MONERO RESEARCH LAB

ИССЛЕДОВАТЕЛЬСКИЙ БЮЛЛЕТЕНЬ MRL-0008

Двойные связываемые кольцевые подписи

Саранг Ноезер (Sarang Noether)* Брэндон Гуделл (Brandon Goodell†
Исследовательская лаборатория Monero (Monero Research Lab)
01 Ноября 2018

Аннотация

В данном бюллетене описана модификация схемы связываемых кольцевых подписей Monero, позволяющей включать в кольцо выходы с двойными ключами. Образы ключей привязаны к обоим одноразовым публичным ключам попарно, что не позволяет потратить оба ключа, используемые в транзакции, по отдельности. Этот метод применим к неинтерактивным транзакциям возмещения. Нами рассматривается, как использование этой схемы влияет на безопасность.

1 Вступление

Оригинальный протокол CryptoNote описывает использование одноразовой связываемой спонтанной анонимной групповой (LSAG) подписи. Подписант выбирает так называемое кольцо, состоящее из ключей публичных выходов, один из которых является его собственным, и формирует подпись к сообщению по своему усмотрению. Схема такова, что каждый верификатор может быть уверен в том, что один из ключей в кольце является ключом действительного подписанта (то есть, подписанту известен соответствующий приватный ключ), и что этот ключ не использовался для подписания какого-либо другого сообщения в каком-либо другом кольце. Из соображений экономии занимаемого места, в ранних транзакциях Monero применялась не зависящая от кольца одноразовая версия схемы LSAG-подписи, описанная в работе [2], которая позволяла отправлять средства, используя кольцо в качестве средства обеспечения анонимности отправителя.

Для проведения конфиденциальных транзакций Monero использует вариант этой схемы, который называется схемой многоуровневой одноразовой связываемой спонтанной анонимной групповой (MLSAG) подписи. Такие подписи позволяют подписанту включать векторы ключей, использующие обязательства Педерсена по суммам. Как это описано в работе [4].

Как в случае с LSAG, так и в случае с MLSAG-подписями члены кольца (за исключением обязательств по сумме) являются публичными ключами выходов, которые генерируются при проведении транзакций Monero. В одной отдельно взятой транзакции обычно содержится множество выходов, при этом отправитель отправляется часть средств из предыдущего выхода на некоторый адрес, а также отправляет сдачу назад самому себе, поэтому транзакция остаётся сбалансированной. Каждый раз получатель может восстановить приватный ключ выхода и использовать его позднее в кольцевой подписи.

В этом исследовательском бюллетене нами описана модификация структуры выходов транзакции и структуры кольцевых подписей. Сначала мы описываем изменение, при реализации которого отправитель генерирует выход с двойным ключом и указанной триггерной высотой блока, на которой

*sarang.noether@protonmail.com
†surae.noether@protonmail.com

«переключается» валидность двух ключей. Кроме того, нами описана модификация LSAG и MLSAG-подписей, схема двойной связываемой спонтанной анонимной групповой (DLSAG) подписи, позволяющая отправителю включать один из этих выходов с двойными ключами в связываемую кольцевую подпись. Если двойной ключ, состоящий из двух отдельных публичных ключей выхода, принадлежит действительному отправителю, любой верификатор сможет связать две кольцевые подписи, если они были вычислены при помощи любого из ключей, составляющих такую пару. Помимо этого, членами кольца в DLSAG-подписи могут являться как выходы с двойными ключами, так и обычные (одиночные) выходы. Это обеспечивает подписантов максимально возможным набором доступных членов кольца.

Эта схема подписи применима к транзакциям возмещения Monero, которые сами по себе важны для определённых решений второго уровня. Чтобы сгенерировать такую транзакцию возмещения, отправителю необходимо сгенерировать выход с двойным ключом и указать триггерную высоту блока. До триггерной высоты блока протокол консенсуса мог бы определить, что только один из ключей в паре является действительным и принадлежит отправителю, но после триггерной высоты только другой ключ в паре будет действительным. Это позволяет отправителю вернуть средства, если они не будут потрачены получателем своевременно.

