DOI: 10.22184/1992-4178.2023.229.8.20.23

Как противостоять грядущим угрозам взлома криптографических систем

Рассказывают руководитель научной группы компании QRate Р. А. Шаховой и руководитель отдела разработки ДОФ компании QRate А. В. Лосев

Р. А. Шаховой

А. В. Лосев

Упоминание понятия «квантовые технологии» до сих пор может вызвать ощущение, что речь идет о некой научной фантастике. Тем не менее широкое практическое применение квантовых вычислений, а тем более квантовой криптографии – по всей видимости, вопрос не столь отдаленной перспективы. В этих направлениях ведутся активные разработки, практические вопросы обсуждаются на различных мероприятиях. Не является исключением и Российский форум «Микроэлектроника», в рамках научной конференции которого уже не первый год проводится секция по квантовым технологиям, а в деловой программе запланирован круглый стол «Квантовые алгоритмы и облачные квантовые вычисления».

ООО «КуРэйт» (QRate) с 2015 года занимается разработкой оборудования и программного обеспечения для квантового шифрования, а также развитием и внедрением данных технологий в инфраструктуры российских организаций. Представители компании – руководитель научной группы Роман Алексеевич Шаховой и руководитель отдела разработки ДОФ Антон Вадимович Лосев – рассказали нам, в чем заключается актуальность квантовой криптографии, какие задачи решаются для ее практического применения, а также поделились некоторыми сведениями о разработках предприятия.

Роман Алексеевич, расскажите, пожалуйста, о компании QRate. Когда она была образована и какие цели ставились перед ней при ее создании?

Предшественницей компании QRate можно считать лабораторию квантовых коммуникаций Российского квантового центра. В 2015 году в рамках этой лаборатории был организован стартап, который в итоге превратился в самостоятельную компанию. Основной ее целью было и остается создание устройств для квантовых коммуникаций: систем квантового распределения ключей, квантовых генераторов случайных чисел, детекторов одиночных фотонов и др.

В чем заключается актуальность обеспечения информационной безопасности с помощью квантовых технологий? Какими специфическими

возможностями обладают данные решения и от каких угроз, которым не способен противостоять классический подход, они защищают?

Развитие квантовых технологий, а именно создание полноценного квантового компьютера, не только открывает новые горизонты в области вычислений, но и несет угрозу существующим криптографическим системам, использующим методы асимметричного шифрования. Термин «асимметричное» в названии метода отражает тот факт, что в нем используются два ключа: открытый – необходимый для того, чтобы зашифровать сообщение, и закрытый – для расшифровки. Безопасность асимметричных методов шифрования основывается на вычислительной сложности некоторых математических задач, например так называемой задачи факторизации. Однако для квантового компьютера данная задача уже не является сложной в вычислительном смысле, поэтому злоумышленник, имеющий в своем распоряжении квантовый компьютер, сможет, например, легко узнать данные вашей банковской карты, которые в зашифрованном виде передаются в банк при оплате покупок.

Чтобы нивелировать данную угрозу, уже в ближайшем будущем придется отказаться от некоторых современных криптографических методов. Одной из возможных альтернатив является переход к симметричным методам шифрования, в которых для шифрования и дешифровки используется один и тот же ключ. Данные методы устойчивы к взлому с помощью квантового компьютера, однако они обладают существенным недостатком: для их использования участники секретной передачи данных должны предварительно распределить между собой криптографические ключи. Традиционный способ распределения ключей – обмен ключами в заранее оговоренном месте или использование курьера с флеш-накопителем. Это неудобно и дорого. Кроме того, это не позволяет обеспечить требуемый уровень секретности.

Распределить ключ, однако, можно удаленно, если использовать для этого одиночные кванты света. Кодируя биты в поляризации одиночных фотонов, передаваемых, например, по оптоволокну, можно быть уверенным, что злоумышленник не сможет перехватить данные незаметно. Эта технология называется квантовым распределением ключей (КРК).

Является ли технология КРК единственной в защите информации от взлома квантовым компьютером или есть другие подходы?

Этот подход не единственный. Одновременно с ним развиваются методы постквантовой криптографии. Постквантовые алгоритмы строятся на сложных математических задачах, при решении которых квантовые компьютеры не получают вычислительного преимущества. В частности, это алгоритмы, основанные на линейных кодах, теории решеток и хеш-функциях.

Какие существуют препятствия на пути практической реализации квантового распределения ключей и как они преодолеваются?

КРК теоретически обеспечивает безусловную секретность при распределении криптографических ключей, которые затем можно использовать в схемах шифрования, устойчивых к взлому с помощью квантового компьютера. Но при практической реализации протоколов КРК приходится иметь дело с различными аппаратными несовершенствами, которые могут дать злоумышленнику возможность взломать систему.

