ПРАКТИЧЕСКИЕ КВАНТОВЫЕ КОММУНИКАЦИИ

ЮРИЙ КУРОЧКИН
РУКОВОДИТЕЛЬ ЛАБОРАТОРИИ КВАНТОВЫХ КОММУНИКАЦИЙ

Мы развиваем технологию квантовых коммуникаций, в частности квантовой криптографии и квантового распределения ключа. В лекции я хочу рассказать, почему важно и интересно развивать эту технологию, а главное — где она применяется, каким компаниям она интересна и как они собираются применять ее в своем бизнесе.

ПОЧЕМУ НУЖНЫ КВАНТОВАЯ КРИПТОГРАФИЯ И КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА?

Основной угрозой для современной криптографии является квантовый компьютер. Он потенциально может взломать существующие методы защиты информации.

Квантовая криптография же обещает защиту на уровне законов физики, а не на уровне вычислительной сложности.

Поэтому нам нужно внедрить квантовую криптографию с учетом 2-х интервалов времени:

- Время внедрения квантовой криптографии
- Время, необходимое для защиты информации

Сумма этих периодов должна быть меньше ожидаемого времени появления квантового компьютера.

Сейчас в мире мы видим ситуацию, когда это условие начало выполняться. Множество групп и компаний стало работать в этом направлении.

АЛЬТЕРНАТИВЫ КВАНТОВОЙ КРИПТОГРАФИИ

На самом деле, альтернатив квантовой криптографии практически нет. У нас есть защита информации на уровне вычислительной сложности (ассиметричные ключи). Есть еще доверенный курьер, который, с одной стороны, является хорошим решением, но при этом мы вносим в систему человеческий фактор и должны доверять этому человеку.

И, наконец, есть квантовое распределение ключа, где этим самым доверенным курьером является элементарная частица — одиночный фотон. В соответствие с законами физики, любая попытка прочтения информации, передаваемой с помощью одиночного фотона, неизбежно ее изменяет. Соответственно, мы можем проверить, была ли попытка перехвата ключа или нет. Если ее не было, то мы можем использовать этот ключ для защиты информации.

ВОЗНИКАЮЩИЙ РЫНОК

Сейчас уже существует рынок квантовой криптографии, на котором есть международные стартапы — IDQ, QuantumCTek.

В России также существуют 3 команды, которые занимаются разработкой, и я представляю одну из них — QRate. Мы работаем совместно с Газпромбанком и проводим опытные демонстрации со Сбербанком.

КАК ВЫГЛЯДИТ В РЕАЛЬНОЙ ЖИЗНИ КВАНТОВАЯ КРИПТОГРАФИЯ?

На самом деле это телекоммуникационное оборудование со специфическими оптическими схемами и протоколами. То есть, если мы откроем систему и посмотрим внутрь, то мы увидим стандартные оптоволоконные элементы, используемые в Телекоме.

Тем не менее, эти элементы работают на уровне сигнала порядка 1 фотона на импульс или даже меньше.

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ

Перспективным направлением является технология планарных волноводов, когда оптоволокно можно уменьшить и сделать на маленьком чипе, соответственно, уменьшив все системы.

Как я уже сказал, за рубежом есть проекты квантовой криптографии. Мы представили устройство квантового распределения ключа, и в основном это устройство, работающее в оптоволокне, т. к. основные потребители обмениваются информацией через оптоволоконные линии.

Тем не менее, перспективным направлением является еще и спутниковая квантовая криптография, когда мы можем запустить спутник, и он обменивается ключом с произвольными точками на поверхности Земли.

Почему это важно? Потому что в оптоволокне сигнал теряется, и сейчас, при современных технологиях, мы ограничены расстоянием порядка 100 км. В лабораториях, конечно, есть демонстрации и до 400 км, но это непрактичные демонстрации. А спутником можно соединить 2 произвольные точки на поверхности Земли, потому что потери, вносимые столбом атмосферы по вертикали, ковалентны 10 км на уровне моря.

ПРИЛОЖЕНИЯ

Первый продукт, над которым мы начали работать, нацелен на научно-образовательные приложения. Почему? Потому что мы верим в появление этой технологии на рынке, и мы должны готовить кадры. Мы должны учить людей основам квантовой криптографии, физики, телекоммуникации и защиты информации.

Следующий набор приложения не ограничивается только защитой информации. Есть еще проблемы аутентификации.

Еще одно направление — распределенное хранение данных. Дело в том, что надо защищать данные не только в процессе передачи, но и во время хранения. Для этого мы можем распределить данные по нескольким серверам и построить систему таким образом, что невозможно будет получить никакой полезной информации, не получим доступ, скажем, сразу к 3-ем из 5-ти серверов.

Следующее направление — блокчейн. Дело в том, что блокчейн как раз подвержен атакам квантового компьютера. В первую очередь, его аутентификация. То есть, взломав цифровую подпись с помощью квантового компьютера, кто-то может расплачиваться с вашего кошелька. В случае защищенного блокчейна этот недостаток закрывается квантовым распределением ключа.

Для демонстрации этой технологии мы построили квантовую сеть и продемонстрировали ее совместно с Газпромбанком.

Этой технологией также интересуются крупные международные компании, например, PWC. У них есть продукты по анализу кибербезопасности больших компаний, и уже сейчас для этого требуются квантово защищенные решения.

ПОЛЕВОЕ ИСПЫТАНИЕ В СБЕРБАНКЕ

Мы в первые в России продемонстрировали полный цикл распределения квантового ключа между 2-мя офисами и использование этого ключа в классическом шифраторе для того, чтобы обновлять ключи не вручную и достаточно редко, а часто и с использованием квантового распределения ключа. Это позволяет многократно повысить уровень защиты информации между офисами Сбербанка.

НА ПУТИ К КВАНТОВОМУ ИНТЕРНЕТУ

Следующим шагом развития технологии на горизонте 3-5 лет является уменьшение и удешевление устройств.

Для чего это важно? Для расширения различных рынков. И точно так же, как оптоволоконный интернет пришел к нам в квартиры, так и квантовое распределение ключа может прийти к конечному пользователя для того, чтобы пользователь мог получать различные услуги с защитой квантовым ключом.

Следующий горизонт — 10-15 лет, где мы ожидаем появление полноценных квантовых компьютеров. Они должны будут общаться друг с другом, а для этого им нужно будет передавать квантовые состояния. Поэтому сейчас так важно изучать, как приготовить квантовые состояния, как их правильном передать и исправить ошибки. И таким образом мы сможем шагнуть к квантовому интернету.