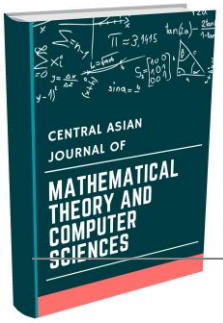

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.centralasianstudies.org

Volume: 03 Issue: 12 | Dec 2022 ISSN: 2660-5309

КОЛИЧЕСТВО В КРИПТОГРАФИИ КЛЮЧИ РАСПРЕДЕЛЕНИЕ ПРИНЦИПЫ РАБОТЫ ПРОТОКОЛОВ, ИСПОЛЬЗУЕМЫХ ПРИ РЕШЕНИИ ЗАДАЧ

Худайкулов Зариф Торакулович

Ташкентский университет информационных технологий имени Мухамада ал-Хоразми

Саидахмедов Элдор Исломович

Институт предпринимательства и педагогикиим. Денова ш

techmespeaker@gmail.com

Аннотация

В этой статье я сначала объясню некоторые принципы квантовой механики, затем перейду к обсуждению основ квантовых криптографических протоколов BB84, B92 и протоколов на основе ЭПР, и, наконец, я завершу статью несколькими комментариями о стратегиях отслеживания. и практическое применение квантовой криптографии.Я рассмотрю некоторые технологические вопросы, которые необходимо решить перед внедрением.

ARTICLEINFO

Article history:
Received 23 Oct 2022
Revised form 24 Nov 2022
Accepted 26 Dec 2022

Ключевые слова: *Квантовая механика , Квантовая криптография, BB84, B92, бит, кубит.*

---***---

В этой статье мы обсудим одну из самых важных проблем в криптографии, проблему распределения ключей, как осуществляется этот процесс и как отправитель и получатель согласовывают секретный ключ, гарантируя, что никакая третья сторона не сможет его получить. информацию о ключе.Хотя ключевая криптография предлагает такие алгоритмы, как RSA или Elgamal для решения этой проблемы, до сих пор нет математического доказательства того, что не существует полиномиального алгоритма для взлома ключа этих алгоритмов.Мы получим понимание существующих квантовых алгоритмов для факторизация и вычисления дискретного логарифма, фундаментальная проблема распределения квантовой связи, процедура, используемая для согласования безопасного ключа с использованием квантовой связи, «квантовое распределение ключей» и «квантовая криптография единства».

важнейших особенностей квантовой криптографии является то, что третья сторона не может получить достоверную информацию путем прослушивания квантового канала, и любая попытка сделать это будет неэффективной. Именно эта последняя особенность делает квантовую криптографию особенной, поскольку ни один из классических криптографических протоколов не имеет этой функции.

Истоки квантовой криптографии можно проследить до работы Стивена Визнера в 1970-х годах, который предложил использовать отдельные квантовые состояния в качестве поддельных денег. Виснер опубликовал свои идеи в 1983 году , которые Беннетт и Брассард использовали для создания

первого квантового криптографического протокола, известного как протокол BB84 в 1984 году. Однако только в 1989 году стало возможным реализовать его в лаборатории, где с помощью поляризованных фотонов был создан защищенный канал связи длиной 32 см. В начале 90-х был достигнут прогресс, когда Эккерт предложил новый протокол, основанный на Парадокс Эйнштейна, Подольского, Розена (ЭПР). Примерно в то же время, в 1992 году, Беннет опубликовал протокол под названием BB92, который можно было реализовать с использованием однофотонного шума.

технологические проблемы остаются серьезной проблемой в современных условиях, область квантовых вычислений и квантовой криптографии добилась быстрого прогресса в решении этих проблем.

Методы

Принципы квантовой механики. Мы начнем обсуждение квантовой механики с введения квантового бита, называемого кубитом. Самая большая разница между классическим компьютерным битом и кубитом заключается в том, что кубит может быть одновременно 0 с 1. Теперь мы используем состояния поляризации фотона для реализации кубита.

