Protocol Boldyreva03

t-out-of-n threshold signing protocol of [Bol03], realizing a distributed BLS signing scheme over elliptic curve BLS 123-81 [BGW+22], instantiated with short keys w.l.o.g. and employing rogue key prevention mechanisms. It uses Sha256 [Dan15] for hash functions $\mathsf{H}_{\mathbb{G}_1}$ and $\mathsf{H}_{\mathbb{G}_2}$ to output a random group elements in $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively.

Players: t players out of the n private-key share holders $\mathcal{P}_1, \ldots, \mathcal{P}_n$. At least one signature aggregator $\mathcal{P}_{SA}$ (may be a share holder or a separate entity)

Inputs: A unique session identifier *sid*, and a message $\boldsymbol{m}$ to be signed.

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,

$\mathcal{P}_i \forall i \in [n].\textbf{Init}()$--→

1: All n parties jointly run DKG to generate their signing key shares.

$\mathcal{P}_i.\textbf{Sign}(m)$--→$\sigma_i$

1: Run $(\sigma_i, \pi_i) \leftarrow \mathsf{BLS.Sign}(x_i, \boldsymbol{m})$.

2: $\mathsf{Send}(\sigma_i, \pi_i) \rightarrow \mathcal{P}_{SA}$

$\mathcal{P}_{SA}.\textbf{Aggregate}(\{\sigma_i\}_{i\in[t]})$--→$\sigma$

1: Parse σ_i and π_i from all participating parties.

2: **for** $i \in [t]$ **do**

3: Run steps 2-4 of $\mathsf{BLS.Verify}(Y_i, \sigma_i)$.

4: $\sigma \leftarrow \sum_{i\in[t]} \lambda_i \cdot \sigma_i$, where λ_i is the Lagrange coefficient of $\mathcal{P}_i$.

return σ.

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.

[Bol03] Alexandra Boldyreva. Efficient threshold signature, multisignature and blind signature schemes based on the gap-diffie-hellman-group signature scheme, pkc 2003, lncs 2139, 2003.

[Dan15] Quynh Dang. Secure hash standard, 2015-08-04 2015.