Концептуальные (неупорядоченные) компоненты **RCTTypeCLSAG (тип 5)**

Вход (здесь обозначение **для каждого фактического** входящего UTXO)

	ложное UTXO **смещение**	**фактическое** UTXO **смещение**	ложные UTXOs **смещения**	подпись CLSAG (c_1, r_i)
уровень j=1 Публичные CLSAG ключи: X_i	$X_{...}$	$X_{i=\pi}$	$X_{...}$	Подписывается вся транзакция, исключение - поля подписи
уровень j=2 Публичные CLSAG ключи: $C_i - C_{pseudo}$	$C_{...}$	$C_{i=\pi} = bG + aJ$	$C_{...}$	
		$C_{pseudo} \triangleq b'G + aJ$		
Образы ключей:		действительный X^* артефакт C^* (⟹ CLSAG's pseudo W^*)	$(C_{i=\pi} - C_{pseudo}) = (b - b')\,G$ Способность подписаться, используя эту EC пару из публичного/приватного ключа, доказывает, что обязательства $C_{i=\pi}$ и C_{pseudo} относятся к одному "a"	

UTXO выход "t"

скрытый адрес **X**

обязательство $\mathbf{C \triangleq bG + aJ}$

где:

a : кол-во Monero в UTXO (**простое** значение)

b ≙ H("commitment_mask" , H(r V_i , t))
= H("commitment_mask" , H(v_0 R , t))

обычная "платёжная хитрость" отправителя/получателя при наличии транзакции и ключей просмотра

сумма

Зашифрованное значение:
≙ **a** ⊕ H("amount" , H(r V_i , t))
= **a** ⊕ H("amount" , H(v_0 R , t))

Комиссия за транзакцию

f
простое значение, чтобы майнеры могли оценить его

в обязательствах выражено как "**a**" в **атомных единицах** ($1/10^{12}$ XMR)

Время разблокировки выходов

<u>абсолютное</u> время, выраженное как:

- **Блокировка отключена** (0)
- **Высота блока** (< 500.000.000)
- **Время периода** (≥ 500.000.000)

Протоколом также предусмотрен <u>относительный</u> период блокировки на **10 блоков**

Bulletproof

Доказательства диапазона "a", которых следует избегать с доказательствами по выходу

входы — выходы

$5\mathbf{J} + 6\mathbf{J} = 21\mathbf{J} + (\ell - 10)\mathbf{J}$
$= (21 - 10)\mathbf{J} + \ell\mathbf{J}$

Инфляция по переполнению циклической группы ↻

Продолжение следует…

Дополнение

- Публичный ключ транзакции (ий) **R**
- Зашифрованный **payID** (если присутствует)
- ...

ПРИМЕЧАНИЕ: слабо структурированное поле, подписанное, но не являющееся частью консенсуса (⟹ задача для кошельков)

Обязательства Педерсена 101

Обязательства являются способом привязки к значению без его раскрытия (возможно, раскрытие при этом произойдёт позже). Обязательства Педерсена в форме EC выглядят следующим образом:

$$\mathbf{C \triangleq bG + aJ}$$

где:

a : значение, по которому даётся обязательство;

b : случайный "ослепляющий фактор", отвечающий за создание энтропии, чтобы затруднить вычисление "a" посредством радужной таблицы;

G : общая базовая точка;

J : точка на EC, для которой значение "j", находящееся в пределах J ≙ j G, неизвестно (DLP).

<u>СВОЙСТВА</u>

Теоретически скрывает сумму : множество пар (a,b) может дать одно и то же значение обязательства C

Обязательное вычисление: попытка предоставления обязательства по ложному значению эквивалентна решению системы DLP:
$C(a_2 , b_2) = C(a , b) \Longrightarrow j = (b - b_2)/(a_2 - a) \Longrightarrow$ DLP решена

