Protocol Joint - Feldman DKG

Maliciously secure threshold DKG protocol from [GJKR07] for a group $\mathbb{G}(q, G)$, using t-out-of-n Pedersen VSS and a ZKPoK of the discrete log (e.g., Fischlin)

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.

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

$\mathcal{P}_i.\mathsf{Round2}(\{\boldsymbol{B}_j\}_{j\in[n]}, \{x_{(j,i)}, x'_{(j,i)}\}_{j\in[n]}) \dashrightarrow (\boldsymbol{C}_i, \boldsymbol{\pi})_i$
    Check $\mathsf{Pedersen.Verify}(j, x_{(j,i)}, x'_{(j,i)}, \boldsymbol{B}_j) \ \ \forall j \in [n]$; ABORT if it fails
    $x_i \leftarrow \sum_{j\in[n]} x_{(j,i)}$ as the private key share of $\mathcal{P}_i$
    $\mathcal{F}^{Broadcast}(\boldsymbol{C}_i, \boldsymbol{\pi}_i)$

$\mathcal{P}_i.\mathsf{Round3}(\{\boldsymbol{C}_j\}_{j\in[n]}, \{\boldsymbol{\pi}_j\}_{j\in[n]}) \dashrightarrow (x_i, Y)$
    Run $\mathsf{Fischlin.Verify}(j, \boldsymbol{\pi}_j) \ \ \forall j \in [n]$; ABORT if it fails
    Run $\mathsf{Feldman.Verify}(j, x_{(j,i)}, \boldsymbol{C}_j) \ \ \forall j \in [n]$; ABORT if it fails
    $Y \leftarrow \sum_{j=1}^{n} \boldsymbol{C}_{(j,0)}$ as the public key
    **return** $(x_i, Y)$
```

References

[GJKR07] Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. Secure distributed key generation for discrete-log based cryptosystems. *Journal of Cryptology*, 20:51–83, 2007.