Mercle Signature, IA2303, Gutu Nicolae

**One time Lamport Signature**

**Теория**

Подпись Лэмпорта (Lamport Signature) — это простая криптографическая схема цифровой подписи, основанная на одноразовых ключах. Подпись Лэмпорта считается криптографически устойчивой даже против квантовых атак и применима для защиты важных данных. Схема, будучи одноразовой, особенно удобна в схемах с небольшим количеством подписей, таких как Merkle Tree, который позволяет создавать один корневой публичный ключ для множества одноразовых подписей.

Суть подписи Лампорта в том – что она одноразовая, ее нельзя подделать, она будет эффективна даже при наличии квантовых компьютеров, так как она состоит из публичного и секретного ключей.

**Основные элементы**: документ для подписи, секретный ключ, публичный ключ

**Формирование подписи**

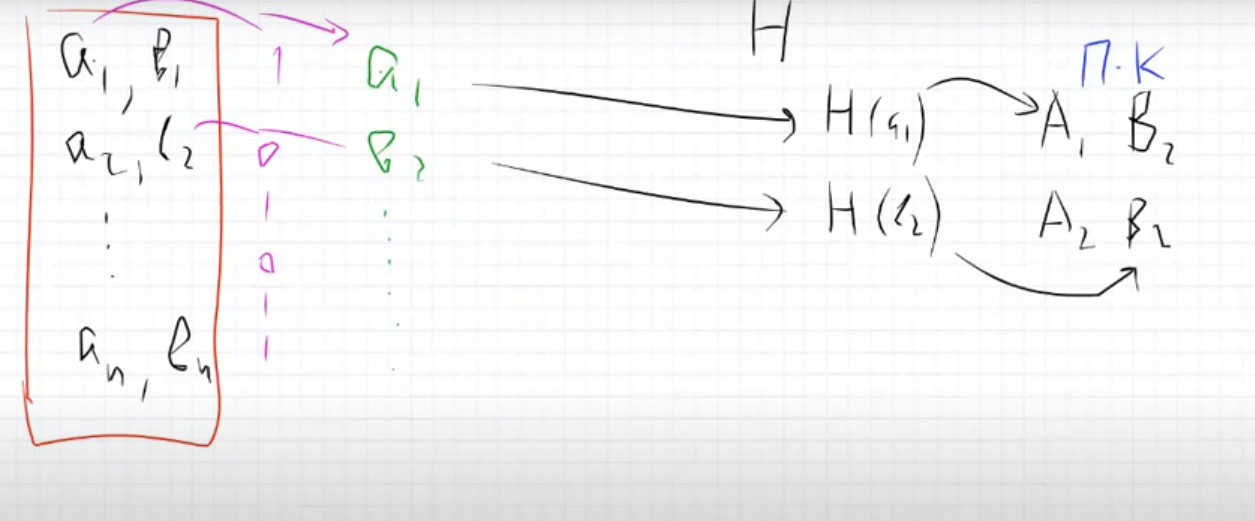
**1)Как формируется секретный ключ** – генерируются пары случайных чисе(a,b)л, число которых равно длине документа в двоичном виде (либо хэшу документа)

**2)Публичный ключ** - хэши от всех элементов секретного ключа

**3)Подпись** – документ (либо его хэш) представляются в двоичном виде, и каждый бит сопоставляется (по порядку) 1 паре случайных чисел из секретного ключа.

Если бит = 0, то берется число a, если бит = 1, то b

**4) Проверка**. Получатель должен иметь публичные ключи.  
Для проверки валидности подписи, ему отправляются: документ и подпись.  
Он имея публичные ключи, вычисляет хэши от значений в подписи, и сопоставляет с уже имеющимися у него публичными ключами. Если они совпадают – значит подпись верна.



Для оптимизации, можно давать получателю изначально не сами публичные ключи, так как их много, а хэш всех этих ключей, который он сам вычислит после получения документа.

Однако данная подпись является одноразовой, и ею можно подписать только 1 документ.

