Arcturus: эффективные доказательства для конфиденциальных транзакций

Саранг Ноезер (Sarang Noether)
Исследовательская лаборатория Monero (Monero Research Lab)
sarang.noether@protonmail.com

6 ноября 2020 г.

Аннотация

В случае с распределёнными цифровыми активами конфиденциальные транзакции используются для демонстрации равенства значений, скрытых в обязательствах при сохранении неопределённости подписанта. В прошлой работе было описано доказательство знания открытия обязательств по нулю с одинаковым индексом для всего множества наборов обязательств с сохранением неопределённости подписанта, а также оценка верифицируемой случайной функции, используемой в качестве связующего тега и использующей это с целью построения связываемой кольцевой подписи, под названием Triptych, которое может использоваться как структурный элемент модели конфиденциальных транзакций. В данной работе нами предлагается расширение Triptych для построения Arcturus, системы доказательства, позволяющей доказать знание открытия множества обязательств по нулю в пределах одного набора, правильность структуры верифицируемой случайной функции, оцениваемой при каждом открытии, и равенство значений в отдельном списке обязательств в пределах одного доказательства. Несмотря на то, что надёжность зависит от нового допуска сложности двойного дискретного логарифма, мы используем данные, взятые из блокчейна Monero, чтобы продемонстрировать, что Arcturus может использоваться в рамках модели конфиденциальных транзакций с целью обеспечения более быстрой групповой верификации в сравнении с существующими на сегодня конструкциями без каких-либо доверенных настроек.

1 Введение

Распределённые цифровые активы, начиная с Bitcoin, при авторизации транзакций и передаче прав на трату средств используют кольцевые подписи. Несмотря на то, что ранние протоколы, в основе которых лежит модель, предложенная Bitcoin, имеют преимущество, связанное с простотой, им не хватает необходимых свойств, обеспечивающих приватность и неотличимость транзакций. В частности, граф адресов и подписи, формируемый блокчейном для таких цифровых активов, очень просто отследить, а суммы, которые в соответствии с подписью разрешено переводить в транзакции, видимы. Чтобы защитить пользователей распределённых активов и обеспечить более высокий уровень неотличимости транзакций в целях взаимозаменяемости, на пути к конфиденциальным транзакциям было предложено и реализовано несколько методов.

Протокол CryptoNote, его раннее предложение, связанное с сокрытием графов транзакций, полагается на связываемые кольцевые подписи в ключе выходов транзакций с обозначенными суммами [17]; транзакция включает в себя отдельную подпись для каждой такой суммы, в результате чего возникают проблемы с масштабированием.

Другим усовершенствованием стал протокол RingCT [13], который использовал обязательства Педерсена по суммам, связанным с выходами транзакций, и расширял структуру кольцевой подписи, предложенную Лю и др. (Liu et al.) в работе [10], так чтобы поддерживались параллельные подписи в матричном расположении, что устраняло необходимость в обозначенных выходах транзакций. Тем не менее, обе эти конструкции используют связываемые кольцевые подписи, размер которых масштабируется линейно с размером анонимной группы, используемой для создания каждой подписи. Более поздние методы обеспечения приватности транзакций используют аккумуляторы, чтобы представить

заданное состояние выходов транзакций. Zerocoin [11] для подтверждения правильности транзакций задействовал аккумуляторы RSA и связанные доказательства, но суммы были фиксированными, протокол использовал очень большие и неэффективные доказательства, транзакции ограничивались простой операцией сжигания-создания монет в прозрачном блокчейне, а применение групп RSA требовало процесса доверенной настройки. Другой, более поздней работой стал Zerocash [15], который заменил аккумуляторы RSA и связанные доказательства более краткими доказательствами, относящимися к аккумуляторам дерева Меркла, позволяя совершать анонимные переводы с произвольными суммами. Тем не менее, Zerocoin как и Zerocash использовал систему доказательства, требующую доверительной настройки; в конечном счёте это послужило основанием для протоколов Zcash.

До недавнего времени протоколы транзакций, целью которых являлось обеспечение устойчивого сокрытия подписанта, гибкой непосредственной анонимной передачи произвольных сумм, подразумевали некоторый компромисс между реализацией не требующей доверия структуры и эффективности с точки зрения размера доказательств и времени верификации.

Последняя работа в этой области опирается на одну из двух новых систем доказательства для построения транзакций, которая масштабируется логарифмически с размером указываемой доказывающей стороной анонимной группы, но при этом не требует доверенных настроек. Система доказательства, использующая одно из многих обязательств по нулю, предложенная Гротом и Кёльвейсом (Groth and Kohlweiss) в работе [7], использовалась для построения простых кольцевых подписей и транзакций в стиле Zerocoin, а позднее была расширена Бутлем (Bootle) [1] так, чтобы более эффективно поддерживать рассчитываемые кольцевые подписи.

Эта система доказательства формирует основу протокола Lelantus [8], расширяющего модель транзакций в стиле Zerocoin, предложенную в работе [7], за счёт использования обязательств Педерсена с множеством оснований, включающих в себя суммы наряду с порядковыми номерами; изменённые доказательства демонстрируют равенство, а множественные доказательства необходимы для создания типичных транзакций.

Тем не менее транзакции Lelantus позволяют идентифицировать отправителя транзакции позднее, когда получатель решит потратить их средства; внесение соответствующих исправлений решает проблему отслеживания, но это делается за счёт устранения полезной конструкции одноразовых адресов, гарантирующих анонимность получателя.

Та же система доказательства, что была описана в работе [7], используется и в Triptych [12], а если точнее, это конструкция многомерной связываемой кольцевой подписи, которая может использоваться для построения конфиденциальных транзакций подобно тому, как это описано в работе [13]; что важно, Triptych поддерживает одноразовые адреса и произвольные суммы, но при этом по-прежнему требует использования множества доказательств для траты множества выходов транзакций.

Что интересно, последняя независимая работа расширяет схему [7] так, чтобы поддерживались обязательства по множеству обязательств в одном списке (что мы также показываем ниже), что определённым образом применимо в отношении Zether [4]; тем не менее, в данном случае используется подход, отличающийся от того, что мы используем в данной работе, и, по-видимому, предполагающий больший размер доказательств.

Система доказательства Bulletproofs [2] использует метод сжатия скалярного произведения для построения доказательств диапазона и соответствия схемы с возможностью их логарифмического масштабирования. Помимо большее широкого развёртывания доказательств диапазона обязательств, структура, лежащая в основе Bulletproofs, используется для построения более специализированных систем доказательства конфиденциальных транзакций. Omniring [9] использует этот метод для построения транзакций, демонстрирующих право на трату множества входов транзакций с сокрытием подписанта в рамках одного единственного доказательства, а доказательство диапазона при этом интегрируется напрямую. В результате получаются очень маленькие доказательства; тем не менее, если сравнивать с другими подходами, время верификации увеличивается, а требования к генерированию уникальной группы означают, что доказательства нельзя эффективно верифицировать группами.

RingCT 3.0 [18] также использует структуру в стиле Bulletproofs.

В ранней версии транзакции требовали использования отдельных доказательств для множества входов; и, несмотря на то, что обновлённые версии уже позволяли использовать одно доказательство для всех входов транзакции, также требовалось, чтобы количество входов дополнялось и становилось больше в два раза, что повышало сложность верификации.

1.1 Наш вклад

Нами была расширена система доказательства Triptych, предложенная в работе [12], по двум важным направлениям, и полученная система была названа Arcturus.

