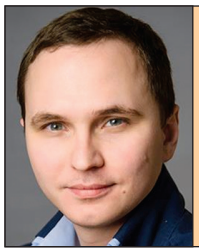
КВАНТОВАЯ КРИПТОГРАФИЯ НА СТРАЖЕ СЕКРЕТНОСТИ



ПОЗДНЯКОВ
Александр,
менеджер отдела развития продуктов
АО «ИнфоТеКС»

Квантовые технологии, квантовые коммуникации, квантовый компьютер – эти слова все чаще мелькают в новостях. Об этом говорят, как о революционном технологическом скачке, который отразится на многих сферах нашей жизни, и на кибербезопасности в том числе.

Стремительное развитие технологий дает все больше возможностей: покупки совершаются онлайн, оплата услуг происходит с помощью мобильного банкинга, учиться и работать сегодня можно удаленно. Ежедневно мы обмениваемся большим количеством информации по различным каналам связи, поэтому кибербезопасность выходит на первый план. Киберпреступление, направленное против частного лица, например, взлом аккаунта, кража банковских данных, шантаж после получения злоумышленником личных фотографий, хранившихся в «облаке», может значительно навредить человеку. А в случае успешной кибератаки на инфраструктуру компании последствия могут быть и вовсе фатальными. Утечка или блокирование критически важной информации могут привести к серьезным финансовым потерям и даже к полной остановке работы предприятия.

А если это электростанция или газо- нефтепровод? Последствия могут быть печальными, уже есть примеры. Кроме того, взлом технических систем или кража персональных данных клиентов может серьезно навредить репутации компании.

Для начала давайте разберемся, как защищать информацию, что такое криптография, почему до сих пор не существует абсолютно надежного способа защитить данные и с чем связан все нарастающий интерес к квантовой криптографии?

Основы криптографии

В основе решения большинства задач, связанных с защитой информации, лежит криптография. Это наука о методах обеспечения конфиденциальности, целостности и аутентичности информации. Попросту, следует обеспечить, чтобы посторонний не мог прочитать ваше сообщение, не мог внести изменения в передаваемое вами сообщение, а принимающая сторона была уверена, что оно отправлено вами.

Конфиденциальность информации традиционно достигается путем шифрования, то есть обратимого видоизменения исходного текста на основе алгоритма преобразования – криптографического алгоритма. На первый взгляд может показаться, что главное правило безопасности – держать в секрете криптографический алгоритм, но это не так. Криптографические алгоритмы не являются секретными, более того, они публикуются для широкого круга лиц, такая открытость позволяет выявлять в них различные уязвимости. В основе средств защиты информации лежат криптостойкие алгоритмы, то есть те, которые по итогам тестирования показали невозможность успешной атаки в настоящий момент. А так как криптографический алгоритм всем известен, то необходима некая секретная информация, с помощью которой при использовании криптоалгоритма будет зашифровываться и расшифровываться сообщение. Этой информацией является ключ. При условии его секретности обеспечивается конфиденциальность и аутентичность.

Традиционная криптография, даже при условии соблюдения жестких требований и регламентов, не может гарантировать полную защиту информационных систем от всех известных угроз безопасности. Практика показывает, что невозможно гарантировать и абсолютную секретность ключа.

Золотой ключик

В современной криптографии используется симметричное и асимметричное шифрование. В обоих методах применяются криптографические ключи, которые представляют собой последовательность бит. Симметричное шифрование работает следующим образом:

1. Берем известный криптоалгоритм и случайный криптографический ключ, который будет служить для зашифрования и расшифрования информации. Этот ключ должен быть известен отправителю и получателю.
2. С помощью ключа шифрования и криптографического алгоритма, трансформируем сообщение, которое нужно зашифровать, в бессвязную последовательность символов. Полученную последовательность теперь можно передавать по любому каналу связи, так как без ключа ее будет невозможно прочитать.
3. Тот, кто обладает ключом шифрования и знает алгоритм, может расшифровать последовательность символов обратно в исходное сообщение.
4. Если не знать ключ, то, даже зная алгоритм, расшифровать информацию почти невозможно.

Преимущество симметричного шифрования заключается в быстроте операций, а недостаток этого метода – в сложности доставки криптографического ключа от отправителя получателю с абсолютной гарантией секретности.