Например, фотон может находиться в вертикально поляризованном квантовом состоянии $|\updownarrow|$, которое мы обозначаем как однобитовое изображение, или в горизонтально поляризованном квантовом состоянии $|\leftrightarrow|$, которое мы обозначаем как нуль-битное изображение. Фотон также может существовать в линейной комбинации этих состояний, которую мы называем суперпозицией. В этом случае результирующее состояние представляет собой и ноль, и бит одновременно.

Обозначение Дирака: квантовые состояния представляют собой H элементов гильбертова пространства, обычно называемых кетами. Строки отмечены символом, где символ — это название страны, которую мы хотим дать. Гильбертово пространство определяется как векторное пространство над комплексными числами C со скалярным произведением.

$$(,): H \times H \to C$$

было полно по сравнению с нормой

$$||u|| = \sqrt{(u,u)}$$

Следовательно, кубит — это всего лишь кет в двумерном гильбертовом пространстве. Например, если 0 и 1 обозначают произвольный ортонормированный базис двумерного гильбертова пространства, то каждый кубит можно записать как

$$|qubit) = \alpha|0) + \beta|1) \text{ и } \alpha, \beta \in C$$

любой скалярный мультиплет представляет собой одно и то же состояние квантовой системы , мы можем считать, что кубит нормирован на единицу длины, другими словами, мы можем себя ограничить.

$$a^2 + b^2 = 1$$

Рассматривая гильбертово пространство, H^*мы можем определить H^*его как $H^* = Hom(H, C)$ Гильбертово пространство, называемое вторичным пространством H , обозначает множество всех линейных отображений из H в C . Элементы H называются бюстгальтерами и обозначаются (символ). Теперь мы можем определить $H^* \times H \to C$билинейное отображение $((\psi|)(|\psi))) = (\psi|\psi) \in C$, вызвав круглые скобки последнего выражения. Кроме того, если φ_i— ортонормированный базис гильбертова пространства, φ_iто H — ортонормированный базис бинарного пространства.

Он связан через два основания.

$$(\varphi_i|\varphi_i) = \delta_{ij}, \delta_{ij} = 1 \text{ если } i = j \text{ если, иначе } 0$$

Наблюдения в квантовой механике: k - эрмитов оператор, наблюдаемый в квантовой механике, который представляет собой линейное преобразование из гильбертова пространства H в себя. Если мы выражаем линейную транспозицию в виде матрицы, то эрмитовым оператором является матрица A, которая совпадает с ее транспонированной сопряженной, которую мы обозначаем клином :

$$A^{\dagger} = A \text{ если } A^{\dagger} \coloneqq \bar{A}\,T$$

Наблюдаемая A имеет набор собственных векторов $|\varphi_i\rangle$и собственных векторовλ_i

$$A\varphi_i\rangle = \lambda_i|\varphi_i\rangle$$

В случаях, которые я здесь рассматриваю, свойства образуют полный ортонормированный базис гильбертова пространства, и поэтому H $|\psi\rangle \in H$представляет каждое состояние. Эти свойства можно записать в виде линейной комбинации:

$$|\psi\rangle \sum_i a_i|\phi_i\rangle \text{ если } \sum_i |a_i|^2 = 1$$

Мы можем написать это так.

$$|\psi) \sum_i |\phi_i\rangle(\,\phi_i|\psi) \text{ если } (\phi_i|\psi) = a_i$$

Это видно из последнего уравнения. Полнота A выражается

$$\sum_i |\phi_i)(\phi_i) = 1$$

Вот почему у нас это есть

$$A = \sum_i \lambda_i|\phi_i)(\phi_i|$$

В квантовой механике мы можем измерять только наблюдаемые величины, и только если мы $|\psi) = \sum a_i\,|\phi_i$измеряем наблюдаемое A в его состоянии. $|a_i|^2$возвращает возможные собственные значения A . λ_iИ шкала $|\psi$меняет свое состояние. Если мера λ_iвозвращает собственное значение A , то $|\psi$случай ϕ_i.

