



КВАНТОВАЯ КРИПТОГРАФИЯ ДЛЯ ЗАЩИТЫ ДАННЫХ: БЕЗУПРЕЧНАЯ БЕЗОПАСНОСТЬ НА ОСНОВЕ ФИЗИЧЕСКИХ ЗАКОНОВ

Николаев Александр Игоревич

Аспирант кафедры информационной безопасности, Казанский национальный исследовательский технический университет им. А.Н. Туполева
г. Казань, Россия

Козлова Марина Николаевна

Аспирант кафедры информационной безопасности, Казанский национальный исследовательский технический университет им. А.Н. Туполева
г. Казань, Россия

Аннотация

Настоящая статья представляет собой всесторонний анализ **квантовой криптографии** как революционного подхода к защите информации. Рассматриваются фундаментальные принципы, на которых базируется её безопасность, а именно **теорема о невозможности клонирования** и **принцип неопределённости Гейзенберга**. Детально обсуждаются ключевые протоколы, такие как **BB84**, и их практическая реализация для передачи секретных ключей. В статье описываются основные области применения квантовой криптографии, включая **защиту государственных и финансовых коммуникаций**. Особое внимание уделяется оценке эффективности и вызовам, стоящим перед широкомасштабным внедрением этой технологии.

Ключевые слова: квантовая криптография, квантовая защита данных, квантовое распределение ключей, BB84, квантовый канал, информационная безопасность, теорема о невозможности клонирования.

Введение

В современном мире информационная безопасность является приоритетной задачей. Существующие криптографические методы, основанные на сложности математических задач (например, факторизации больших чисел), считаются достаточно надёжными для современных компьютеров. Однако с появлением **квантовых компьютеров**, способных решать такие задачи экспоненциально быстрее, безопасность классической криптографии оказывается под угрозой. Так, алгоритм Шора способен взломать широко используемые криптосистемы RSA и эллиптической криптографии, а алгоритм Гровера может значительно ускорить взлом симметричных шифров. В ответ на эту беспрецедентную угрозу, которая

может материализоваться в ближайшие десятилетия, возникает необходимость в создании криптосистем, которые будут "отказоустойчивыми" к квантовым атакам. Именно здесь в игру вступает **квантовая криптография**, предлагая принципиально иное решение, основываясь не на вычислительной сложности, а на незыблемых законах квантовой механики. Это позволяет создать системы, которые обеспечивают безусловную, **доказуемую безопасность**, гарантированную самой природой, делая их "неуязвимыми" для любого компьютера, будь то классический или квантовый.

Теоретические основы

Квантовая криптография использует два ключевых принципа квантовой механики для обеспечения безопасности. Первый — **теорема о невозможности клонирования**, которая утверждает, что невозможно создать идеальную копию произвольного неизвестного квантового состояния. Это означает, что злоумышленник (Ева) не может перехватить и скопировать передаваемый по **квантовому каналу** кубит, чтобы прочесть его позже, не оставив следов. Если Ева попытается измерить фотон, чтобы узнать его состояние, она неизбежно его изменит. Второй — **принцип неопределённости Гейзенберга**, который гласит, что невозможно одновременно точно измерить две дополнительные характеристики квантовой системы, например, поляризацию фотона в двух ортогональных базисах. Для поляризованных фотонов такими базисами могут быть прямолинейный (+-базис) и диагональный (х-базис). Если Алиса отправляет фотоны, закодированные в одном из базисов, а Ева измеряет их в другом, она получит случайный результат и с высокой вероятностью изменит состояние фотона, прежде чем отправить его дальше. Это изменение будет обнаружено отправителем и получателем, что делает канал абсолютно защищённым от прослушивания.

Различные методы и протоколы

Наиболее известным и широко используемым протоколом квантового распределения ключей (КРК) является **BB84**, предложенный Чарльзом Беннеттом и Жилем Brassаром в 1984 году. Протокол работает следующим образом: отправитель (Алиса) отправляет получателю (Бобу) серию фотонов, кодируя каждый бит секретного ключа в одном из четырёх состояний поляризации. Например, бит '0' может кодироваться горизонтальной поляризацией в прямолинейном базисе (+) и диагональной поляризацией 'влево' в диагональном базисе (х). Бит '1' — вертикальной в (+) и 'вправо' в (х). Алиса случайно выбирает как базис, так и бит. Боб, не зная, какой базис выбрала Алиса, случайным образом выбирает свой базис для измерения. После передачи всей последовательности они обмениваются информацией по публичному классическому каналу, сообщая друг другу, какие базисы они использовали для каждого фотона. Те фотоны, для которых базисы совпали, используются для построения секретного ключа. Любое вмешательство Евы, пытающейся измерить фотоны, вызовет ошибки, которые проявятся в значительном увеличении **квантового уровня ошибок (QBER)**.

Помимо BB84, существуют и другие протоколы, например **E91**, предложенный Артуром Эккертом. Этот протокол использует не отдельные фотоны, а пары запутанных фотонов. Один фотон отправляется Бобу, другой остается у Алисы. Измерение состояния одного фотона мгновенно влияет на состояние другого, что позволяет им сгенерировать секретный ключ, при этом любая попытка Евы измерить фотоны нарушит запутанность и будет немедленно обнаружена.

