Scheme BLS

The pairing-based signing scheme from [BLS01] over curve BLS 123 81 [BGW+22], instantiated with short keys *wlog* and with all rogue key prevention schemes. It uses hash functions $\mathsf{H}_{\mathbb{G}_1}$ and $\mathsf{H}_{\mathbb{G}_2}$ over $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. **BLS123-81**.Verify(m, σ) is a pairing-based verification function returning $(\mathsf{H}_{\mathbb{G}_1}(m) \times Y^{-1}) \cdot (G_1 \times \sigma) \overset{?}{=} 1$.

Inputs: A unique session identifier *sid*, a message $\boldsymbol{m}$ to be signed, a public key Y_i, and a private key x_i for each signer $\mathcal{P}_i$ $\forall i \in [t]$.

Outputs: A partial signature σ_i for each player $\mathcal{P}_i$ $\forall i \in [t]$ after round 1, and a signature σ after aggregation,

```
Sign_i($\boldsymbol{m}$) $\dashrightarrow \sigma_i$
  If MessageAug, $\boldsymbol{m} \leftarrow Y_i \,||\, \boldsymbol{m}$.
  If PoP, $\pi_i \leftarrow \mathsf{x}_i \times \mathsf{H}_{\mathbb{G}_2}(Y_i)$.
  $\sigma_i \leftarrow x_i \times \mathsf{H}_{\mathbb{G}_2}(\boldsymbol{m})$
  return $\sigma_i$ as the partial signature, attaching $\pi_i$ to it if PoP.

Verify($\{\sigma_i\}_{i \in [t]}$) $\dashrightarrow$ valid
  for $i \in [t]$ do
      If Basic, ensure all $m_{(i)}$ are unique. ABORT otherwise.
      If PoP, check if BLS123-81.Verify($Y_i, \pi_i$) is valid. ABORT otherwise.
      If MessageAug, $\boldsymbol{m} \leftarrow Y_i \,||\, \boldsymbol{m}$.
      Check if BLS123-81.Verify($Y_i, \sigma_i$) is valid. ABORT otherwise.
  return valid.
```

References

[BGW+22] Dan Boneh, Sergey Gorbunov, Riad S. Wahby, Hoeteck Wee, Christopher A. Wood, and Zhenfei Zhang. BLS Signatures. Internet-Draft draft-irtf-cfrg-bls-signature-05, Internet Engineering Task Force, June 2022. Work in Progress.

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. asiacrypt 2001. lncs 2248, 2001.