Однако квантовая механика имеет ограничения на то, что мы можем наблюдать, из-за принципа неопределенности Гейзенберга. Предположим, у нас есть два наблюдателя A и B, и мы определяем переключатель [A, B] следующим образом.

$$[A, B] \;=\; AB - BA$$

Два наблюдателя A и B совпадают, если они коммутируют; $[A, B] \;=\; 0$и если они не коммутируют, они не подходят. Наконец, $\measuredangle A = A - (A)$если тогда принцип неопределенности Гейзенберга утверждает, что

$$((\measuredangle A)^2)((\measuredangle B)^2) \geq \frac{1}{4}||([A, B])||^2 \text{ если } ((\measuredangle A)^2) = (\psi|(\measuredangle A)^2|\psi)$$

Это означает, что если A и B не совпадают, мы не можем измерить A и B с бесконечной точностью.

Состояния поляризации фотона: Рассмотрим пример состояний поляризации фотона в двумерном гильбертовом пространстве. Ч мы $|\updownarrow||$ и $|\leftrightarrow|$ Уходите мы получаем ортонормированный базис, состоящий из состояний, и $|\nearrow\rangle$мы получаем второй ортонормированный базис, состоящий из состояний и . $|\searrow\rangle$Эти два основания связаны:

$$|\nearrow) = \frac{1}{\sqrt{2}}(|\updownarrow) + |\leftrightarrow)) \text{ и } |\searrow) = \frac{1}{\sqrt{2}}(|\updownarrow) - |\leftrightarrow))$$

Обозначим наблюдаемые A и B следующим образом

$$A = \lambda_{\updownarrow}|\updownarrow\rangle + \lambda_{\leftrightarrow}|\leftrightarrow\rangle \text{ и } B = \lambda_{\nearrow}|\nearrow\rangle + \lambda_{\searrow}|\searrow\rangle$$

и предположим, что у нас есть нормализованный случай $|\psi\rangle = |\updownarrow\rangle$. Согласно теории квантовых измерений, $|\psi\rangle$измерение наблюдаемого A состояния λ_iвозвращает собственное значение с вероятностью.

$$|\langle\updownarrow|\psi\rangle|^2 = |\langle\updownarrow|\updownarrow\rangle|^2 = 1$$

и собственное значение $\lambda_{\leftrightarrow}$с вероятностью

$$|(\leftrightarrow|\psi)|^2 = |(\leftrightarrow|\updownarrow)|^2 = 0$$

из-за ортонормированности состояний. Предположим, мы хотим измерить наблюдаемые состояния B..

$$||\updownarrow) = \frac{1}{\sqrt{2}}(\nearrow) + |\searrow))$$

Мера B $\lambda_{\nearrow}$возвращает значение, соответствующее вероятности.

$$|(\leftrightarrow|\psi)|^2 = |(\nearrow|\frac{1}{\sqrt{2}}(|\nearrow) + |\searrow))|^2 = \frac{1}{2}$$

Второй член равен нулю из-за ортонормированности. По тому же аргументу мера $\lambda_{\searrow}$с вероятностью $\frac{1}{2}$ni возвращается Если $|\psi_1$мы определим состояние как состояние, сформированное после измерения, ψ_1или $|\nearrow)$или $|\searrow)|$ мы видим, что это (неразборчиво)

$$||\nearrow) = \frac{1}{\sqrt{2}}(\updownarrow) \pm |\leftrightarrow))$$

Если ψ_1мы измерим наблюдаемую A состояния , то получим для каждого $\frac{1}{2}$с вероятностью $\lambda_{\updownarrow}$или $\lambda_{\leftrightarrow}$для Это иллюстрирует принцип неопределенности Гейзенберга, и этот пример показывает, что измерения наблюдаемых параметров могут изменить состояние, что повлияет на будущие измерения.

Протокол BB84: Протокол BB84 был разработан Беннеттом и Брассартом в 1984 году и используется для случаев поляризации фотонов. В предыдущем разделе мы видели , что состояния поляризации фотона лежат в двумерном пространстве Гилберта . Прежде чем описывать этот протокол, сначала нам понадобятся два ортонормированных базиса этого двумерного гильбертова пространства. Для простоты мы выбираем два ортонормированных базиса в качестве основы нашего примера в предыдущем разделе.

Итак, первый базис состоит $|\updownarrow\rangle$ и $\leftrightarrow\rangle$из падежей, а второй базис $|\nearrow)$ и $|\searrow)$.