Соответствующая версия этой схемы впервые была описана в личном разговоре с Педро Монеро-Санчесом (Pedro Moreno-Sanchez) и другим соавтором под псевдонимом `donut`. Эта схема предполагала использование обязательств по триггерной высоте блоков, чтобы скрыть фактическую высоту переключения.

2 Описание

Допустим, $\mathbb{G}$ является аддитивной группой порядка, равного простому числу ℓ. Допустим, $H_s : \{0,1\}^* \to \mathbb{Z}_\ell$ и $H_p : \{0,1\}^* \to \mathbb{G}$ являются криптографическими хэш-функциями. Допустим, $G \in \mathbb{G}$ является общеизвестным генератором группы.

При отправке средств в транзакции Monero отправитель использует публичный пользовательский адрес получателя $(A, B) := (aG, bG) \in \mathbb{G} \times \mathbb{G}$ вместе с произвольным нонсом r, чтобы сгенерировать одноразовый публичный адрес выхода, определяемый как $P := H_s(rA, t)G + B$, где t является индексом выхода в пределах транзакции. Получатель использует свой приватный пользовательский ключ (a, b) и точку $R := rG$, чтобы восстановить приватный ключ выхода $p := H_s(aR, t) + b$, который используется траты средств в качестве части более поздней кольцевой подписи.

Чтобы облегчить транзакции возмещения, мы предполагаем, что отправитель сгенерировал модифицированный выход, состоящий из двух одноразовых публичных ключей. Один такой ключ направляется на адрес получателя, в то время как второй направляется обратно отправителю. Эти одноразовые ключи называются *двойными* или *парой*, и как таковые присутствуют в структуре транзакции для последующей идентификации. Пара также имеет связанное с ней значение триггерной высоты блока, чтобы перед переключением только первый одноразовый ключ считался действительным и использовался для траты соответствующих средств, а после переключения действительным будет считаться уже только второй ключ. В результате получатель может забрать средства только до наступления определённого момента, после которого отправитель уже может вернуть их себе.

Несмотря на простоту процесса генерирования отдельных выходов, обозначающих правомочность траты средств на основе заданной высоты блока, недостаточно просто использовать традиционную кольцевую подпись LSAG или MLSAG, включающую в себя один из публичных ключей в паре, не изменив процесс вычисления образов ключей. Поскольку образы ключей вычисляются для каждого

Двойной ключ		Одиночный ключ
$m_\pi \equiv H_s(\mathsf{txid}, \mathsf{index})$		
$J \equiv m_\pi p_\pi Q_\pi$		$J \equiv p_\pi H_p(P_\pi)$
$F_\pi \equiv m_\pi Q_\pi$		$F_\pi \equiv H_p(P_\pi)$
	выбрать произвольное u	
	$c_{\pi+1} \equiv H_s(\mathsf{txdata}, uG, uF_\pi)$	
	для каждого $i \neq \pi$	
	выбрать произвольное s_i	
$m_i \equiv H_s(\mathsf{txid}, \mathsf{index})$		
$F_i \equiv m_i Q_i$		$F_i \equiv H_p(P_i)$
	$c_{i+1} \equiv H_s(\mathsf{txdata}, s_i G + c_i P_i, s_i F_i + c_i J)$	
	$s_\pi \equiv u - c_\pi p_\pi$	
	выход $(c_1, \{s_i\}_{i=1}^n, J)$	

Таблица 1: Формирование DLSAG-подписи

потраченного выхода в кольцевой подписи, можно было бы использовать как ключ, считающийся действительным до переключения, так и ключ, считающийся действительным после него, в отдельных подписях не обнаруженными. Чтобы избежать этого, мы модифицировали схему LSAG таким образом, что одноразовые публичные ключи выходов объединяются в пары, совместно использующие один и тот же образ ключа. Далее нами будет рассмотрен эквивалент MLSAG для этой структуры.