Развитие квантовых технологий не только открывает новые горизонты в области вычислений, но и несет угрозу существующим криптографическим системам

Так, вместо идеальных одиночных фотонов мы обычно используем слабые лазерные импульсы, которые с некоторой вероятностью могут содержать более одного фотона. Фазовые модуляторы имеют конечную полосу пропускания, модуляторы интенсивности – конечную экстинкцию, а высокочастотные драйверы, используемые для управления ими, могут искажать форму электрических сигналов. Наконец, реальные детекторы одиночных фотонов характеризуются эффективностью, отличной от 100%, а также имеют конечное мертвое время и ненулевую вероятность темновых отсчетов. Все эти несовершенства делают реальную систему КРК уязвимой для различных атак, которые злоумышленник может реализовать, оставшись при этом незамеченным.

Существуют как минимум три возможных подхода, позволяющих избежать квантового взлома и обеспечить безопасность. Во-первых, можно попытаться создать точную математическую модель всех элементов системы КРК, которую затем можно использовать в доказательстве секретности. К сожалению, данный подход непросто реализовать на практике из-за сложности устройств, составляющих систему КРК. Второй подход мы называем «заплатки». Он подразумевает разработку мер противодействия всем известным атакам на реализацию выбранного протокола КРК и напоминает подход, используемый в классической криптографии. Основным недостатком данного метода является то, что он позволяет защитить систему

только от известных атак, но при этом может оставаться уязвимым для атак, еще не изобретенных. Наконец, третий подход, который мы называем «аппаратно-независимое КРК», предполагает, что все устройства – лазеры, детекторы, модуляторы – являются потенциальными источниками уязвимостей и их следует рассматривать как «черные ящики», находящиеся в руках злоумышленника. Данный подход, однако, вряд ли является оптимальным решением с практической точки зрения из-за чрезвычайно низкой скорости передачи квантовых ключей.

Квантовое распределение ключей с недоверенным центральным узлом является сегодня одним из наиболее перспективных направлений развития систем КРК

Поскольку ни один из перечисленных подходов пока не позволяет эффективно решить проблему квантового взлома, приходится искать промежуточные варианты. Считается, что наиболее уязвимым местом системы КРК является измерительное устройство – детектор одиночных фотонов, поэтому особое место среди таких промежуточных решений занимает протокол детектор-независимого КРК. С его помощью можно полностью избавиться от всех каналов утечки информации, связанных с детекторами, и поместить детекторы в недоверенном центральном узле. Как и в аппаратно-независимом подходе, в КРК с недоверенным центральным узлом используются белловские измерения: Алиса и Боб одновременно посылают на центральный узел фотоны либо лазерные импульсы, где они запутываются, а затем измеряются в базисе Белла. Даже если злоумышленник узнает все результаты измерений, это не позволит ему определить секретный ключ: он сможет понять только одинаковые или разные биты послали Алиса и Боб. Именно КРК с недоверенным центральным узлом является сегодня одним из наиболее перспективных направлений развития систем КРК.

Почему в системах КРК используется именно детектор одиночных фотонов?

В протоколах КРК на дискретных переменных – например, в протоколе BB84 – безусловная секретность квантовых ключей может быть достигнута только в том случае, когда биты ключа получены из измерения одиночных фотонов, переданных по квантовому каналу. Для выполнения данного измерения классические фотоприемники использоваться не могут, поскольку они не обладают необходимой чувствительностью. Нужны именно детекторы одиночных фотонов.

Детекторы являются главной частью приемного устройства. Центральным компонентом передатчика, в свою очередь, является источник одиночных фотонов или – чаще – лазер, импульсы которого ослабляются до квазиоднофотонного уровня. Кроме того, в состав передатчика входят различные модуляторы, которые позволяют осуществлять кодирование битов.

Еще одним важным компонентом системы КРК является генератор случайных чисел (ГСЧ), который также иногда называют датчиком случайных чисел. Это устройство генерирует случайные последовательности бит. Именно ГСЧ является «сердцем» системы КРК, поскольку генерируемые им биты в итоге становятся битами квантового ключа. В компании QRate разработка ГСЧ занимает особое место: мы разработали несколько вариантов датчиков случайных чисел, использующих различные эффекты в полупроводниковых лазерах и разнообразные способы оцифровки случайных сигналов.

Антон Вадимович, компания QRate разработала также полупроводниковый однофотонный детектор QButterfly. Если вкратце, в чем физическая основа работы данного типа устройств?

Основным компонентом полупроводникового детектора одиночных фотонов является однофотонный лавинный фотодиод, вокруг которого строится схема электронной обвязки, обеспечивающая его работу. Для того чтобы диод был в состоянии зарегистрировать одиночный фотон, он должен находиться в так называемом гейгеровском режиме, то есть при напряжении обратного смещения выше напряжения пробоя. В таком режиме попадание в зону поглощения диода даже одиночного фотона способно спровоцировать лавинную генерацию тока через структуру диода, достаточного для регистрации данного события с помощью электронной обвязки. Эти сигналы могут быть преобразованы в калиброванные импульсы стандартной логики для передачи информации любому потребителю.

