Хацкевич М.В.

**Современные методы защиты компьютерных систем**

**Блок-чейн и криптовалюты**

**Криптовалюты** ­­– набор концептов и технологий, который образует, экосистему цифровых денег.

Есть **ряд отличий** цифровых денег от обычной валюты:

* Ничем не подкреплены
* Полностью анонимны
* Децентрализация
* Невозможность отмены платежей
* Прозрачность транзакций

Любой пользователь может в любой момент просмотреть цепочку транзакций осуществляемую с монетой, но лица осуществлявшие покупку-продажу монеты полностью анонимны.

Платеж невозможно отменить. Отсутствие необратимых транзакций увеличивают стоимость сервиса, чьи услуги являются неотменяемыми.

Нет единого центра управления отсутствует посредник, система является саморегулирующей и самоподдерживающей.

**Блок-чейн** – длинная цепочка блоков или транзакций производимых в одно и тоже время.

Данная цепочка растет неограниченно долго, пока существуют система.

За майнинг каждой монеты вознаграждение уменьшается.

Блок-чейн не хранится на одном носителе, он существует в распределенном виде, на компьютерах или сетевых узлах. У владельцев с электронными кошельками. Электронные кошельки – программы с установленным паролем доступа с помощью которой можно управлять своим счетом.

Данное распределенное хранилище обеспечивает ведение главного журнала, что обеспечивает его легитимность и защищенность. Этой системе можно доверять, осуществляется подтверждение личности.

**Майнинг** – добыча полезных ископаемых. Появляется новый информационный блок, появляется новая монета в обороте.

На данный момент отпадает необходимость ферм и майнинговых пулов, потому что появились новые консенсусы для майнинга и облачные технологии.

Каждый занятый в майнинге сетевой узел или компьютер собирает информацию о транзакции и включает её в зашифрованную буквенно-цифровую последовательность знаков, называемую хэшем.

**Приобретение и хранение валюты**

**Варианты приобретения:**

* Майнинг
* Продажа или услуга
* Покупка за любую другую валюту

Помимо самостоятельного майнинга существует возможность подключения к майнинг пулу. Пользователь вступает в группу занимающуюся майнингом, объединяя свои возможности. Пул – это сервер, к которому подключаются для совместного майнинга. В случае успешного майнинга вознаграждение делится между участниками.

**Хранение электронных денег**

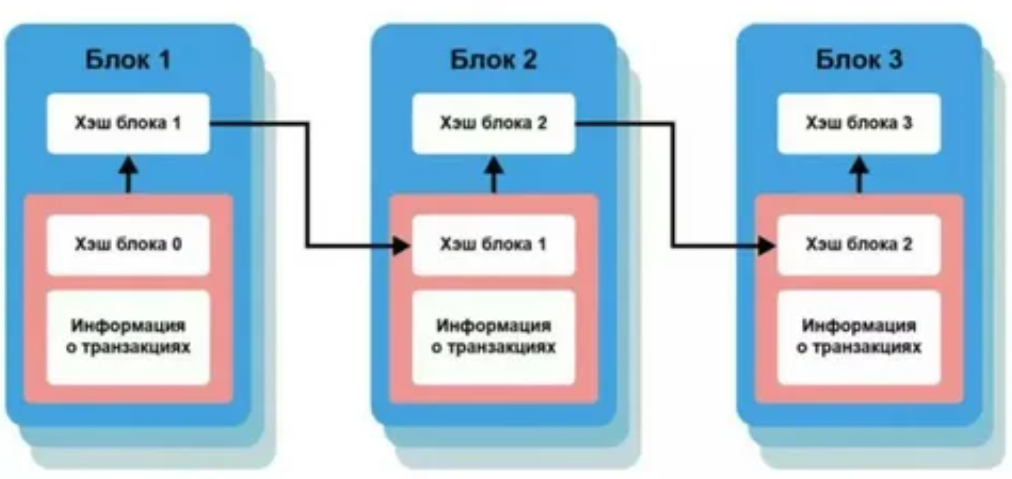
* Крипто-кошельки
  + Стационарный кошелек
  + Мобильный кошелек
  + На внешних носителях
  + Бумажные кошельки
* На бирже

Мобильный и стационарный кошелек – это приложения, которое хранит ключи для электронных кошельков, которые позволяют управлять криптовалютой.

Для получения бумажного кошелька нужно зарегистрироваться на соответствущеюм сайте, далее мы получаем биткоин адрес, сервис создаст изображение кошелька, содержащий 2 QR-code: публичный адрес и секретный ключ. Преимущества бумажного кошелька: дешево, секретный ключ не хранится в цифровом виде нигде.

