ЮФУ (Таганрог) и узлом МКС (Ростов-на-Дону), между МГУ им. М.В. Ломоносова и МСЦ РАН (Москва) строятся на оборудовании «Инфотекс». Сегмент МИСИС–МСЦ РАН использует оборудование КРК «КуРэйт» и СКЗИ «Код безопасности».

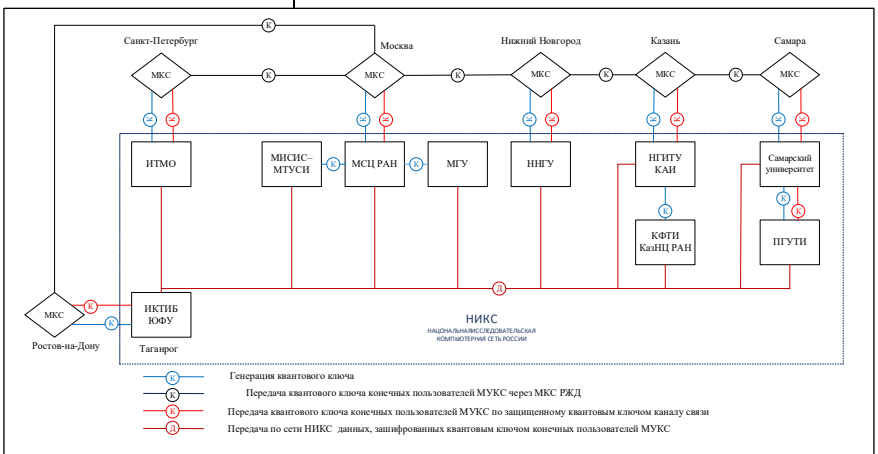

Рис. 1. Схема МУКС. Пилотный проект

Fig. 1. Interuniversity quantum network scheme. Pilot project

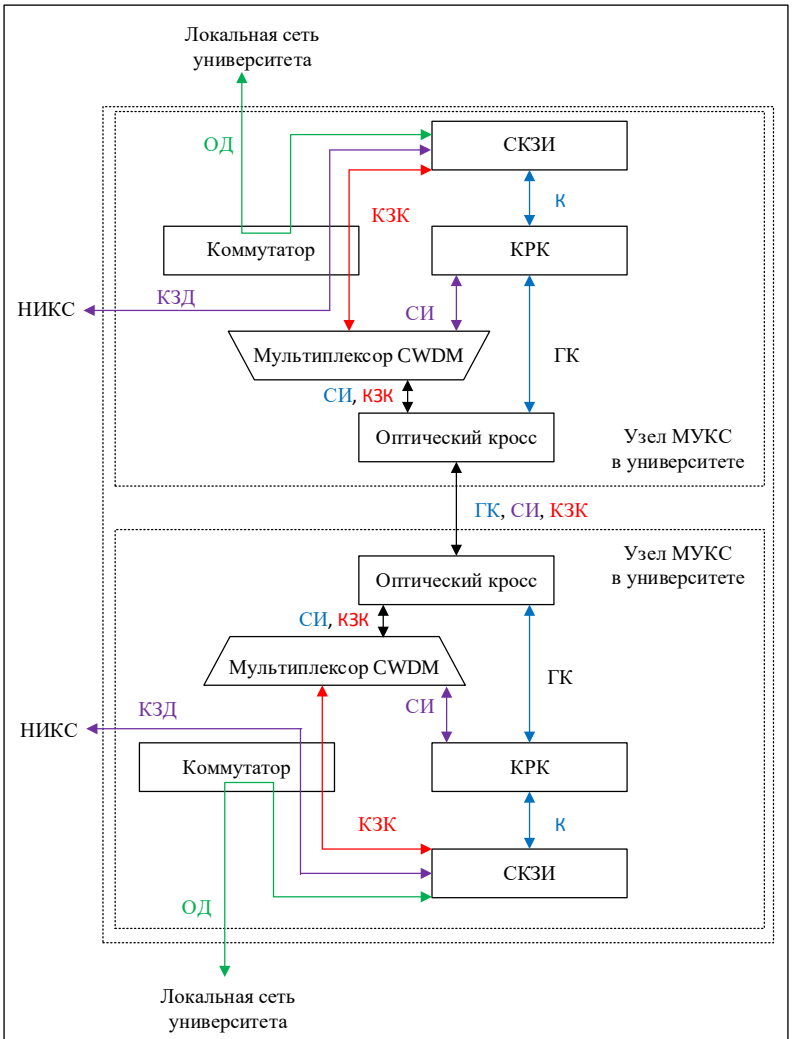

Рис. 2. Типовая схема сегмента между университетами:
ГК – генерация квантового ключа;
К – просеянный квантовый ключ; СИ – служебная информация;
КЗК – криптозащищенный ключ конечного пользователя;
КЗД – криптозащищенные данные; ОД – нешифрованные данные