Для решения этой проблемы и используется **дерево Меркла:** изначально генерируются множество подписей, и чтоб не проверять каждую по отдельности, их проверяют через 1 общий “root hash”.

**1. Введение в Merkle Tree**

Дерево Меркла (Merkle Tree) — это структура данных, основанная на бинарном дереве и широко применяемая в криптографии и компьютерных науках. Основной идеей дерева Меркла является организация иерархии хэшей таким образом, чтобы можно было эффективно проверять целостность и подлинность данных без необходимости хранить весь набор данных.

**2. Структура и основные элементы дерева Меркла**

Каждый узел дерева Меркла представляет собой хэш определенного фрагмента данных. Дерево состоит из трех типов узлов:

* **Листья (лицевые узлы)**: каждый лист в дереве представляет хэш некоторого элемента данных. Если нужно проверить подлинность одного конкретного блока, то хэши его соседей позволяют пройти вверх по дереву, проверяя целостность каждого узла до самого корня.
* **Внутренние узлы**: создаются путем объединения и хэширования парных хэшей с нижележащего уровня. Каждый внутренний узел связан с двумя дочерними узлами. Хэш узла верхнего уровня создается из хэшей его дочерних узлов, что позволяет минимизировать размер хранимой информации при проверке.
* **Корневой узел (root hash)**: результат объединения всех внутренних узлов на последнем уровне. Этот корневой хэш — главное значение, представляющее все дерево и позволяющее проверять любые данные в структуре.

**3. Процесс построения дерева Меркла**

1. **Инициализация листьев**: Вначале для каждого блока данных вычисляется хэш, который будет представлять его в дереве.
2. **Объединение хэшей**: Далее хэши листьев объединяются попарно и хэшируются заново. Результаты этих операций формируют следующий уровень.
3. **Построение уровней до корня**: Процесс объединения продолжается до тех пор, пока не останется только один хэш, который становится корнем дерева.
4. **Дублирование узлов для нечетных листьев**: если на каком-то уровне оказывается нечетное количество узлов, последний узел дублируется, чтобы можно было объединить его с самим собой. Это гарантирует, что каждый уровень полностью заполнен парами.

**4. Проверка подлинности с помощью дерева Меркла (Merkle Proof)**

Merkle Proof позволяет проверить подлинность отдельных данных, входящих в структуру, без необходимости полностью загружать или хранить весь набор данных.

1. **Формирование Merkle Proof**: Для проверки подлинности какого-либо блока данных нужно получить "доказательство" — хэш соседа каждого узла, который находится на пути от листа до корневого узла.
2. **Проверка доказательства**: имея документ и Merkle Proof, получатель может хэшировать документ и объединять его с хэшами из proof на каждом уровне. Если финальный хэш совпадает с корневым узлом, подлинность документа подтверждается.

**5. Применение Merkle Tree**

* **Криптовалюты и блокчейн**: В блокчейне дерево Меркла используется для хранения хэшей транзакций. Это упрощает процесс проверки транзакций и снижает нагрузку на сеть.
* **Системы контроля версий**: дерево Меркла помогает хранить и проверять целостность версий данных, что делает его полезным для децентрализованных хранилищ.
* **Цифровые подписи и сертификаты**: в некоторых схемах подписи дерево Меркла позволяет проверять иерархию сертификатов, облегчая управление.

**6. Преимущества Merkle Tree**

* **Эффективность проверки**: Merkle Tree позволяет проверять подлинность отдельных данных без необходимости обращаться ко всему набору.
* **Экономия пространства**: возможность хранить только корневой хэш для проверки всех данных позволяет сократить объем передаваемой информации.
* **Безопасность**: структура дерева затрудняет подмену данных или взлом, так как любой малейший сдвиг на нижних уровнях изменит корневой хэш.

**7. Недостатки Merkle Tree**

* **Одноразовое использование**: Для создания и проверки нового набора данных необходимо заново строить дерево.
* **Ограничения изменения данных**: Вносить изменения в дерево после его создания сложно, так как это изменяет всю структуру.

