Основные- / Под- ($i \geq 1$)

		Основные- Приватные	Основные- Публичные	Под- ($i \geq 1$) Публичные	Под- ($i \geq 1$) Приватные
ВНЕ БЛОКЧЕЙНА (данные получателя платежа)	**Ключи траты**	**Общий способ выведения ключей**: “ограниченная” 256-битная мнемоническая фраза → H_s → **Мнемоническая** фраза из 24 + 1 (контрольная сумма) слов, среди 1626 ($1626^{24} \gtrsim 2^{256}$)	$s_0 \cdot G \rightarrow \mathbf{S_0 = s_0 G}$	$\mathbf{S_i = H_s(“SubAddr” \mid v_0 \mid i)\, G + S_0}$	$S_i = H_s(“SubAddr” \mid v_0 \mid i) + s_0$
	Ключи просмотра	v_0	$v_0 \cdot G \rightarrow \mathbf{V_0 = v_0 G}$	$\mathbf{V_i = v_0 S_i}$	$V_i = v_0 S_i$ **Фактически никогда не использовались:** подадреса были введены для общего использования v_0 (для эффективности сканирования блокчейна)
	Адреса	$\mathbf{Base58(0x12 \mid S_0 \mid V_0 \mid checksum) = “4 \ldots\ldots\ldots”}$ [95 знаков] — 4-байтный урезанный хеш Keccak256		$\mathbf{Base58(0x2A \mid S_i \mid V_i \mid checksum) = “8 \ldots\ldots\ldots”}$ [95 знаков] — 4-байтный урезанный хеш Keccak256	
	Интегрированные адреса	8-байтный компактный ID платежа, зашифрованный в платёжной транзакции (в сравнении с 32-байтным, который использовался ранее) → $\mathbf{Base58(0x13 \mid S_0 \mid V_0 \mid payID \mid checksum) = “4 \ldots\ldots\ldots”}$ [106 знаков] — 4-байтный урезанный хеш Keccak256		**Не используются, поскольку интегрированные адреса и подадреса некоторым образом решают ту же проблему** Взято из https://monerodocs.org/public-address/integrated-address/ : “ […] для приёма платежей **отдельным пользователям** лучше использовать **подадреса**. В некоторых ситуациях это повышает уровень анонимности. Подробности содержатся в статье, посвящённой подадресам. **Предприятиям**, принимающим платежи автоматически, лучше использовать **интегрированные адреса**. Это объясняется следующим образом: […] ”	
В БЛОКЧЕЙНЕ (по инициативе плательщика)	**Ключи транзакции**	$r \cdot G \rightarrow \mathbf{R = r G}$		$\mathbf{R = r S_i}$	$r \cdot S_i$
	Скрытые адреса ($t \geq 0$) — **POV отправителя**	**Приватный ключ нельзя вывести на основе POV отправителя**, так как адрес является адресом назначения транзакции, получателя, которому переводятся средства отправителя	$\mathbf{X_t = H_s(r\, V_0 \mid t)\, G + S_0}$ = $r\,(v_0 G)$ = $v_0\,(r G)$	$\mathbf{X_t = H_s(r\, V_i \mid t)\, G + S_i}$ = $r\,(v_0 S_i)$ = $v_0\,(r S_i)$	**Приватный ключ нельзя вывести на основе POV отправителя**, так как адрес является адресом назначения транзакции, получателя, которому переводятся средства отправителя
	Скрытые адреса ($t \geq 0$) — **POV получателя**	**Используется для создания кольцевых подписей**, когда получатель становится отправителем и тратит свой UTXO $\cdot G$ $\mathbf{x_t = H_s(v_0 R \mid t) + s_0}$	$\mathbf{X_t = H_s(v_0 R \mid t)\, G + S_0}$	$\mathbf{X_t = H_s(v_0 R \mid t)\, G + S_i}$ $\cdot G$	**Используется для создания кольцевых подписей**, когда становится отправителем и тратит свой UTXO $\mathbf{x_t = H_s(v_0 R \mid t) + s_i}$

Равенства остаются действительными благодаря связности r, R, v_0, V_0, V_i обеспечиваемой протоколом Диффи-Хеллмана

“Эллиптические примечания” ☺

Строчными буквами обозначены **скалярные** величины, которыми также являются и выходы H_s. **ЗАГЛАВНЫМИ** буквами обозначены **точки** на эллиптической кривой, используемой Monero (скрученная кривая Эдвардса Ed25519), даже если они могут быть представлены одним 256-битным значением благодаря технологии, известной как сжатие (в случае с адресами в полях протокола применялось представление, используемое при хешировании в соответствии с правилами арифметики на эллиптических кривых). Таким образом, при использовании точек эллиптической кривой, произведения и суммы должны восприниматься как их вариант на эллиптической кривой (при совершении действия в дискретном 2D пространстве), а не как обычные скалярные величины при работе со «значениями сжатых точек». $\mathbf{H_s(\,) = sc\_reduce32(\,Keccak256(\,)\,)}$: выход хеша Keccak ограничивается **sc_reduce32( )** из-за цикличности природы точек эллиптической кривой (отдельное спасибо Кое за соответствующее замечание); следует отметить, что то же ограничение применяется к приватному ключу транзакции **r** и к указанному **методу выведения ключа мнемонической фразы, состоящей из 25 слов** (равно как и к любому другому).

Примечания и ссылки

Изучаем Monero [RU] (первая редакция - декабрь 2018 / бесплатная PDF версия - 18 апреля 2019 - SerHack и Сообщество Monero)
От нуля к Monero: Вторая редакция [RU] (v2.0.0 - 4 апреля2020 - Кое, Курт М. Алонсо, Саранг Нёзер) главы 1, 2, 4
Обзор белой книги Cryptonote (июль 2014 ? - Брэндон Гуделл AKA Шурэ Нёзер)
Как создаются адреса в Cryptonote (luigi1111)
Различные темы на **Monero Stack Exchange** и **Monerodocs**

ПРИМЕЧАНИЕ: форма этой шпаргалки немного отличается от исходного варианта в целях обеспечения “понимания с первого взгляда”