**Блок-чейны бывают трех типов:**

* Публичный (цепочка блоков доступная всем пользователям)
* Сервисный (цепочка блоков доступная всем пользователям, но количество блоков ограничено)
* Приватный (цепочка блоков доступна только приоритетным узлам)



**Пример работы блок-чейна:**

1. Пользователь Х переводит деньги пользователю Y
2. Сведенья об операции передаются в сеть и объединяются в блоки, каждый элемент содержит номер и хэш прошлого блока
3. Происходит рассылка блоков участникам криптовалютной сети, которая выполняет проверки
4. При отсутствии ошибок проверяемы блок размещается в блок-чейне
5. Пользователь Y получает деньги от пользователя X

Стоимость BTC = 55 000 $

Стоимость ETH = 2 292 $

На сегодняшний день 19 млн битков доступно, 200 млн биткоин кошельком и 100 млн владельцев валют, должно быть 21 млн битков

Каждые 4 года происходит снижение вознаграждение вдвое – калминг

За сутки майнится 144 BTC. Последний биткоин будет намайнен в 2140 году. Потеряно около 4 млн BTC.

Задача майнинга:

Хеш предыдущего блока плюс все транзакции в memory pool, находим X из случайного диапазона

Hash + market\_root + x < TARGET

Майнер имеет право записи блока, право получить вознаграждение за майнинг.

Адрес с которого пришла транзакция 🡺 Суммируется валюта 🡺 генерируются адреса куда переводятся битки.

Откуда 🡺 Что 🡺 Куда

Участники системы назваются Nodes

Майнинг случайный перебор чисел с целью найти решение, если решение найдено, то майнер получает права на вознаграждение и на запись. Для майнинга применяется консенсус доказательства работы.

**Плюсы:**

* Высокая скорость
* Низкие комиссии
* Децентрализованность
* Анонимность
* Прозрачность
* Надежность

**Минусы:**

* Невозвратность
* Маштабируемость (при текущем размере блока система обрабатывает до 7 операций в секунду)
* Неопределенный статус

**Сферы применения:**

* Защита авторства
* Голосование
* Биржи
* Сфера услуг
* Недвижимость

**Консенсус** – согласие по общему вопросу всех участников сети**. Основная работа блок-чейна** – генерация блока. При генерации блока требуется достижение консенсуса между майнерами. Это необходимо для синхронизациии копий цепочек с настоящей цепью. Алгоритм консенсуса это схема или путь достижения согласия. Например, мы рассматривали блок-чейн, где консенсус – это математические правила и функции, по которым майнеры будут приходить к общему решению.

Основные 4 консенсуса:

1. Proof-of-work – доказательство работы
2. Proof-of-stake – доказательство доли владения
3. Proof-of-importance – доказательство важности
4. Proof-of-activity – доказательство активности = Proof-of-work + Proof-of-stack

Принцип защиты сетевых систем от злоупотребления услугами, организованный на необходимости выполнения на стороне клиента некоторой достаточно длительной работы результат которой можно быстро проверить на стороне сервера. Подобные методы называют функции клиентской головоломки, наибольшее распространение в криптовалюте.

Закон Мура – это эмпирическое наблюдение согласно которому кол-во транзисторов размещаемых на кристальной схеме удваивается раз в 2 года.

В 2007 году Мур заявил что закон фактически не работает из-за атомарной природы вещества и ограничения скорости света.

Proof-of-stake – метод защиты в криптовалютах при которых вероятность формирования участником очередного блока в блок-чейне пропорциональна доле, которую составляют принадлежащие этому участнику расчётные единицы данной криптовалюты от их общего количества. При использовании данного метода алгоритм формирования блока не зависит от мощности оборудования, но с большей вероятностью блок будет сформирован в той учетной записи у которой больше текущий баланс. На практике часто применяются оба метода. Если консенсус POS, то участник ограничен процессом транзакции.

1. Проекты на основе POW подвержены атаке 51%. Атакующие могут направить большие мощности создавая параллельную цепь, потом внезапно опубликовать её с другим движением по счетам.
2. Майнерам ПО необходимо вкладываться в оборудование.
3. Владельцы всегда будут стремиться поддерживать покупательную способность валюты.

Преимущества POS:

1. Минимальные энергозатраты
2. Нет смысла совершать атаку 51%
3. Не имеет ограничений по вычислениям

Недостатки POS:

1. Сложность старта, нужен начальный капитал
2. Высокий порог входа
3. Высокая централизация
4. Необходимость быть постоянно онлайн со включенным устройством

Как начать майнить POS:

1. Нужно завести кошелек (скачать с официального сайта)
2. Синхронизируем кошелек
3. Покупаем валюту размещаем на локальном кошельке. Для нашего пк будет использоваться уникальный IP и валюта всегда должна находиться на нем. Держим ПК всегда включенным.

При отсутствии устройства можно арендовать место на ферме. POS в 20 году вошли в топ 10 используемых криптовалют.