Две базы связаны:

$$||\nearrow) = \frac{1}{\sqrt{2}}(|\updownarrow) + |\leftrightarrow)) \; va \; |\searrow) = \frac{1}{\sqrt{2}}(|\updownarrow) - |\leftrightarrow))$$

так что мы видим $|(\phi|\psi)|^2 = \frac{1}{2}|$ если ψи ϕвозникает из разных оснований. Во-вторых, протокол BB84 использует для связи два несовместимых ортонормированных квантовых алфавита, поэтому мы определяем наш первый алфавит как

$$|\updownarrow\rangle = 1 \; c \; |\leftrightarrow\rangle = 0$$

и как наш второй алфавит

$$|\nearrow\rangle = 1 \; c \; |\searrow\rangle = 0$$

Если Алиса и Боб хотят сгенерировать секретный ключ, теперь они могут начать общение по квантовому каналу с использованием протокола BB84 следующим образом:

1. Алиса генерирует случайную последовательность битов A, которая используется как часть секретного ключа.
2. Для каждого бита последовательности A A_i Алиса a_i выбирает случайный бит. A_iбит a_iиспользуется для определения того, какой алфавит используется для передачи.
3. С каждым полученным фотоном Боб выбирает случайный алфавит для выполнения своих измерений. В 50% случаев выбранный алфавит соответствует алфавиту Алисы и B_iсовпадает с результатом измерения Боба. Во всех остальных случаях выбранный алфавит не совпадает с алфавитом Алисы, а A_iрезультат измерения A_i Боба B_iравен , только в 50% случаев. В целом это означает, что только 75% измеренной последовательности B Боба A_iсовпадает с последовательностью Алисы.

Согласно протоколу BB84 Алиса и Боб теперь общаются по общему каналу:

1. Боб сообщает Алисе, какой квантовый алфавит он использовал для своих измерений, и Алиса сообщает Бобу, правильный ли он. Так это становится известно Алисе и Бобу.
2. удалили все биты и B_i из A и B соответственно , используя для связи несовместимые алфавиты. A_i Полученные последовательности называются открытыми ключами, и они совпадают, если нет прослушивания квантового канала.
3. Наконец, Алиса и Боб сравнивают биты своего открытого ключа, чтобы оценить частоту ошибок, а затем удаляют биты, использованные для сравнения, чтобы создать предполагаемый окончательный ключ. Если они обнаруживают какие-либо ошибки, они знают, что их прослушивает третья сторона. Если это так, Алиса и Боб могут начать сначала. Если нет, Алиса и Боб устанавливают секретный ключ.

Идентификация Оскара в протоколе BB84: Представьте, что Оскар — сторонний слушатель. Мы видели, что если алфавиты, выбранные Алисой и Бобом, одинаковы, то соответственно A_i и B_iтоже одинаковы. Впрочем, если Оскар решит послушать квантовый канал, то некоторые A_iи B_iотличаются от . Например, предположим, что Алиса использует алфавит для отправки одного бита Бобу, а Оскар использует другой алфавит для выполнения измерений. Состояние после измерения будет $a|\nearrow$ или $a|\searrow$. В любом случае, если Боб произведет измерение с использованием алфавита, используемого Алисой, он найдет $|\leftrightarrow$)состояние с вероятностью $\frac{1}{2}$. Это означает, что $B_i = 0$ и A_i=1. Из этого примера видно, что подслушивание Оскара вызывает ошибки в ключе Алисы и Боба.