Во-первых, мы даём доказывающей стороне возможность демонстрировать одновременное знание множества подписывающих ключей в рамках единственного доказательства, использующего один набор комбинированных элементов доказательства; в отличие от того, что предлагалось в работе [18], наше изменение допускает использование любого количества входов транзакции без каких-либо ограничений.

Мы сохраняем оценку верифицируемой случайной подписи, создающей связующие теги, необходимые для обнаружения повторного подписания с использованием того же открытия обязательства по доказательствам.

Во-вторых, мы демонстрируем равенство значения обязательства Педерсена напрямую в пределах того же доказательства; в частности, мы показываем, что определённая комбинация обязательств по входам и выходам суммируется в обязательство по нулю. Мы отмечаем, что надёжность полученной системы доказательства зависит от нового допуска сложности двойного дискретного логарифма. И, несмотря на то, что мы считаем использование этого нового допуска разумным, он ещё не тестировался.

В совокупности эти изменения могут найти применение в протоколе транзакций, обеспечивая эффективность конфиденциальных транзакций в блокчейне при отсутствии необходимости в доверенных настройках.

В рамках транзакции может быть подписано множество входов с сокрытием подписанта, а также может быть доказана сбалансированность транзакции при помощи единственного доказательства, что является главным усовершенствованием используемых в настоящее время конструкций, требующих множества доказательств и отдельных вспомогательных обязательств Педерсена по сумме.

Кроме того, нами используются фактические данные блокчейна Monero, цифрового актива, чтобы напрямую сравнить общий размер и время верификации Arcturus и Triptych, и двух отдельных конструкций RingCT 3.0. Нами было выявлено, что Arcturus обеспечивает превосходные показатели верификации, если сравнивать с другими конструкциями конфиденциальных транзакций, не требующих доверенных настроек, при сравнимых показателях по масштабированию с точки зрения размера.

2 Предварительные данные

2.1 Публичные параметры

Допустим, $\mathbb{G}$ является циклической группой, в которой задача дискретного логарифмирования является сложной, но F является её полем скалярных величин.

Допустим, $\mathsf{H} : \{0,1\}^* \to \mathbb{F}$ и $\mathcal{H} : \{0,1\}^* \to \mathbb{G}$ является криптографической хеш-функцией.

Допустим, $N = n^m$ является положительным целым числом, где $m > 1$ (в случае с нашей конструкцией мы используем $n = 2$).

Допустим, G, H, U и любая точка в форме G_i или H_i (возможно, с множеством индексов) являются единообразно случайными генераторами $\mathbb{G}$, отношение дискретных логарифмов друг к другу не известно. Следует отметить, что все такие генераторы могут быть получены при помощи случайных публичных параметров; например, использование соответствующей хеш-функции с разделением доменов может подойти.

Подразумевается, что все такие публичные параметры включают в себя строку глобальной ссылки, известную всем участникам; в частности, для удобочитаемости нами в целом исключается явная ссылка на публичные параметры в определениях алгоритма и хешей транскрипта Фиата-Шамира.

2.2 Тензорное обязательство

Допустим, Com является схемой аддитивно гомоморфного обязательства, обеспечивающего совершенное сокрытие, и (по крайней мере) являющегося обязательным для вычисления.

В данной работе мы допускаем использование простого расширения схемы обязательства Педерсена: для $x, r \in \mathbb{F}$ определяем $\mathrm{Com}(x, r) \equiv rG + xH$ как обязательство по значению x со степенью случайности r.

Для трёхмерного тензора $f \equiv (f_{i,j,k}) \subset \mathbb{F}$ и скрывающего фактора $r \in \mathbb{F}$ определяем тензорное обязательство Педерсена

$$\mathrm{Com}(f, r) \equiv rG + \sum_{i,j,k} f_{i,j,k} G_{i,j,k}$$

используя фиксированные независимые генераторы, как было описано выше.

Подразумевается, что операции по тензорам производятся покомпонентно, например, если $f \equiv (f_{i,j,k})$ и $g \equiv (g_{i,j,k})$ являются такими тензорами для $\mathbb{F}$, то $f + g \equiv (f_{i,j,k} + g_{i,j,k})$ и так далее.

2.3 Другая система обозначений

Для целых чисел или элементов поля i, j дельта-символ Кронекера $\delta(i, j)$ будет равен 1, если $i = j$ и 0 в противном случае, если берётся выход из соответствующего набора.

Иногда мы используем нижний индекс в форме i_j, чтобы обозначить разряд j для i, где разложение i берётся по основанию n с заполнением длинны m:

$$\sum_{j=0}^{m-1} i_j n^j = i$$

Такая система обозначений используется там, где может возникнуть путаница.

2.4 Сигма-протоколы

Для заданного отношения $\mathcal{R}$ сигма-протокол $\mathcal{R}$ будет интерактивным протоколом запроса-ответа между доказывающей стороной и верификатором, в рамках которого доказывающая сторона желает убедить верификатора в том, что ей известно свидетельство, соответствующее утверждению, содержащемуся в $\mathcal{R}$.

Сигма-протокол является полным, надёжным и подразумевает нулевое разглашение информации.

Эти определения хорошо известны, и найти их можно, например, в работе [7].

По существу, эти свойства предполагают следующее:

- *Абсолютная полнота*: В случае со свидетельством по утверждению, содержащемуся в $\mathcal{R}$, добросовестная доказывающая сторона всегда сможет убедить добросовестного верификатора в его достоверности.
- *Особая надёжность*: При наличии утверждения в $\mathcal{R}$ это означает, что если доказывающая сторона способна выдать транскрипты действительных доказательств в ответ на множество запросов верификатора, то из этих транскриптов также можно извлечь и свидетельство по такому утверждению.
- *Особое нулевое разглашение при наличии добросовестного верификатора*: При наличии утверждения и запроса известного верификатора можно произвести смоделированный транскрипт без знания соответствующего действительного свидетельства.

Сигма-протоколы можно сделать неинтерактивными, если заменить случайные запросы верификатора запросами транскриптов на основе хешей в соответствии с моделью случайного оракула; это называется эвристическим подходом Фиата-Шамира [6].

2.5 Допуск сложности

Нами даётся определение новому допуску криптографической сложности, используемому далее для того, чтобы продемонстрировать надёжность нашей конструкции.

Определение 1 (Задача двойного дискретного логарифмирования)**.** Допустим, $\mathbb{G}$ является группой, для которой задача дискретного логарифмирования является сложной, допустим, $\mathbb{F}$ является её полем скалярных величин. Допустим, $n > 0$. Рассмотрим следующую игру между запрашивающей стороной и игроком $\mathcal{A}$ с вероятностным полиномиальным временем:

- Запрашивающая сторона единообразно случайным образом выбирает значения $G, H \in \mathbb{G}$ и отправляет оба эти значения $\mathcal{A}$.
- $\mathcal{A}$ выбирает и отправляет обратно множества $\{G_i\}_{i=0}^{n-1}, \{H_i\}_{i=0}^{n-1} \subset \mathbb{G}$ запрашивающей стороне.
- Запрашивающая сторона единообразно случайным образом выбирает множество $\{\mu^i\}_{i=0}^{n-1} \subset \mathbb{F}$ и отправляет его $\mathcal{A}$.
- $\mathcal{A}$ выбирает и отправляет обратно множество $\{x_i\}_{i=0}^{n-1} \subset \mathbb{F}$ запрашивающей стороне.