2.1 Формирование подписи

Этапы формирования DLSAG-подписи показаны нами в таблицы Таблице 1, где любой из участников кольца (включая реального отправителя) может как являться, так и не являться частью пары. В последующей схеме мы предполагаем, что отправитель желает потратить средства, связанные с одноразовым ключом $P_\pi = p_\pi G$ с размером кольца n, где $1 \leq \pi \leq n$ является секретным индексом. Мы также допускаем, что любой ключ P_i являющийся частью пары, имеет парный ключ Q_i. Роли P_i и Q_i в паре произвольны.

Следует отметить, что DLSAG-подпись полностью сводится до версии LSAG, если все ключи в кольце, включая ключ действительного отправителя, не являются частью пары, то есть, если подпись соответствует только правой части показанной диаграммы.

Отправитель может подписываться, используя любой тип ключа. Тем не менее, ему необходимо учитывать ограничение, связанное с допустимым количеством элементов кольца. Если потенциальный элемент кольца не является частью пары, то отправитель должен посмотреть оригинальную транзакцию и определить, является ли такой ключ действительным для текущей высоты блока. Если нет, то отправитель должен выбрать «партнёрский» ключ в паре. Далее отправитель может пожелать избегать ключей триггерная высота которых слишком близка к текущей высоте блока, если его транзакция будет включена в новый блок недостаточно быстро. Эти ограничения гарантируют, что недобросовестные верификаторы подписи не смогут с лёгкостью выявить недействительные элементы кольца в попытке определить действительный выход траты.

Также следует отметить, что партнёрские ключи P и Q в паре совместно используют один и тот же образ ключа, если они генерируются в одной и той же транзакции, так как $mpQ = mqP = mpqG$ по структуре. Включение хэша m, который кодирует как происходящую транзакцию, так и индекс

Двойной ключ		Одиночный ключ
	для каждого $1 \leq i < n$	
$m_i \equiv H_s(\mathsf{txid}, \mathsf{index})$		
$F_i \equiv m_i Q_i$		$F_i \equiv H_p(P_i)$
	$c_{i+1} \equiv H_s(\mathsf{txdata}, s_i G + c_i P_i, s_i F_i + c_i J)$	
$m_n \equiv H_s(\mathsf{txid}, \mathsf{index})$		
$F_n \equiv m_n Q_n$		$F_n \equiv H_p(P_n)$
	$c_1^* \equiv H_s(\mathsf{txdata}, s_n G + c_n P_n, s_n F_n + c_n J)$	
	принимать только если $c_1^* = c_1$	

Таблица 2: Проверка DLSAG-подписи

выхода в пределах транзакции, не позволяет никому из получателей пары сжечь средства другого за счёт генерирования другой пары с тем же образом ключа, который недобросовестный получатель тратит первым.

2.2 Верификация подписи

Верификация DLSAG происходит подобно верификации LSAG, и может быть произведена любым наблюдателем. Если она представлена списком публичных ключей выходов, используемых в кольцевой подписи, верификатор сначала должен убедиться в том, что для любого ключа пары выбранный ключ является действительным на текущей высоте блока транзакции. Если это не так, верификатор отклоняет подпись. Верификатор также проверяет образ ключа J. Если он является частью любой предшествующей действительной LSAG или DLSAG-подписи, подпись отклоняется. Затем верификатор выполняет шаги, показанные в Таблице 2.

3 Применение транзакций возмещения

Полезным способом применения DLSAG-подписи являются транзакции возмещения. Некоторые структуры каналов платежей, позволяющих проводить транзакции между сторонами вне блокчейна с последующим фиксированием, также требуют использования неинтерактивных транзакций возмещения. Предположим, Элис хочет отправить средства Бобу, но также хочет быть уверена в том, что эти средства вернутся к ней, если спустя согласованный промежуток времени Боб не потратит их. Для этого Элис создаёт транзакцию, в которой средства, предназначенные Бобу, являются частью пары: один ключ P направляется Бобу, а его парный ключ Q предназначен для самой Элис. Оба ключа в паре совместно используют доказательство диапазона. В данные транзакции включается значение высоты блока h, при этом значение h должно быть выше значения высоты текущего блока в сети.

