Разновидности ЭП

Пороговая подпись

Определение. Пороговая подпись (Threshold Signature Scheme или TSS) представляет собой метод создания и проверки цифровых подписей, который может использоваться для улучшения безопасности и управления ключами в блокчейн-системах. Она позволяет группе участников создавать подпись сообщения без необходимости раскрывать свои секретные ключи целиком.

История. Начинается в 1970 гг, когда американский криптограф Ади Шамир разработал схему секретного разделения подписи, которая позволяла разделить секретный ключ на несколько частей и определить порог, при котором можно восстановить секретный ключ и создать подпись (один из первых примеров пороговой подписи). Далее были разработаны различные схемы, которые позволяли группе участников совместно создавать подпись сообщения. Эти схемы предоставили инструменты для улучшения безопасности мультиподписей в различных приложениях. С появлением блокчейн-технологий многие криптографические методы были адаптированы для использования в блокчейне. Это позволило повысить безопасность подписей в криптовалютных кошельках, обеспечить безопасность смарт-контрактов и дать возможность группам участников совместно управлять активами и данными на блокчейне.

Принцип работы. Схема цифровой подписи — это тройка алгоритмов: KeyGen, Sign и Verify.

- Алгоритм KeyGen выводит пару открытого / закрытого ключей; закрытый ключ используется для подписи, а открытый ключ используется для проверки подписей.

Каждый раз алгоритм создания ключей выдает новую пару чисел (*sk, pk)=KeyGen( )*, где *sk* — секретный ключ, а *pk* — публичный.

Число *sk* выбирается случайным образом, а ключ *pk* получается применением к *sk* некоторого заранее установленного одностороннего преобразования. Одностороннее преобразование — это математическая операция, которая не позволяет восстановить входные параметры по результатам. В результате, по полученному числу *pk* нельзя определить исходное *sk*, так что никакой опасности в том, чтобы делать *pk* публичным значением, нет.

Классический пример одностороннего преобразования — возведение в степень по модулю. Обычное возведение в степень, $pk=a^{sk}$, где *a* — какое-то фиксированное число, является взаимно однозначным: зная pk, можно единственным образом восстановить *sk*.

Добиться одностороннего преобразования из операции возведения в степень, можно дополнительной операций, взятием модуля: $pk = a^{sk} mod\ q$, где *q* — еще одно целое положительное число. Эта операция возвращает остаток от деления на число *q*.

- Алгоритм подписи принимает закрытый ключ и сообщение и генерирует подпись.

Подпись вычисляется на основе двух параметров: секретного ключа *sk* и сообщения, на которое она в этот момент ставится. Однако сообщение может быть совершенно произвольным, поэтому применяется криптографически стойкое хэширование, то есть любую функцию, которая в качестве аргумента принимает произвольный набор символов и на выходе выдает число в фиксированном диапазоне, например, 256 бит. Это число называется хэшем, а сам процесс — хэшированием. На одном и том же входном сообщении хэш всегда одинаковый. Однако при малейшем изменении сообщения выдаваемое число (хеш) меняется так сильно, что связать изменения в сообщении с изменениями в хеш, становится невозможно. Помимо удобства использования, криптографически стойкий хеш также гарантирует целостность сообщения, т.е. что сообщение не менялось после создания подписи.

- Наконец, алгоритм Verify принимает открытый ключ, сообщение и подпись и проверяет правильность подписи.

На вход этот алгоритм получает публичный ключ *pk* того, кто оставил подпись, хэш *m* сообщения, на котором эта подпись стоит, и саму подпись *s*.

На выходе алгоритм выдает значение 1 (TRUE), если подпись прошла проверку, и значение 0 (FALSE), если нет.

Успешно пройденная проверка означает:

1. Публичный ключ pk и тот секретный ключ sk, что использовался при создании подписи, соответствуют друг другу. То есть тот, кто оставил подпись обладает секретным ключом *sk*.

2. Само подписанное сообщение (хеш) не менялось с момента создания подписи.

Пороговая схема подписи — это метод, который заменяет алгоритмы KeyGen и Sign схемы цифровой подписи интерактивным протоколом между несколькими сторонами.