Мы можем утверждать, что игрок $\mathcal{A}$ победил в игре (n, ϵ, t) с решением задачи двойного дискретного логарифмирования, если в течение времени, не превышающего значение t и с вероятностью, равной, по крайней мере, ϵ, действительными были следующие условия:

- $\sum_{i=0}^{n-1} \mu^i \left(G_i - x_i G\right) = 0$
- $\sum_{i=0}^{n-1} \mu^i \left(H - x_i H_i\right) = 0$
- Существовал такой индекс $0 \leq i < n$, что либо $x_i G \neq G_i$, либо $x_i H_i \neq H$.

3 Система доказательства

Нами предлагается сигма-протокол для следующего отношения:

$$\mathcal{R} \equiv \Bigg\{ \{M_i\}_{i=0}^{N-1}, \{P_i\}_{i=0}^{N-1}, \{J^{(u)}\}_{u=0}^{w-1}, \{Q_j\}_{j=0}^{T-1} \subset \mathbb{G} \,;\, \left(\{l^{(u)}\}_{u=0}^{w-1}, \{r^{(u)}\}_{u=0}^{w-1}, y\right) : M_{l^{(u)}} = r^{(u)} G \;\forall\, u \in [0, w) \text{ and } r^{(u)} J^{(u)} = U \;\forall\, u \in [0, w) \text{ and } \sum_{u=0}^{w-1} P_{l^{(u)}} - \sum_{j=0}^{T-1} Q_j = yG \Bigg\}$$

Здесь охвачены элементы, необходимые для авторизации транзакции, о которых мы будем говорить далее; знание подписывающих ключей $\{r^{(u)}\}$ демонстрирует, что у доказывающей стороны есть право на подписание входов транзакции, а также, а знание секретного ключа y к разнице обязательства по сумме показывает, что суммы транзакции сбалансированы.

Наконец, сравнение верифицируемой случайной функции, используемой для получения $\{J^{(u)}\}$, будет использоваться для предотвращения попыток подписания одним и тем же секретным ключом без раскрытия соответствующего публичного ключа, что важно с точки сокрытия подписанта и защиты от попыток двойной траты в пределах доказательств или между ними.

На рисунках 1 и 2 показано взаимодействие доказывающей стороны и верификатора. Затем мы доказываем, что действия доказывающей стороны и верификатора составляют сигма-протокол, являющийся совершенно правильным, и что он обладает свойствами особой надёжности и особого нулевого разглашения при наличии добросовестного верификатора.

4 Безопасность

Теорема 1. *Сигма-протокол, представленный на рисунках1 и 2, отражает отношение $\mathcal{R}$ и является совершенно правильным, обладает свойствами особой надёжности $(m + 1)$ и особого нулевого разглашения при наличии добросовестного верификатора.*

$\underline{\mathcal{P}:}$

- Выбираем случайное $r_A \in \mathbb{F}$ и $\left\{a_{j,i}^{(u)}\right\}_{i=1,j,u=0}^{n-1,m-1,w-1} \subset \mathbb{F}$. Задаём

$$\{a_{j,0}^{(u)}\}_{j,u=0}^{m-1,w-1} \equiv -\sum_{i=1}^{n-1} a_{j,0}^{(u)}$$

  и определяем $A \equiv \mathrm{Com}(a, r_A)$.

- Определяем $\left\{\sigma_{j,i}^{(u)}\right\}_{i,j,u=0}^{n-1,m-1,w-1} \subset \mathbb{F}$ так, чтобы $\sigma_{j,i}^{(u)} \equiv \delta\left(l_j^{(u)}, i\right)$ (пользуясь нашим обозначением разложения) и выбираем случайное $r_B \in \mathbb{F}$. Определяем $B \equiv \mathrm{Com}(\sigma, r_B)$.

- Выбираем случайное $r_C \in \mathbb{F}$ и определяем $C \equiv \mathrm{Com}(a(1-2\sigma), r_C)$.

- Выбираем случайное $r_D \in \mathbb{F}$ и определяем $D \equiv \mathrm{Com}(-a^2, r_D)$.

- Для $0 \leq u < w$ определяем такие коэффициенты $\left\{p_{k,j}^{(u)}\right\}_{k,j=0}^{N-1,m-1}$, чтобы

$$p_k^{(u)}(x) \equiv \prod_{j=0}^{m-1}\left(\sigma_{j,k}^{(u)} x + a_{j,k}^{(u)}\right) = \delta\left(l^{(u)}, k\right) x^m + \sum_{j=0}^{m-1} p_{k,j}^{(u)} x^j$$

  (пользуясь нашим обозначением разложения). Затем определяем $p_{k,j} \equiv \sum_{u=0}^{w-1} p_{k,j}^{(u)}$ и $p_k(x) \equiv \sum_{u=0}^{w-1} p_k^{(u)}(x)$ соответственно.

- Выбираем случайное $\{\rho_j\}_{j,u=0}^{m-1,w-1}, \left\{\overline{\rho}_j^{(u)}\right\}_{j,u=0}^{m-1,w-1} \subset \mathbb{F}$.

- Задаём $\mu \equiv \mathsf{H}(\{M_k\}, \{P_k\}, \{J^{(u)}\})$ (так же и для включения всех публичных параметров).

- Определяем $\{X_j\}_{j=0}^{m-1} \subset \mathbb{G}$ так, чтобы

$$X_j \equiv \sum_{k=0}^{N-1} p_{k,j} \mu^k M_k + \sum_{u=0}^{w-1} \rho_j^{(u)} G$$

- Определяем $\{Y_j\}_{j=0}^{m-1} \subset \mathbb{G}$ так, чтобы

$$Y_j \equiv U \sum_{k=0}^{N-1} p_{k,j} \mu^k + \sum_{u=0}^{w-1} \rho_j^{(u)} J^{(u)}$$

- Определяем $\{Z_j\}_{j=0}^{m-1} \subset \mathbb{G}$ так, чтобы

$$Z_j \equiv \sum_{k=0}^{N-1} p_{k,j} P_k + \sum_{u=0}^{w-1} \overline{\rho}_j^{(u)} G$$

$\underline{\mathcal{P} \to \mathcal{V}:}$
$A, B, C, D, \{X_j\}, \{Y_j\}, \{Z_j\}$

Рис. 1: Сигма-протокол для $\mathcal{R}$

$\underline{\mathcal{V} \to \mathcal{P}:}$
$\xi \in \{0,1\}^*$

$\underline{\mathcal{P}(\xi):}$

- Определяем $\left\{f_{j,i}^{(u)}\right\}_{i=1,j,u=0}^{n-1,m-1,w-1}$ так, чтобы $f_{j,i}^{(u)} \equiv \sigma_{j,i}^{(u)}\xi + a_{j,i}^{(u)}$.
- Определяем $z_A \equiv r_A + \xi r_B$ и $z_C \equiv \xi r_C + r_D$.
- Определяем $\left\{z_R^{(u)}\right\}_{u=0}^{w-1} \subset \mathbb{F}$ так, чтобы

$$z_R^{(u)} \equiv \mu^{l^{(u)}} r^{(u)} \xi^m - \sum_{j=0}^{m-1} \rho_j^{(u)} \xi^j$$

- Определяем:

$$z_S \equiv \xi^m \left(\sum_{u=0}^{w-1} s^{(u)} - \sum_{j=0}^{T-1} t_j \right) - \sum_{j=0}^{m-1} \left(\xi^j \sum_{u=0}^{w-1} \overline{\rho}_j^{(u)} \right)$$

$\underline{\mathcal{P} \to \mathcal{V}:}$
$\{f_{j,i}^{(u)}\}_{j=0,i=1,u=0}^{m-1,n-1,w-1}, z_A, z_C, \{z_R^{(u)}\}, z_S$

