Triptych

Логарифмически масштабируемые связываемые кольцевые подписи и их применение

Саранг Ноезер, кандидат технических наук

Исследовательская лаборатория Monero

17 сентября 2020

Цель

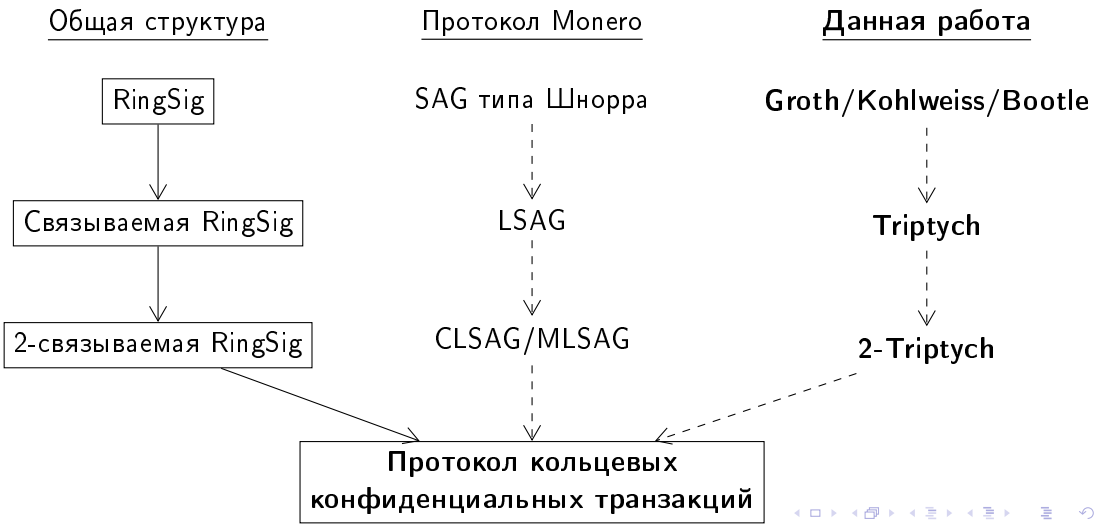
Мы хотим построить схему **конфиденциальных транзакций**, обладающую следующими свойствами:

- не требующими доверия настройками и параметрами
- сублинейным масштабированием размера в зависимости от размера анонимной группы
- возможностью групповой верификации $O(n/\log(n))$
- безопасной совместимостью с одноразовой адресацией
- поддержкой выполнения операций с использованием мультиподписей

Наша схема называется **Triptych**.

Это результат совместной работы с **Брэндоном Гуделлом**.

Наша стратегия



Кольцевые подписи

Кольцевые подписи является схемой подписи, используемой для подписания сообщения от лица неинтерактивной анонимной группы, представленной публичными ключами. Подписанту известен секретный ключ (по крайней мере) к одному из публичных ключей, входящих в группу.

Верификатору известно, что только один из ключей в наборе публичных ключей принадлежит подписанту, но ему не известно, какой именно. Поэтому

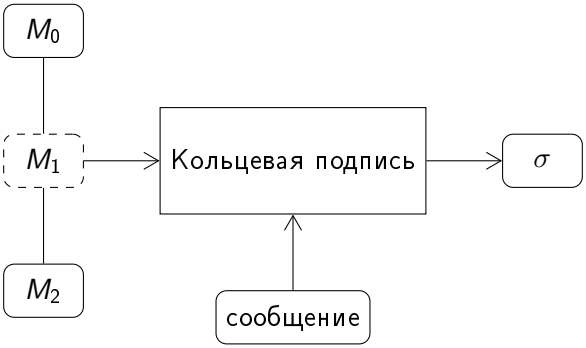
$$\mathrm{Sign}(m, \{M_0, M_1, \ldots\}; (l, r)) \to \sigma$$

подписывает сообщение m так, что M_l использует r как секретный ключ и

$$\mathrm{Verify}(m, \{M_0, M_1, \ldots\}, \sigma) \to \{0, 1\}$$

верифицируется.

Кольцевые подписи



Кольцевые подписи Groth/Kohlweiss/Bootle (GKB)

В работе (IACR 2014/764) **Groth** и **Kohlweiss** предлагается новая система доказательства с нулевым разглашением, позволяющая построить схему кольцевой подписи. **Bootle** и его соавторы в своей работе (IACR 2015/643) описали более эффективный вариант этой системы.

