ДОВЕРИЕ К ТЕХНОЛОГИЯМ

Криптография как наука о защите информации насчитывает тысячелетия своего развития. Системы шифрования сообщений существовали еще у древних цивилизаций – в Египте, Китае, Греции и Риме. В средние века появились новые шифры и коды, которые использовались для дипломатической переписки и переговоров, передачи секретных сведений. В конце XIX в. все большую роль в криптографии стала играть математика, что привело к зарождению математической криптографии, а компьютерные технологии подтолкнули последующее усовершенствование методов шифрования и криптоанализа. Разработанный алгоритм открытого ключа, получивший название алгоритма Диффи-Хеллмана, был дополнен криптосистемой Ривеста-Шамира-Адлемана, что позволило не только шифровать сообщения, но и подписывать их с помощью закрытого ключа.

С развитием технологий и потребностей в безопасности данных криптография продолжает свое победное шествие. Так, принципы квантовой механики стали базой квантовой криптографии, которая, основываясь на квантовых явлениях, таких как квантовая суперпозиция и квантовая измеримость, защищает от перехвата информации, обнаруживает любые попытки взлома. Можно сказать, что сегодня это важный инструмент обеспечения безопасности государственных, персональных и финансовых данных, промышленных и научных секретов. Действительно ли квантовая криптография – критически важный аспект защиты от различного уровня информационных угроз и рисков? В чем ее преимущества и недостатки, каковы перспективы? На эти и другие вопросы мы попросили ответить специалистов центра «Квантовая оптика и квантовая информатика» Института физики имени Б.И. Степанова НАН Беларуси.

Дмитрий Хорошко,
старший научный сотрудник центра, приглашенный научный сотрудник лаборатории лазерной, атомной и молекулярной физики Национального центра научных исследований Франции, доктор физико-математических наук

– Квантовое шифрование для записи передаваемого символа состоит в использовании так называемых взаимно дополнительных физических величин. Каждая из них требует определенной настройки измерительного аппарата для распознавания ее значения. Если он настроен на измерение величины Q, а значение передаваемого символа несет дополнительная к ней величина P, то показание аппарата будет случайным, никак не связанным с P. Таким образом, квантовое шифрование происходит на уровне физического носителя информации, которым, как правило, выступает импульс света в оптической линии связи. Примерами взаимно дополнительных физических величин являются частота и время прибытия отдельного фотона, линейная и круговая поляризация света и т.п. Квантовое шифрование дает доступ к записанному символу только тому участнику, чей аппарат настроен на измерение правильной физической величины. Фундаментальное свойство неклонируемости квантовых объектов не позволяет создать две копии исходного носителя квантовой информации для того, чтобы измерить величину Q у одной и P – у другой. Следствием квантового принципа дополнительности является также искажение величины Q при измерении P и наоборот. Таким образом, любой перехват информации, записанной с использованием квантового шифрования, во-первых, дает результат только при случайном совпадении измеряемой величины с величиной записи, и во-вторых, вносит искажения в передаваемый сигнал каждый раз, когда эти величины не совпадают. В технологии, известной как квантовое распределение ключей, это позволяет установить верхнюю границу информации J, доступной для перехвата, по уровню ошибок и потерь в оптической линии связи. В том случае, когда эта информация не превышает информацию I, переданную за сеанс связи, пользователи могут создать криптографический ключ длины K=I-J. Основные области приложения квантового шифрования – те, в которых применяется криптография с открытым ключом: распределение ключей, цифровые подписи, электронное голосование.

– Дмитрий Борисович, не могли бы вы очертить горизонты развития квантовых технологий для криптографии?

– Современная криптография успешно справляется с задачей защиты информации от угроз, существующих сегодня, однако развитие информационных технологий требует постоянного обновления ее методов. Основной вид криптографии нашего времени – криптография с открытым ключом, основанная на так называемых односторонних функциях $y=f(x)$, которые требуют малого числа шагов алгоритма для вычисления y по известному x, но большого числа этих шагов для вычисления x по известному y. Понятия «малого» и «большого» в данном контексте имеют строгие значения – полиномиальный и экспоненциальный законы роста числа шагов при увеличении длины числа x в двоичной записи. Эта длина подбирается таким образом, чтобы вычисление прямой функции занимало доли секунды, а обратной – большой временной промежуток, за который секрет успеет устареть, например сотни лет. С ростом вычислительной мощности обычных классических компьютеров длину блока необходимо увеличивать, чтобы держать время вычисления обратной функции на уровне