Более сложным является асимметричное шифрование, оно применяется, например, при совершении покупок в интернете или при создании электронной подписи. В асимметричном шифровании используются два ключа, пара чисел, которые также являются последовательностью бит. Одно число является открытым, то есть доступно всем, а второе – это секретный ключ, известный только владельцу. Эта пара чисел не является случайной, она связана между собой определенным алгоритмом, который производит на их основе третье секретное число. Важно отметить, что мы говорим о больших числах. В основе стойкости криптографического алгоритма в этом случае лежит сложность задачи разложения больших чисел на простые множители. Если мы не знаем ни одно из исходных простых чисел, то разложить на множители такое огромное число будет очень сложной задачей.

Преимущество асимметричного шифрования заключается в том, что ключи высчитываются математиче-

ски, так решается проблема их доверенной доставки. Криптостойкость в асимметричной криптографии основывается на вычислительной сложности, поэтому с развитием технических возможностей приходится увеличивать длину ключа и менять алгоритмы. Например, в RSA (криптографическом алгоритме с открытым ключом, который основывается на вычислительной сложности задачи факторизации больших чисел), в настоящий момент длина ключа должна составлять минимум 2048 бит, а рекомендуемая – 3072 бит и более. Чтобы усложнить взлом, длину ключа приходится постоянно увеличивать, а это приводит к усложнению вычислений, и, соответственно, замедлению всего процесса шифрования. Кроме того, на практике невозможно доказать отсутствие эффективного средства, которое бы справилось с известными алгоритмами асимметричного шифрования. Из-за вычислительной сложности метода он становится значительно более медленным, чем симметричное шифрование, поэтому его тоже нельзя считать безупречным.

Вернемся к золотому ключику, которым зашифровывают и расшифровывают информацию. Специалисты по информационной безопасности решают проблему доверенной доставки криптографических ключей организационно-техническими мерами: доступ к информации защищают механически – устанавливают физические барьеры на пути у злоумышленника, выстраивают сложную процедуру авторизации и т.д. Это ведет к дополнительным затратам, но все равно не гарантирует абсолютную безопасность, ведь есть еще человеческий фактор. Злоумышленники виртуозно пользуются человеческой глупостью/невнимательностью/ наивностью, чтобы получить доступ к ключу. Помимо этого, сотрудника, имеющего доступ к секретному ключу, можно подкупить или он может украсть информацию злонамеренно.

Специалисты в области криптографии начали поиск решения, как сделать так, чтобы шифрование информации не требовало все более сложных и дорогих вычислительных ресурсов и организационно-технических мер, и при этом исключало человеческий фактор при доставке секретных ключей.

Новая веха в развитии криптографии началась в 1984 году, когда был разработан первый протокол квантового распределения ключей BB84. Главным преимуществом квантовых криптографических протоколов по сравнению с классическими стало строгое научно-теоретическое обоснование их стойкости. Секретность ключа гарантируется не вычислениями, а фундаментальными законами квантовой физики. Давайте посмотрим, как именно в этом случае удается получить секретный ключ без участия оператора, полностью исключая человеческий фактор.

Куда и как бегут фотоны

Из квантовой физики специалисты по криптографии позаимствовали техническое решение, основанное на измерении физического состояния фотонов. Этот способ получил название технология квантового распределения ключей (КРК).

Задача доставки симметричных ключей (а при КРК используется этот метод), фактически сводится к обеспечению генерации случайных, но одинаковых последовательностей одновременно на двух удаленных друг от друга узлах. При этом информация об этих последовательностях не должна передаваться между узлами. КРК решает эту задачу при помощи манипуляций с физическим состоянием фотонов.

Между двумя узлами связи, передающим и принимающим, организуется оптический канал связи, предназначенный для передачи квантовых состояний. В качестве физического объекта для передачи квантового состояния используется фотон. Перед тем, как передать фотон, его квантовое состояние необходимо подготовить, то есть преобразовать его определенным образом. В процессе преобразования случайным образом выбирается базис квантового состояния и значение какой-либо характеристики, при этом количество вариантов базисов заранее известно. Базис, участвующий в процессе передачи состояния, выбирается случайным образом. Значение параметра фотона также выбирается случайным образом, на этом этапе кодируется логический 0 или логическая 1. Таким образом, мы получаем последовательность бит, как в традиционной криптографии.

