Signature Scheme NCS1

setup.

1. Given a pairing friendly elliptic curve with groups $\mathbb{G}_1,\ \mathbb{G}_2,$ and $\mathbb{G}_T$, choose generators $p \in \mathbb{G}_1$ and $q \in \mathbb{G}_2$.

2. Choose a random value, $sk \xleftarrow{\$} \mathbb{F}_r$, where $\mathbb{F}_r$ is the scalar field of the elliptic curve, and set $r := \ sk \ \times q$. Note that the operation $\times$ corresponds to elliptic curve scalar multiplication.

3. Output the public key $pk \ := \ (p,\ q,\ r)$ and the secret key sk.

sign(sk, pk, id, index, m).

Given a secret key, sk, the point p from the public key pk, an identifier, id, an $index$ corresponding to the row being signed and message, m, output the signature as

$$signature := sk \times (\text{hash\_to\_curve}(id,\ index) + m \times p)$$

Note that + corresponds to elliptic curve point addition.

verify(pk, id, index, m, signature).

Given a public key, $pk = (p,\ q,\ r)$, an identifier, id, an $index$ corresponding to the row being verified, a message, m, and a $signature$, calculate

$$\begin{aligned} left \ &= \ e(signature,\ q) \\ right \ &= \ e(\text{hash\_to\_curve}(id,\ index) + m \times p,\ r) \end{aligned}$$

where the function $e(.,.)$ is the bilinear pairing.

If $left = right$ output $true$, else output $false$.

combine(weights, signatures).

Given a vector of $weights$ and vector of $signatures$, each of length n, calculate the aggregate signatures as

$$aggregate\_signature \ = \ \sum_{i=0}^{n-1} weight_i \times signature_i$$

verify_aggregate(pk, id, weights, m, aggregate_signature).

Given a public key $pk = (p,\ q,\ r)$, an identifier id, a vector of $weights$ of length n, a message m, and an $aggregate\_signature$, verify that the message m corresponds to the weighted average of signed original messages by calculating

$$\begin{aligned} left \ &= \ e(signature,\ q) \\ right \ &= \ e\left(\sum_{i=0}^{n-1} weight_i \times \text{hash\_to\_curve}(id,\ i) + m \times p,\ r\right) \end{aligned}$$

If $left = right$ output $true$, else output $false$.

(See *HSS Exercise.pdf* if the Latex is not rendering.)