Protocol HJKY

An interactive protocol [HJKY95] based on PedersenDKG to generate shares of zero among n parties, parametrized by a group $\mathbb{G}$ with identity I.

Players: $\mathcal{P}_1, \ldots, \mathcal{P}_n$, with symmetric behavior.
Outputs: $\mathcal{P}_i$: o_i, a share of zero $\forall i \in [n]$ s.t. $\sum_{i\in[n]} o_i = 0_{\mathbb{G}}$

$\mathcal{P}_i$.Round1()$\dashrightarrow(\boldsymbol{x}_i, \boldsymbol{C}_i)$
1: Set $a_{i,0} \xleftarrow{\$} 0$
2: Run steps 2-3 of PedersenDKG.Round1(), obtaining $x_{(i,j)}$ $\forall j \in [n]$ and $\boldsymbol{C}_i$
3: Send$(x_{(i,j)}) \rightarrow \mathcal{P}_j$ $\forall j \in [n]$
4: $\mathcal{F}^{Broadcast}(\boldsymbol{C}_i)$

$\mathcal{P}_i$.Round2$(\{\boldsymbol{C}_j, \pi_j\}_{j\in[n]})\dashrightarrow(o_i)$
1: Run $o_i, Y \leftarrow$ PedersenDKG.Round2$(\{\boldsymbol{C}_j, \pi_j\}_{\forall j})$
2: Check if $\boldsymbol{C}_{j,0} \stackrel{?}{=} I$; otherwise ABORT
3: Check if $Y \stackrel{?}{=} I$; otherwise ABORT (sanity check)
return o_i

References

[HJKY95] Amir Herzberg, Stanisław Jarecki, Hugo Krawczyk, and Moti Yung. Proactive secret sharing or: How to cope with perpetual leakage. In *Advances in Cryptology—CRYPT0'95: 15th Annual International Cryptology Conference Santa Barbara, California, USA, August 27–31, 1995 Proceedings 15*, pages 339–352. Springer, 1995.