Генерация блока

Hash(prevBlockData, timeInSecondsm txountA) <= do \* coins(txountA) \* timeweight(txountA)

Первоначальная задача принципа POW для того чтобы заработать первоначальный капитал.

timeInSeconds – текущее время ограничивающее попытки хэширования

txountA – результат транзакции

coins – кол-во монет

timeweight – время прошедшее с момента включения блока результата транзакции txountA

prevBlockData – данные предыдущего блока

Если у заинтересованных пользователей есть ключ то она может сгенерировать блок. Подпись в данном случае служит доказательством выполнения условия.

Вещи, которые мы упустили:

1. Логирование Windows, Linux (Изменение журнала после атаки)
2. PowerShell и Bash
3. CyberKillChain
4. MIITEATT&CK
5. SIEM
6. SOC
7. FW/NGFW
8. IDS/IPS
9. NTA
10. Netflow
11. WAF
12. DCShadow, DCSync
13. DNS, ICMP, SSH

Side Chain – это механизм позволяющий перемещать криптовалюту в другой полностью независимый блок-чейн обменивать его там, а затем возвращать обратно в главный блок-чейн. Это тип блок-чейна, который существует в стороне от главной ветви блок-чейна

Нужно понимать что существует 2 цепи: главная и боковая цепь. Side Chain – это отдельная цепочка которая присоединяется к блок-чейну с помощью двусторонней привязки. Двустороння привязка помогает обмениваться между главной и дочерней. Скорости обмена предопределены. Форки возникают по разным причинам: например, сформировалась новая монета, сеть не устраивает внешнее положение дел.

Существую следующие типы форков:

* Soft-форки
* Hard-форки
* Спорные форки

Не все форки приводят к созданию новых криптовалют. Криптовалюты это сети которые работают на основе консенсуса которые влияют на работу сети. Сеть представляет собой ПО с открытым исходным кодом, форки возникают когда ПО майнеров не согласовано. Если они не достигнут консенсуса, то это влечет повышение цены актива. Нет ни одного человека, который контролирует цену монеты. Никто не принимает решения какие проблемы решать в первую очередь. Форк – изменение базовых правил по работе с блок-чейном.

Soft-форк – то, что происходит, когда ПО на котором работает блок-чейн обновляется. Уникальность Soft-форк в том, что он позволяет пользователю обновлять платформу, но присутствует обратная совместимость. По сути это простое внутреннее обновление. Участники без обновлений будут видеть новые транзакции, но дело в том, что когда они будут пытаться добавлять новые блоки, операция будет отклонена.

Hard-форки – это изменение в блок-чейне, которое не является обратно совместными и это заставляет всех участников сети обновляться до последнего ПО. Обычно все форки запланированные, если что-то происходит не так, то это все называется спорные Hard-форки. В технологии блок-чейна Hard-форки могут привести к радикальному изменению протокола блок-чейна. Hard-форк разделяет одну криптовалюту на 2, что приводит к проверке этих цепочек блок-чейна.

Разница hard-форков и soft-форков. При soft-форках старые узлы могут принимать данные, которые кажутся недействительными для новых версий. А в hard-форках старые злы перестают обрабатывать блоки. 2 версии ПО могут быть совместны в soft-форках, в hard-форках такого нет. В hard-форках создается 2 блок-чейна а в soft-форках один. Пользователь предпочитает hard-форк, но разработчик больше любит soft-форки.

Клоны – когда берется ПО криптовалюты и немного изменяется.

Side chain и каналы состояний являются технологиями для улучшения плохой маштабируемости блок-чейна в целом. Оба этих подхода работают по похожим моделям: 1) выполняют заморозку состояния активов 2) выполнение транзакций вне блок-чейна цепи 3) разблокировка состояния активов.

Канал состояния – это процесс, в котором пользователи взаимодействуют друг с другом на за пределами блок-чейна и минимизируют операции друг с другом. Каналы состояний – это увеличение риска для любого участника. Внутри блок-чейна выполняется какой-то смарт контракт, затем блокируется, выводится за пределы блок-чейна, внутри него производятся расчеты между, участникам и когда расчеты завершены, разблокируется канал и происходит завершение транзакции. Например, сторона А и Б хотят провести некоторую последовательность транзакций, они для этого должны использовать ресурсы сети, заплатить каждый деньги, поэтому сторона А и Б могут оплатить только транзакцию при открытии канала, затем вне блок-чейна выполнить все свои транзакции, вернуться к основному блок-чейну и закрыть канал.

