Scheme Shamir Secret Sharing (SSS)

Shamir's Secret Sharing Scheme [Sha79] based on polynomial interpolation. This scheme is parametrized by a finite field $\mathbb{F}$, the number of shares produced n, and the number of shares required to reconstruct t (threshold).

$\textsf{Split}_{t,n}(s \in \mathbb{F}) \dashrightarrow (\boldsymbol{y})$

Set $\mathbf{p}_0 \leftarrow s$ as the constant term of a polynomial $\mathbf{p}(x)$ of degree $t-1$.
for $k \in [t-1]$ **do**
  Sample $\mathbf{p}_k \xleftarrow{\$} \mathbb{F}$ as the random coefficients of the polynomial $\mathbf{p}$.
for $i \in [n]$ **do**
  $y_{(i)} \leftarrow \Sigma_{k=0}^{t-1}(\mathbf{p}_k \cdot i^k)$ as the evaluation of $\mathbf{p}(x)$ in $x = i$.
return $(\boldsymbol{y} = \{y_{(i)}\}_{i \in [n]})$ as the n shares.

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

for $i \in \mathrm{X}$ **do** *(Iterate over the indices of the t shares)*
  Set $\mathrm{X}' \leftarrow \mathrm{X} \setminus \{i\}$
  $\ell_i \leftarrow \Pi_{k \in \mathrm{X}'} \frac{k}{k-i}$ as the Lagrange coefficient i
$s \leftarrow \sum_{i \in \mathrm{X}} \ell_i \cdot y_{(i)}$ for the Lagrange interpolation of $\mathbf{p}(x)$ in $x = 0$.
return s as the reconstructed secret.

References

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