Fig. 2. Typical scheme of a segment between universities:
QK – quantum key generation;
K – sifted quantum key; PI – proprietary information;
CPK – end-user crypto-protected key;
CPD – crypto-protected data; UD – unencrypted data

Оборудование «Инфотекс» использует основанный на геометрически однородных состояниях оригинальный протокол [15], разработанный в МГУ им. М.В. Ломоносова. Оно предназначено для защиты государственной критической информационной инфраструктуры государства и крупных госкомпаний, обеспечивает высокую производительность по генерации и обновлению ключа, максимальную скорость передачи. Оборудование производится серийно, более 75 % стоимости изделия приходится на российские компоненты. Ожидается завершение его сертификации.

Оборудование «СМАРТС-Квантелеком» реализует уникальный российский протокол генерации квантового ключа на боковых частотах, созданный учеными ИТМО (Санкт-Петербург) [16, 17]. Комплект предназначен для защиты критической информационной инфраструктуры крупных и средних российских компаний, обладает уникальным сочетанием производительности, возможностей и стоимости. Первое поколение этого оборудования уже применяется в крупных российских компаниях. Находится в процессе прохождения сертификации. Использование его в рамках МУКС позволит существенно поднять качество работы и его характеристики, откроет возможность защиты критической информационной инфраструктуры широкого круга российских компаний.

Оборудование «КуРэйт» реализует метод обманных состояний (decoy states) протокола BB84 [18], используемый в мировом сообществе, в том числе в зарубежном оборудовании. Его особенностями являются применение однофотонных детекторов и односторонней (поляризационной) оптической схемы, а также повышенная эффективность исправления ошибок. Оборудование проходит процедуру сертификации в испытательной лаборатории «Код Безопасности» и интегрировано с многофункциональным межсетевым экраном «Континент», что обеспечивает подключение к МУКС организаций, использующих решения компании «Код Безопасности».

Использование в МУКС оборудования всех трех российских производителей КРК позволит продемонстрировать возможности масштабирования квантовых сетей на каждом типе оборудования, исследовать возможности сов-