**Заключение**

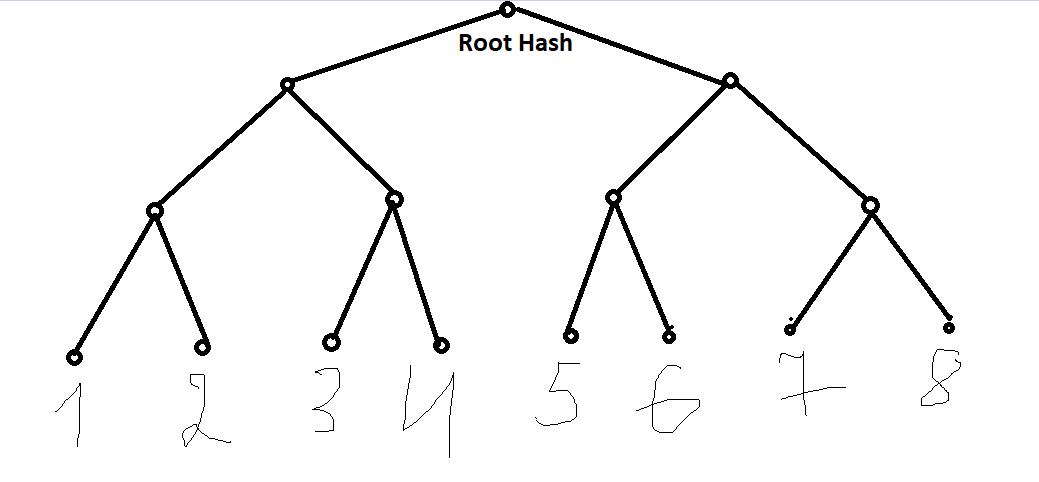
Merkle Tree — это мощный инструмент для безопасного и эффективного управления данными. Его применение в блокчейне, системах версионирования и цифровых подписях делает его ценным компонентом в современной криптографии и информационной безопасности.

Кратко о самом алгоритме и его реализации:

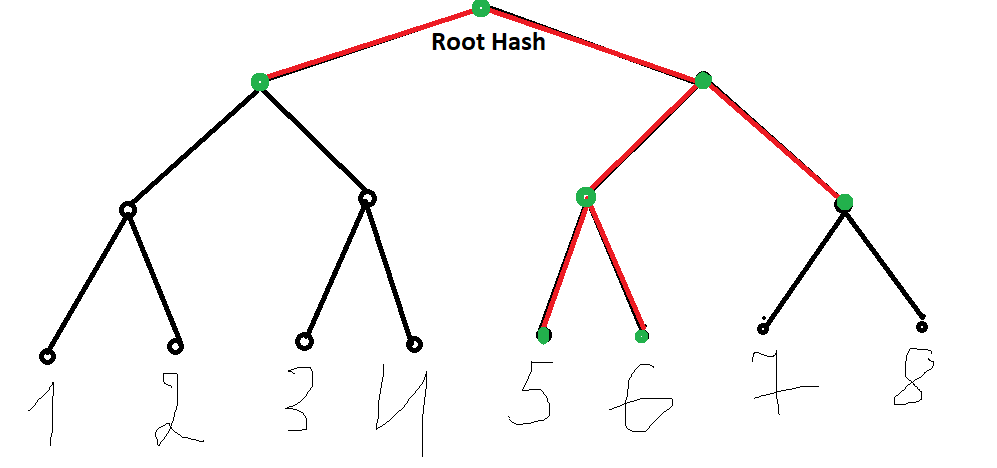
Дерево меркла – это структура, позволяющая создать систему из большого числа подписей, создавая единый коренной хэш, для проверки всех подписей, не выгружая все транзакции, а лишь малую ветвь, соединяющую конкретную подпись и корневой хэш.

Как это работает:

Для всех подписей, мы создаем единых хэш, благодаря которому можно проверить любой документ на подлинность, имея корневой хэш и путь от документа до него.

Корневой Хэш  


Допустим, проверяем путь от документа №5, тогда путь будет выглядеть так:



Так как при изменении любого документа, root-hash изменится, то проверка таким образом гарантирует, что ни 1 документ не был изменён после отправки.