Шумный протокол BB84: в предыдущем разделе мы предполагали, что связь по квантовому каналу бесшумна. Но на практике всегда будет шум, влияющий на частоту ошибок последовательностей A и B. Таким образом, мы не можем сказать, вызваны ли ошибки шумом или сторонним прослушиванием Оскара. Решение этой проблемы состоит в том, что мы предполагаем, что все ошибки вызваны Оскаром. Поэтому окончательный ключ лишь частично секретен. Чтобы согласовать закрытый ключ, Алиса и Боб должны стереть все ошибки из своего общего ключа. Один из способов сделать это — разбить открытый ключ на блоки определенной длины, а затем выполнить для них проверку параметров. Если средства проверки параметров не согласны, они выполняют бинарный поиск ошибки, разбивая блок на два подблока и сравнивая параметры этих подблоков. После сравнения всех блоков этот шаг повторяется путем выполнения случайной общедоступной перестановки их оставшегося открытого ключа, разделения его на блоки и сравнения проверок параметров. После этого Алиса и Боб выбирают случайное подмножество своих оставшихся открытых ключей для сравнения параметров и применения стратегии бинарного поиска в случае обнаружения ошибки. Если ошибок не обнаружено, Алиса и Боб могут объявить свои оставшиеся ключи согласованными ключами. Наконец, Алиса и Боб выбирают n случайных подмножеств своих пользовательских ключей, не раскрывая их содержимого, после чего их окончательный секретный ключ определяется как параметры этих подмножеств. Поскольку Оскар вызывает все ошибки, число n зависит от частоты ошибок исходного открытого ключа.

Протокол B92: Протокол B92 использует только один алфавит вместо двух. Кроме того, алфавит, используемый в этом протоколе, не является ортонормированным. Итак, давайте определим наш алфавит следующим образом.

$$|\updownarrow) \; c \; |\nearrow) = 0$$

Этот в отделе _ мы предыдущий в разделах _ что случилось _ между базами вроде от отношений мы используем Кроме того, мы определяем два проекционных оператора.

$P_{\leftrightarrow} = |\leftrightarrow)(\leftrightarrow|$ c $P_{|\searrow)} = |\searrow)(\searrow||$

мы это увидим

$$\left(\updownarrow P_{|\leftrightarrow}| \updownarrow\right) = \left(\nearrow |P_{|\searrow}| \nearrow\right) = 0 \text{ c } \left(\nearrow P_{|\leftrightarrow}| \nearrow\right) = \left(\updownarrow |P_{|\searrow}| \updownarrow\right) = \frac{1}{2}$$

скажем Алиса _ а также Боб конфиденциальный ключ хочет создать если они _ _ _ Протокол B 92 с использованием квант канал через следующее путь коммуникация сделать Начало можно _

1. Алиса а также Боб случайный A а также Б кусочек последовательность _ _ они создают _ в протоколе BB 84 такие как конфиденциальный ключа один часть в качестве используется .
2. Алиса отправляет свою битовую последовательность A, используя квантовый алфавит, а Боб измеряет полученные состояния в соответствии с битовой последовательностью B. Если B_iбит B равен 0, он измеряется с помощью Bob, $P_{|\leftrightarrow\rangle}$a B_iесли он равен 1, он измеряется с $P_{|\searrow\rangle}$c' i.
3. Если Боб измеряет состояния, посланные Алисой, он находит один из следующих результатов: состояние, $|\updownarrow\rangle$представляющее один бит, состояние, представляющее нулевой бит , или $\nearrow\rangle$неопределенное $\searrow\rangle$состояние в нашем алфавите $\leftrightarrow\rangle$. В последнем случае мы говорим, что измерение не удалось, и привело к отключению. Мы видим, что еслиB_i A_iотличается от , то измерение Боба не удается, потому что оператор измерения Боба ортогонален состояниям Алисы. ЕслиB_i va A_iимеют одинаковые битовые значения, то $|\updownarrow\rangle$или $\nearrow|$вероятность выхода $\frac{1}{2}$равна . Таким образом, мы видим, что только одно из четырех измерений дает результат. Во всех остальных случаях измерение можно удалить. Таким образом, процент удаления составляет 75%.
4. Боб сообщает Алисе, какие из его измерений были успешными, и Алиса сохраняет только те биты из A, где измерения Боба были успешными. Алиса и Боб теперь имеют общий ключ.
5. Наконец, Алиса и Боб сравнивают небольшие части своих общих ключей, как в протоколе BB84, чтобы оценить частоту ошибок. Если они обнаружат какие-либо ошибки, они будут знать, что их прослушивает третья сторона.