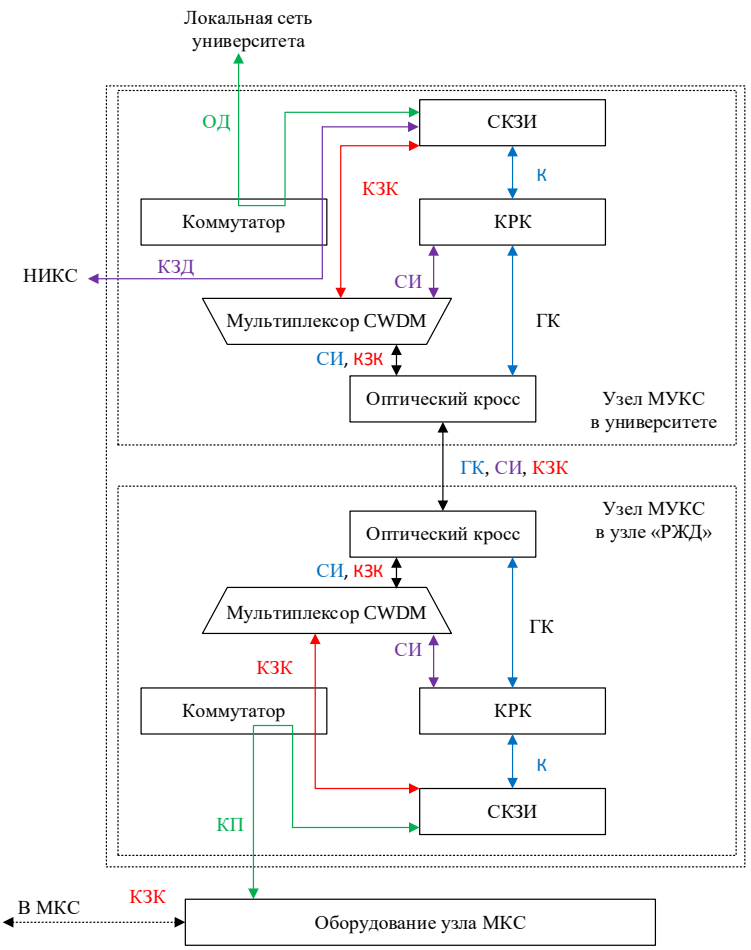

Рис. 3. Типовая схема сегмента между узлом МУКС в университете и узлом МКС: ГК – генерация квантового ключа; К – просеянный квантовый ключ; СИ – служебная информация; КЗК – криптозащищенный ключ конечного пользователя; КП – ключ конечного пользователя (внутри доверенного сегмента); КЗД – криптозащищенные данные; ОД – нешифрованные данные

Fig. 3. Typical segment diagram between an interuniversity quantum network node and a backbone quantum network node: QK – quantum key generation; K – sifted quantum key; PI – proprietary information; CPK – end-user crypto-protected key; EUK – end-user key (within a trusted segment); CPD – crypto-protected data; UD – unencrypted data

местной работы оборудования разных производителей и адаптировать его к совместному использованию в мультидоменной сети с КРК. По мере сертификации оборудования КРК может быть организован защищенный доступ с использованием квантовых сетей на оборудовании разных производителей к суперкомпьютерным ресурсам МГУ им. М.В. Ломоносова и МСЦ РАН – ведущих суперкомпьютерных центров страны.

Заключение

Описанный пилотный проект создания МУКС рассчитан на реализацию в 2023–2024 гг. В 2023 году на Форуме будущих технологий «Вычисления и связь. Квантовый мир» на базе опытного сегмента МУКС был проведен тестовый сеанс квантовой связи между МГУ им. М.В. Ломоносова и ННГУ им. Н.И. Лобачевского.

В дальнейшем планируются опытная эксплуатация пилотного сегмента МУКС с целью разработки сервисов (в рамках НИКС) по передаче информации, защищенной квантовым ключом, а также масштабирование сети, в том числе с использованием КРК через спутник. Предполагается также развитие МУКС как научной квантовой сети для повышения ее функциональности в области передачи квантовых состояний по линиям связи для объединения квантовых объектов – квантовых вычислителей и сенсоров.

Список литературы

1. Shor P.W. Algorithms for quantum computation: Discrete logarithms and factoring. Proc. 35th Annual Symposium on Foundations of Comput. Sci., 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.
2. Shor W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. on Computing, 1997, vol. 26, no. 5, pp. 1484–1509. doi: 10.1137/S0097539795293172.
3. Bernstein D.J., Lange T. Post-quantum cryptography. Nature, 2017, no. 549, pp. 188–194. doi: 10.1038/nature23461.
4. Chen Y.A., Zhang Q., Chen T.Y. et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature, 2021, no. 589, pp. 214–219. doi: 10.1038/s41586-020-03093-8.

5. Qin H. Towards large-scale quantum key distribution network and its applications. Proc. ITU QIT4N Workshop, 2019. URL: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Hao_Qin_Presentation.pdf (дата обращения: 25.08.2023).

6. The European Quantum Communication Infrastructure (EuroQCI) Initiative. URL: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (дата обращения: 01.09.2023).

7. Абрамов А.Г., Гончар А.А., Евсеев А.В., Шабанов Б.М. Национальная исследовательская компьютерная сеть нового поколения: текущее состояние и концепция развития // Информационные технологии. 2021. Т. 27. № 3. С. 115–124. doi: 10.17587/it.27.115-124.

8. Абрамов А.Г. Защита от DDoS-атак своими руками: оперативные разработка и внедрение сервиса в Национальной исследовательской компьютерной сети России // Программные продукты и системы. 2022. Т. 35. № 4. С. 572–582. doi: 10.15827/0236-235X.140.572-582.

9. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dušek M., Lütkenhaus N., Peev M. The security of practical quantum key distribution. Rev. Mod. Phys., 2009, vol. 81, pp. 1301–1350. doi: 10.1103/RevModPhys.81.1301.

10. Zhang Q., Xu F., Chen Y.-A., Peng C.-Zh., Pan J.-W. Large scale quantum key distribution: Challenges and solutions [Invited]. Opt. Express, 2018, vol. 26, no. 18, pp. 24260–24273. doi: 10.1364/OE.26.024260.

11. Elliot C. Building the quantum network. New J. of Phys., 2002, vol. 4, pp. 46.1–46.12. doi: 10.1088/1367-2630/4/1/346.