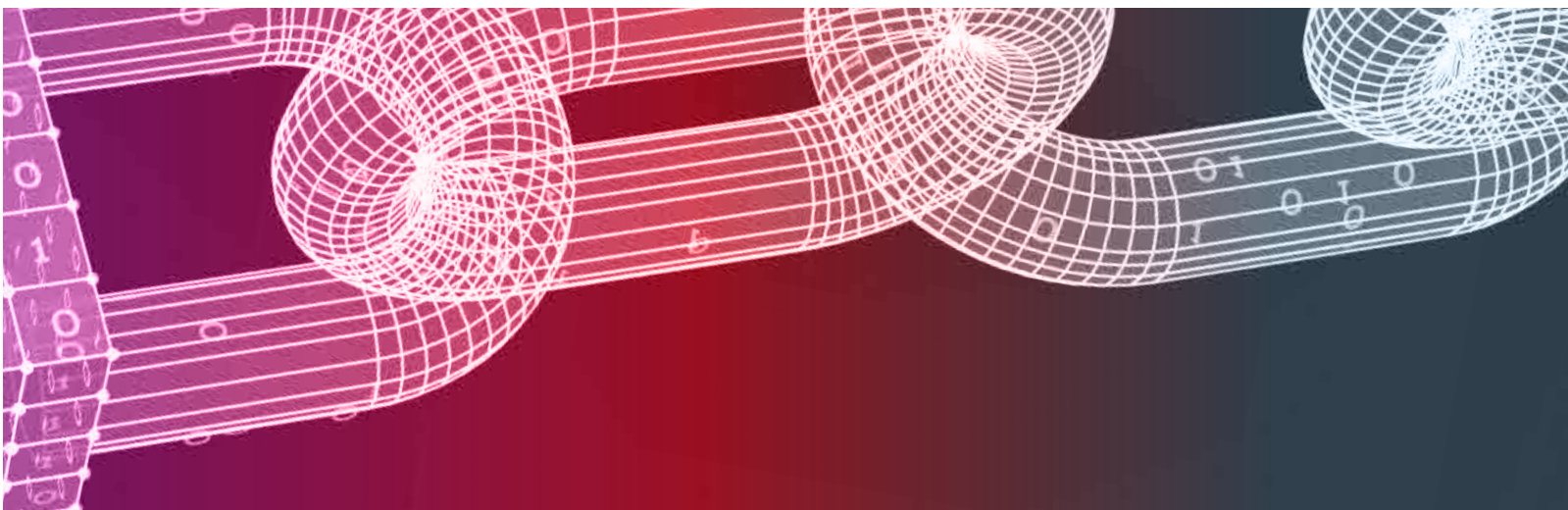
времени устаревания секрета. При этом работа с блоками большей длины не представляет серьезной проблемы ввиду возросшей вычислительной мощности ЭВМ. Основные угрозы для криптографии будущего связаны с развитием теории чисел, которое может привести к открытию более быстрых алгоритмов расчета обратных функций, и с появлением универсальных квантовых компьютеров, когда все современные односторонние функции становятся «двусторонними», так как расчет прямой и обратной функций занимает одинаково «малое» число шагов квантового алгоритма. Потенциально существует два решения проблемы защиты информации в грядущую эпоху. Первое известно как постквантовая криптография и состоит в поиске новых односторонних функций, но представляется временным, так как в любой момент могут возникнуть новые квантовые алгоритмы для быстрого обращения этих функций. Второе решение дают те же квантовые информационные технологии, что привели к созданию квантовых компьютеров. Оно называется квантовой криптографией и основано на квантовом шифровании, которое обеспечивает безусловную защиту информации в том смысле, что она не ставит условием ограниченность вычислительной мощности противника.

– Насколько широко и где используется квантовая криптография?