Идентификация Оскара в протоколе B92: мы видели, что если измерение Боба проходит успешно, другими словами, если результат измерения возвращает состояние нашего алфавита,B_i va A_iбудет то же самое. Однако, если Оскар $P_{|\nearrow}$решит прослушать измерение с помощью, например, оператора, A_iB_iу него будет отличное от некоторых из проведенных измерений Мы можем видеть это в следующем примере: если бы Оскар был в середине между Алисой и Бобом битовое состояние $|\updownarrow\rangle|$ отправляет, меняет Оскар, a $\nearrow|$ или a $\searrow$состояние. Это означает, что если Боб измерит сгенерированное состояние, он, $\langle\nearrow |P_{\leftrightarrow}| \nearrow\rangle = \frac{1}{2}$вероятно, $\nearrow\rangle$получит состояние с нулевым битом вместо обычного результата стирания.

Другие протоколы. Помимо BB84 и B92, существует множество других протоколов квантовой криптографии, и было бы слишком громоздко перечислять их все здесь. Поэтому я выбрал несколько примеров, которые кратко опишу.

Квантовая криптография на основе ЭПР : этот вариант протокола BB84 использует парадокс Эйнштейна Подольского-Розена (ERP), который Эйнштейн, Подольский и Розен опубликовали в 1935 году, чтобы бросить вызов основам квантовой механики. Эта идея принадлежит Артуру

Эккерту, опубликовавшему в 1991 году. Предлагаемая схема состоит в использовании двух кубитов вместо одного. Два кубита происходят из общего источника, где один кубит достается Алисе, а другой — Бобу. Кубиты называются ЭПР-парами, состояния которых соотносятся таким образом, что измерение выбранной наблюдаемой A одного состояния автоматически определяет результат измерения A другого состояния. Это означает, что если Алиса и Боб будут измерять свои кубиты на одной и той же основе, они получат коррелированный результат. Кроме того, они знают, что такое корреляция, поэтому таким образом они могут договориться об общем ключе. Поскольку парадокс ERP охватывает основы квантовой физики, я не буду идти другим путем, объясняя квантовую криптографию на основе ERP.

Изменения в протоколе BB84. В протокол BB84 внесено большое количество изменений. Например, можно предположить, что два основания не выбираются с равной вероятностью. Это повышает вероятность того, что Алиса и Боб выберут одно и то же основание, но Оскару будет легче правильно угадать используемое основание. Поэтому пока неясно, лучше реальный результат или нет. Есть много других изменений, которые я не буду здесь упоминать. Точный результат некоторых из них пока сомнителен, но есть и другие изменения, облегчающие практическую реализацию.

Тактика прослушивания: В протоколах, которые я обсуждал в предыдущих разделах, я рассматривал только непрозрачное прослушивание, что означает, что Оскар захватывает и отслеживает фотоны Алисы, после чего отправляет измеренные состояния Бобу. Однако Оскар может использовать и другие методы прослушивания.

Причина, по которой я не рассматривал их в предыдущих разделах, заключается в том, что анализ всех схем прослушивания был бы слишком долгим и технически сложным. В этом разделе я кратко перечислю несколько стратегий слушания, которые может использовать Оскар.

Прозрачно слушать . Когда Алиса отправляет кубит Бобу, Оскар может позволить системе по своему выбору, называемой зондом, взаимодействовать с кубитом, а затем передать его Бобу в измененном состоянии. Он может свободно выбирать зонд, а также его начальное состояние и взаимодействие, поскольку подчиняется квантовым правилам, то есть взаимодействие описывается специальным оператором.

Прозрачное слушание с замешательством . В этом подходе Оскар привязывает свой чек к состоянию, отправленному Алисой, а затем передает его Бобу. Поскольку это один из самых сложных способов слушать, я не буду больше говорить об этом.

Слух на основе уязвимости реализации. В следующем разделе мы увидим, что квантовую криптографию по-прежнему трудно реализовать на практике, поскольку современные технологии еще не догнали ее. Например, сегодня вероятность того, что один фотонный лазер будет генерировать несколько фотонов, $\frac{1}{200}$равна Следовательно, если у Оскара есть подслушивающее устройство, обнаруживающее несколько фотонов, он может направить один из фотонов для измерения. Таким образом, Оскар $\frac{1}{200}$ может прочитать статус Алисы, не будучи обнаруженным.

