Автор:

Наумчик Анастасия Сергеевна

ученица 10 класса

Научный руководитель:

Арьяева Людмила Владимировна

канд. пед. наук, методист

ГБОУ лицей №590 Красносельского района Санкт-Петербурга

г. Санкт-Петербург

ГЕНЕЗИС КВАНТОВОЙ ИНФОРМАТИКИ

Аннотация*: с древних времен людям необходимо зашифровывать информацию. На передаче секретных сообщений основываются многие аспекты нашей жизни – например, передача конфиденциальной информации компаний (отчеты, бухгалтерская база и т. д.) и персональных данных (таких как личная переписка, фотографии). С развитием человечества развиваются и способы шифрования. На современном этапе создан новый вектор – квантовая информация – «направление физики, включающее в себя вопросы квантовых вычислений, квантовых компьютеров, квантовой телепортации и квантовой криптографии». Преимущества использования квантовой информации заключается в том, что, используя законы квантовой механики, можно повысить уровень защиты данных и ускорить математические вычисления. В статье будут рассмотрены некоторые аспекты квантовой информатики: квантовое шифрование; квантовый компьютер; квантовая хэш-функция и квантовые цифровые подписи; квантовое распознавание лиц; квантовая визуальная криптография; квантовая телепортация; квантовые деньги.*

Ключевые слова*: квантовое шифрование, BB84, квантовая информация, квантовый компьютер.*

Квантовое шифрование основывается на теореме о запрете клонирования (невозможно точно скопировать состояние квантового объекта без его

изменения) и невозможности достоверно различить неортогональный базис (непрямоугольный вектор) состояния.

Идея использовать законы квантовой физики для защиты информации впервые была высказана Стефаном Вейснером в 1970 году. Позже, в 1984 году, Чарльз Беннетт из IBM и Жиль Брассар из Монреальского университета предположили, что фотоны могут быть использованы в криптографии. Для представления нулей и единиц они решили взять фотоны, поляризованные в различных направлениях, и предложили простую схему квантового распределения ключей шифрования, названную ими BB84 [5].

Принцип работы BB84. Первый этап квантового распределения ключей называется первичной квантовой передачей. Сначала Алиса (типичное имя отправителя при описании криптографических систем) посылает Бобу (получателю) последовательность фотонов (квантов света), поляризация которых выбрана случайно и может быть 0°, 45°, 90°, 135°. Боб случайно решает, каким образом их замерять – перпендикулярно или диагонально. По открытому (незащищенному) каналу Боб объявляет Алисе, какой тип измерений он использовал; Алиса объявляет, в каких случаях использовался правильный способ измерения. Оставшиеся после сверки виды поляризации являются секретной информацией, переданной Алисой Бобу.

Следующий этап – оценка попыток перехвата информации. Это может производиться путем сравнения случайно выбранных подмножеств или, что более эффективно, проверкой на четность – сравнением каждого четного бита. Если сравнение выявляет большой процент ошибок, считается, что производился перехват информации, и квантовая передача начинается сначала.

Если сравнение не выявляет перехвата информации, Алиса и Боб принимают фотоны с 0° или 45° за двоичный «0», а 90° или 135° – за двоичную «1».

Согласно одному из следствий квантовой механики – принципу неопределенности Гейзенберга, злоумышленник не может одновременно замерить прямоугольную и диагональную поляризацию. Если же он произведет измерение для какого-либо фотона и перешлет Бобу свой результат, это приведет к большему

количеству ошибок, т.к. согласно одному из основополагающих принципов квантовой механики, нельзя измерить состояние без изменения других состояний [5].

Другие алгоритмы квантового шифрования. Общий принцип этих алгоритмов основан на схеме BB84.

1. Протокол, использующий 2 состояния.

В 1992 году Чарльз Беннетт заметил, что 4 состояния (0°, 45°, 90°, 135°) – больше, чем необходимо для работы алгоритма. Использование двух состояний, неортогональных друг другу (т. е. 0° и 45° или 90° и 135°), является более легким в постановке эксперимента, однако, в практическом использовании оно невыгодно. Такой протокол менее устойчив к перехвату информации и атакам.

2. Протокол, использующий 6 состояний.

Такой протокол содержит 3 базиса (в BB84 – 2: перпендикулярный и диагональный), следовательно, шанс того, что Боб выберет верный базис – $\frac{1}{3}$. Однако такой протокол уменьшает процент максимальной информации, которая может быть получена злоумышленником.

3. ЭПР протокол.