Если Боб захочет забрать средства, он должен потратить их до того, как будет достигнута высота блока h в транзакции, использующей ключ P в DLSAG-подписи. Верификаторы видят, что среди элементов кольца присутствует ключ P , и что этот выход является действительным. Образ ключа имеет форму $J = mpQ$, которая не использовалась ранее. Верификаторы принимают транзакцию как действительную.

Тем не менее, если Боб не заберёт средства до того, как будет достигнута высота блока h, Элис может вернуть их, отправив свой ключ Q с DLSAG-подписью. Теперь верификаторы видят, что транзакция включает ключ Q, и что этот ключ теперь является действительным. Образом ключа является

Двойной ключ	Одиночный ключ
для каждого $1 \le j \le k$	
$m_{\pi,j} \equiv H_s(\mathsf{txid}, \mathsf{index})$	
$J_j \equiv m_{\pi,j} p_{\pi,j} Q_{\pi,j}$	$J \equiv p_{\pi,j} H_p(P_{\pi,j})$
$F_{\pi,j} \equiv m_{\pi,j} Q_{\pi,j}$	$F_{\pi,j} \equiv H_p(P_{\pi,j})$
выбрать случайный u_j	
$c_{\pi+1} \equiv H_s(\mathsf{txdata}, \{u_j G, u_j F_{\pi,j}\}_{j=1}^{k})$	
для каждого $i \neq \pi, 1 \le j \le k$	
выбрать случайный $s_{i,j}$	
$m_{i,j} \equiv H_s(\mathsf{txid}, \mathsf{index})$	
$F_{i,j} \equiv m_{i,j} Q_{i,j}$	$F_{i,j} \equiv H_p(P_{i,j})$
$c_{i+1} \equiv H_s(\mathsf{txdata}, \{s_{i,j} G + c_i P_{i,j}, s_{i,j} F_{i,j} + c_i J_j\}_{j=1}^{k})$	
для каждого $1 \le j \le k$	
$s_{\pi,j} \equiv u_j - c_\pi p_{\pi,j}$	
выход $(c_1, \{s_{i,j}\}_{i,j=1}^{n,k}, \{J_j\}_{j=1}^{k})$	

Таблица 3: Формирование обобщенной DLSAG-подписи

$J = mqP$, и он не использовался, так как Боб не потратил P. Верификаторы принимают эту транзакцию как действительную.

Следует отметить, что если бы Боб потратил P до того, как была бы достигнута высота блока h, но Элис разозлилась и пожелала бы потратить Q после прохождения высоты h (в результате чего возникла бы ситуация двойной траты), то это бы не удалось. Верификаторы увидят, что образ ключа Элис $J = mqP = mpQ$ такой же, как у Боба, и отклонили бы её транзакцию. Такая структура совместно используемого образа ключа важна, так как в противном случае транзакция разгневанной Элис не была бы отклонена верификаторами. С другой стороны, если бы блокчейн, в котором Боб подписал транзакцию, позже был бы обойдён блокчейном с более высокой совокупной сложностью, в который не входила бы транзакция Боба, Элис всегда смогла бы позже вернуть свои средства. Такая вероятность рассматривается нами, но находится вне контекста этой работы.

4 Расширение со множеством входов

Структура DLSAG, представленная выше, применима только к отмершему на данный момент CryptoNote варианту реализации кольцевой подписи. Тем не менее, современные транзакции требуют применения более устойчивой подписи со множеством ключей, которая позволила бы использовать обязательства по сумме, которые предусматривает модель конфиденциальных транзакций Monero. Следовательно нам необходимо обеспечить соответствующую генерализацию структуры DLSAG.