Отмечу, что подобные детекторы могут применяться не только в системах КРК, но и в таких областях, как спутниковая лазерная дальнометрия, построение 3D-изображений объектов, микроскопия и др. В целом, их сфера применения определяется их способностью детектировать оптические сигналы с чувствительностью, недоступной неквантовым устройствам того же класса, таким как лавинные и pin-фотодиоды.

Какие вы бы выделили основные характеристики детектора QButterfly, влияющие на его применение

на практике, и как бы вы охарактеризовали его возможности на фоне зарубежных аналогов?

Основными параметрами детектора одиночных фотонов с точки зрения его практического применения являются не только его сигнальные и шумовые характеристики, такие как квантовая эффективность, темновые отсчеты и вероятность послеимпульса, но и его эргономика, размеры, а также удобство интеграции в измерительные системы пользователя, если мы говорим о его применении как измерительного прибора вне системы КРК.

Могу сказать, что сигнальные и шумовые характеристики нашего детектора соответствуют уровню ведущих мировых аналогов, таких как детекторы серии ID Qube компании ID Quantique. Были проведены и опубликованы сравнительные исследования их характеристик. Помимо этого, он обладает компактными размерами и удобным интерфейсом управления с возможностью гибкой подстройки параметров детектора под конкретную задачу.

Роман Алексеевич, насколько удается локализовать производство ваших аппаратных решений, возможно ли их построение на основе отечественной компонентной базы?

Задача создания отечественной компонентной базы для систем КРК вполне достижима, причем в ближайшем будущем. Оптоэлектронные устройства, полупроводниковые лазеры, оптоволоконные компоненты умеют делать многие отечественные производители, и в компании QRate мы пытаемся по возможности использовать именно российскую компонентную базу. К сожалению, это не всегда просто с бюрократической точки зрения и подчас невыгодно с экономической, но работа в данном направлении ведется.

Если переходить от компонентов системы КРК к вопросам ее развертывания, требуется ли для этого специализированная инфраструктура?

Для построения сетей КРК в настоящее время предлагается использовать разветвленную систему доверенных узлов, в которых находятся устройства для распределения ключей: передатчики и приемники. Они должны быть соединены квантовыми каналами, которые на самом деле являются не чем иным, как стандартными волоконно-оптическими линиями связи. Таким образом, специальных каналов передачи для систем КРК не требуется – можно использовать существующую инфраструктуру. В перспективе вместо доверенных узлов предполагается использовать так называемые квантовые повторители, с помощью которых квантовые состояния будут телепортироваться от одного передатчика к другому, что позволит решить проблему затухания квантовых сигналов в оптоволокне.

Для проведения исследований и разработок в области квантовых технологий защиты информации нужны высококвалифицированные, возможно даже уникальные, специалисты. Как решается кадровый вопрос в вашей компании?

Квантовая криптография находится на стыке нескольких областей: информационной безопасности, квантовой физики и квантовой информатики. Кроме того, от сотрудников компании QRate зачастую требуются знания в области физики лазеров, фотоники и радиофизики. Специалиста, являющегося экспертом во всех этих областях, найти очень сложно, поэтому мы стараемся брать студентов старших курсов естественно-научных и технических вузов, как правило студентов-физиков, и обучаем их сами. Так, например, в Российском квантовом центре совместно с МФТИ создана базовая кафедра, на которой студенты слушают курсы по квантовой связи, выполняют лабораторные работы на специально разработанном в нашей компании научно-образовательном комплексе QLab, а некоторые устраиваются на работу в QRate младшими научными сотрудниками, где они пишут свои выпускные работы по наиболее интересным для нашей компании темам.

Задача создания отечественной компонентной базы для систем КРК вполне достижима, причем в ближайшем будущем

Существуют ли примеры проектов внедрения ваших систем квантовой защиты информации?

Всю информацию о наших проектах мы стараемся размещать в открытом доступе. Первые пилотные проекты в интересах финансовой индустрии были реализованы еще в 2017 году. После этого спектр возможных вариантов применения систем КРК в информационных системах различных потенциальных потребителей стал расширяться. Так, совместно с Университетом Иннополис компания QRate впервые в мире продемонстрировала возможность использования квантового распределения ключей для беспилотного транспорта.

Кроме того, сегодня любой желающий может прийти в НИТУ МИСИС или МТУСИ и посмотреть, как выглядят оконечные узлы первой в России межвузовской квантовой сети.

Спасибо за интересный рассказ.

С Р. А. Шаховым и А. В. Лосевым беседовал Ю. С. Ковалевский