Система предполагает построение сигма-протокола для отношения

$$\left\{\{M_0, \ldots, M_{N-1}\}; (l, r) : 0 \leq l < N, M_l = \mathrm{Com}(0, r)\right\}$$

для схемы обязательства Com, логарифмически масштабируемой по размеру относительно N.

Для преобразования в схему кольцевой подписи используется эвристический подход Фиата-Шамира и сообщение встраивается в хеш транскрипта.

Свойства

Неформально нам бы хотелось достичь нескольких полезных свойств. Они вытекают непосредственно из свойств лежащего в основе сигма-протокола.

- **Правильность**. Действительные подписи всегда будут верифицироваться.
  - Полнота
- **Анонимность**. Невозможность определения подписывающего индекса.
  - Нулевое разглашение
- **Невозможность подделки**. Невозможность формирования подписи без известного секретного ключа.
  - (Особая) устойчивость

Связываемые кольцевые подписи

Что, если бы нам захотелось выявить двойное подписание безопасным способом?

Связываемая кольцевая подпись является кольцевой подписью, также обеспечивающей связываемость подписи. Любые две действительные подписи, которые можно связать, используют один и тот же (неизвестный) секретный ключ. Таким образом,

$$\mathsf{Link}(\sigma, \sigma') \to \{0, 1\}$$

позволяет определить, были ли две подписи подписаны одним и тем же секретным ключом.

Выбор анонимной группы может оказаться критически важным с точки зрения практической безопасности.

Можно создавать схемы, которые будут либо зависимы, либо независимы от анонимной группы.

Связываемая кольцевая подпись Triptych

Путём добавления свойства связываемости в схему GKB мы получаем **Triptych** (IACR 2020/018).

Это сводит сигма-протокол к отношению

$$\left\{\{M_0, \ldots, M_{N-1}\}, J; (l, r) : 0 \leq l < N, M_l = \mathsf{Com}(0, r), rJ = U\right\}$$

с глобально постоянной U, где J является связующим тегом. Для проверки связываемости следует сравнить теги.

Для преобразования в схему кольцевой подписи используется эвристический подход Фиата-Шамира и сообщение встраивается в хеш транскрипта.

Расширение схемы GKB до Triptych

Возможно ли расширение схемы с GKB до Triptych? Обязательства по нулевой сумме следует рассматривать в качестве публичных ключей с групповым генератором G.

В случае с GKB мы доказываем знание r таким образом, что некоторое обязательство будет иметь форму $rG = M$.

В случае с Triptych мы повторно используем некоторые из скрытых данных данного доказательства об r, чтобы показать, что U соответствует форме $rJ = U$. Поскольку U имеет глобально постоянное значение, доказывающая сторона может сделать это только в том случае, если укажет $J \equiv (1/r)U$, являющуюся верифицируемой случайной функцией.

Поскольку сигма-протокол является (особо) устойчивым и преобразование $r \mapsto J$ является биекцией, мы получаем свойство связываемости.

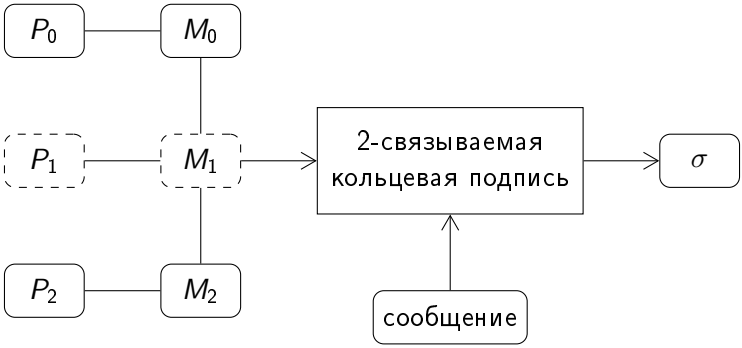
2-связываемые кольцевые подписи

Мы расширяем схему связываемой кольцевой подписи, чтобы продемонстрировать знание ключей в параллельных списках публичных ключей.