$\underline{\mathcal{V}:}$

- Для $0 \le u < w$ и $0 \le j < m$ задаём:

$$f_{j,0}^{(u)} \equiv \xi - \sum_{i=1}^{n-1} f_{j,i}^{(u)}$$

- Принимаем результат исключительно в том случае, если:

$$A + \xi B = \mathrm{Com}(f, z_A) \quad (1)$$

$$\xi C + D = \mathrm{Com}(f(\xi - f), z_C) \quad (2)$$

$$\sum_{k=0}^{N-1} \mu^k M_k \left[\sum_{u=0}^{w-1} \left(\prod_{j=0}^{m-1} f_{j,k_j}^{(u)} \right) \right] - \sum_{j=0}^{m-1} \xi^j X_j - \sum_{u=0}^{w-1} z_R^{(u)} G = 0 \quad (3)$$

$$U \sum_{k=0}^{N-1} \mu^k \left[\sum_{u=0}^{w-1} \left(\prod_{j=0}^{m-1} f_{j,k_j}^{(u)} \right) \right] - \sum_{j=0}^{m-1} \xi^j Y_j - \sum_{u=0}^{w-1} z_R^{(u)} J^{(u)} = 0 \quad (4)$$

$$\sum_{k=0}^{N-1} P_k \left[\sum_{u=0}^{w-1} \left(\prod_{j=0}^{m-1} f_{j,k_j}^{(u)} \right) \right] - \sum_{j=0}^{m-1} \xi^j Z_j - \xi^m \sum_{j=0}^{T-1} Q_j - z_S G = 0 \quad (5)$$

Рис. 2: Сигма-протокол для $\mathcal{R}$ (продолжение)

Доказательство. Доказательство подобно тому, что приводится в работе [12] и которое, в свою очередь, следует методам, описанным в работах [7, 1].

Чтобы показать, что протокол является абсолютно полным, предположим, что верификатор получает честное доказательство. Нам необходимо продемонстрировать, что все уравнения верификатора выполняются.

Чтобы показать, что уравнение 1 выполняется, отмечаем, что поскольку

$$\begin{aligned} A + \xi B &= \mathrm{Com}(a + \xi\sigma, r_A + \xi r_B) \\ &= \mathrm{Com}(a + \xi\sigma, z_A), \end{aligned}$$

достаточно продемонстрировать, что $f_{j,i}^{(u)} = a_{j,i}^{(u)} + \xi\sigma_{j,i}^{(u)}$ для всех $0 \leq i < n$ и $0 \leq j < m$, и $0 \leq u < w$. Если $i \neq 0$, значит, данное уравнение выполняется по определению $f_{j,i}^{(u)}$. В случае если $i = 0$ всё будет иначе. Чтобы показать это, воспользуемся тем фактом, что

$$\sum_{i=0}^{n-1} \sigma_{j,i}^{(u)} = 1$$

для всех $0 \leq j < m$ и $0 \leq u < w$, в соответствии с конструкцией:

$$\begin{aligned} f_{j,0}^{(u)} &= \xi - \sum_{i=1}^{n-1} f_{j,i}^{(u)} \\ &= \xi - \sum_{i=1}^{n-1} \left(a_{j,i}^{(u)} + \xi\sigma_{j,i}^{(u)} \right) \\ &= \xi - \sum_{i=1}^{n-1} a_{j,i}^{(u)} - \xi \sum_{i=1}^{n-1} \sigma_{j,i}^{(u)} \\ &= \xi + a_{j,0}^{(u)} - \xi \left(1 - \sigma_{j,0}^{(u)} \right) \\ &= a_{j,0}^{(u)} + \xi\sigma_{j,0}^{(u)} \end{aligned}$$

Мы демонстрируем, что уравнение 2 выполняется. Так как:

$$\begin{aligned} \xi C + D &= \mathrm{Com}(\xi a(1 - 2\sigma) - a^2, \xi r_C + r_D) \\ &= \mathrm{Com}(\xi a(1 - 2\sigma) - a^2, z_C), \end{aligned}$$

достаточно показать, что

$$f_{j,i}^{(u)} \left(\xi - f_{j,i}^{(u)} \right) = \xi a_{j,i}^{(u)} \left(1 - 2\sigma_{j,i}^{(u)} \right) - \left(a_{j,i}^{(u)} \right)^2$$

для всех $0 \leq i < n$ и $0 \leq j < m$ и $0 \leq u < w$. Мы используем нашу предшествующую работу и тот факт, что $\left(\sigma_{j,i}^{(u)} \right)^2 = \sigma_{j,i}^{(u)}$, поскольку $\sigma_{j,i}^{(u)} \in \{0, 1\}$:

$$\begin{aligned} f_{j,i}^{(u)} \left(\xi - f_{j,i}^{(u)} \right) &= \left(a_{j,i}^{(u)} + \xi\sigma_{j,i}^{(u)} \right) \left(\xi - a_{j,i}^{(u)} - \xi\sigma_{j,i}^{(u)} \right) \\ &= a_{j,i}^{(u)}\xi - \left(a_{j,i}^{(u)} \right)^2 - 2a_{j,i}^{(u)}\xi\sigma_{j,i}^{(u)} + \left(\xi^2\sigma_{j,i}^{(u)} - \xi^2 \left(\sigma_{j,i}^{(u)} \right)^2 \right) \\ &= a_{j,i}^{(u)}\xi - \left(a_{j,i}^{(u)} \right)^2 - 2a_{j,i}^{(u)}\xi\sigma_{j,i}^{(u)} + \left(\xi^2 \left(\sigma_{j,i}^{(u)} \right)^2 - \xi^2 \left(\sigma_{j,i}^{(u)} \right)^2 \right) \\ &= \xi a_{j,i}^{(u)} \left(1 - 2\sigma_{j,i}^{(u)} \right) - \left(a_{j,i}^{(u)} \right)^2 \end{aligned}$$

Затем мы демонстрируем, что уравнение 3 выполняется:

$$
\begin{aligned}
& \sum_{k=0}^{N-1} \mu^k M_k \left[\sum_{u=0}^{w-1} \left(\prod_{j=0}^{m-1} f_{j,k_j}^{(u)} \right) \right] - \sum_{j=0}^{m-1} \xi^j X_j - \sum_{u=0}^{w-1} z_R^{(u)} G \\
= & \sum_{k=0}^{N-1} \mu^k M_k p_k(\xi) - \sum_{j=0}^{m-1} \xi^j \left(\sum_{k=0}^{N-1} p_{k,j} \mu^k M_k + \sum_{u=0}^{w-1} \rho_j^{(u)} G \right) - \sum_{u=0}^{w-1} z_R^{(u)} G \\
= & \sum_{k=0}^{N-1} \mu^k M_k \left(p_k(\xi) - \sum_{j=0}^{m-1} \xi^j p_{k,j} \right) - \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \rho_j^{(u)} G - \sum_{u=0}^{w-1} z_R^{(u)} G \\
= & \sum_{k=0}^{N-1} \mu^k M_k \left[\xi^m \sum_{u=0}^{w-1} \delta\left(l^{(u)}, k \right) \right] - \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \rho_j^{(u)} G - \sum_{u=0}^{w-1} \left[\mu^{l^{(u)}} r^{(u)} \xi^m - \sum_{j=0}^{m-1} \rho_j^{(u)} \xi^j \right] G \\
= & \xi^m \sum_{u=0}^{w-1} \mu^{l^{(u)}} r^{(u)} G - \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \rho_j^{(u)} G - \xi^m \sum_{u=0}^{w-1} \mu^{l^{(u)}} r^{(u)} G + \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \rho_j^{(u)} G \\
= & 0
\end{aligned}
$$