Смарт-контракт – это компьютерный алгоритм содержащий условия договора и предназначенный для автоматического контроля и исполнения договорных отношений. Для работы смарт-контракта все условия и обязательства договора описываются на ЯП. При этом программа запускается на доверенной вычислительной системе. В настоящее время смарт-контракты встречаются на платформах криптовалют. Первой страной, которая признала подлинность смарт-контракта является Беларусь. Появление технологии блок-чейн позволило контрактам получить полную автономность, что позволило отказаться от сторонних администраторов. Первые версии биткоина для реализации умных контрактов использовали скрипты. Из соображения безопасности первые биткоин-скрипты не обладали полнотой по Тьюрингу и широкое применение смарт-контракты не получили. Однако потом стали появляться протоколы более высокого уровня. Распространение контрактов получила в криптовалюте эфириум, в котором изначально была встроена виртуальная машина, которая позволяла разрабатывать код на разных ЯП. После этого пришли к выводу, что технология блок-чейн может использоваться не только в криптовалютах. Также предложили создать универсальную блок-чейн платформу в которой каждый желающий может программно реализовать систему хранения и обработки информации. Но для этого было выдвинуто одно требование – главное условие, чтобы все действия были описаны через математические формулы.

Принцип работы:

Стороны подписывают контракт аналогично подписанию отправки средств в криптовалютных сетях, после подписания контракт сохраняется в блок-чейне. Для автоматизации исполнения обязательств контракта требуется специализированная среда, это могут быть узлы блок-чейна. Данная среда полностью автоматизирует выполнение пунктов контракта. Получается что контракт существует только внутри среды и имеет доступ к коду и объектам умного контракта. Все условия контракта должны иметь программное описание и понятную логику исполнения. Стоит острая задача формализации отношений. И таким образом достигается полная автоматизация и исполнение договорных отношений. Умные контракты смарт-контракты могут взаимодействовать с внешней системой через блок-чейн оракл, они сопоставляют информацию контракта с информацией внешней среды.

Условия для существования умных контрактов:

* Использование современных методов ЭЦП
* Открытые децентрализованные БД для выполнения транзакций
* Децентрализация среды исполнения
* Достоверность источника цифровых данных

Подписанты – стороны умного контракта, которые принимают или отказываются от приведенных условий с использованием ЭЦП.

Предмет договора – предмет, находящийся внутри умного контракта.

Условия – математическое описание условий, которое можно запрограммировать внутри контракта.

Применение:

* Финансовая
* Рынок ценных бумаг
* Децентрализованные финансовые сервисы
* Кредитование
* Платформы обучения
* Голосование
* Оформление договоров без натариусов

Недостатки:

* Ослабление социальных институтов
* Недостаточная функциональная гибкость
* Сложный процесс создания

Разобраться с технологией Atomic Swap

Квантовые компьютеры ломают все алгоритмы с открытым ключом, кроме постквантовой криптографии, это говорит от том что все секреты мира будут под угрозой. В том числе общественные протоколы безопасности https, ssh, wi-fi сети, vpn, криптовалюты, смарт-карты, многофакторная аутентификация и т д.

Свойства квантов:

* Одна квантовая частица может находиться в двух местах и быть одновременно двумя разными частицами
* Одна квантовая частица может разделиться на 2, столкнуться или смешаться и восстановиться или исчезнуть
* В реально пустом пространстве, где абсолютно ничего нет, квантовые частица могут появиться и исчезнуть
* Кажется, что квантовая частица ведет себя одним образом, когда её измеряют, другим, когда её измерят
* Две квантовые частицы могут быть спутаны
* Квантовые состояние – это все возможные состояния. Суперпозиция.

Логика квантовой механики отличается от классической логики. Классический бит заменяется квантовым битом, который называется кубитом. Вектор состояния которого может принимать значение 1, 0, а может любую комбинацию. |ф>= |0> |ф> = |1>. |ф> = C0|0> + C1|1>. С0 – комплексные числа называемые амплитудой вероятности. Сама суперпозиция ненаблюдаемая. При изменении кубита мы получим 0 с вероятностью |С0>^2 и 1 – |С1>^2. Над кубитом можно производить некоторые унарные операции, которые изменяют численные значения коэффициента С0 и С1. Работу квантового компьютера можно рассмотреть на примере квантового алгоритма Дойча. Допустим есть черный ящик, который вычисляет некоторую булевую функцию f(x). На вход мы можем подать либо 0, либо 1, на выходе мы можем получить либо 0, либо 1. Всего возможно 4 варианта таких функций они бывают константные и сбалансированные. Задача Дойча состоит в том, чтобы определить к какому из этих двух категорий относиться функция в черном ящике. На классическом компьютере нам нужно подать на вход 0 и 1, после этого мы обозначим вид функции а не только её категорию. Определить категорию за один вызов функции на обычном компьютере не получится, в отличии от квантового. В квантовом случае кубит содержит суперпозицию 0 и 1. Возьмем кубит вида. |ф> = 1/sqrt(2) |0> + 1/sqrt(2) |1>

🡪[F]🡪[H]🡪[->)]

Операция F изменяет значение кубита следующим образом: по сути F – это квантомеханический аналог классического черного ящика.

