

Функция `ge_fromfe_frombytes_vartime`

Шен Ноезер (Shen Noether)*

Исследовательская лаборатория Monero (Monero Research Lab)

Аннотация

Мною рассматривается функция `ge_fromfe_frombytes_vartime`, используемая с функциями образов ключей Monero.

1 Вступление

В этой короткой технической заметке мною рассматривается функция `ge_fromfe_frombytes_vartime`, используемая в образах ключей Monero. Следует отметить, что этот код был унаследован от разработчиков оригинального протокола CryptoNote, которые, безусловно, являются специалистами в области криптографии, но чей недостаток заключается в неумении объяснять и комментировать свою работу. Также хотелось бы отметить, что прошлым летом мною уже была заменена большая часть криптографической библиотеки `ed25519`, используемой Monero, на вариант `ref10`, предложенный Бернштейном.

В недавно появившихся исследовательских работах (довольно известных авторов) рассматривалась возможность наложения случайной строки на точку на эллиптической кривой [см. [BCI⁺10, FFS⁺13]]. Интересно, что функция «хеширования по точке», `ge_fromfe_frombytes_vartime`, используемая протоколом CryptoNote [vS13], кажется, не упоминалась ни в одной из этих работ, но потенциально является более эффективным алгоритмом.

2 `fe_frombytes`

Очевидно, что эта часть является `fe_frombytes` из `ref10`.

3 Неизвестная часть

Предположим, что сначала $y \equiv 0$, а $\text{sign} \equiv \text{sign}$.

Следовательно, получаем:

$$2u^2 + 1 - x \equiv 0$$

что даёт нам $x \equiv 2u^2 + 1$.

Таким образом,

$$2u^2 + 1 \equiv r_x^2(w^2 - 2A^2u^2)$$

что даёт нам

$$r_x = \left(\frac{2u^2 + 1}{w^2 - 2A^2u^2} \right)^{\frac{1}{2}}.$$

*shen.noether@gmx.com

В этом случае мы правильно вычисляем квадратный корень с первой попытки. Теперь нам необходимо убедиться в том, что y и x находятся на эллиптической кривой.

$$x_p = w^2 - 2A^2u^2 = (2u^2 + 1)^2 - 2A^2u^2$$

$$rxt = (w/x_p)^{.5}$$

$$x_t = rxt^2 (w^2 - 2A^2u^2) \rightarrow \left(\frac{w}{w^2 - 2A^2u^2} \right) (w^2 - 2A^2u^2) \rightarrow w$$

(если rxt действительно является квадратным корнем).

$$y = (2u^2 + 1 - x_t)$$

$$rx = -u \left(2A(A+2) \frac{w}{x_p} \right)^{\frac{1}{2}} = - \left(2A(A+2) \frac{u^2w}{w^2 - 2A^2u^2} \right)^{\frac{1}{2}}$$

$$z = -2Au^2 = -(w-1)A = (1-w)A$$

(следует отметить, что $-z = 2Au^2$, $zA = -2A^2u^2$)

$$ry = z - w$$

$$Y^2 = (z - w)^2$$

$$rz = z + w$$

$$Z^2 = (z + w)^2$$

$$r_{x-final} = (z + w) \left(2A(A+2) \frac{u^2w}{w^2 + zA} \right)^{\frac{1}{2}}$$

$$X^2 = Z^2 \left((A+2) \frac{2Au^2w}{w^2 + zA} \right)$$

$$= Z^2 (A+2) \frac{-zw}{w^2 + Az}$$

$$d = -\frac{A-2}{A+2}$$

проверяем, действительно ли

$$-X^2Z^2 + Y^2Z^2 = (Z^2)^2 + dX^2Y^2$$

или, другими словами, что

$$Z^4 (A+2) \frac{zw}{w^2 + Az} + Z^2 (z-w)^2 = Z^4 + (A-2) Z^2 \frac{zw}{w^2 + Az} (z-w)^2$$

сокращаем Z^2 :

$$(z+w)^2 (A+2) \frac{zw}{w^2 + Az} + (z-w)^2 \stackrel{?}{=} (z+w)^2 + (A-2) \frac{zw}{w^2 + Az} (z-w)^2$$

После этого умножаем на $w^2 + Az$

$$\begin{aligned} & (z + w)^2 (A + 2) zw + (z - w)^2 (w^2 + Az) \\ & \stackrel{?}{=} (z + w)^2 (w^2 + Az) + (A - 2) (zw) (z - w)^2 \end{aligned}$$

После включения $z = (1 - w)A$ при помощи компьютерной алгебраической системы, такой как Maxima, проверяем равенство двух сторон.

Теперь у нас имеется несколько операторов «если» для различных случаев. В первом случае проверяется, был ли в результате вычислений действительно получен отрицательный квадратный корень. Если это не так, проверяется, не был ли вычислен квадратный корень для отрицательного начального значения. Наконец, отметив, что $p = 2^{255} - 19 \equiv 1 \pmod{4}$, так что -1 является невычетом, и если взять произведение невычетов, то получится вычет, мы умножаем нашу попытку на -1 .

Ссылки

- [BCI⁺10] Eric Brier, Jean-Sébastien Coron, Thomas Icart, David Madore, Hugues Randriam, and Mehdi Tibouchi. Efficient indifferentiable hashing into ordinary elliptic curves (Эффективное недифференцируемое хеширование на обычных эллиптических кривых). In *Advances in Cryptology—CRYPTO 2010 (Опубликовано в «Прогресс в криптологии»)*, pages 237–254. Springer, 2010.
- [FFS⁺13] Reza R Farashahi, Pierre-Alain Fouque, Igor Shparlinski, Mehdi Tibouchi, and J Voloch. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves (Недифференцируемое детерминированное хеширование на эллиптических и гиперэллиптических кривых). *Mathematics of Computation (Вычислительная математика)*, 82(281):491–512, 2013.
- [vS13] Nicolas van Saberhagen (Николас Ван Саберхаген). Cryptonote v 2. 0. Ссылка: <https://cryptonote.org/whitepaper.pdf>, 2013.