Алгоритмы обнаружения вторжений доступны для всех этих схем прослушивания. Однако на самом деле нам нужен алгоритм, который может обрабатывать большие классы шаблонов прослушивания, а не алгоритм обнаружения для одного конкретного шаблона прослушивания. Поэтому анализ схем прослушивания еще не завершен.

Технологические проблемы квантовой криптографии. Чтобы построить квантовое криптографическое устройство, нам необходимо учитывать генерацию, распространение и обнаружение одиночных фотонов. Во-первых, нам нужно устройство, излучающее один фотон. К сожалению, это трудно сделать экспериментально из-за пуассоновской статистики доступных источников света. Например, при использовании слабых лазерных импульсов вероятность одного фотона в импульсе составляет всего 10%.

Есть и другие способы получения фотонов, но они все еще не преодолевают тот факт, что процесс создания фотонов неэффективен, а устройства все еще слишком сложны для использования в практических ситуациях.

Как только один фотон создан, фотон отправляется через квантовый канал. Квантовый канал может быть оптическим волокном или просто свободным пространством. Распространение фотонов по оптическим волокнам было бы наиболее логичным способом, так как они широко используются в телекоммуникациях и обладают высоким качеством. Длина волны, используемая для фотонов в оптических волокнах, составляет около 1300 или 1500 нм. Затухание оптических волокон для этих длин волн составляет 0,35 и 0,20 дБ/км, что означает, что половина фотонов теряется через 9 и 15 км соответственно.

Однако одним из основных недостатков использования оптических волокон является то, что до сих пор не существует детекторов, способных обнаруживать фотоны с длиной волны более 1000 нм. Разработка этих детекторов все еще продолжается, и я вернусь к этому позже. Хотя не существует хороших детекторов фотонов с длиной волны более 1000 нм, существуют эффективные детекторы фотонов с длиной волны около 800 нм, которые также имеются в продаже. Однако, если используется длина волны 800 нм, существующие в настоящее время оптические волокна нельзя использовать в качестве квантового канала из-за несоответствия длин волн. В этом случае для распространения фотонов требуется космическая передача или использование специальных волокон. К сожалению, качество любого специального волокна не такое высокое, как у оптического волокна. Помимо более низкого качества, специальные волокна имеют еще и практический недостаток по сравнению с оптическими волокнами, поскольку оптоволоконные сети уже существуют, а специальные волокна используются нечасто.

Помимо оптических волокон можно также рассмотреть космическую передачу, которая имеет некоторые преимущества перед использованием оптических волокон. Атмосфера имеет высокое окно пропускания на длине волны около 770 нм, где фотоны могут быть обнаружены с помощью коммерческих высокопроизводительных вычислительных модулей. Более того, на этих длинах волн состояние поляризации фотона не изменяется атмосферой. Однако есть и ряд недостатков пространственного переноса. В отличие от оптических волокон, передаваемая энергия рассеивается в свободном пространстве, что вызывает различные потери при передаче. Кроме того, в приемник может попадать окружающий свет, что увеличивает частоту ошибок. К счастью, эти ошибки можно уменьшить, используя спектральные фильтры и временную дискриминацию. Наконец, космическая передача зависит от атмосферных условий и возможна только на открытом воздухе. Поэтому космические каналы необходимо совершенствовать, прежде чем их можно будет применять на практике.

Хотя самым безопасным вариантом является использование оптических волокон в качестве переносчиков фотонов, мы увидели необходимость разработать для этого новый детектор. Обнаружение фотонов, в принципе, можно осуществить с помощью таких методов, как умножители фотонов, лавинные фотодиоды, многоканальные пластины или сверхпроводящие переходы Джозефсона. Идеальный детектор должен отвечать следующим требованиям:

1. Он должен иметь квантовую эффективность обнаружения в большом спектральном диапазоне.
2. Уровень шума, то есть генерация сигнала без прихода фотона, должен быть небольшим
3. Время детектора, т. е. разница во времени между обнаружением фотона и электрическим сигналом, должно быть небольшим.
4. Время восстановления должно быть небольшим, чтобы обеспечить высокую скорость передачи данных.
5. Детектор должен быть пригоден для коммерческого использования.