Измерив кубит сразу за блоком F, вне зависимости блоков F(x) мы все равно получаем 50% вероятность 0 либо 1. Т. к. она может изменить только знак.

Применив к кубиту преобразование Адамара H мы получим для константной функции мы получаем C0 и C1. С0 = 1 С1 = 0. Для функции, которую мы назвали сбалансированной мы получаем C0 = 0, C1 = 1.

Мы можем однозначно сказать к какой категории относится функция, но к какому виду остается неясным. Это пример квантового параллелизма. Для описания двухкубитного состояния нам понадобится 4 комплексных числа.

Если у нас двухкубитная система, мы можем работать с 4мя состояниями. C00 C01 C10 C11. |ф = С00|00> + С01|01> + С10|10> + С11|11>.

Представим что мы хотим получить решение при каждом ходе на шахматной доске. Каждый возможный ход мы представим количеством рисовых зерен и это создало бы гору риса размером с Эверест. Количество риса необходимое для того чтобы представить 2048 битное разложение, получается нужно 1985 гор размером с Эверест. Классический ПК работает с бинарной системой. Квантовый ПК использует квантовые частицы, при измерении частицы он видит заряд, спин, поляризация. Базовое состояние квантового ПК таково, что он может представлять все состояния частиц одновременно.

Наличие большого количества кубитов – это хорошо, но некоторые квантовые ПК не завися от кубитов, не могут решить одни и теже задачи.

Для двух или более кубитов определим вектор столбец описывающий системы через тензорное произведение векторов кубитов.

Таким образом система из 3 кубитов описывается вектором в 8мимерном пространстве из 10 кубитов, это 1024. Для 1000 кубитов это число с 300 нулями. В данном пространстве с 300 нулями мы можем описать состояние через 10^30 степени комплексных чисел, это больше чем частиц в наблюдаемых вселенных.

Существует множество протоколов, основная проблема квантовых каналов – дороговизна, нужны усилители сигналов.

Первый квантовый протокол был создан в 1984 году. В протоколе BB84 используется 4 состояния фотона, направление вектора поляризации выбирается в зависимости от передаваемого бита и может быть 90, 135 для единицы и 45, 0 градусов для нуля. Существуют следующие анализаторы, принадлежность к какому-либо базису (+ - прямоугольный, × - диагональный). Одна пара квантовых состояний 0 и 1 принадлежит базису +, другая принадлежит базису ×. Внутри обоих базисов состояния ортогональные. Состояния из разных базисов попарно неортогональны. Ортогональность необходима для попыток для определения попыток несанкционированного считывания информации.

Схема

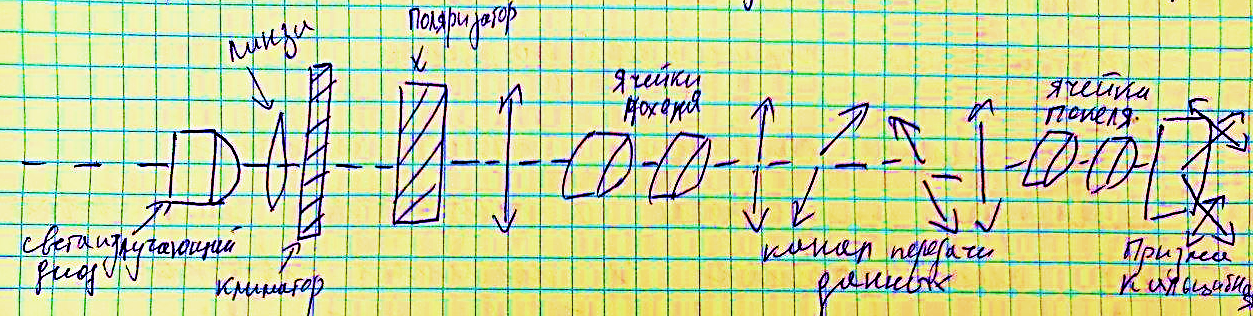
Отправитель генерирует и отправляет получателю последовательность фотонов, поляризацию которых выбирают случайным образом, она может быть 0, 45, 90, 135. Получатель принимает фотоны и по каждому из фотонов случайным образом решают замерять поляризацию данного фотона как горизонтальную или вертикальную. По открытому каналу получатель отправляет для каждого фотона какую поляризацию он использовал и при этом не сообщает результат измерений. По этому же каналу отправитель сообщает ему правильно ли был выбран вид измерения. Отправитель и получатель отбрасывает все случаи, когда получатель сделал неправильные замеры. Если квантовый канал не перехватывался оставшиеся виды поляризации и будут поделены между отправителем и получателем, и будут являться секретной информацией или ключом. Этот этап работы квантовой криптографической системы называется первичной квантовой передачей.

