**Protocol** $\mathsf{COT}_{\mathbb{G},\xi,\ell}$

Correlated OT protocol from any $\mathsf{ROT}$ protocol and a uniform mapper $\mathsf{H}\colon \mathbb{Z}_2^{\kappa} \mapsto \mathbb{G}$ (e.g., Hash2Field [FHSS+23] for EC), parametrized by a group $\mathbb{G}$

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

**Inputs:** $\mathcal{S}\colon \boldsymbol{a} \in \mathbb{G}^{\xi\times\ell}$, group elements

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

**Outputs:** $\mathcal{S} \leftarrow \boldsymbol{z_A} \in \mathbb{G}^{\xi\times\ell}$

$\mathcal{R} \leftarrow \boldsymbol{z_B} \in \mathbb{G}^{\xi\times\ell}$ s.t. $z_{A(i,j)} + z_{B(i,j)} = a_{(i,j)} \cdot x_{(i)} \quad \forall i \in [\xi]\ \forall j \in [\ell]$

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

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 $\boldsymbol{r_b} \in \mathbb{Z}_2^{\xi\times\ell\times\kappa}$

$\mathcal{S}.\textsf{\textbf{CreateCorrelation}}(\boldsymbol{r_0}, \boldsymbol{r_1}, \boldsymbol{a}) \dashrightarrow (\boldsymbol{\tau})$

1: $\boldsymbol{z_A} \leftarrow \big\{\{\mathsf{H}(r_{0(i,j)})\}_{j\in[\ell]}\big\}_{i\in[\xi]}$

2: $\boldsymbol{\tau} \leftarrow \big\{\{\mathsf{H}(r_{1(i,j)}) - z_{A(i,j)} + a_{(i,j)}\}_{j\in[\ell]}\big\}_{i\in[\xi]}$

3: $\mathsf{Send}(\boldsymbol{\tau}) \rightarrow \mathcal{R}$

**return** $\boldsymbol{z_A}$

$\mathcal{R}.\textsf{\textbf{ApplyCorrelation}}(\boldsymbol{\tau}) \dashrightarrow \boldsymbol{z_B}$

**return** $\boldsymbol{z_B} \leftarrow \big\{\{\tau_{(i,j)} \cdot b_{(i)} - \mathsf{H}(r_{b(i,j)})\}_{j\in[\ell]}\big\}_{i\in[\xi]}$

# References


[FHSS+23] Armando Faz-Hernandez, Sam Scott, Nick Sullivan, Riad S. Wahby, and Christopher A. Wood. Hashing to Elliptic Curves. RFC 9380, August 2023.