Применимость в блокчейне. Помогает повысить безопасность и уменьшить риски, связанные с утечкой ключей, компрометацией участников или другими атаками на систему. Применяется в следующих ситуациях:

- Безопасность мультиподписи (Multisignature Security).

В блокчейне часто используются мультиподписи, когда для проведения транзакции требуется подпись нескольких участников. Пороговая

подпись позволяет более гибко управлять этими подписями, обеспечивая дополнительный уровень безопасности.

- Распределенное управление ключами.

В блокчейн-системах, особенно в многопользовательских и многоконтролируемых средах (например, корпоративных блокчейнах), ключи могут быть распределены между разными участниками. Пороговые подписи позволяют этим участникам совместно управлять ключами без необходимости доверять одному центральному участнику.

- Безопасность смарт-контрактов.

В контексте смарт-контрактов, которые выполняются на блокчейне, пороговые подписи могут использоваться для обеспечения безопасности и согласования важных действий. Например, несколько сторон могут совместно подписать смарт-контракт для его активации.

Примечание. Мультиподпись является разновидностью пороговой подписи.

Групповая подпись

Определение. Схема реализации электронной подписи, которая позволяет члену группы анонимно подписывать сообщение от имени группы.

Существенной особенностью групповой подписи является наличие администратора группы, который обеспечивает добавление в группу и имеет возможность раскрыть подписанта в случае возникновения споров.

История. Концепцию групповой подписи представили Дэвид Чаум и Евген Ван Хейст в 1991 году.

Принцип работы.

Следующий протокол предусматривает одного администратора:

- Администратор создаёт множество пар из открытых и закрытых ключей. Каждый член группы получает m уникальных закрытых ключей. (Если в группе n членов, то общее число пар ключей должно быть m*n.)
- Администратор публикует все открытые ключи в случайном порядке, не уточняя, кому какие ключи принадлежат.
- Для подписи член групп использует случайный секретный ключ из своего списка.
- Проверяющий последовательно перебирает список открытых ключей, пока один из них не удостоверит, что подписант принадлежит данной группе.
- В случае споров, администратор знает персональные списки открытых ключей и может узнать, кто был подписантом.

Предложенная схема обеспечивает:

- правом подписи обладают только члены группы подписывающих и каждый может подписать сообщение самостоятельно (в отличие от множественной подписи, где подпись коллективная);
- проверяющий может убедиться, что подписант из группы подписывающих, но не может установить, кто именно (частичная анонимность);
- сравнивая подписи под двумя одинаковыми сообщениями не должно быть понятно, один ли это подписант или нет;
- при необходимости администратор группы может установить, кто сгенерировал подпись;
- администратор не может объявить, что подпись принадлежит тому, кто её не накладывал;
- даже если все члены группы, включая администратора, объединят усилия, они не могут создать подпись, принадлежащую не члену группы;
- договорившаяся между собой подгруппа не может сгенерировать действительную подпись, которую администратор не сможет связать с одним из «заговорщиков».

Применение в блокчейне.

- Анонимность. Групповая подпись позволяет участникам создать общую подпись, не раскрывая свои индивидуальные ключи. Это может быть полезным в случаях, когда требуется анонимность участников транзакции.
- Масштабируемость. В блокчейне может быть много участников, и использование групповых подписей позволяет сократить количество необходимых подписей на транзакции, что снижает объем данных и уменьшает нагрузку на сеть.
- Эффективность. Групповая подпись может быть проверена как одна подпись, что упрощает процесс верификации для узлов блокчейна и снижает вычислительные затраты.
- Управление доступом. Групповая подпись может использоваться для определения прав доступа к ресурсам в блокчейне. Например, групповая подпись может быть создана для управления доступом к смарт-контрактам или активам.
- Доверие и безопасность. Групповая подпись обеспечивает высокий уровень безопасности и доверия, так как она требует согласия нескольких участников для создания подписи. Это делает ее надежным инструментом для защиты блокчейн-транзакций и данных.