В обычной MLSAG-подписи каждый из k входов имеет связанное с ним кольцо, содержащее n публичных ключей выходов (в дополнение к отдельному обязательству по сумме, которое не рассматривается нами в этом документе). Отправитель выбирает такой секретный индекс $1 \le \pi \le n$ который позволяет ему контролировать публичные ключи $P_{\pi,j} \equiv p_{\pi,j} G$ для $1 \le j \le k$. Формирование подписи происходит в соответствии с этапами, указанными в Таблице 3.

Как и раньше, если ни один из элементов кольца не является частью пары, всё полностью сводится к MLSAG-подписи. Далее, если $k = 1$, всё сводится к структуре DLSAG с одним входом, показанной

Двойной ключ	Одиночный ключ
для каждого $1 \leq i < n, 1 \leq j \leq k$	
$m_{i,j} \equiv H_s(\mathsf{txid}, \mathsf{index})$	
$F_{i,j} \equiv m_{i,j} Q_{i,j}$	$F_{i,j} \equiv H_p(P_{i,j})$
$c_{i+i} \equiv H_s(\mathsf{txdata}, \{s_{i,j}G + c_i P_{i,j}, s_{i,j}F_{i,j} + c_i J_j\}_{j=1}^{k})$	
для каждого $1 \leq j \leq k$	
$m_{n,j} \equiv H_s(\mathsf{txid}, \mathsf{index})$	
$F_{n,j} \equiv m_{n,j} Q_{n,j}$	$F_{n,j} \equiv H_p(P_{n,j})$
$c_1^* \equiv H_s(\mathsf{txdata}, \{s_{n,j}G + c_n P_{n,j}, s_{n,j}F_{n,j} + c_n J_j\}_{j=1}^{k})$	
принимать только если $c_1^* = c_1$	

Таблица 4: Верификация обобщенной DLSAG-подписи

выше. При наличии подписи и описания соответствующего набора одноразовых публичных ключей выхода происходит верификация подписи, согласно этапам, указанным в Таблице 4.

5 Безопасность

Схожесть DLSAG-подписей и схемами LSAG (описана в работе [2]) и MLSAG (описана в работе [4]) приводит к подобию доказательств безопасности. Как и в случаях, на которые мы ссылаемся, нам хотелось бы продемонстрировать, что наши подписи исключают возможность подделки, являются связываемыми и не позволяют однозначно определить подписанта. Так как доказательства практически идентичны доказательствам, представленным для оригинальных схем подписи, нами выделяются только примечательные различия.

5.1 Невозможность подделки

Доказательства невозможности подделки LSAG/MLSAG используют ряд обращений к модели случайных оракулов с целью установления границ преимуществ определённого злоумышленника в решении задачи дискретного логарифма при восстановлении приватного ключа подписанта. Эта модель определяет поведение функции скалярного хеширования H_s, функции точечного хеширования H_p и действительного подписания. Нами отмечено, что для образа двойного ключа $J = mpqG$ значение m равномерно распределяется в соответствии с моделью случайных оракулов. При равномерном распределении значения xG, распределение (pG, qG, J) and (pG, qG, xG) невозможно вычислить при использовании алгоритма Диффи-Хеллмана.

Следовательно, доказательство невозможности подделки, которое приводится в работе [4], имеет одну небольшую модификацию, когда мы рассматриваем обращение к произвольному оракулу точечного хеширования для двойных ключей, заменённое обращением к оракулу Диффи-Хеллмана.

5.2 Связываемость

Если злоумышленнику удастся создать две подписи, подписанные векторами ключей, использующими общий действительный ключ подписи, то возможны два варианта. Если общий ключ подписи не является частью пары, доказательство будет идентичным описанному в работе [4]. Если общий ключ

подписи является частью пары, то мы увидим, что:

$$\log_G(s_i G + c_i P_i) = \log_{m_i Q_i}(s_i F_i + c_i J)$$

где i является индексом общего ключа подписи в одной из подписей. Это приводит нас к тому же заключению, что изложено в работе [4].

