Protocol Lindell22.Sign

An instantiation of the three-round threshold protocol of Lindell22 [Lin22], parametrized by a group $\mathbb{G}$ of prime order q with generator G, a hash function H, a Commitment scheme, a zero-sharing protocol Przs and a dlog PoK Fischlin.

Players: Key share holders: $\{\mathcal{P}_i\}_{i\in[n]}$ holding $\{x_i\}_{i\in[n]}$ and public key Q
Quorum of signers: $\{\mathcal{P}_i\}_{i\in \mathrm{S}}$ for $\mathrm{S}\in[n]^t$ and $\mathrm{S}^* = \mathrm{S}\setminus\{i\}$

Inputs: sid: unique session id
m: message to sign
$taproot$: flag to indicate compatibility with BIP341

$\mathcal{P}_i$.Round1()$\dashrightarrow(c_i, \{z^a{}_{(i,j)}\}_{j\in \mathrm{S}^*})$

1: Sample $k_i \xleftarrow{\$} \mathbb{Z}_{q^*}$ and compute $R_i \leftarrow k_i \cdot G$
2: $(c_i, w_i) \leftarrow \mathsf{Commit}(R_i \,||\, i \,||\, sid \,||\, S)$
3: $\mathcal{F}^{Broadcast}(c_i)$

$\mathcal{P}_i$.Round2($\{c_j, z^a{}_{(j,i)}\}_{j\in \mathrm{S}^*}$)$\dashrightarrow(\pi_i^{dl}, R_i, w_i, \{z^b{}_{(i,j)}\}_{j\in \mathrm{S}^*})$

1: $\pi_i^{dl} \leftarrow \mathsf{Fischlin.Prove}(k_i)$
2: $\mathcal{F}^{Broadcast}(\pi_i^{dl}, R_i, w_i)$

$\mathcal{P}_i$.Round3($\{\pi_j^{dl}, R_j, w_j, z^b{}_{(j,i)}\}_{j\in \mathrm{S}^*}$)$\dashrightarrow\sigma_i$

1: **for** $j \in \mathrm{S}^*$ **do**
2: Run $\mathsf{Open}(R_j \,||\, j \,||\, sid \,||\, S, c_j, w_j)$, ABORT if it fails
3: Run $\mathsf{Fischlin.Verify}(R_j, \pi_j^{dl})$, ABORT if it fails
4: $R \leftarrow \sum_{j\in \mathrm{S}*} R_j$
5: $d_i' \leftarrow \mathsf{ShamirToAdditive}(i, \mathrm{S}, x_i)$
6: Run $(R_i, s_i) \leftarrow \mathsf{Schnorr.Variant}(R_i, d_i')$
return $\sigma_i = \{R_i, s_i\}$

Aggregate$(\sigma_i\ \forall i \in \mathrm{S})\dashrightarrow\sigma$

1: $r \leftarrow \sum_{i=1}^{n} R_i$
2: $s \leftarrow \sum_{i=1}^{n} s_i$
return $\sigma \leftarrow (r, s)$

References

[Lin22] Yehuda Lindell. Simple three-round multiparty schnorr signing with full simulatability. Cryptology ePrint Archive, Paper 2022/374, 2022. https://eprint.iacr.org/2022/374.