Кольцевая подпись

Определение. Кольцевая подпись – разновидность криптографической цифровой подписи, которую может поставить любой член группы пользователей, каждый из которых имеет ключ.

История. Кольцевые подписи изобрели криптографы Рон Ривест, Ади Шамир и Яэль Тауман Калай и представили эту технологию на международной конференции ASIACRYPT в 2001 году.

Изначальная концепция предусматривала, что кольцевые подписи будут функционировать в качестве способа защиты от утечки секретной информации – в частности, из правительственных офисов. Впоследствии первоначальная модель была оптимизирована.

В 2006 году Эйитиро Фуджисаки и Котаро Судзуки предложили решение под названием Traceable Ring Signatures, позволяющее исправить уязвимость технологии кольцевых подписей (риск манипуляции со стороны злокозненных или безответственных подписантов). Оптимизированная версия этой разновидности кольцевой подписи в настоящее время применяется в монетах CryptoNote и обеспечивает неотслеживаемость отправителя в транзакции P2P, скрывая источник входов в транзакции.

В 2015 году Monero Research Labs выдвинула концепцию кольцевых конфиденциальных транзакций (Ring Confidential Transactions), которую представил и имплементировал разработчик Bitcoin Core Грегори Максвелл. Расширяя возможности анонимизации, присущие изначальной кольцевой подписи, кольцевые конфиденциальные транзакции скрывают не только тождество отправителя, но и суммы транзакций между отправителем и получателем.

Принцип работы. Кольцевые подписи выводят технологию групповых подписей на новый уровень, обеспечивая пользователю повышенный уровень конфиденциальности. В формате транзакций P2P в криптовалютах криптовалют – например, CryptoNote – кольцевые подписи защищают отправителя, скрывая принимающую сторону транзакции таким образом, что вычислительными средствами невозможно определить, кто является подписантом транзакции. Кольцевые подписи могут требовать множества различных открытых

ключей для верификации. «Кольцевой» подпись называется потому, что она состоит из ряда частичных цифровых подписей от разных пользователей. Вместе эти подписи образуют уникальную подпись. Группа подписей известна как кольцо и может быть произвольно выбрана из выходов от других пользователей на блокчейне.

Концептуально, кольцевые подписи аналогичны схеме, в рамках которой несколько сторон подписывают чек из совместного банковского счета, однако средствами криптографии подписант из числа членов группы скрывается.

Кольцевые изображения.

Конфиденциальные валюты, такие как Monero, сталкиваются с проблемой двойной траты. Отсутствие решения делает эти сети бесполезными в качестве цифровой валюты, поэтому нашлось решение в виде использования ключевых изображений в сочетании со схемой кольцевых подписей.

Ключевое изображение – это криптографический ключ, получаемый из потраченного выхода, и является частью каждой транзакции кольцевой подписи. Существуют только одно уникальное ключевое изображение для каждого выхода на блокчейне. Список всех использованных ключевых изображений сохраняется на блокчейне.

В силу криптографических особенностей ключевых изображений невозможно провести корреляцию между выходом на блокчейне и его ключевым изображением. Любые новые кольцевые подписи, использующие дубликат ключевого изображения, автоматически отвергаются как попытка двойной траты.

Применимость в блокчейне.

- Конфиденциальность транзакций. Кольцевые подписи могут использоваться для обеспечения анонимности при проведении транзакций в блокчейне. Когда пользователь отправляет транзакцию, его подпись объединяется с подписями других случайно выбранных участников сети, создавая кольцо подписей. Проверяющие узлы не могут однозначно определить, кто из участников создал подпись.

- Защита личных данных. Это позволяет пользователям обмениваться активами или информацией в блокчейне, не раскрывая свои идентификационные данные.

- Блокчейны с фокусом на приватности. Некоторые блокчейны, такие как Monero, используют кольцевые подписи как часть своих приватных транзакций. Это обеспечивает высокий уровень анонимности и конфиденциальности для пользователей.

- Смешивание транзакций. Кольцевые подписи также могут использоваться в процессе смешивания транзакций, чтобы усложнить отслеживание путей передачи средств и обеспечить анонимность.