Подписант даёт два списка публичных ключей и показывает, что ему известен секретный ключ к обоим публичным ключам с одним и тем же неизвестным индексом в обоих списках.

Таким образом, мы сохраняем свойство связываемости, но только для одного из списков (вскоре мы более подробно расскажем об этом)!

2-связываемые кольцевые подписи



2-связываемые кольцевые подписи Triptych

Мы изменяем Triptych, чтобы построить 2-связываемую кольцевую подпись; это даже можно сделать в более общем плане.

Это сводит сигма-протокол к отношению

$$\Big\{\{M_0,\dots,M_{N-1}\},\{P_0,\dots,P_{N-1}\},J;(l,r,s):$$
$$0\le l<N, M_l=\mathrm{Com}(0,r), P_l=\mathrm{Com}(0,s), rJ=U\Big\}$$

в которое теперь включены два списка публичных ключей.

Несмотря на то, что нам необходимы новые данные доказательства секретного ключа s, мы можем повторно использовать уже существующие данные доказательства по индексу l.

Протокол кольцевых конфиденциальных транзакций

Нам бы хотелось построить протокол **конфиденциальных транзакций**, который бы позволил:

- использовать множество выходов транзакций
- генерировать множество выходов транзакций
- скрывать суммы выходов
- скрывать подписывающие индексы
- поддерживать скрытую адресацию в сети

Мы можем сделать, используя произвольные 2-связываемые кольцевые подписи, такие как 2-Triptych или CLSAG.

Протокол кольцевых конфиденциальных транзакций

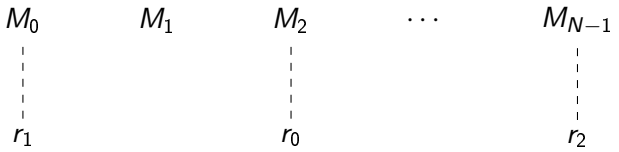
Определяем обязательство Педерсена $\mathrm{Com}(v, r) \equiv vH + rG$ для групповых генераторов G, H.

Нам необходимо сгенерировать транзакцию, использующую W существующих выходов и генерирующую T новых выходов.

Формируем одиночную анонимную группу с $N \geq W$ публичных ключей $\{M_k\}_{k=0}^{N-1}$ так, чтобы для набора секретных индексов $\{l_u\}_{u=0}^{W-1} \subset [0, N)$ у нас было $M_{l_u} = r_u G$ для всех $0 \leq u < W$, где каждый r_u являлся бы секретным ключом.

Протокол кольцевых конфиденциальных транзакций

Рассмотрим пример, где $W = 3$, а $N \geq 3$ являются произвольными.



Таким образом, набором секретных индексов будет $\{I_u\}_{u=1}^{W-1} = \{2, 0, N-1\}$.

Протокол кольцевых конфиденциальных транзакций

Каждый из использованных выходов $0 \leq u < W$ связан с обязательством по сумме a_u:

$$P_{l_u} \equiv \mathrm{Com}(a_u, s_u)$$

Поскольку система доказательства Triptych подразумевает знание обязательства по нулевой сумме, формируем офсет обязательства для каждого использованного выхода с одинаковым значением, но единообразной случайной маской:

$$P'_u \equiv \mathrm{Com}(a_u, s'_u)$$

Это сводит обязательства к нулю:

$$P_{l_u} - P'_u = \mathrm{Com}(a_u, s_u) - \mathrm{Com}(a_u, s'_u) = \mathrm{Com}(0, s_u - s'_u)$$

Протокол кольцевых конфиденциальных транзакций

Генерируем $0 \leq j < T$ пновых выходов, где каждый имеет связанное с собой обязательство по суме (и доказательство диапазона):

$$Q_j \equiv \mathrm{Com}(b_j, t_j)$$

Для $1 \leq j < T$ выбираем случайные маски t_j. Затем задаём

$$t_0 \equiv \sum_{u=0}^{W-1} s'_u - \sum_{j=1}^{T-1} t_j$$

так, чтобы верификатор смог произвести эту проверку, если соотношение использованных и новых выходов будет нормальным