Отправитель отправляет фотоны имеющие одну из 4 возможных поляризаций, которую он выбирает случайным образом. | / - \ - - / | | Для каждого фотона получатель выбирает случайным образом тип измерения + или x. Допустим получатель выбрал + + x x + x x x +. Получатель записывает результаты измерений и сохраняет их в тайне. |1> |0?> |1?> |1> |0> |0?> |1> |0?> |1>. Допустим у отправителя была последовательность 111101101.

Следующим важным этапом является оценка попыток перехвата информации в канале. Оценку можно произвести отправителем либо получателем по открытому каналу путем сравнения и отбрасывания случайно выбранных ими подмножеств полученных данных. Если такое сравнение выявит наличие перехвата, отправитель и получатель отбрасывает все свои данные и начинает повторное выполнение первичной квантовой передачи. Будет эффективной проверкой для отправителя и получателя является проверкой на четность осуществляемая по открытому каналу. Например, отправитель сообщает 234, 3, 324 из 1000 бит. Достаточно повторить тест 20 раз, чтобы вычислить 20 ошибок.

Проблема заключается в том что это дорогие системы и что эти системы достаточно неустойчивые.

Практическая схема реализации схемы Коханена. В качестве канала данных может выступать оптоволокно. Источник – это диод или лазер. На принимающей стороне стоит призма, которая расщепляет пучок света на детектор и измеряет ортогональные поляризации. Для того чтобы противодействовать злоумышленнику применяют следующий подход, при транспортировке данных логическому 0 или 1 могут соответствовать определенные последовательности состояний, также они допускают коррекцию одной и более ошибок.

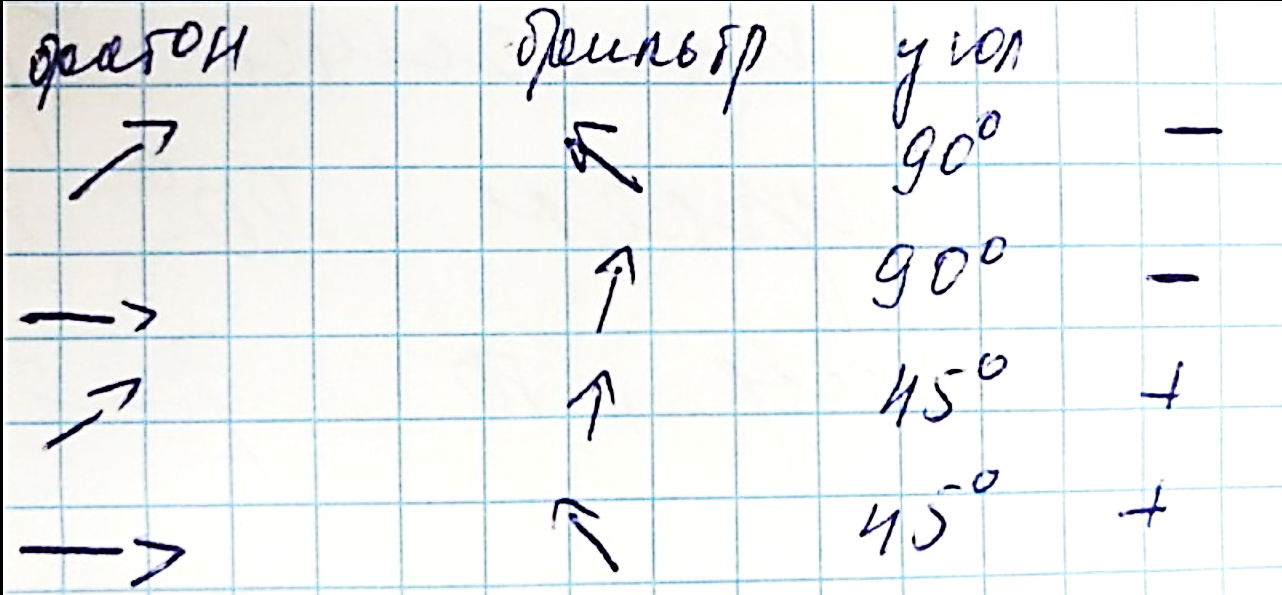


Протокол BB-92. В данном протоколе используют фотоны поляризованные в двух различных направлениях для представления 0 и 1, фотоны поляризованные вдоль направления 45 градусов несут информацию о 1 бите, фотоны поляризованные вдоль направления 0 градусов несут информацию о 0 бите.

