
Protocol **Przs**

A protocol to generate shares of zero among n parties, parametrized by a group \mathbb{G} . It requires a commitment scheme (e.g., Scheme ??) and a pseudo-random number generator \mathcal{F}^{PRNG} . In all cases, $j \in [n] \setminus \{i\}$. The setup rounds are run once, and the sample can be run multiple times.

Players: $\mathcal{P}_1, \dots, \mathcal{P}_n$, with symmetric behavior.

Outputs: \mathcal{P}_i : o_i , a share of zero $\forall i \in [n]$ s.t. $\sum_{i \in [n]} o_i = 0_{\mathbb{G}}$

$\mathcal{P}_i.$ Setup1() $\dashrightarrow c_{i,j}$

- 1: Sample $r_{i,j} \xleftarrow{\$} \{0,1\}^\lambda \forall j$ as the $n-1$ seeds of \mathcal{P}_i , one with each party \mathcal{P}_j
- 2: Run $c_{i,j}, w_{i,j} \leftarrow \text{Commit}(r_{i,j}) \forall j$ as the commitments $c_{i,j}$ and witnesses $w_{i,j}$
- 3: Send($c_{i,j}$) $\rightarrow \mathcal{P}_j$ to distribute each commitment to its respective party \mathcal{P}_j

$\mathcal{P}_i.$ Setup2($c_i = \{c_{j,i}\}_{\forall j}$) $\dashrightarrow \{r_{i,j}, w_{i,j}\}_{\forall j}$

- 1: Send($r_{i,j}, w_{i,j}$) $\rightarrow \mathcal{P}_j \forall j$ to reveal each $r_{i,j}$ and $w_{i,j}$ to each party \mathcal{P}_j

$\mathcal{P}_i.$ Setup3($r_j = \{r_{j,i}\}_{\forall j}$, $w_j = \{w_{j,i}\}_{\forall j}$) $\dashrightarrow \{\text{PRNG}_j\}_{\forall j}$

- 1: Open($r_{j,i}, c_{j,i}, w_{j,i}$) $\forall j$, **ABORT** if it fails
- 2: $s_{i,j} \leftarrow r_{i,j} \oplus r_{j,i} \forall j$ *May use $s_{i,j} \leftarrow H(r_{i,j}, r_{j,i})$ instead*
- 3: Initialize $\text{PRNG}_j \leftarrow \text{PRNG.Seed}(s_{i,j})$ as a fresh instance for each party \mathcal{P}_j
 return PRNG_j

$\mathcal{P}_i.$ Sample($X' \subseteq [n] \setminus \{i\}$) $\dashrightarrow o_i$

- 1: Initialize $o_i \leftarrow 0$
 - 2: **for** j in X' **do**
 - 3: Run $z_j \leftarrow \text{PRNG}_j.\text{Sample}(1)$
 - 4: $o_i \leftarrow o_i + z_j \cdot \text{sgn}(i - j)$
 - return** o_i as its share of zero
-

References