Этот протокол, предложенный Артуром Экертом в 1991 году, основывается на парадоксе Энштейна – Подольски – Розена [6]. Идея протокола состоит в замене канала между Алисой и Бобом на канал, переносящий 2 кубита (квантовый бит) из общего источника – один к Алисе и один к Бобу. Источник отправляет кубиты в одинаковом состоянии, выбранном случайно из четырех (как и в BB84). Алиса и Боб замеряют состояния в одном из двух базисов, случайно и независимо друг от друга. Источник объявляет базис, Алиса и Боб сохраняют данные, если базисы совпадают.

Если использовать перепутанные состояния (связь между квантами сохраняется независимо от расстояния), то, когда Алиса и Боб используют один и тот же базис (примерно в половине случаев), их результаты идентичны.

Практическое применение других алгоритмов квантового шифрования, которые основаны на схеме BB84, невыгодно:

– при увеличении вероятности угадывания правильного базиса упрощается работа для злоумышленника;

– подготовительные процедуры затратны [9].

Проблемы и недостатки. Существуют проблемы при подготовке оборудования (лазеры могут выпускать не единичные фотоны, а мульти-фотоны; импульс может затухать и пр.) и детектировании фотонов (детектор может быть рассинхронизирован). Для решения подобных проблем необходима настройка, установка светоделителя, смена источника и др. Кроме того, из-за технических сложностей максимальная длина квантового канала сильно ограничена по сравнению с другими каналами передачи. Окружающая среда может создавать помехи в канале [8].

Для более эффективной защиты данных можно скомбинировать квантовое и классическое шифрование. Для этого необходимо разрабатывать специальные технологии, трудность которых заключается в поиске баланса между названными видами шифрования [11].

Иные направления квантовой информатики. Квантовое шифрование – не единственное применение квантовой физики в современных технологиях.

Квантовый компьютер. «Квантовая гонка» – погоня за созданием квантового компьютера – стремительно набирает обороты. Квантовый компьютер позволяет ускорить решение таких задач, как:

– факторизация (разложение чисел на множители) за полиноминальное (значительно меньшее) количество шагов (и времени). На большой вычислительной сложности задачи факторизации основывается стойкость некоторых алгоритмов шифрования с открытым ключом (например, RSA), которые станут бесполезными;

– поиск элементов среди базы данных, каждый из которых может давать ответ (да/нет) на запрос;

– проблема коммивояжера (поиск самого короткого пути из возможных).

Главные проблемы при создании квантового компьютера – быстрый распад суперпозиционных состояний, с помощью которых производятся вычисления

(квантовая декогерентность) и поиск конкретных процессоров, выполняющих вычисления [2].

Появление квантового компьютера приведет к тому, что эффективная длина ключа криптосистемы уменьшится в 2 раза, из чего следует, что многие криптосистемы (прежде всего асимметричные) станут нестойкими [3].

Квантовая хэш-функция, квантовые цифровые подписи. Хэш-функция – функция, используемая для преобразования данных произвольного размера в данные фиксированного размера. Она используется для шифрования паролей в базах данных и создания электронных подписей – особых реквизитов документа, позволяющих удостовериться в целостности информации и авторстве создателя подписи.

Применяя законы квантовой механики, можно получить квантовые хэш-функции и квантовые цифровые подписи. Их преимущество перед классическими – в невозможности коллизий (одинаковых значений хэш-функций) на квантовом уровне и, следовательно, в более эффективном использовании ресурсов. Например, при использовании 10 кубитов (квантовых битов) можно будет зашифровывать сообщения длиной до 1000 бит [1].

Квантовое распознавание лиц. Распознавание лиц необходимо в таких отраслях, как охранные системы, криминалистика, шифрование данных и т. д.

Использование квантовых алгоритмов в сочетании с классическими дает эффективный метод, позволяющий преодолеть некоторые недостатки современных систем распознавания (погрешности при работе с большими базами данных, изменении ракурса, возрастными изменениями и т. д.). Применение квантовых вычислений – совершенно новый подход в распознавании лиц, почти не зависящий от помех окружающей среды и статичности объекта [7].

Квантовая визуальная криптография. Визуальная криптография – шифрование текста или изображения путем разбиения исходного изображения на несколько шифрованных. Шифрованные изображения не дают никакой информации об исходном, кроме его размера. При их наложении друг на друга можно получить первоначальное изображение.

Расширение классической схемы визуальной криптографии законами квантовой физики позволяет увеличить скорость кодирования/декодирования изображений, что позволит повысить безопасность видеосвязи [7].