Уравнение 4 выполняется с использованием той же алгебры:

$$
\begin{aligned}
& \sum_{k=0}^{N-1} \mu^k U \left[\sum_{u=0}^{w-1} \left(\prod_{j=0}^{m-1} f_{j,k_j}^{(u)} \right) \right] - \sum_{j=0}^{m-1} \xi^j Y_j - \sum_{u=0}^{w-1} z_R^{(u)} J^{(u)} \\
= & \sum_{k=0}^{N-1} \mu^k U p_k(\xi) - \sum_{j=0}^{m-1} \xi^j \left(\sum_{k=0}^{N-1} p_{k,j} \mu^k U + \sum_{u=0}^{w-1} \rho_j^{(u)} J^{(u)} \right) - \sum_{u=0}^{w-1} z_R^{(u)} J^{(u)} \\
= & \sum_{k=0}^{N-1} \mu^k U \left(p_k(\xi) - \sum_{j=0}^{m-1} \xi^j p_{k,j} \right) - \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \rho_j^{(u)} J^{(u)} - \sum_{u=0}^{w-1} z_R^{(u)} J^{(u)} \\
= & \sum_{k=0}^{N-1} \mu^k U \left[\xi^m \sum_{u=0}^{w-1} \delta\left(l^{(u)}, k \right) \right] - \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \rho_j^{(u)} (r^{(u)})^{-1} U - \sum_{u=0}^{w-1} \left[\mu^{l^{(u)}} r^{(u)} \xi^m - \sum_{j=0}^{m-1} \rho_j^{(u)} \xi^j \right] (r^{(u)})^{-1} U \\
= & x^m \sum_{u=0}^{w-1} \mu^{l^{(u)}} U - \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \rho_j^{(u)} (r^{(u)})^{-1} U - \xi^m \sum_{u=0}^{w-1} \mu^{l^{(u)}} U + \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \rho_j^{(u)} (r^{(u)})^{-1} U \\
= & 0
\end{aligned}
$$

Наконец мы показываем, что выполняется уравнение 5:

$$
\begin{aligned}
& \sum_{k=0}^{N-1} P_k \left[\sum_{u=0}^{w-1} \left(\prod_{j=0}^{m-1} f_{j,k_j}^{(u)} \right) \right] - \sum_{j=0}^{m-1} \xi^j Z_j - \xi^m \sum_{j=0}^{T-1} Q_j - z_S G \\
= & \sum_{k=0}^{N-1} P_k p_k(\xi) - \sum_{j=0}^{m-1} \xi^j \left(\sum_{k=0}^{N-1} p_{k,j} P_k + \sum_{u=0}^{w-1} \overline{\rho}_j^{(u)} G \right) - \xi^m \sum_{j=0}^{T-1} Q_j - z_S G \\
= & \sum_{k=0}^{N-1} P_k \left(p_k(\xi) - \sum_{j=0}^{m-1} \xi^j p_{k,j} \right) - \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \overline{\rho}_j^{(u)} G - \xi^m \sum_{j=0}^{T-1} Q_j - z_S G \\
= & \xi^m \sum_{u=0}^{w-1} (s^{(u)} G + a_u H) - \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \overline{\rho}_j^{(u)} G - \xi^m \sum_{j=0}^{T-1} (t_j G + b_j H) - \xi^m \left(\sum_{u=0}^{w-1} s^{(u)} - \sum_{j=0}^{T-1} t_j \right) G + \\
& \sum_{j=0}^{m-1} \xi^j \sum_{u=0}^{w-1} \overline{\rho}_j^{(u)} G \\
= & \left(\sum_{u=0}^{w-1} a_u - \sum_{j=0}^{T-1} b_j \right) H \\
= & \ 0
\end{aligned}
$$

Следовательно, протокол является совершенно полным.

Затем мы демонстрируем, что сигма-протокол обладает свойством особого нулевого разглашения при наличии добросовестного верификатора. Для этого мы строим симулятор, который при заданном запросе случайного верификатора ξ, может построить транскрипт доказательства с идентифчным распределением по действительному доказательству.

Сначала отмечаем, что симулятор, представленный в доказательстве Леммы 1 в работе [1], переводится практически так же, как в нашем случае, так как мы можем преобразовать тензорные обязательства в матричную структуру с необходимым свойством суммы. Сначала единообразно случайным образом симулятор выбирает $B \in \mathbb{G}$; затем упомянутая лемма гарантирует действительное моделирование элементов доказательства $A, C, D, z_A, z_C, \{f_{j,i\neq 0}^{(u)}\}$, и на этой основе мы можем вычислить $\{f_{j,0}^{(u)}\}$. В действительном доказательстве B так же единообразно распределяется.

Элементы доказательства $\{X_j\}_{j=1}^{m-1}, \{Y_j\}_{j=1}^{m-1}, \{Z_j\}_{j=1}^{m-1}$ являются независимыми и единообразно распределяются в действительном доказательстве, так как элементы $\{\rho_j\}, \{\overline{\rho}_j\}$ распределяются единообразно, а задача дискретного логарифмирования в $\mathbb{G}$ является сложной; следовательно, симулятор выбирает их единообразно случайным образом. Поскольку верификация требует, чтобы значения X_0, Y_0, Z_0 уникально определялись другими элементами в соответствующих множествах, они выбираются симулятором именно таким образом.

Наконец элементы $\{z_R^{(u)}\}_{u=0}^{w-1}$ и z_S являются независимыми и единообразно распределяются в действительном доказательстве при наличии запроса случайного верификатора ξ, поэтому симулятор может выбирать их единообразно случайным образом. Следовательно, протокол обладает свойством особого нулевого разглашения при наличии добросовестного верификатора.

Мы утверждаем, что протокол обладает свойством особой надёжности $(m+1)$ при $m > 1$. Чтобы продемонстрировать это, мы строим экстрактор, который при наличии $m+1$ действительных ответов на $m+1$ отдельных запросов верификатора по одному и тому же начальному утверждению производит действительное свидетельство для данного утверждения. В частности, мы производим изменённое свидетельство для следующего отношения на базе информации, представленной в алгоритме доказы-

вающей стороны, где μ определяется, как и раньше:

$$\mathcal{R}' \equiv \Bigg\{ \{M_k\}_{k=0}^{N-1}, \{P_k\}_{k=0}^{N-1}, \{J^{(u)}\}_{u=0}^{w-1}, \{Q_j\}_{j=0}^{T-1} \subset \mathbb{G}\,;\, \left(\{l^{(u)}\}_{u=0}^{w-1}, \{r^{(u)}\}_{u=0}^{w-1}, y\right) : \\ \sum_{u=0}^{w-1} \mu^{l^{(u)}} M_{l^{(u)}} = \sum_{u=0}^{w-1} \mu^{l^{(u)}} r^{(u)} G \text{ and } \sum_{u=0}^{w-1} \mu^{l^{(u)}} r^{(u)} J^{(u)} = \sum_{u=0}^{w-1} \mu^{l^{(u)}} U \text{ and } \sum_{u=0}^{w-1} P_{l^{(u)}} - \sum_{j=0}^{T-1} Q_j = yG \Bigg\}$$

Отмечаем, что в том случае, если мы допускаем, что задача двойного дискретного логарифмирования в $\mathbb{G}$ является сложной, а H смоделировано как случайный оракул, свидетельство для $\mathcal{R}'$, созданное экстрактором, также должно являться свидетельством для $\mathcal{R}$, использующим то же утверждение. Это означает, что выделение свидетельства для $\mathcal{R}'$ является достаточным для обеспечения желаемой надёжности.

