Равенство дискретного логарифма в различных группах

Саранг Ноезер (Sarang Noether)*
Исследовательская лаборатория Monero (Monero Research Lab)
04 Декабря 2018

Аннотация

В данной технической записке содержится описание алгоритма, обеспечивающего доказательство знания дискретного логарифма в различных группах. Схема выражает общее значение в виде скалярного представления битов и использует набор кольцевых подписей для доказательства того, что значение каждого бита действительно и одинаково (вплоть до полной эквивалентности) в обеих скалярных группах.

1 Обозначения

Нами используется $\mathbb{Z}_n$ для короткого обозначения группы $\mathbb{Z}/n\mathbb{Z}$. Допустим, $\mathbb{G}$ и $\mathbb{H}$ являются группами первого порядка, в которых задача доказательства дискретного логарифма является
сложной: например, `secp256k1` или l-подгруппой `curve25519`. Допустим, $G, G' \in \mathbb{G}$ и $H, H' \in \mathbb{H}$ будет являются генераторами соответствующих групп. Предположим, $|G| = p$ и $|H| = q$. Допустим, $\mathrm{H}_\mathbb{G} : \{0,1\}^* \to \mathbb{Z}_p$ и $\mathrm{H}_\mathbb{H} : \{0,1\}^* \to \mathbb{Z}_q$ являются криптографическими хеш-функциями.

Без потери общности, допустим, что $p \leq q$. Выберем такое значение $x \in \mathbb{Z}$, чтобы $0 \leq x < p$. Рассмотрим естественные проекции $\mathbb{Z} \to \mathbb{Z}_p$ и $\mathbb{Z} \to \mathbb{Z}_q$ с таким ограничением области определения, и увидим взаимно-однозначное соответствие между элементами $\mathbb{Z}_p$ и ограничением $\mathbb{Z}_q$. Учитывая это, нам нужно доказать, что только при наличии значений xG' и xH' (и, при необходимости, других элементов доказательства) дискретный логарифм обеих будет представлением одного и того же числа. В частности, при этом мы не хотим раскрывать x верификатору.

Так как значимая связь между двумя группами отсутствует, наш подход состоит в разложении x на биты. При этом каждый бит будет рассматриваться как скалярная величина как в $\mathbb{Z}_p$, так и в $\mathbb{Z}_q$ в рамках нашей эквивалентности, а обязательства будут генерироваться для каждого бита в обеих группах. Для каждого бита нами будет построена кольцевая подпись Шнорра, что продемонстрирует, что обязательство по биту является действительным и имеет одно и то же значение в каждой группе.

Данный метод был изначально предложен Эндрю Поэлстра (Andrew Poelstra).

2 Алгоритм

2.1 Доказывающая сторона

У нас есть число $0 \leq x < p$, выраженное в битах:

$$x = \sum_{i=0}^{n-1} b_i 2^i$$

*sarang.noether@protonmail.com

Следует отметить, что из-за эквивалентности, о которой говорилось выше, каждый b_i по необходимости может рассматриваться в качестве элемента либо группы $\mathbb{Z}_p$, либо группы $\mathbb{Z}_q$, в результате чего x будет представлен в каждой группе. Для каждого $i \in [0, n-2]$ генерируем произвольные блайндеры $r_i \in \mathbb{Z}_p$ и $s_i \in \mathbb{Z}_q$. Для $i = n-1$ устанавливаем блайндеры

$$r_{n-1} = (2^{n-1})^{-1} \sum_{i=0}^{n-2} r_i 2^i \in \mathbb{Z}_p$$

и

$$s_{n-1} = (2^{n-1})^{-1} \sum_{i=0}^{n-2} s_i 2^i \in \mathbb{Z}_q$$

чтобы гарантировать, что $\sum_{i=0}^{n-1} r_i 2^i = \sum_{i=1}^{n-1} s_i 2^i = 0$.

Для каждого $i \in [0, n-1]$ используем блайндеры, чтобы вычислить два обязательства Педерсена:

$$\begin{aligned} C_i^G &:= b_i G' + r_i G \in \mathbb{G} \\ C_i^H &:= b_i H' + s_i H \in \mathbb{H} \end{aligned}$$

Из-за такой конструкции взвешенными суммами обязательств в соответствующих группах будут $\sum_{i=0}^{n-1} 2^i C_i^G = xG'$ и $\sum_{i=0}^{n-1} 2^i C_i^H = xH'$.

Затем строим кольцевую подпись, по каждому биту, чтобы продемонстрировать, что значение будет либо 0, либо 1, и это значение будет одним и тем же (вплоть до полной эквивалентности) в обеих группах. В частности, для каждого $i \in [0, n-1]$ нами рассматриваются два варианта:

Вариант: $b_i = 0$. Выбираем произвольные $j_i \in \mathbb{Z}_p$ и $k_i \in \mathbb{Z}_q$. Задаём

$$\begin{aligned} e_{1,i}^G &:= \mathrm{H}_{\mathbb{G}}\left(C_i^G, C_i^H, j_i G, k_i H\right) \in \mathbb{Z}_p \\ e_{1,i}^H &:= \mathrm{H}_{\mathbb{H}}\left(C_i^G, C_i^H, j_i G, k_i H\right) \in \mathbb{Z}_q \end{aligned}$$