Квантовая телепортация – возможность переноса квантового состояния одного объекта на другой. Ключевую роль в квантовой телепортации играют перепутанные фотоны. Данная возможность подтверждена экспериментально в 1997 году. Реализация квантовой телепортации дает новые возможности в решении проблемы быстрого разрушения суперпозиционных состояний, что является одной из главных проблем при создании квантового компьютера [2] «На базе каналов телепортации квантовых состояний в дальнейшем могут быть созданы квантовые сети, которые смогут использоваться как для передачи квантовой и классической информации, так и для организации распределенных квантовых вычислений» [4, с. 13].

Квантовые деньги. На основе законов квантовой физики предложена модель квантовых денег. При использовании квантовых состояний для представления денежных средств можно решить проблемы электронных денег. Теорема о запрете клонирования позволяет предотвратить их кражу и подделку. По прогнозам, к 2038 году квантовые деньги полностью заменят обычные [10].

Заключение. Развитие квантовой информатики происходит чрезвычайно быстро. Её практическое применение в различных отраслях принесет преимущества в скорости обработки данных, безопасности передачи информации и др. Применение квантового шифрования на практике поднимет методы защиты информации на новый уровень

Появление квантового компьютера изменит многие аспекты современной жизни. Предполагается, что, будут найдены оптимальные пути для доставки товаров. Некоторые современные алгоритмы защиты данных станут бесполезными. Проблемы создания квантового компьютера могут быть решены с помощью квантовой телепортации. Использование квантовых хэш-функций позволит работать с большими объемами данных более эффективно. Основанные на квантовых хэш-функциях, квантовые цифровые подписи обеспечат

конфиденциальность и целостность информации. Применение квантовых вычислений в распознавании лиц позволит преодолеть проблемы, связанные с изменением ракурса, помехами окружающей среды и др.

Список литературы

1. Аблаев Ф. О квантовом хешировании в постквантовой криптографии / Ф. Аблаев, М. Аблаев // Itsec.Ru. – 2016 [Электронный ресурс]. – Режим доступа: http://www.itsec.ru/articles2/crypto/o-kvantovom-heshirovanii-v-postkvantovoy-kriptografii/ (дата обращения: 15.01.2018).

2. Килин С.Я. Квантовая информация // Успехи физических наук. – 1999. – №5. –С. 507–527.

3. Ключарев П.Г. Квантовый компьютер и криптографическая стойкость современных систем шифрования // Естественные науки. – 2007. – №2. – С. 113–120.

4. Корольков А.В. О некоторых прикладных аспектах квантовой криптографии в контексте развития квантовых вычислений и появления квантовых компьютеров // Вопросы кибербезопасности. –2015. – №1 (9). – С. 6–13

5. Красавин В. Квантовая криптография // Online библиотека padaread.com [Электронный ресурс]. – Режим доступа: http://padaread.com/?book=9794 (дата обращения: 03.11.2017).

6. Рыбаков Ю.П. Эйнштейна – Подольского – Розена парадокс // Энциклопедия физики и техники. – 2010 [Электронный ресурс]. – Режим доступа: http://femto.com.ua/ articles/part_2/4613.html (дата обращения: 12.01.2018).

7. Ульянов С.В. Квантовое распознавание лиц и квантовая визуальная криптография: модели и алгоритмы / С.В. Ульянов, С.П. Петров // Системный анализ в науке и образовании. – 2012. – №1. – С. 1–17.

8. Gilles Brassard, Norbert Lütkenhaus, Tal Mor, Barry C. Sanders. Limitations on Practical Quantum Cryptography // Physical Review Letters. – 2000. – №6. – С. 1330–1333.

9. Nicolas Gisin, Gr´egoire Ribordy, Wolfgang Tittel and Hugo Zbinden. Quantum cryptography // CORNELL UNIVERSITY LIBRARY. – 2008 [Электронный

ресурс]. – Режим доступа: http://arXiv.org/abs/quant-ph/0101098v2 (дата обращения: 19.11.2017).

10. Stebila D., Mosca M. Uncloneable Quantum Money // Institute for Quantum Science and Technology at the University of Calgary. – 2006 [Электронный ресурс]. – Режим доступа: http://www.iqis.org/events/cqisc06/papers/Mon-1130-Stebila.pdf (дата обращения: 20.11.2017).

11. Valerio Scarani, Christian Kurtsiefer. The black paper of quantum cryptography: real implementation problems // CORNELL UNIVERSITY LIBRARY. – 2012 [Электронный ресурс]. – Режим доступа: http://arxiv.org/abs/0906.4547v2 (дата обращения: 10.11.2017).