После того, как случайным образом выбран базис и случайным образом выбрано значение, подготовленный фотон отправляется на принимающий узел. На принимающем узле нужно измерить значение квантового состояния фотона, но для этого ему нужно выбрать базис, в котором он будет измеряться, который, как и на узле отправителя, также выбирается случайным образом. В результате измерения получается значение параметра, представляющее собой ноль или единицу.

Таким образом, закодированные фотоны в большом количестве отправляются на принимающий узел. В результате «отстрела» у передающего узла образуется последовательность значений, которые были закодированы в квантовых состояниях фотонов и базисах, в которых они приготавливались. У принимающего узла образуется своя независимая последовательность значений вместе с набором случайных базисов, в которых были получены эти значения.

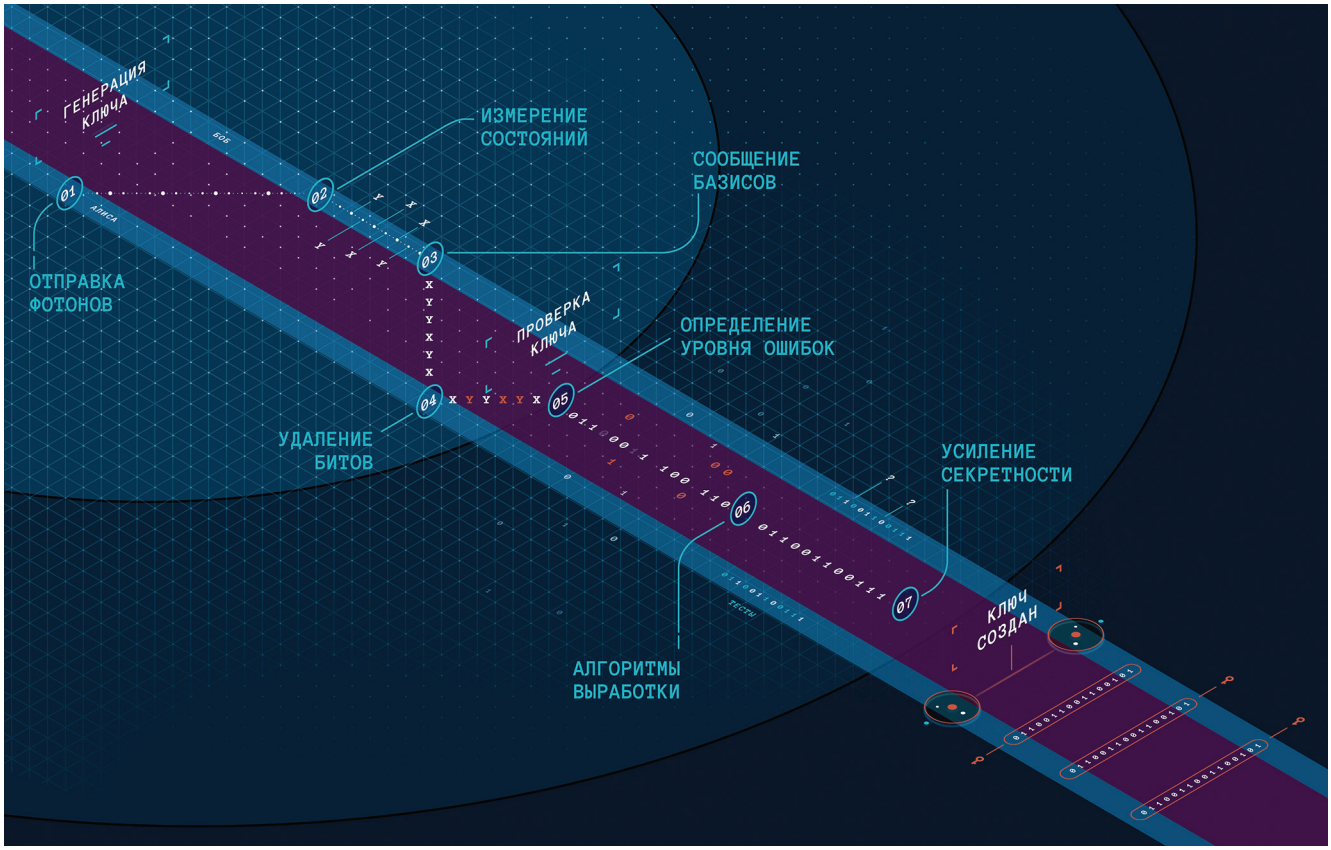
Конкретный квантовый протокол выбирается таким образом, чтобы узлы смогли определить, какое значение получилось у другой стороны, опираясь только на значения базисов.

