Protocol PedersenDKG

A Distributed Key Generation protocol from [Ped91] using t-out-of-n Feldman VSS and a ZKPoK of the discrete log (e.g., Fischlin), for a group $\mathbb{G}(q, G)$

Players: $\mathcal{P}_1, \ldots, \mathcal{P}_i, \ldots, \mathcal{P}_n$, a set of n share holders.
Inputs: *sid*, a unique session identifier (e.g., obtained from Protocol **??**)
Outputs: A public key Y and n secret shares x_i of the private key x.

```
$\mathcal{P}_i.\mathsf{Round1}() \dashrightarrow (\boldsymbol{x}_i, \boldsymbol{C}_i)$
    Sample $a_{i,0} \xleftarrow{\$} \mathbb{Z}_q$
    $(\boldsymbol{x}_i, \boldsymbol{C}_i) \leftarrow \mathsf{Feldman.Split}(a_{i,0})$ as shares $\boldsymbol{x}_i$ and public key shares $\boldsymbol{C}_i$
    $\pi_i \leftarrow \{\mathsf{Fischlin.Prove}(s)\}\ \forall s \in \{a_{i,0}, x_{(i,1)}, \ldots, x_{(i,n)}\}$
    $\mathsf{Send}(x_{(i,j)}) \rightarrow \mathcal{P}_j \ \ \forall j \in [n]$
    $\mathcal{F}^{Broadcast}(\boldsymbol{C}_i)$

$\mathcal{P}_i.\mathsf{Round2}(\{\boldsymbol{C}_j, \pi_j\}_{j \in [n]}) \dashrightarrow (x_i, Y)$
    Run $\mathsf{Feldman.Verify}(j, x_{(j,i)}, \boldsymbol{C}_j) \ \ \forall j \in [n]$; ABORT if it fails
    Run $\mathsf{Fischlin.Verify}(j, \boldsymbol{\pi}_j) \ \ \forall j \in [n]$; ABORT if it fails
    $x_i \leftarrow \sum_{j=1}^{n} x_{(j,i)}$ as the secret key share of $\mathcal{P}_i$
    $Y \leftarrow \sum_{j=1}^{n} \boldsymbol{C}_{(j,0)}$ as the public key
    return $(x_i, Y)$
```

References

[Ped91] Torben Pryds Pedersen. A threshold cryptosystem without a trusted party. In *Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'91, pages 522–526, Berlin, Heidelberg, 1991. Springer-Verlag.