– Из всех ее разновидностей только квантовое распределение ключей получило массовое применение. Оптоволоконные линии связи, обеспечивающие генерацию безусловно защищенных ключей на дистанции порядка 100 км, доступны на рынке от производителей из Швейцарии, США, Франции и других стран. Основными покупателями являются частные компании, желающие обезопасить свои коммуникации от атаки в будущем, когда квантовые компьютеры смогут расшифровывать криптограммы, созданные на основе криптографии с открытым ключом. Эти криптограммы можно без особого труда перехватить сегодня и сохранить для расшифровки в будущем с помощью квантового алгоритма. Компании, оценивающие срок секретности своих коммуникаций выше, чем ориентировочный срок создания универсальных квантовых компьютеров (10–50 лет),– основной потребитель рынка квантового распределения ключей. Другой пример применения квантовой криптографии – квантовые сети, составленные из «доверенных узлов», соединенных оптоволоконными линиями квантового распределения ключей. Они существуют во многих городах мира (например, квантовые сети Бостона, Женевы, Вены, Токио, Кембриджа, квантовые линии связи Пекин – Шанхай и Москва – Санкт-Петербург) и, как правило, финансируются научными фондами или правительствами этих стран. Небольшая квантовая линия связи, дальностью до 50 км, была создана и в НАН Беларуси при выполнении задания программы Союзного государства «Совершенствование системы защиты общих информационных ресурсов Беларуси и России на 2006–2010 гг.».

– Одна из главных проблем существующих криптографических методов – возможность их взлома с ростом вычислительных мощностей, которые становятся все более доступными с каждым годом, а также появление квантовых компьютеров. Не повлияют ли эти факторы на взлом квантовых криптографических систем и существующих криптографических методов и, соответственно, безусловную безопасность? Насколько серьезна эта угроза?

– Квантовая криптография не использует математическое шифрование и, как следствие, совершенно не чувствительна к вычислительной



мощности противника. Качественный перехват в квантовой линии связи реализуется при помощи высокоточного измерения импульсов света, а не решения сложных математических задач. Даже для самых точных измерительных приборов квантовые принципы дополнительности и неклонируемости определяют фундаментальный предел количества извлекаемой информации при заданном уровне вносимого шума и потерь. Этот предел не может быть превышен с использованием компьютеров любой мощности, в том числе квантовых.

– С какими препятствиями могут столкнуться конечные пользователи?

– Основная проблема современных систем квантового распределения ключей – ограниченная дальность, исчисляемая сотнями километров. Создание крупных сетей с безусловной защитой информации связано с использованием «доверенных узлов», где информация записана обычным классическим образом и может быть скопирована и прочитана противником. Хотя они предполагаются хорошо защищенными от несанкционированного проникновения, сам факт их применения означает, что защита информации больше не основана исключительно на законах квантовой физики, а включает предположение о защищенности узлов. Создание подлинно квантовой сети, в которой сигнал существует в квантовой записи на всем пути от клиента к серверу и обратно, требует разработки квантовых повторителей, способных усиливать квантовый сигнал без его клонирования. К сожалению, прогресс в данной области идет сравнительно медленно, несмотря на наличие проработанного теоретического обоснования подобных устройств. Некоторое неудобство также может быть связано с необходимостью использования волоконно-оптического входа в персональном компьютере для защищенной связи, так как сверхвысокочастотные волны, на которых передается сигнал Wi-Fi, пока не удается сделать носителями квантовой информации должного качества. Хорошим решением может оказаться технология Li-Fi, обеспечивающая беспроводную связь в помещениях на основе оптической связи через открытое пространство, что позволит естественным образом интегрировать системы квантовой криптографии и беспроводной связи.

Вячеслав Чижевский,
ведущий научный сотрудник Центра «Квантовая оптика и квантовая информатика» Института физики им. Б.И. Степанова НАН Беларуси, кандидат физико-математических наук

– Какую функцию в криптографии выполняет квантовая генерация случайных чисел?

– Случайные числа играют важную роль в различных областях науки и техники, и прежде всего в системах защиты информации, в задачах математического моделирования методом Монте-Карло, программировании, в ряде коммерческих приложений. Получение высококачественных случайных чисел критически значимо как для криптографии – математической, стохастической, квантовой, так и в схемах цифровой подписи, алгоритмов шифрования. Они должны обладать свойством истинной случайности, то есть демонстрировать отсутствие каких-либо закономерностей. Для чего, как правило, создаются устройства, в основе работы которых лежат измерения некоторой характеристики физического стохастического процесса с внутренне присущей случайностью и преобразование полученных данных по заданным алгоритмам в последовательность случайных чисел. Существует достаточно большое количество различных физических явлений со сложной динамикой, используемых в качестве источника энтропии для генерации случайных чисел. Прежде всего можно отметить применение хаотической лазерной динамики полупроводниковых лазеров, которые позволяют получить скорости генерации в гигабитном и терабитном диапазоне. Однако подобные генераторы являются устройствами с детерминированной, хотя и сложной динамикой. Это ограничивает их применение для криптографических систем, где противник может использовать суперкомпьютер для расчета этой сложной динамики, установления закономерности в числовой последовательности и как следствие – раскрытия шифра. Подлинная случайность, которую невозможно просчитать на компьютере, свойственна внутренним качествам квантовых процессов, которые лежат в основе реализации ряда квантовых генераторов случайных чисел. Эти устройства создают случайный битовый поток чисто физических явлений с квантовой неопределенностью. В этом контексте генераторы случайных чисел обладают преимуществом безусловной слу-