Предположим, что для данного утверждения у нас имеется множество $(m+1)$ отдельных запросов верификатора $\{\xi_e\}_{e=0}^{m}$, соответствующих отдельным действительным ответам следующей формы:

$$\left\{ \{{}_e f_{j,i}^{(u)}\}, \{{}_e z_R^{(u)}\}, {}_e z_S \right\}_{e=0}^{m}$$

В соответствии со свойством 3-особой надёжности, описанным в работе [1], и при $m > 1$ мы получаем действительные выделения $\{\sigma_{j,i}^{(u)}\}_{u=0}^{w-1}$ и $\{a_{j,i}^{(u)}\}_{u=0}^{w-1}$, а свойство обязательства Педерсена гарантирует, что (с высокой степенью вероятности) мы получим:

$${}_e f_{j,i}^{(u)} = \sigma_{j,i}^{(u)} \xi_e + a_{j,i}^{(u)} \;\forall\, e \in [0, m]$$

При помощи выделенных значений вычисляем полином:

$$p_k(x) \equiv \sum_{u=0}^{w-1} \left[\prod_{j=0}^{m-1} \left(\sigma_{j,k}^{(u)} x + a_{j,k}^{(u)} \right) \right]$$

для всех $k \in [0, N)$. В результате выделения $\{\sigma_{j,i}^{(u)}\}_{u=0}^{w-1}$ получаем множество подписывающего индекса $\{l^{(u)}\}_{u=0}^{w-1}$.

Мы видим, что p_k имеет степень m только если $k \in \{l^{(u)}\}_{u=0}^{w-1}$. Следовательно, существуют такие множества коэффициентов $\{\overline{X}_j, \overline{Y}_j, \overline{Z}_j\}_{j=0}^{m-1}$, уникально вычисленные на основе утверждения и выделенных значений, что уравнения 3, 4 и 5 имеют следующую форму:

$$\begin{aligned} \xi^m \sum_{u=0}^{w-1} \mu^{l^{(u)}} M_{l^{(u)}} + \sum_{j=0}^{m-1} \xi^j \overline{X}_j &= \left(\sum_{u=0}^{w-1} z_R^{(u)} \right) G \\ \xi^m \sum_{u=0}^{w-1} \mu^{l^{(u)}} U + \sum_{j=0}^{m-1} \xi^j \overline{Y}_j &= \sum_{u=0}^{w-1} z_R^{(u)} J^{(u)} \\ \xi^m \sum_{u=0}^{w-1} P_{l^{(u)}} + \sum_{j=0}^{m-1} \xi^j \overline{Z}_j - \xi^m \sum_{j=0}^{T-1} Q_j &= z_S G \end{aligned}$$

Строим матрицу Вандеромонда V, где ряд e является вектором $(1, \xi_e, \ldots, \xi_e^m)$. Поскольку все ξ_e являются отдельными, ряды V охватывают $\mathbb{F}^{m+1}$; следовательно, существуют такие взвешенные значения $\{\theta_e\}_{e=0}^{m}$, что полученная линейная комбинация рядов даёт вектор $(0, \ldots, 0, 1)$. То есть $\sum_{e=0}^{m} \theta_e \xi_e^j = \delta(j, m)$.

Для каждого из предшествующих трёх уравнений, следовательно, мы можем построить линейную комбинацию по e. Для первого уравнения:

$$\sum_{u=0}^{w-1} \mu^{l^{(u)}} M_{l^{(u)}} = \sum_{e=0}^{m} \theta_e \xi_e^m \left(\sum_{u=0}^{w-1} \mu^{l^{(u)}} M_{l^{(u)}} \right) + \sum_{e=0}^{m} \theta_e \left(\sum_{j=0}^{m-1} \xi_e^j \overline{X}_j \right) = \sum_{u=0}^{w-1} \left(\sum_{e=0}^{m} \theta_{ee} z_R^{(u)} \right) G$$

Следовательно, мы можем определить выделенные значения для каждого $r^{(u)}$:

$$r^{(u)} \equiv \frac{1}{\mu^{l^{(u)}}} \sum_{e=0}^{m} \theta_{ee} z_R^{(u)}$$

Отмечаем, что то же самое свидетельство появляется во втором уравнении:

$$\sum_{u=0}^{w-1} \mu^{l^{(u)}} U = \sum_{e=0}^{m} \theta_e \xi_e^m \left(\sum_{u=0}^{w-1} \mu^{l^{(u)}} U \right) + \sum_{e=0}^{m} \theta_e \left(\sum_{j=0}^{m-1} \xi_e^j \overline{Y}_j \right) = \sum_{u=0}^{w-1} \left(\sum_{e=0}^{m} \theta_{ee} z_R^{(u)} \right) J^{(u)}$$

Это означает, что требования к каждому $r^{(u)}$ соблюдены. То же действительно для третьего уравнения:

$$\sum_{u=0}^{w-1} P_{l^{(u)}} - \sum_{j=0}^{T-1} Q_j = \sum_{e=0}^{m} \theta_e \xi_e^m \left(\sum_{u=0}^{w-1} P_{l^{(u)}} - \sum_{j=0}^{T-1} Q_j \right) + \sum_{e=0}^{m} \theta_e \left(\sum_{j=0}^{m-1} \xi_e^j \overline{Z}_j \right) = \left(\sum_{e=0}^{m} \theta_{ee} z_S \right) G$$

Следовательно, мы получаем $y \equiv \sum_{e=0}^{m} \theta_{ee} z_S$. □

5 Модель транзакций

Теперь опишем, как сигма-протокол в $\mathcal{R}$ применяется в рамках модели конфиденциальных транзакций. Согласно данной модели транзакция использует так называемые *выходы*, которые были сгенерированы при создании прошлых транзакций, и создаёт выходы для последующих транзакций. Примечательно, что в случае с моделью *конфиденциальных* транзакций мы хотим скрыть, какие входы транзакций используются, равно как и их соответствующие значения.

Выходы строятся как обязательства Педерсена по нулю таким образом, что публичный ключ выхода имеет форму $M \equiv rG$ где r является подписывающим ключом. Здесь нами не рассматривается метод создания ключей выходов, но подразумевается, что это происходим в другой части модели транзакций. Каждый выход имеет обязательство по значению $P \equiv sG + aH$, где a является суммой, а s фактором обязательства.

Пользователь протокола формирует анонимную группу $\{M_i\}_{i=0}^{N-1}$, состоящую из выходов, взятых из предшествующих транзакций. Отталкиваясь от этого, предположим, что множество $\{l^{(u)}\}_{u=0}^{w-1}$ представляет индексы w выходов, по которым пользователь хочет подписаться; то есть пользователю известно такое $\{r^{(u)}\}_{u=0}^{w-1}$, что $r^{(u)}G = M_{l^{(u)}}$ для всех $0 \leq u < w$. Для того чтобы поспособствовать сокрытию подписывающих индексов, предположим, что пользователь перемешал анонимную группу. Каждый элемент анонимной группы имеет соответствующее обязательство по значению $\{P_i \equiv s_i G + a_i H\}_{i=0}^{N-1}$.