Алгоритм:

1. Отправитель посылает поляризованные фотоны 0 и 45 градусов, представляющие 0 и 1.
2. Последовательность фотонов случайно ориентирована.
3. Получатель принимает фотоны через фильтры. Фильтры должны быть тоже ориентированы, в этом алгоритме 90, 135 градусов.
4. При этом если переданный фотон будет проанализирован получателем при помощи фильтра ориентированного под углом 90 градусов по отношению к передаваемому фотону, то фотон не пройдет через фильтр, если угол составит 45 градусов, то фотон проходит через фильтр с вероятностью 50%.
5. Для определения поляризации получатель анализирует выбранные случайным образом базисы. Если получатель анализирует принятый фотон с фильтром с ортогональным направлением поляризации, он не может точно определить что за данные представленные этим фотоном: 1 – фотон, который не проходит, 0 – не проходят с вероятностью 50%. Если направление поляризации между фотоном и фильтром не ортогональны, то получатель может определить, что фотон равняется 0. Если фотон был принят удачно, то бит кодирует 0 (если был принят фильтром ориентированным под углом 135 градусов), либо 1 (если был принят фильтром 90 градусов).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Передаваемый бит | 1 | 0 | 1 | 0 |
| Поляризация передачи | 45 | 0 | 45 | 0 |
| Поляризация приёма | -45 | -45 | 90 | 90 |
| Двоичный символ приема | 0 | 0 | 1 | 1 |
| Результат приема | – | – | + | – |



2 и 3 столбик поляризации не ортогональны, по этой причине мы с вероятностью 50% можем получить успешный результат. Допустим у нас успешное детектирование произошло в 3ей колонке.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Передаваемый бит | 1 | 0 | 1 | 0 | 1 | 0 |
| Поляризация передачи | 45 | 0 | 45 | 0 | 45 | 0 |
| Поляризация приёма | -45 | -45 | 90 | 90 | 90 | -45 |
| Двоичный символ приема | 0 | 0 | 1 | 1 | 1 | 0 |
| Результат приема | – | – | + | – | + | + |

Минимальное количество фотонов которое может быть принято – это порядка 20% от общего числа. Чтобы злоумышленник не узнал информацию о ключе по открытому каналу нужно передавать информацию только о том какие по порядку фотоны были приняты не называя состояния фильтров и полученные значения поляризации. Для обнаружения факта съема информации применяют подход как в BB-84.

Квантовый протокол E-91. Он использует ЕПР. Эффект ЕПР возникает когда сферический симметричный атом излучает 2 фотона противоположных направлениях в сторону двух наблюдателей. Фотоны излучаются с неопределенной поляризацией. Но в силу симметрии их поляризации всегда противоположны. Отправитель генерирует некоторое количество ЕПР фотонных пар. Один фотон из каждой пары он оставляет себе, другой отправляет. Если эффективность регистрации близка к 1, при получении отправителем значения поляризации 1, его партнер зарегистрирует 0, и наоборот. Данную схему проблематично реализовать из-за низкой эффективности регистрации и измерения поляризации единичного фотона. При горизонтальной поляризации H и использовании вертикального поляризатора V фотон не будет зарегистрирован. При 45 градусов поляризации фотона и вертикальном поляризаторе V вероятность регистрации составляет 50%. Далее в таблице предполагается, что для передатчика логическому 0 соответствует поляризация V, а 1 – +45 градусов для передатчика. Для принимающей стороны логическому 0 соответствует поляризация -45 градусов, а 1 – H.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Переданный бит | 1 | 0 | 1 | 0 |
| Поляризация передатчика | +45 | V | +45 | V |
| Поляризация приемника | -45 | -45 | H | H |
| Двоичный сигнал приема | 0 | 0 | 1 | 1 |
| Результат | - | - | + | - |

Первая и четверная колонки поляризации ортогональны, поэтому результат детектирования будет отсутствовать. В колонках 2 и 3 коды двоичных сигналов совпадают и поляризации ортогональны. Поэтому с вероятностью 50% мы можем получить позитивный результат в любой из этих колонках или в обоих. В нашем примере успешное детектирование произошло в третьей колонке и этот бит становится первым битом секретного ключа.

Управление кубитами с помощью квантовых вентелей. Вентелями являются базовые строительные блоки квантового компьютера. Как и их классические аналоги. Виртуализация – это представление набора вычислительных ресурсов или их логического объединения, абстрагировнание от аппаратной реализации и обеспечивая при этом логическую изоляцию друг от друга вычислительных процессов выполняемых на одном физическом ресурсе. Аппаратная виртуализация – виртуализация на уровне операционных систем. Виртуализация памяти – объединение нескольких устройств памяти представляемое как одно адресное пространство. Как и их классические аналоги они оперируют набором входов для получения выходом, основное отличие в том, что они работают одновременно во всех возможных состояниях кубита. Начнем с повтора квантовых состояний, все эти состояния являются чистыми однокубитными состояниями. |0> =[1 0] |1> = [0 1] |+> = (|0> + |1>) / sqrt(2) |-> = (|0> - |1>) / sqrt(2).