чайности, что делает их наиболее востребованными для различных применений, к примеру, в медицинской диагностике, банковском секторе для шифрования финансовых транзакций, квантовой физике для тестирования квантовых систем, в различных приложениях, связанных с искусственным интеллектом, робототехникой и другими технологиями. То есть квантовый генератор случайных битов – физическое устройство, генерирующее последовательность классических бит таким образом, что их значение не содержит никакой информации ни о ранее созданных, ни о последующих битах.

– Существует немало методов генерации случайных бит, в том числе на основе физических и квантовых процессов, блокчейна и пр. Какие из них наиболее востребованы?

– Выбор конкретного метода зависит от требуемой степени случайности, скорости генерации и других факторов, связанных с конкретным применением, большинство из них оптические, хотя есть и неоптические методы, основанные, например, на радиоактивном распаде, электронном шуме элементов электронных схем (резисторы, диоды). Среди оптических реализаций можно отметить такие физические явления, как выбор пути одиночным фотоном на светоделителе 50/50, регистрации времени прихода одиночного или ослабленного до уровня одиночных фотонов лазерного излучения. При этом регистрация фотонов производится с помощью детекторов одиночных фотонов либо массивов детекторов. Наличие мертвого времени и послеимпульсов ограничивает скорость генерации случайных бит с использованием подобных детекторов. Тем не менее она может достигать сотен Мбит/с даже в получаемых на лабораторных установках.

Достаточно большое количество исследований квантовых генераторов случайных бит основано на измерении характеристик квантовых случайных процессов с помощью макроскопических детекторов. К ним можно отнести такие процессы, как вакуумные флуктуации, люминесценция в волоконно-оптическом усилителе, фазовый шум в одномодовых полупроводниковых лазерах, флуктуации излучения светоизлучающих суперлюминесцентных диодов, фазовые флуктуации в спонтанно индуцированном вынужденном комбинационном рассеянии, спонтанное параметрическое преобразование частоты, поляризационный шум в многомодовых вертикально-излучающих лазерах и др. Использование макроскопических быстродействующих фотодетекторов позволяет получать скорости генерации значительно выше, чем в работе с дискретными детекторами одиночных фотонов, которые могут достигать десятков Гбит/с.

В последнее время появился ряд коммерческих предложений квантовых генераторов случайных бит, основанных на различных физических принципах, со скоростями генерации от 1 Мбит/с до 1 Гбит/с. Однако, несмотря на значительные успехи в разработке квантовых генераторов случайных бит, дальнейшие исследования направлены на разработку устройств, сочетающих в себе надежность, простоту реализации, высокие скорости, долговечность, низкую стоимость и компактность. Помимо перечисленных свойств, одной из важнейших характеристик квантовой генерации случайных чисел является наличие системы самотестирования генерируемых данных, что позволяет оценивать в реальном масштабе времени энтропию источника случайности и качество генерируемых последовательностей. Это направление исследований – одно из наиболее актуальных в настоящее время. В Центре «Квантовая оптика и квантовая информатика» Института физики им. Б.И. Степанова НАН Беларуси проводились исследования по генерации случайных бит на основе многомодового вертикально-излучающего полупроводникового лазера, в котором интенсивность света на заданной поляризации меняется случайно со временем. В результате был разработан и изготовлен квантовый генератор случайных бит со скоростью генерации до 100 Мбит/с в реальном масштабе времени.

Квантовые генераторы случайных чисел имеют большой потенциал для использования в различных областях, включая криптографию, статистику, моделирование и тестирование программного обеспечения.

Исходя из задач, которые решает квантовая криптография благодаря надежности, базирующейся на использовании фундаментальных законов квантовой механики, она может стать одной из основных технологий будущего в области защиты конфиденциальности информации, в том числе передачи метаданных. Безусловно, сегодня квантовые криптосистемы требуют дорогостоящего оборудования и высокой технической квалификации сотрудников для работы с ними, но возможно, вскоре появятся более простые и дешевые методы реализации квантовых криптосистем, что позволит использовать эту технологию в широком спектре приложений. ИИ

Жанна КОМАРОВА