Далее, пользователь генерирует множество новых выходов, которые создаются при проведении транзакции, с соответствующими обязательствами по значению в форме $\{Q_j \equiv t_j G + b_j H\}_{j=0}^{T-1}$. Так как значения в транзакции должны быть сбалансированы, должно соблюдаться следующее условие:

$$\sum_{u=0}^{w-1} a_{l^{(u)}} = \sum_{j=0}^{T-1} b_j$$

Следует отметить, что для выходов, генерируемых при проведении транзакции, нет никакой анонимной группы.

Это используется для создания последовательность значений утверждения для отношения $\mathcal{R}$:

$$\left(\{M_i\}_{i=0}^{N-1}, \{P_i\}_{i=0}^{N-1}, \{(r^{(u)})^{-1} U\}_{u=0}^{w-1}, \{Q_j\}_{j=0}^{T-1} \; ; \; \left(\{l^{(u)}\}_{u=0}^{w-1}, \{r^{(u)}\}_{u=0}^{w-1}, \sum_{u=0}^{w-1} a_{l^{(u)}} - \sum_{j=0}^{T-1} b_j \right) \right)$$

Пользователь генерирует доказательство, подтверждающее правильность этого утверждения, используя соответствующие секретные значения в качестве множества свидетельства; доказательство демонстрирует знание подписывающих ключей $\{r^{(u)}\}_{u=0}^{w-1}$, а свидетельство y, сформированное с использованием разницы в обязательствах, демонстрирует, что значения входов и выходов равны. Предполагается,

что схема обязательства, используемая для представления значения, является (по крайней мере) вычислительно обязательной. Пользователь не может получить такое значение y, если значения не будут сбалансированы надлежащим образом; в нашем случае обязательства Педерсена соответствуют этому требованию.

Мы называем элементы множества $\{J^{(u)}\}_{u=0}^{w-1}$ *связующими тегами* транзакции. Как и в случае со связываемыми кольцевыми подписями, они используются верификатором для обнаружения попыток многократного повторного подписания при помощи одного и того же секретного ключа как в рамках одной транзакции, так и в случае со множеством транзакций. Преобразование $r^{(u)} \mapsto J^{(u)} \equiv (r^{(u)})^{-1}U$ является инъективной односторонней псевдослучайной функцией [5]; если верификатор видит один и тот же связующий тег, который используется в нескольких случаях, он понимает, что (неизвестный) секретный ключ использовался снова. В случае с нашей моделью конфиденциальных транзакций это равносильно попытке двойной траты средств, которая отклоняется верификатором.

Поскольку сигма-протокол обладает свойством особого нулевого разглашения при наличии добросовестного верификатора, свидетельства неотличимы друг от друга [3]. Тем не менее следует отметить, что наблюдатель, который видит анонимную группу входов, содержащую обязательство, открытие которого известно такому наблюдателю, может просто проверить связующие теги при помощи собственных секретных ключей и определить, использовались ли они в доказательстве. Следовательно, предполагается, что неотличимость свидетельств применяется в отношении тех обязательств по входам, открытия которых не известны наблюдателю.

6 Эффективность

Отметим, что все групповые операции, связанные с верификацией, производятся как операции мультискалярного умножения, которые должны сводиться к нулю; методы, подобные тем, что описаны в работах [16, 14], обеспечивают эффективную оценку этих операций. Кроме того, многие групповые элементы этих операций представляют собой глобально фиксированные генераторы, встречающиеся во всех доказательствах. В результате верификация множества отдельных независимых доказательств может также быть групповой, как в случае с методом, описанным в работе [2] и других работах, где производится случайное взвешивание уравнений верификации, а общие генераторы используются лишь единожды. Как результат, верификация группы независимых доказательств производится с большей эффективностью при использовании одной операции мультискалярного умножения, так как затраты на верификацию отдельного доказательства снижаются.

Мы используем те же обозначения, что и раньше: $N = 2^m$ является размером анонимной группы входов для переменной $m > 1$, w обозначает количество подписывающих индексов, а T указывает количество обязательств по выходам, используемых для проверки равенства. Предположим, оба элемента $\mathbb{G}$ и $\mathbb{F}$ занимают 32 байта памяти (как в случае с обычными группами эллиптической кривой, где используется сжатое представление точек). Мы сравниваем размер доказательств RingCT 3.0 (двух вариантов) [18], Triptych [12] и представленных в данной работе. Следует отметить, что для того, чтобы сравнение было честным, мы делаем некоторые допуски. В случае с Triptych и оригинальной версией RingCT 3.0 при проверке равенства требуется определённое смещение обязательств, которое учитывается нами наряду со множеством доказательств, необходимых в транзакции, в которой должно быть подписано множество входов. Тем не менее нами игнорируется представление множества входов (которое зависит от реализации), доказательства диапазона (которые требуются в случае со всеми протоколами и не являются частью систем доказательства) и любые вспомогательные данные, которые в ином случае могли бы стать частью транзакций. В Таблице 1 приводятся результаты.

Также нами изучается сложность верификации этих протоколов. Для этого нами рассматривается размер всех операций мультискалярного умножения, необходимых для верификации одного или нескольких доказательств в транзакции, а также доказательства равенства. В Таблице 2 приводятся результаты для различных параметров транзакции.

Поскольку каждый из протоколов масштабируется по-своему в зависимости от параметров транзакции, представляется полезным рассмотреть влияние общего размера в условиях реального мира.

Для этого нами были изучены данные, взятые из блокчейна Monero; в частности, для каждой транзакции начиная с 18 октября 2018 по 14 февраля 2020 нами было выделено количество использованных

Протокол	Размер (элементы доказательства)
RingCT 3.0 (оригинальная версия) [18]	$w(2\lg N + 18) + w + 2$
RingCT 3.0 (обновлённая версия) [18]	$2\lceil\lg(Nw)\rceil + w + 17$
Triptych [12]	$w(3\lg N + 8) + w$
Arcturus (данная работа)	$(w + 3)\lg N + w + 7$

Таблица 1: Размер доказательства (элементы группы/поля) с различным размером анонимной группы N и различными подписывающими ключами w

Протокол	Сложность верификации
RingCT 3.0 (оригинальная версия) [18]	$w(2\lg N + 11) + 4N + M + T + 7$
RingCT 3.0 (обновлённая версия) [18]	$2\lceil\lg(Nw)\rceil + N(w + 3) + M + T + 13$
Triptych [12]	$(2 + 2w)\lg N + 2N + 4w + T + 2$
Arcturus (данная работа)	$(3 + 2w)\lg N + 2N + M + T$

Таблица 2: Сложность верификации при различном размере анонимной группы N, различных подписывающих w и выходами T

выходов, а также количество вновь созданных выходов. Coinbase-транзакции, в случае с которыми путём майнинга поблочно генерируются новые активы, нами игнорировались, поскольку они не требуют этого типа доказательства. На рисунке 3 эти данные приводятся относительно значений, представленных в Таблице 1 , наряду с дополнительными вспомогательными данными транзакций (включая доказательства диапазона и данные, являющиеся специфическими для получателя) при повышении размера анонимной группы N. Поскольку сложность верификации в случае со всеми протоколами масштабируется практически линейно с N, значение общего времени верификации на основе этого параметра является важным обязывающим фактором.

Несмотря на то, что обновлённая версия протокола RingCT 3.0, представленная в работе [18], обеспечивает превосходное масштабирование, требование, согласно которому w должно быть возведено во вторую степень (заполнено до этого значения), является причиной плохого масштабирования времени верификации. В сравнении предлагаемая нами конструкция обеспечивает более низкую общую сложность верификации за счёт масштабирования общего размера.

