zkHack — Let's hash it out

Manuel B. Santos

December 2022

Puzzle: `https://zkhack.dev/events/puzzle1.html`.

1 Solution

We are told we have access to 256 messages $m_1, \ldots, m_{256}$ and their corresponding BLS signatures $\sigma_1, \ldots, \sigma_{256}$.

Recall how these signatures are generated:

$$\sigma_i = sk \cdot H(m_i),$$

where $H(m_i)$ is the Pedersen hash. We can expand the above signature expression by plugging in the definition of $H(m)$. For some general message m and random elements $g_1, \ldots, g_n$,

$$H(m) := \sum_{j=1}^{n} h(m)_j \cdot g_j,$$

where h is some $n-$bit hash function and $h(m)_j$ is its $j-$th bit. In the context of the challenge, $n = 256$ and h is the blake2s hash.

By linearity we have,

$$\begin{aligned} \sigma_i &= sk \cdot \sum_{j=1}^{256} h(m_i)_j \cdot g_j \\ &= \sum_{j=1}^{256} h(m_i)_j \cdot (sk \cdot g_j) \\ &= \sum_{j=1}^{256} h(m_i)_j \cdot pk_j, \end{aligned} \tag{1}$$

where we denote $pk_j = sk \cdot g_j$ for short.

Therefore, in order to sign some general message m, we need to know the elements pk_j:

$$\sigma_m = \sum_{j=1}^{256} h(m)_j \cdot pk_j. \tag{2}$$

To find the elements pk_j, let us rewrite the expression (1) in matrix format:

$$\boldsymbol{\sigma} = M \cdot \boldsymbol{pk}$$

$$\begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_{256} \end{pmatrix} = \begin{pmatrix} h(m_1)_1 & h(m_1)_2 & \dots & h(m_1)_{256} \\ h(m_1)_2 & h(m_2)_2 & \dots & h(m_2)_{256} \\ \vdots & \vdots & \ddots & \vdots \\ h(m_{256})_1 & h(m_{256})_2 & \dots & h(m_{256})_{256} \end{pmatrix} \begin{pmatrix} pk_1 \\ pk_2 \\ \vdots \\ pk_{256} \end{pmatrix}$$

So, we have the vector P is given by

$$\boldsymbol{pk} = \boldsymbol{\sigma} \cdot M^{-1}. \tag{3}$$

From expression (2) and (3), the solution is given by:

$$\boxed{\sigma_m = h(m) \cdot \boldsymbol{\sigma} \cdot M^{-1}}\ .$$