Scheme Additive Secret Sharing (SS)

Additive Secret Sharing Scheme. This scheme is parametrized by a group $\mathbb{G}$ in and the number of shares produced n.

```
$\mathit{Split}_n(x \in \mathbb{G}) \dashrightarrow (\boldsymbol{y} = \{y_{(1)}, \dots y_{(n)}\})$
**for** $i \in [n-1]$ **do**
    Sample $y_{(i)} \xleftarrow{\$} \mathbb{G}$ as $n$ - 1 random shares
$y_{(n)} \leftarrow x - \sum_{iins[n-1]} y_{(i)}$ as the last random share
**return** $\boldsymbol{y} = \{y_{(i)}\}_{i \in [n]}$ as the $n$ shares
```

```
$\mathit{Combine}_n(\boldsymbol{y'} = \{y_{(i)} \in \mathbb{G}\}_{i \in [n]}) \dashrightarrow x$
$x \leftarrow \sum_{i \in [n]} y_{(i)}$
**return** $x$ as the reconstructed secret
```

References