

---

**Algorithm**     $\text{ShamirToAdditive}_{t,n,\mathbb{F}}(i, X, y_{(i)}) \leftarrow x_{(i)}$

---

**Inputs:**  $i \in [n]$  as the party index

$X \in [n]^t$  as a subset of  $t$  indices

$y_{(i)} \in \mathbb{F}$  as a  $t$ -out-of- $n$  shamir share

**Outputs:**  $x_{(i)} \in \mathbb{F}$  as the corresponding  $t$ -out-of- $t$  additive share

1: Set  $X' \leftarrow X \setminus \{i\}$

2:  $\ell_i \leftarrow \prod_{j \in X'} \frac{k}{k-i}$  as the Lagrange coefficient

**return**  $x_{(i)} \leftarrow y_{(i)} \cdot \ell_i$  as the additive share

---

## References