и выбираем произвольные $a_{0,i} \in \mathbb{Z}_p$ и $b_{0,i} \in \mathbb{Z}_q$. Задаём

$$\begin{aligned} e_{0,i}^G &:= \mathrm{H}_{\mathbb{G}}\left(C_i^G, C_i^H, a_{0,i}G - e_{1,i}^G(C_i^G - G'), b_{0,i}H - e_{1,i}^H(C_i^H - H')\right) \in \mathbb{Z}_p \\ e_{0,i}^H &:= \mathrm{H}_{\mathbb{H}}\left(C_i^G, C_i^H, a_{0,i}G - e_{1,i}^G(C_i^G - G'), b_{0,i}H - e_{1,i}^H(C_i^H - H')\right) \in \mathbb{Z}_q \end{aligned}$$

а затем определяем:

$$\begin{aligned} a_{1,i} &:= j_i + e_{0,i}^G r_i \in \mathbb{Z}_p \\ b_{1,i} &:= k_i + e_{0,i}^H s_i \in \mathbb{Z}_q \end{aligned}$$

Вариант: $b_i = 1$. Выбираем произвольные $j_i \in \mathbb{Z}_p$ и $k_i \in \mathbb{Z}_q$. Задаём

$$\begin{aligned} e_{0,i}^G &:= \mathrm{H}_{\mathbb{G}}\left(C_i^G, C_i^H, j_i G, k_i H\right) \in \mathbb{Z}_p \\ e_{0,i}^H &:= \mathrm{H}_{\mathbb{H}}\left(C_i^G, C_i^H, j_i G, k_i H\right) \in \mathbb{Z}_q \end{aligned}$$

и выбираем произвольные $a_{1,i} \in \mathbb{Z}_p$ и $b_{1,i} \in \mathbb{Z}_q$. Задаём

$$\begin{aligned} e_{1,i}^G &:= \mathrm{H}_{\mathbb{G}}\left(C_i^G, C_i^H, a_{1,i}G - e_{0,i}^G C_i^G, b_{1,i}H - e_{0,i}^H C_i^H\right) \in \mathbb{Z}_p \\ e_{1,i}^H &:= \mathrm{H}_{\mathbb{H}}\left(C_i^G, C_i^H, a_{1,i}G - e_{0,i}^G C_i^G, b_{1,i}H - e_{0,i}^H C_i^H\right) \in \mathbb{Z}_q \end{aligned}$$

а затем определяем:

$$\begin{aligned} a_{0,i} &:= j_i + e_{1,i}^G r_i \in \mathbb{Z}_p \\ b_{0,i} &:= k_i + e_{1,i}^H s_i \in \mathbb{Z}_q \end{aligned}$$

Доказательством является кортеж $\left(xG', xH', \{C_i^G\}, \{C_i^H\}, \{e_{0,i}^G\}, \{e_{0,i}^H\}, \{a_{0,i}\}, \{a_{1,i}\}, \{b_{0,i}\}, \{b_{1,i}\}\right)$.

2.2 Верификатор

Учитывая кортеж доказательства, нам следует убедиться в том, что обязательства по битам верно представляют доказательства дискретного логарифма. Это проверяется при помощи следующих уравнений:

$$
\begin{aligned}
\sum_{i=0}^{n-1} 2^i C_i^G &= xG' \in \mathbb{G} \\
\sum_{i=0}^{n-1} 2^i C_i^H &= xH' \in \mathbb{H}
\end{aligned}
$$

Для каждого $i \in [0, n-1]$ вычисляем следующее:

$$
\begin{aligned}
e_{1,i}^G &:= \mathrm{H}_{\mathbb{G}}\left(C_i^G, C_i^H, a_{1,i}G - e_{0,i}^G C_i^G, b_{1,i}H - e_{0,i}^H C_i^H\right) \in \mathbb{Z}_p \\
e_{1,i}^H &:= \mathrm{H}_{\mathbb{H}}\left(C_i^G, C_i^H, a_{1,i}G - e_{0,i}^G C_i^G, b_{1,i}H - e_{0,i}^H C_i^H\right) \in \mathbb{Z}_q \\
(e_{0,i}^G)' &:= \mathrm{H}_{\mathbb{G}}\left(C_i^G, C_i^H, a_{0,i}G - e_{1,i}^G (C_i^G - G'), b_{0,i}H - e_{1,i}^H (C_i^H - H')\right) \in \mathbb{Z}_p \\
(e_{0,i}^H)' &:= \mathrm{H}_{\mathbb{H}}\left(C_i^G, C_i^H, a_{0,i}G - e_{1,i}^G (C_i^G - G'), b_{0,i}H - e_{1,i}^H (C_i^H - H')\right) \in \mathbb{Z}_q
\end{aligned}
$$

Проверяем соответствие $(e_{0,i}^G)' = e_{0,i}^G$ и $(e_{0,i}^H)' = e_{0,i}^H$ в кортеже доказательства.

Если все проверки будут успешными, верификатор примет доказательство. В противном случае доказательство будет отклонено. Предполагается, что верификатор также проверяет каждый элемент кортежа доказательства, чтобы доказать его принадлежность к ожидаемой группе. Это делается, чтобы вычислить злоумышленника, которым может оказаться доказывающая сторона.