К сожалению, соблюсти все указанные критерии невозможно. В настоящее время лучшим выбором являются кремниевые лавинные фотодиоды. Для фотонов ниже 1100 нм существуют коммерческие детекторы с квантовой эффективностью 70% на длине волны 700 нм, временным джиттером около 300 пс, максимальной скоростью счета выше 5 МГц и частотой шума 50 Гц. 20 С. Для фотонов выше 1100 нм единственными доступными лавинными фотодиодами являются фотодиоды.

Изготовлен из германия или InGaAs. Эти детекторы имеют плохие характеристики по сравнению с кремниевыми фотодиодами. К сожалению, в промышленности не было предпринято никаких усилий по оптимизации фотодиодов для работы на длинах волн выше 1100 нм. Однако нет физической причины, по которой фотодиоды, работающие на длинах волн выше 1100 нм, должны быть тоньше, чем фотодиоды ниже. Практическая причина отсутствия коммерческих продуктов заключается в том, что ширина запрещенной зоны кремния слишком велика и, следовательно, недостаточно чувствительна для подсчета фотонов. Кроме того, рынок фотонных вычислений еще незрел. Но если эти проблемы будут решены, будущее квантовой криптографии сделает гигантский скачок вперед.

Резюме

Если мы сравним квантовую криптографию с классической криптографией, уникальный вклад квантовой криптографии заключается в том, что она предоставляет механизм для обнаружения подслушивающих устройств. С другой стороны, самым большим недостатком квантовой криптографии является то, что она не обеспечивает механизма аутентификации. Следовательно, квантовая криптография и классическая криптография могут использоваться как дополнительные инструменты. Например, небольшой ключ аутентификации сначала передается по защищенному каналу с использованием классических методов. Затем этот ключ можно увеличить до произвольной длины с помощью квантовых криптографических методов.

Используемая литература

1. Адамс, К. Построение симметричных шифров с использованием процедуры проектирования приведения. В проц. Проекты, коды и криптография 12 (1997), Kluwer Academic Publishers, стр. 283–316.
2. Администратор, A.L. Advanced Access Content System, Технический обзор (информативный). Администратор лицензирования AACS, 2004 г.
3. Экерт А., Хаттнер Б. Г. М. П., Перес А. Подслушивание квантово-криптографических систем. физ. преп. А 50, 2 (1994), 1047–1055.
4. Дж. Брассард. Современная криптология. Москва 2006.
5. Беннетт, Ч.Х. «Экспериментальная квантовая криптография». США 2020
6. Бернштейн, Д.Дж. (2009). Введение в постквантовую криптографию. Сообщение 1. Ааронсон, С. (2008). «Квантовые пределы». Scientific American 298(3): 62-69. квантовая криптография
7. Мамажанов, Р. Я., & Хайдаров, Ш. И. (2022). РАЗРАБОТКА МЕТОДОВ И АЛГОРИТМОВ ДЛЯ РАСПОЗНАВАНИЕ ДОРОЖНЫХ ЗНАКОВ. *CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES*, *3*(10), 50-57.
8. Мамажанов, Р. Я., & Хайдаров, Ш. И. (2022). Создания Web Приложения И Расспознования Ограничения Скорости Дорожных Знаков. CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES, 3(4), 57-61.
9. Хайдаров, Ш. И. (2022). Разработка Программного Обеспечения QR-Code Для Формирования Электронных Баз Данных И Систем Управления Высшими Учебными Заведениями. CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES, 3(1), 3-8.

10. Mamajanov, R. Y., & Xaydarov, S. I. (2022). KORXONA VA TASHKILOTLARDA ELEKTRON TABEL VA SAMARADORLIKNING MUHIM KO'RSATKICHINI BELGILASH. Central Asian Research Journal for Interdisciplinary Studies (CARJIS), 2(5), 281-289.
11. Xaydarov, S. I. (2022). KORXONA VA TASHKILOTLARDA ELEKTRON TABEL DASTURINI ISHLAB CHIQISH. Scientific progress, 3(1), 465-469.