Основы диаграмм квантовой цепи.

* Время на квантовой диаграмме движется слева направо.
* Каждому кубиту соответствует одиночная горизонтальная линия.
* Вентили обычно обозначаются квадратами.\
* Тип вентиля обозначается буквами или другими символами в этом квадрате. Исключениями являются кубитные вентили у которых есть классические аналоги, например, НОД.

В результате измерения кубита все суперсозиции коллапсируют, квантовые свойства кубита исчезают и он превращается в обычный бит. Обозначение этих элементов на схеме. Однокубитные вентили – это самые простые элементы операцию выполняемую любым однокубитным вентилем можно представить как поворот вектора характеризующего состояние кубита в другую точку сверы блоха. Самые элементарные однокубитнные вентили – это вентили Паули: X Y Z.

* Вентиль Паули X (NOT) обозначает переключение. X = [[0 1] [1 0]]. Вращает кубит на 180 градусов вокруг оси X преобразует состояние 0 в 1, 1 в 0.
* Вентиль Паули Y. Y = [[0 –i] [i 0]]. Производит поворот вокруг оси Y сферы блока на 180 градусов. Состояние 0 в i|1>, в 1 в -i|0>
* Вентиль Паули Z. Z = [[1 0] [0 -1]]. Производит поворот вокруг оси Z сферы блока на 180 градусов. Состояние 0 остается 0, а 1 переходит в -|1>.
* Вентиль Адамара H. Воздействует на одиночные кубиты. И является комбинацией двух поворотов – поворот на 180 вокруг X и поворот на 90 градусов вокруг оси Y. Преобразование Адамара можно использовать при шифромании данных, в алгоритмах сжатия. То есть представляет собой (X + Y) / sqrt(2). Состояние |0> переходит в (|0> + |1>) / sqrt(2), а |1> = (|0> - |1>) / sqrt(2)
* SWAP(S) ж – ж. Данный вентиль меняет состояние двух кубитов в соответствии с базисом. |0>|1>=|1>|0>
* Управляемый cX –[x]–, cY –[y]–, cZ –[z]– Данный вентиль действует на 2 или более кубитов, где один и более кубитов является управляющими.
* Фазовый сдвиг pi/4 –[S]–.
* Фазовый сдвиг pi/8 –[T]–.
* СNOT •–(+) и CCNOT – управляемые вентили. Управляемые вентили – класс многокубитных вентилей, в котором на вход любого управляемого вентиля подается по меньшей мере один управляющий и один управляемый кубит. При чем вентиль выполнит операцию над управляемым кубитом, если управляющий кубит находится в определенном состоянии. Вентили, которые выполняют операцию при управляющем кубите |1> обозначаются заполненным кругом на проводе управляющего кубита. Вентили, которые выполняют операцию при управляющем кубите |0> обозначаются пустой окружностью на проводе управляющего кубита. Для того чтобы составить матрицу любого управляющего вентиля нужно дописать единичную матрицу в левом верхнем углу матрицы нужного вентиля, а все остальные ячейки заполнить 0, например вентиль NOT эквивалентен X Паули. CCNOT – вентиль TOFFOLI •–•–(+). Обратимый вентиль – его выход можно восстановить по его входу. Имея трехбитные входы и выход, если для первых двух бит установлено значение 1, то инвертируют третий бит, в противном случае все биты остаются неизменные. Обратимые вентили рассеивают меньше тепла, когда логические элементы поглащают свои входные данные, информация теряется, так как на выходе меньше информации чем на входе, такие потери информации – это рассеивание энергии в окружающую среду в виде тепла. Данный вентиль важен по следующим причинам: 1) квантовая механика требует чтобы преобразования были обратимые. 2) допускает более общие состояния – суперпозицию, чем классические системы компьютеров. Таким образом квантовый вентиль управляет вводом суперпозиций, вращает вероятности и создает другую суперпозицию в качестве своего выхода. Физически кубиты могут создаваться различными способами.

Авторизация, Идентификация

Есть специальные сервисы по тестированию безопасности web-ресурса.

Идентификация заключается в том что субъект сообщает ОС идентифицирующую информацию о себе.

Аутентификация заключается в том что субъект представляет ОС помимо идентифицирующей информации ещё и аутентифицирующую информацию подтверждающую, что пользователь является именно тем субъектом доступа, которому соответствует идентифицирующая информацию.

Авторизация субъекта доступа происходит после успешной идентификации и аутентификации. При авторизации субъекта ОС выполняет действия необходимые для того чтобы субъект мог выполнять действия в данной системе.

Д/з Виртуализация.