Protocol TrustedDealer

A centralized Key Generation algorithm based on t-out-of-n Pedersen VSS run by a trusted dealer t, parametrized by a group $\mathbb{G}(q, G)$.

Players: $\mathcal{D}$, a trusted dealer, and $\mathcal{P}_1, \ldots, \mathcal{P}_i, \ldots, \mathcal{P}_n$, a set of n share holders.

```
$\mathcal{D}$.KeyGen() $\dashrightarrow (\boldsymbol{x}, \boldsymbol{b}, Y, D)$
  Sample $x \xleftarrow{\$} \mathbb{Z}_q$ as the private key
  $Y \leftarrow x \cdot G$ as the public key
  Run $(\boldsymbol{x}, \boldsymbol{b}, C, D) \leftarrow$ Pedersen.Split($x$) to get private key shares $\boldsymbol{x}$, blinding shares $\boldsymbol{b}$ and blinded commitments $D$
  Send($x_{(i)}, b_{(i)}, Y, D$) $\rightarrow \mathcal{P}_i$
```

References