$$\sum_{u=0}^{W-1} P'_u - \sum_{j=0}^{T-1} Q_j = 0$$

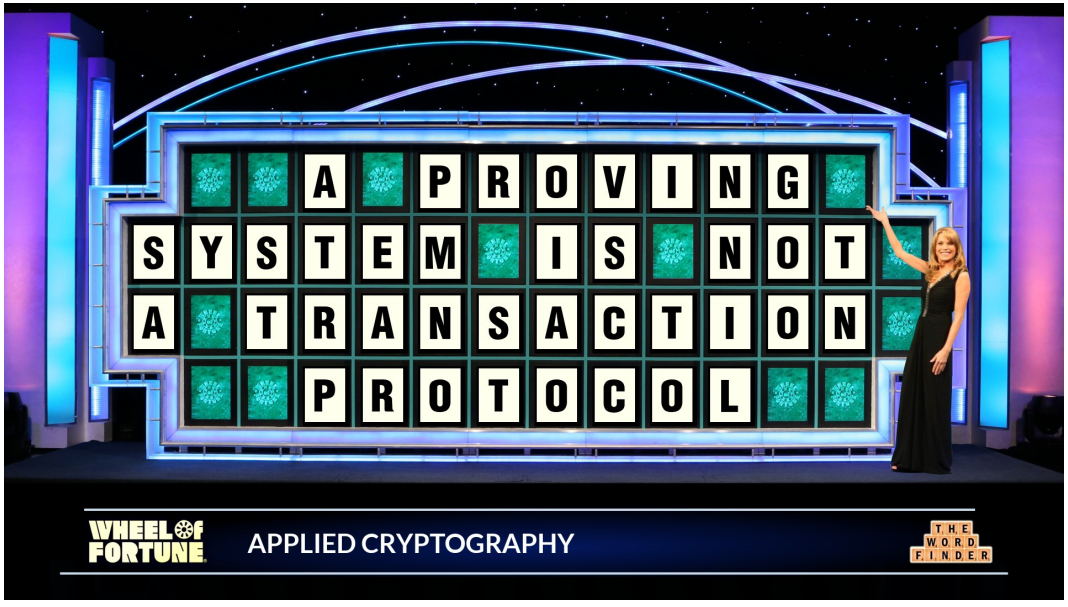
Протокол кольцевых конфиденциальных транзакций

Наконец, генерируем подпись для каждого из использованных выходов $0 \leq u < W$, используя следующие входы отношения 2-Triptych:

$$\left\{\{M_k\}_{k=0}^{N-1}, \{P_k - P'_u\}_{k=0}^{N-1}, (1/r_u)U; (l_u, r_u, s_u - s'_u)\right\}$$

Чтобы верифицировать каждую транзакцию, необходимо:

- верифицировать каждую из связываемых кольцевых подписей
- произвести тест на связываемость для всех подписей
- выполнить успешную проверку правильности соотношения
- верифицировать доказательства диапазона всех выходов


A PROVING
SYSTEM IS NOT
A TRANSACTION
PROTOCOL
WHEEL of FORTUNE
APPLIED CRYPTOGRAPHY
THE WORD FINDER

Сравнение

	Размер	Верификация	Группирование	Адресация	Накопление
Triptych	$O(\log N)$	$O(N/\log N)$	есть	есть	нет
Arcturus	$O(\log N)$	$O(N/\log N)$	есть	есть	есть
CLSAG	$O(N)$	$O(N)$	нет	есть	нет
Lelantus	$O(\log N)$	$O(N/\log N)$	есть	нет	нет
Omniring	$O(\log N)$	$O(N/\log N)$	нет	есть	есть
RingCT 3.0	$O(\log N)$	$O(N/\log N)$	есть	есть	частично

Данная таблица умышленно упрощена.

Заключение

Triptych вляется системой доказательства с нулевым разглашением, которая может использоваться для построения схемы связываемой (и 2-связываемой!) кольцевой подписи, которая, в свою очередь, может усилить модель конфиденциальных транзакций. Система:

- не требует доверенных настроек или параметров
- масштабируется логарифмически по размеру (при этом увеличение размера зависит от рациональности используемого размера анонимной группы)
- масштабируется (суб)-линейно во время верификации с возможностью группирования
- полностью совместима со скрытой адресацией в сети
- поддерживает выполнение операций с использованием мультиподписей посредством общего секрета Пэйе

Вопросы?