12. Lucamarini M., Yuan Z.L., Dynes J.F., Shields A.J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature, 2018, no. 557, pp. 400–403. doi: 10.1038/s41586-018-0066-6.

13. Жиляев А.Е. Классификация схем выработки и распределения ключей в сетях квантового распределения ключей произвольной топологии // Докл. ТУСУР. 2021. Т. 24. № 4. С. 33–39. doi: 10.21293/1818-0442-2021-24-4-33-39.

14. Кулик С.П., Молотков С.Н. MDI – Measurement Device Independent квантового распределения ключей // Письма в ЖЭТФ. 2023. Т. 118. № 1-2. С. 62–70.

15. Молотков С.Н. О геометрически однородных когерентных состояниях в квантовой криптографии // Письма в ЖЭТФ. 2012. Т. 95. № 6. С. 361–366. doi: 10.1134/S0021364012060070.

16. Kiselev F., Goncharov R., Veselkova N., Samsonov E., Kiselev A.D., Egorov V. Performance of subcarrier-wave quantum key distribution in the presence of spontaneous Raman scattering noise generated by classical DWDM channels. JOSA B, 2021, vol. 38, no. 2, pp. 595–601. doi: 10.1364/JOSAB.412289.

17. Samsonov E., Goncharov R., Gaidash A. et al. Subcarrier wave continuous variable quantum key distribution with discrete modulation: Mathematical model and finite-key analysis. Sci. Rep., 2020, no. 10, art. 10034. doi: 10.1038/s41598-020-66948-0.

18. Трушечкин А.С., Киктенко Е.О., Кронберг Д.А., Федоров А.К. Стойкость метода обманных состояний в квантовой криптографии // УФН. 2021. Т. 191. № 1. С. 93–109. doi: 10.3367/UFNr.2020.11.038882.

Software & Systems doi: 10.15827/0236-235X.142.695-702 2023, vol. 36, no. 4, pp. 695–702

On an interuniversity quantum network project

Aleksey P. Ovsyannikov
Boris M. Shabanov

For citation
Ovsyannikov, A.P., Shabanov, B.M. (2023) 'On an interuniversity quantum network project', *Software & Systems*, 36(4), pp. 695–702 (in Russ.). doi: 10.15827/0236-235X.142.695-702
Article info
Received: 21.08.2023 After revision: 18.09.2023 Accepted: 13.10.2023

Abstract. The paper discusses the issues of creating an interuniversity quantum network, a so-called national infrastructure testbed for quantum key distribution (QKD). It is designed for testing solutions for building networks with quantum key distribution, equipment checking and benchmarking in practice, education and personnel training. Currently all advanced countries are showing interest in creating QKD networks. Russia developed its own QKD equipment and is building a backbone QKD quantum network. A Concept for creating, developing and operating an Interuniversity Quantum Network (IUQN) based on a National Research Computer Network (NICS) was developed in order to accelerate practical implementation of quantum communications and to solve a variety of related research, technical, regulatory and personnel issues. A pilot project of the IUQN was developed as a part of implementing the concept. IUQN connects universities and scientific organizations that have their own quantum communication infrastructure, have competencies in quantum technologies, conduct research and development and train specialists in this field. The paper describes IUQN topology, gives QKD and data exchange schemes. When considering various QKD schemes, minimal requirements for trusted intermediate nodes protection are preferred. The paper proposes to consider using MDI-QKD protocol through untrusted nodes. The authors briefly describe Russian QKD equipment planned to use in IUQN. The use of equipment from all three Russian manufacturers in IUQN will allow demonstrating the possibilities of scaling quantum networks on each equipment type, explore

the possibilities of different manufacturers' equipment collaboration and adapt it to joint use. It is planned to implement the pilot project of creating IUQN in 2023-2024.

Keywords: quantum key distribution, QKD, quantum communications, information security, national research and educational network

Acknowledgements. The work was carried out at the JSC RAS in terms of FNEF-2022-0014 state assignment

Благодарности. Работа выполнена в МСЦ РАН в рамках государственного задания по теме FNEF- 2022-0014

References

1. Shor, P.W. (1994) 'Algorithms for quantum computation: Discrete logarithms and factoring', *Proc. 35th Annual Symposium on Foundations of Comput. Sci.*, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

2. Shor, W. (1997) 'Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer', *SIAM J. on Computing*, 26(5), pp. 1484–1509. doi: 10.1137/S0097539795293172.

3. Bernstein, D.J., Lange, T. (2017) 'Post-quantum cryptography', *Nature*, (549), pp. 188–194. doi: 10.1038/nature23461.

