Protocol $\mathsf{OT}_{\xi,\ell}$

(Standard) OT protocol from any ROT protocol and one-time-pad encryption

Players: a sender $\mathcal{S}$, and receiver $\mathcal{R}$

Inputs: $\mathcal{R}\colon \boldsymbol{x} \in \mathbb{Z}_2^{\xi}$, the input choice bits

$\mathcal{S}\colon \boldsymbol{m_0}, \boldsymbol{m_1} \in \mathbb{Z}_2^{\xi\times\ell\times\kappa}$, pairs of messages

Outputs: $\mathcal{R} \leftarrow \boldsymbol{m_x} \in \mathbb{Z}_2^{\xi\times\ell\times\kappa}$, the chosen messages

$\mathcal{S}\&\mathcal{R}.\mathbf{RunROT}(b) \dashrightarrow \mathcal{S}\colon (\boldsymbol{r_0}, \boldsymbol{r_1});\ \mathcal{R}\colon \boldsymbol{r_b}$

1: $\mathcal{S}$ runs $\mathsf{ROT}_{\xi,\ell}$ as sender, obtaining $\boldsymbol{r_0}, \boldsymbol{r_1} \in \mathbb{Z}_2^{\xi\times\ell\times\kappa}$

2: $\mathcal{R}$ runs $\mathsf{ROT}_{\xi,\ell}$ as receiver, obtaining $\boldsymbol{r_b} \in \mathbb{Z}_2^{\xi\times\ell\times\kappa}$

$\mathcal{S}.\mathbf{Encrypt}(\boldsymbol{r_0}, \boldsymbol{r_1}, \boldsymbol{m_0}, \boldsymbol{m_1}) \dashrightarrow (\boldsymbol{\tau_0}, \boldsymbol{\tau_1})$

1: $(\boldsymbol{\tau_0}, \boldsymbol{\tau_1}) \leftarrow \left\{\left\{r_{0(i,j)} \oplus m_{0(i,j)}\right\}_{j\in[\ell\times\kappa]}\right\}_{i\in[\xi]}$

2: $\mathsf{Send}(\boldsymbol{\tau_0}, \boldsymbol{\tau_1}) \rightarrow \mathcal{R}$

$\mathcal{R}.\mathbf{Decrypt}(\boldsymbol{\tau_0}, \boldsymbol{\tau_1}) \dashrightarrow \boldsymbol{m_x}$

$$\textbf{return } \boldsymbol{m_x} \leftarrow \left\{\left\{\begin{matrix}\tau_{0(i,j)} \oplus r_{b(i,j)} & \text{if } x_{(i)}=0\\ \tau_{1(i,j)} \oplus r_{b(i,j)} & \text{if } x_{(i)}=1\end{matrix}\right\}_{j\in[\ell\times\kappa]}\right\}_{i\in[\xi]}$$

References