5.3 Неточность определения подписанта

Нами было отмечено, что доказательство неточности определения подписанта, которое приводится в работе [4] не опирается на какую-либо определённую структуру базовой точки, используемую в значениях, передаваемых в функции скалярного хеширования H_s для формирования обязательств. Доказательство заведомо модифицируется с учётом значений F_i, представленных здесь.

5.4 Эвристические атаки

Применение схемы DLSAG даёт гарантию, что при отсутствии внешней информации любой публичный ключ, указываемый в подписи, равновероятно может являться действительным ключом подписанта. Тем не менее злоумышленник может использовать такую внешнюю информацию, чтобы аннулировать эту гарантию, используя эвристический подход.

- *Время траты.* Если Элис запускает транзакцию возмещения с Бобом, а Боб не тратит средства до прохождения триггерной высоты, Элис может попытаться потратить средства вскоре после того, как это произойдёт. Если злоумышленник увидит кольцо, содержащее пару, триггерная высота которой была недавно достигнута (или, возможно, скоро будет достигнута), он может прийти к выводу, что пара принадлежит действительному отправителю. Более того, один из ключей в паре является действительным только в течение небольшого промежутка времени, в то время как его парный ключ будет доступен в течение неограниченного срока. Такой эвристический подход должен рассматриваться в связи с паттернами подозрительных трат, которые рассматриваются во многих работах, например, в работах [3, 1].

- *Доступность двойных выходов.* Доступные выходы заведомо отличимы от одиночных выходов. Если количество доступных двойных выходов в блокчейне будет относительно невелико, если сравнивать с одиночными выходами, они будут выбираться менее часто в качестве элементов кольца. Злоумышленник может прийти к выводу, что любое кольцо, содержащее двойные выходы, скорее всего, будет содержать такой выход в качестве выхода действительного отправителя.

5.5 Повторное использование ключей

Текущий вариант реализации транзакций Monero позволяет избежать как двойных трат, так и повторного использования одноразовых ключей. Если кошелёк пользователя видит множество выходов, связанных с одним и тем же одноразовым ключом, он выбирает выход с самой большой суммой, так как все такие выходы будут иметь одинаковый образ ключа. Следует отметить, что предлагаемая структура разделяет эти роли; вычисление модифицированного образа ключа, рассматриваемое в этом документе, по существу, не исключает траты на один и тот же одноразовый ключ. Для этого понадобится введение альтернативных правил на уровне протокола, касающихся повторного использования ключей, или же введение второго образа ключа и более сложной подписи.

6 Заключительные замечания

Схема подписи, представленная в настоящем документе, представляет собой интересный и новый подход неинтерактивным транзакциям возмещения для использования с Monero. Тем не менее варианты реализации, такие как обязательства по высоте блока и требования к выходам, повлияют на сложность транзакций, их размер и возможность проведения эвристических атак. Неясно, можно ли использовать метод формирования ключей с эффективным использованием места, чтобы описать двойные ключи более практичным способом. Затраты, связанные со сложностью верификации, вероятно, будут недоступны при отсутствии новых схем подписей.

Список литературы

[1] Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena. A Traceability Analysis of Monero's Blockchain (Анализ отслеживаемости блокчейна Monero). Cryptology ePrint Archive, Report 2017/338, 2017. `https://eprint.iacr.org/2017/338`.

[2] Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups (Связываемые спонтанные анонимные групповые подписи для специализированных групп). In Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan, editors, *Information Security and Privacy*, pages 325–335, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[3] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, and N. Christin. An Empirical Analysis of Traceability in the Monero Blockchain (Эмпирический анализ отслеживаемости в блокчейне Monero). *ArXiv e-prints*, April 2017.

[4] Shen Noether, Adam Mackenzie, and the Monero Research Lab. Ring confidential transactions (Кольцевые конфиденциальные транзакции). *Ledger*, 1(0):1–18, 2016.