Гомоморфизм: $C(a_1 , b_1) + C(a_2 , b_2) = C(a_1+a_2 , b_1+b_2)$

Обзор CLSAG и текущей реализации

- CLSAG является видом схемы мультиподписи MLSAG, где каждый "сжатый" уровень имеет свой собственный фактический ключ и набор ложных ключей
- В отличие от MLSAG фактический образ ключа, защищающий от двойной траты, доступен только для первого уровня, поэтому каждый входящий UTXO требует наличия отдельной CLSAG (но и MLSAG использовались подобным образом в целях обеспечения анонимности)
- В рамках протокола RingCT используется двухуровневая схема CLSAG, где подпись 2-го уровня служит доказательством эквивалентности значений фактических UTXO, по которым дано обязательство, и обязательством по псевдовыходу C_{pseudo} : эквивалентность считается доказанной *при* наличии новой специфической пары, состоящей из публичного/приватного ключей на эллиптической кривой, поэтому подписание 2-го уровня CLSAG при помощи такой пары доказывает существование этой пары и их эквивалентность.

Секретный поток значений, передаваемых с UTXOs Monero

Значение UTXO Monero зашифровывается в двух полях: в поле обязательства **C** и поле **суммы**:

- поле **суммы** позволяет отправителю и получателю совместно использовать значение: отправитель вычисляет его на основе простого значения **a** в соответствии с приведённым определением; получатель может проверить простое значение **a** путём применения операции XOR к сумме (**amount**) с использованием той же хеш-функции, что использовалась в рамках определения (две равные XOR исключают друг друга). Чтобы хеш мог вычислить как отправитель, так и получатель, транзакция и ключи просмотра используются подобно тому, как это происходит в случае с протоколом Диффи-Хеллмана при создании скрытых адресов;
- обязательства **C** позволяют каждому узлу в сети убедиться в том, что значения суммы входящих UTXO транзакции равны сумме значений выходящих UTXO транзакции с добавлением комиссии. При этом фактические значения остаются скрытыми (кроме значения комиссии, которое изначально является простым).

В рамках схемы RingCT:

- отправитель проверяет, чтобы исходящие сумма (**amount**) и обязательство **C** соответствовали одному и тому же значению **a** (это обязывает отправителя/получателя обменяться значением, соответствующим тому, что проверяется сетью). Это возможно благодаря уже задокументированному методу определения суммы (**amount**) и **b**;
- для каждого входа отправителем определяется обязательство по псевдовыходу C_{pseudo}, связанное с тем же значением «a» фактического UTXO (при этом не раскрывается его место в кольце, поскольку оно отделяется при помощи подписи CLSAG);
- таким образом, для проверки правильности потока значений узлам в сети требуется проверить только баланс и доказательство Bulletproof:

$$\sum_{inputs} C_{pseudo} = \sum_{outputs} C + f\,J$$

$$\sum_{inputs} b' = \sum_{outputs} b \quad (\text{<u>задаётся отправителем</u>})$$

$$\Longrightarrow \sum_{inputs} a\,J = \sum_{outputs} a\,J + f\,J$$

$$\sum_{inputs} a = \sum_{outputs} a + f$$

← Проверка Bullet proof

Примечания и ссылки

- Данная шпаргалка связана с предыдущими шпаргалками по <u>адресам Monero</u> и <u>кольцевым подписям</u>
- <u>От нуля к Monero: Вторая редакция</u>, главы 5, 6 и приложения A, B (даже если речь идёт о транзакциях, подписанных при помощи MLSAG, CLSAG является простым способом, если вы понимаете разницу между двумя видами колец).
- <u>От доказательств с нулевым разглашением до Bulletproofs</u> (первые 6 страниц, посвящённых обязательствам).
- Множество постов на <u>Monero Stack Exchange</u> (например, "<u>Полная структура дополнительного поля…</u>")
- <u>API блоков Monero</u> (например, <u>данный запрос</u> проверки транзакции TX – предлагается разбор JSON посредством <u>jq</u>)
- <u>Исходный код</u> Monero CLI (например, <u>/src/ringct/rctTypes.h</u> с новым 5 типом подписи), будем надеяться, прошедший проверку специальным ПО (например, <u>Sourcetrail</u>)

Перевод шпаргалки выполнил <u>v1docq47</u>