Список литературы

[1] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, Jens Groth, and Christophe Petit. Short accountable ring signatures based on DDH (Компактные проверяемые кольцевые подписи на базе DDH). In *European Symposium on Research in Computer Security*, pages 243–265. Springer, 2015.

[2] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more (Bulletproofs: компактные доказательства для конфиденциальных транзакций и многого другого). In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 315–334. IEEE, 2018.

[3] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols (Доказательства частичного знания и упрощённая реализация протоколов сокрытия свидетельства). In Yvo G. Desmedt, editor, *Advances in Cryptology — CRYPTO '94*, pages 174–187, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[4] Benjamin E. Diamond. “Many-out-of-many"proofs with applications to anonymous Zether (Применение доказательств по «многим из многих» в анонимной системе zether). Cryptology ePrint Archive, Report 2020/293, 2020. `https://eprint.iacr.org/2020/293`.

[5] Yevgeniy Dodis and Aleksandr Yampolskiy. A verifiable random function with short proofs and keys (Верифицируемая случайная функция с компактными доказательствами и ключами). In Serge

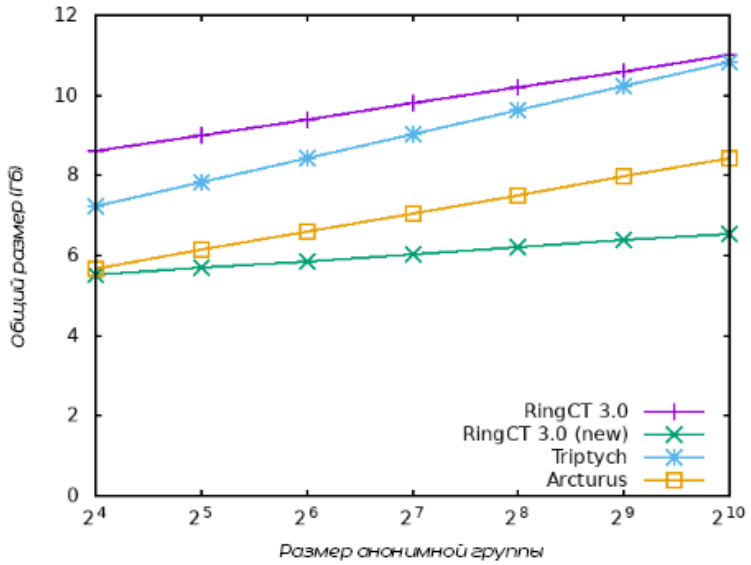

Рис. 3: Общее увеличение размера блокчейна в зависимости от размера анонимной группы

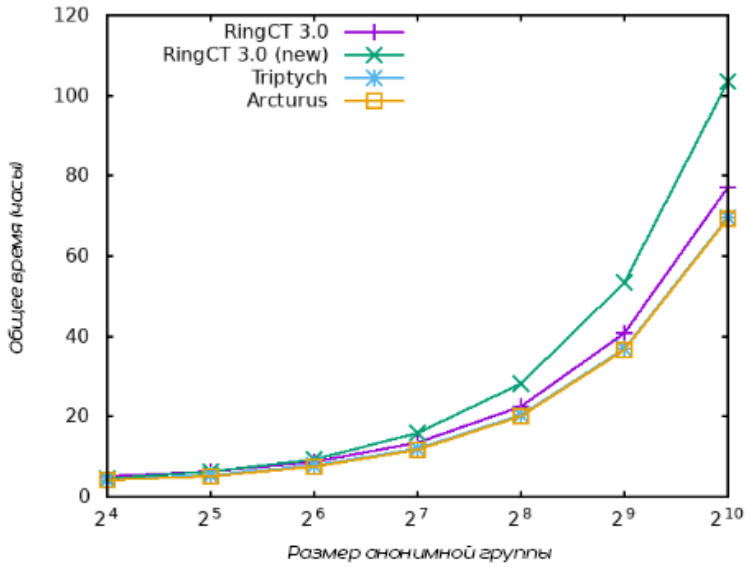

Рис. 4: Общее время верификации в зависимости от размера анонимной группы

Vaudenay, editor, *Public Key Cryptography - PKC 2005*, pages 416–431, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[6] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems (Как доказать, что вы - это вы: практические решения задач идентификации и подписи). In Andrew M. Odlyzko, editor, *Advances in Cryptology — CRYPTO' 86*, pages 186–194, Berlin, Heidelberg, 1987. Springer Berlin Heidelberg.

[7] Jens Groth and Markulf Kohlweiss. One-out-of-many proofs: Or how to leak a secret and spend a coin. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques (Доказательства по «одному из множества» или как раскрыть секрет и потратить монету)*, pages 253–280. Springer, 2015.

[8] Aram Jivanyan. Lelantus: Towards confidentiality and anonymity of blockchain transactions from standard assumptions (Lelantus: как обеспечить конфиденциальность и анонимность транзакций в блокчейне при стандартных допусках). Cryptology ePrint Archive, Report 2019/373, 2019. `https://eprint.iacr.org/2019/373`.

[9] Russell WF Lai, Viktoria Ronge, Tim Ruffing, Dominique Schröder, Sri Aravinda Krishnan Thyagarajan, and Jiafan Wang. Omniring: Scaling private payments without trusted setup (Omniring: масштабирование приватных платежей без доверенных настроек). In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 31–48, 2019.

[10] Joseph K Liu, Victor K Wei, and Duncan S Wong. Linkable spontaneous anonymous group signature for ad hoc groups (Связываемая подпись спонтанной анонимной группы для специальных групп). In *Australasian Conference on Information Security and Privacy*, pages 325–335. Springer, 2004.

[11] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: Anonymous distributed e-cash from Bitcoin (Zerocoin: анонимная распределённая электронная валюта на базе Bitcoin). In *2013 IEEE Symposium on Security and Privacy*, pages 397–411. IEEE, 2013.

[12] Sarang Noether and Brandon Goodell. Triptych: logarithmic-sized linkable ring signatures with applications (triptych: логарифмически масштабируемые связываемые кольцевые подписи и их применение). Cryptology ePrint Archive, Report 2020/018, 2020. `https://eprint.iacr.org/2020/018`.

[13] Shen Noether, Adam Mackenzie, et al. Ring confidential transactions (Кольцевые конфиденциальные транзакции). *Ledger*, 1:1–18, 2016.

[14] Nicholas Pippenger. On the evaluation of powers and monomials (По вопросу оценки показателей степени и одночленов). *SIAM Journal on Computing*, 9(2):230–250, 1980.

[15] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from Bitcoin (Zerocash: система децентрализованных анонимных платежей на базе Bitcoin). In *2014 IEEE Symposium on Security and Privacy*, pages 459–474. IEEE, 2014.

[16] Ernst G Straus. Addition chains of vectors (problem 5125) (Добавление последовательностей векторов (задача 5125)). *American Mathematical Monthly*, 70(806-808):16, 1964.

[17] Nicolas Van Saberhagen. CryptoNote v 2.0, 2013. `https://cryptonote.org/whitepaper.pdf`.

[18] Tsz Hon Yuen, Shi feng Sun, Joseph K. Liu, Man Ho Au, Muhammed F. Esgin, Qingzhao Zhang, and Dawu Gu. RingCT 3.0 for blockchain confidential transaction: Shorter size and stronger security (Протокол RingCT 3.0 для совершения корнфиденциальных транзакций в блокчейне: повышение компактности и уровня безопасности). Cryptology ePrint Archive, Report 2019/508, 2019. `https://eprint.iacr.org/2019/508`.