Scheme Pedersen VSS

Pedersen sharing scheme [Ped91] implements a VSS scheme based on Pedersen Commitment. This scheme is parametrized by a group $\mathbb{G}$ of prime order q with a generator G (e.g., from an elliptic curve $\mathsf{E}(\mathbb{G}, q, G)$), a second generator H chosen independently[1] from G, the number of shares produced n, and the number of shares required to reconstruct t (threshold).

Split$(s \in \mathbb{F}_q) \dashrightarrow (\boldsymbol{y} = \{y_{(i)}\}_{i\in[n]},\ \boldsymbol{b} = \{b_{(i)}\}_{i\in[n]},\ C = \{C_{(j)}\}_{j\in[t]}\ D = \{D_{(j)}\}_{j\in[t]})$

1: Run $\boldsymbol{y}, \mathrm{X}, \boldsymbol{C} \leftarrow \mathsf{Feldman.Split}_G(s)$ to get shares $\boldsymbol{y}$ and commitments $\boldsymbol{C}$
2: Sample $\beta \xleftarrow{\$} \mathbb{Z}_{q^*}$ as a blinding element.
3: Run $\boldsymbol{b}, \boldsymbol{B} \leftarrow \mathsf{Feldman.Split}_H(\beta)$ as blinding shares $\boldsymbol{b}$ and commitments $\boldsymbol{B}$
4: $D \leftarrow \{C_{(j)} + B_{(j)}\}_{j\in[t]}$ as the blinded commitments.
return $(\boldsymbol{y}, \boldsymbol{b}, \boldsymbol{C}, D)$

Verify$(i \in [n],\ y_{(i)} \in \mathbb{F}_q,\ b_{(i)} \in \mathbb{F}_q,\ \boldsymbol{D} = \{D_{(1)}, \ldots, D_{(t)}\}) \dashrightarrow \mathit{valid}$

1: $R \leftarrow D_1 + \sum_{j=1}^{t-1} (j \cdot i) \cdot D_{(j+1)}$ as the expected blinded commitment.
2: $L \leftarrow (y_{(i)} \cdot G) + (b_{(i)} \cdot H)$ as the actual blinded commitment of $y_{(i)}$.
3: Check if $L \stackrel{?}{=} R$, ABORT if not.
return *valid*

Combine$(\mathrm{X}' \in [n]^t,\ \boldsymbol{y'} = \{y_{(i)} \in \mathbb{F}\}_{i\in\mathrm{X}'},\ \boldsymbol{D} = \{D_{(j)}\}_{j\in[t]}) \dashrightarrow s$

1: Run $\mathsf{Pedersen.Verify}_G(i, y_{(i)}, \boldsymbol{D})\ \forall i \in \mathrm{X}'$ to verify all the t shares.
2: Run $\mathsf{SSS.Combine}(\mathrm{X}', \boldsymbol{y'})$ to reconstruct the secret s.
return s

References

[Ped91] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Annual international cryptology conference*, pages 129–140. Springer, 1991.

[1] In the selection of a second generator H, x s.t. $H = x \cdot G$ must remain unknown to the parties. This is effectively achieved in the DKG (**??**) via aggregation of commitments of independent random values, following the instructions of [Ped91].