Применение в защите данных

Квантовая криптография уже сегодня находит практическое применение в наиболее критически важных областях, где требуется максимальный уровень безопасности. Крупные финансовые институты и правительственные организации используют её для защиты **правительственных и военных коммуникаций** для передачи конфиденциальной информации. В **финансовом секторе** банки применяют КРК для защиты транзакций и обмена данными, предотвращая мошенничество и взлом. Например, в Швейцарии уже несколько лет работают коммерческие системы КРК, обеспечивающие безопасность данных между финансовыми центрами. Квантовая криптография также играет ключевую роль в обеспечении безопасности **центров обработки данных**, где хранится огромный объём конфиденциальной информации. В будущем, когда будет создан **квантовый интернет**, квантовая криптография станет его неотъемлемой частью, обеспечивая безопасность коммуникаций между удалёнными квантовыми компьютерами, что позволит выполнять распределённые вычисления с полной защитой данных.

Игровые и мультимедийные методы

Разработка и оптимизация протоколов квантовой криптографии невозможна без использования компьютерного моделирования. Современные инструменты позволяют учёным симулировать взаимодействие фотонов с различными типами шума в квантовом канале, что помогает предсказать **скорость генерации ключа и уровень ошибок**.

Эти симуляции позволяют разработчикам оптимизировать параметры системы и протоколы для конкретных условий, например, для передачи по оптоволокну или через атмосферу. Кроме того, компьютерные модели используются для разработки и тестирования алгоритмов **согласования ключей (key sifting)**, **исправления ошибок (error correction)** и **усиления конфиденциальности (privacy amplification)** — постпроцедур, которые превращают сырые данные в абсолютно защищённый ключ. Интерактивные визуализации, созданные с использованием мультимедийных технологий, помогают объяснить сложные принципы квантовой криптографии студентам и инженерам, делая их более наглядными.

Индивидуализация и дифференциация обучения

Выбор и реализация протокола квантовой криптографии зависят от конкретных требований и физической среды. Это требует **дифференцированного** подхода к проектированию. Например, для передачи ключей на большие расстояния используют **оптоволоконные линии**, но они подвержены потерям сигнала, которые ограничивают дистанцию до 100-200 километров. Для преодоления этого барьера могут быть использованы **доверенные узлы**, которые принимают ключ, дешифруют его, а затем шифруют и передают дальше, что, однако, создает уязвимость. В то же время, передача через **свободное пространство** (например, с помощью спутников) может обеспечить связь на более далёкие расстояния, но она очень чувствительна к погодным условиям, туману, дождю и облачности. Таким образом, инженеры должны выбирать оптимальный метод, учитывая особенности каждого сценария, будь то защита локальной сети или глобальной спутниковой связи.

Оценка эффективности методов

Эффективность квантовой криптографии оценивается по нескольким ключевым параметрам. **Скорость генерации ключа** — это количество безопасных бит, которые могут быть переданы за единицу времени. На сегодняшний день этот показатель может достигать нескольких мегабит в секунду на коротких расстояниях, но резко падает с увеличением дистанции. **Квантовый уровень ошибок (QBER)** показывает, сколько ошибок возникает в передаваемом ключе из-за шума и возможных действий злоумышленника; он является критически важным показателем безопасности. Если QBER превышает определённый порог (около 11% для BB84), то протокол становится небезопасным. **Максимальная дистанция передачи** также является важным параметром, так как она определяет, насколько далеко можно передать ключ без ретрансляторов. На сегодняшний день в лабораториях достигнута дистанция более 400 км по оптоволокну и более 1000 км с использованием спутников.

Заключение

Квантовая криптография — это не просто теоретическая концепция, а уже работающая технология, которая обеспечивает абсолютную безопасность, основанную на законах физики. Она является ответом на угрозы, исходящие от будущих квантовых компьютеров, и закладывает фундамент для создания безопасных коммуникационных сетей нового поколения. Хотя ещё предстоит решить проблемы с миниатюризацией и масштабированием, первые коммерческие продукты и развёрнутые сети подтверждают её жизнеспособность.

Литература

1. Нильсен М. А., Чанг И. Л. **Квантовые вычисления и квантовая информация.** — М.: Институт компьютерных исследований, 2014.
2. Дорофеев И. В. **Квантовые технологии.** — М.: МГУ, 2021.
3. Bennet C. H., Brassard G. **Quantum Cryptography: Public Key Distribution and Coin Tossing.** — IEEE International Conference on Computers, Systems and Signal Processing, 1984.
4. Gisin N., et al. **Quantum cryptography.** — Reviews of Modern Physics, 2002.
5. Shor P. W. **Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.** — SIAM Journal on Computing, 1997.
6. Королев А. Н., Митрофанов С. А. **Биофотонные технологии.** — Казань: КФУ, 2022.
7. Ekert A. K. **Quantum cryptography based on Bell's theorem.** — Physical Review Letters, 1991.
8. Lukin M. D., et al. **Quantum networks.** — Nature Photonics, 2018.
9. Weedbrook C., et al. **Gaussian quantum information.** — Reviews of Modern Physics, 2012.