**Scheme** Feldman

A VSS scheme based on the Feldman commitment scheme [Fel87] and the SSS scheme [Sha79]. The scheme is parametrized by a group $\mathbb{G}$ of prime order $q$ and generator $G$, the number of shares produced $n$, and the number of shares required to reconstruct $t$ (threshold).

$\mathsf{Split}_G(s \in \mathbb{F}_q) \dashrightarrow (\boldsymbol{y} = \{y_{(1)}, \ldots y_{(n)}\},\ C = \{C_{(1)}, \ldots, C_{(t)}\})$

1: Set $\mathbf{p}_0 \leftarrow s$ as the constant term of a polynomial $\mathbf{p}(x)$ of degree $t-1$.
2: Set $C_1 \leftarrow s \cdot G$ as the commitment of the secret.
3: **for** $j \in [t-1]$ **do**
4: Sample $\mathbf{p}_j \xleftarrow{\$} \mathbb{F}_q^*$ as the random coefficients of the polynomial $\mathbf{p}$.
5: $C_{(j+1)} \leftarrow \mathbf{p}_j \cdot G$ as a commitment of each coefficient.
6: **for** $i \in [n]$ **do**
7: $y_{(i)} \leftarrow \Sigma_{k=0}^{t-1}(\mathbf{p}_k \cdot i^k)$ as the evaluation of $\mathbf{p}(x)$ in $x = i$.

**return** $(\boldsymbol{y} = \{y_{(i)}\}_{i \in [n]},\ \boldsymbol{C} = \{C_{(j)}\}_{j \in [t]})$ as $n$ shares and $t$ commitments

$\mathsf{Verify}_G(i \in [n],\ y_{(i)} \in \mathbb{F}_q,\ \boldsymbol{C} = \{C_{(1)}, \ldots, C_{(t)}\}) \dashrightarrow \mathit{valid}$

1: $R \leftarrow C_1 + \sum_{j=1}^{t-1}(j \cdot i) \cdot C_{(j+1)}$ as the expected commitment.
2: $L \leftarrow y_{(i)} \cdot G$ as the actual commitment of the share $y_{(i)}$.
3: Check if $L \stackrel{?}{=} R$, ABORT if not.

**return** *valid*

$\mathsf{Combine}_G(\mathrm{X}' \in [n]^t,\ \boldsymbol{y'} = \{y_{(i)} \in \mathbb{F}\}_{i \in \mathrm{X}'},\ \boldsymbol{C} = \{C_{(1)}, \ldots, C_{(t)}\}) \dashrightarrow s$

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

**return** $s$

# References


[Fel87] Paul Feldman. A practical scheme for non-interactive verifiable secret sharing. In *28th Annual Symposium on Foundations of Computer Science (sfcs 1987)*, pages 427–438, 1987.

[Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.