4. Chen, Y.A., Zhang, Q., Chen, T.Y. et al. (2021) 'An integrated space-to-ground quantum communication network over 4,600 kilometres', *Nature*, (589), pp. 214–219. doi: 10.1038/s41586-020-03093-8.

5. Qin, H. (2019) 'Towards large-scale quantum key distribution network and its applications', *Proc. ITU QIT4N Workshop*, available at: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Hao_Qin_Presentation.pdf (accessed August 25, 2023).

6. *The European Quantum Communication Infrastructure (EuroQCI) Initiative*, available at: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (accessed September 01, 2023).

7. Abramov, A.G., Gonchar, A.A., Evseev, A.V., Shabanov, B.M. (2021) 'The new generation national research computer network: Current status and concept for the development', *Information Technologies*, 27(3), pp. 115–124 (in Russ.). doi: 10.17587/it.27.115-124.

8. Abramov, A.G. (2022) 'DIY DDoS Protection: Operational development and implementation of the service in the National Research Computer Network of Russia', *Software & Systems*, 35(4), pp. 572–582 (in Russ.). doi: 10.15827/0236-235X.140.572-582

9. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M. (2009) 'The security of practical quantum key distribution', *Rev. Mod. Phys*., 81, pp. 1301–1350. doi: 10.1103/RevModPhys.81.1301.

10. Zhang, Q., Xu, F., Chen, Y.-A., Peng, C.-Zh., Pan, J.-W. (2018) 'Large scale quantum key distribution: Challenges and solutions [Invited]', *Opt. Express*, 26(18), pp. 24260–24273. doi: 10.1364/OE.26.024260.

11. Elliot, C. (2002) 'Building the quantum network', *New J. of Phys*., 4, pp. 46.1–46.12. doi: 10.1088/1367-2630/4/1/346.

12. Lucamarini, M., Yuan, Z.L., Dynes, J.F., Shields, A.J. (2018) 'Overcoming the rate-distance limit of quantum key distribution without quantum repeaters', *Nature*, (557), pp. 400–403. doi: 10.1038/s41586-018-0066-6.

13. Zhilyaev, A.E. (2021) 'Key generation and distribution schemes classification for quantum key distribution networks of arbitrary topology', *Proc. of TUSUR University*, 24(4), pp. 33–39 (in Russ.). doi: 10.21293/1818-0442-2021-24-4-33-39.

14. Kulik, S.P., Molotkov, S.N. (2023) 'MDI – Measurement Device Independent quantum key distribution', *JETP Letters*, 118(1-2), pp. 62–70 (in Russ.).

15. Molotkov, S.N. (2012) 'On geometrically uniform states in quantum cryptography', *JETP Letters*, 95(6), pp. 361–366. doi: 10.1134/S0021364012060070 (in Russ.).

16. Kiselev, F., Goncharov, R., Veselkova, N., Samsonov, E., Kiselev, A.D., Egorov, V. (2021) 'Performance of subcarrier-wave quantum key distribution in the presence of spontaneous Raman scattering noise generated by classical DWDM channels', *JOSA B*, 38(2), pp. 595–601. doi: 10.1364/JOSAB.412289.

17. Samsonov, E., Goncharov, R., Gaidash, A. et al. (2020) 'Subcarrier wave continuous variable quantum key distribution with discrete modulation: Mathematical model and finite-key analysis', *Sci. Rep*., (10), art. 10034. doi: 10.1038/s41598-020-66948-0.

18. Trushechkin, A.S., Kiktenko, E.O., Kronberg, D.A., Fedorov, A.K. (2021) 'Security of the decoy state method for quantum key distribution', *Physics-Uspekhi*, 191(1), pp. 93–109 (in Russ.). doi: 10.3367/UFNr.2020.11.038882.

Авторы

Овсянников Алексей Павловмч [1],
ведущий научный сотрудник,
ovsyannikov@jscc.ru
Шабанов Борис Михайлович [1],
д.т.н., чл.-корр. РАН, директор,
jscc@jscc.ru

[1] Межведомственный суперкомпьютерный центр РАН, г. Москва, 119991, Россия

Authors

Aleksey P. Ovsyannikov [1],
Leading Researcher,
ovsyannikov@jscc.ru
Boris M. Shabanov [1], Dr.Sc. (Engineering),
Corresponding Member of the RAS,
Director, jscc@jscc.ru

[1] Joint Supercomputer Center of RAS,
Moscow, 119991, Russian Federation