Если принимающий узел отправит только набор базисов, в которых он измерял значения, то передающий, глядя на этот набор и сравнив со своим набором, сможет определить, что в конкретном измерении получилось у другого. Секретность основывается на специально выбранном наборе базисов, в которых можно подготавливать и измерять фотоны. Набор этих базисов должен быть такой, что при одном сочетании передающий узел мог бы узнать результат измерения принимающего, а при другом сочетании базисов результаты измерения были бы равновероятны.

Позиции последовательностей, в которых передающий узел не может определить полученное принимающим значение, удаляются. В результате остаются только те значения, которые передающему узлу известны, и они совпадают с теми значениями, которые были им закодированы. Таким образом, без передачи самой последовательности, раскрывая только базисы, удается отфильтровать одинаковые последовательности бит.

Итак, одинаковые последовательности остались в секрете, но этого еще недостаточно для того, чтобы использовать их в качестве ключей шифрования. Необходимо обеспечить их защищенность от возможных действий злоумышленника. Для этого нужно обеспечить аутентификацию

Рис. 1.



канала, по которому узлы обмениваются информацией о базисах.

Особенность квантового распределения ключей заключается в том, что при помощи аутентифицированного канала и открытого квантового канала, можно получить уникальный секретный ключ, который никак не будет зависеть от предыдущих или последующих сгенерированных ключей. Следует отметить, что ключи создаются на территориально распределенных узлах, без непосредственной передачи ключевой информации и без участия человека.

Квантовая криптография: настоящее и будущее

Технология КРК уже вышла из лаборатории и готова для применения в промышленных криптографических системах. Однако, непрерывно действующих квантовых систем в мире пока не так много, квантовая криптография находится в самом начале пути своего развития.

Квантовые технологии и основанная на них криптография должны стать фундаментом системы информационной безопасности будущего, поэтому интерес к этой теме крайне высок как в научной среде, так и на государственном уровне. Одной из первых компаний на российском рынке, которая разработала оборудование с применением технологии квантового распределения ключей, является компания «ИнфоТеКС». ИнфоТеКС – признанный эксперт в области криптографии и ведущий отечественный разработчик в области защиты информации. Объединив свои опыт и знания с экспертизой Центра квантовых технологий физического факультета МГУ имени М.В. Ломоносова, компания «ИнфоТеКС» создала инновационные коммерческие продукты, функционирующие на основе КРК – квантовые криптографические системы выработки и распределения ключей ViPNet Quandor и ViPNet QSS. Эти продукты в настоящее время функционируют на действующих сетях передачи данных и находятся в процессе сертификации у регулятора.

ViPNet QSS также используется в рамках совместного проекта ИнфоТеКС и Центра квантовых технологий физического факультета МГУ имени М.В. Ломоносова под названием «Университетская квантовая сеть». Это первый пример непрерывно эксплуатируемой квантово-защищенной сети в образовательной среде. Каналы передачи квантовых состояний объединяют головной офис ИнфоТеКС, кампус МГУ на Ленинских горах, Центр квантовых технологий и здание на Моховой улице в Москве. На данный момент установлено 5 квантовых и 20 телефонных аппаратов, максимальная протяженность квантового канала составляет 30 км. В проекте применяются предсерийные образцы оборудования ViPNet QSS, созданные в соответствии с российскими требованиями к средствам криптографической защиты информации.

В рамках проекта «Университетская квантовая сеть» успешно реализованы все принципы квантового распределения ключей, которые мы рассмотрели ранее. Проект масштабируемый: в перспективе эта квантово-защищенная сеть будет расширяться за счет присоединения других сегментов, а также станет плацдармом для новых исследований в области квантовой криптографии. Развернутая полноценная квантовая сеть позволит специалистам в области криптографии продолжить исследования и эксперименты с КРК уже на новом уровне.