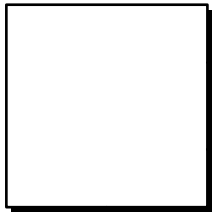


Alice

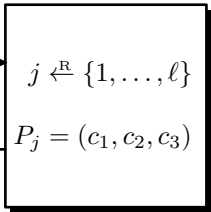


$k \leftarrow s_\ell$

Puzzles P_1, \dots, P_L



Bob



$\ell \leftarrow D(k, c_2)$



$j \xleftarrow{\mathcal{R}} \{1, \dots, \ell\}$

$P_j = (c_1, c_2, c_3)$

$k \leftarrow s_\ell$