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

Endemically secure Batched Base ROT protocol from [MRR21, Figure 3] and a hash function H (for two ROs $\mathsf{H}_0(x)$ and $\mathsf{H}_1(x)$), parametrized by a batch of ξ messages with $\ell \times \kappa$ bits each, a group $\mathbb{G}$ of prime order q with generator G.

Players: a sender $\mathcal{S}$, and receiver $\mathcal{R}$.
Inputs: $\mathcal{R}$: $\boldsymbol{b} \in \mathbb{Z}_2^{\xi}$, the input choice bits.
Outputs: $\mathcal{S} \leftarrow \boldsymbol{m_0}, \boldsymbol{m_1} \in \mathbb{Z}_2^{\xi\times\ell\times\kappa}$, two random messages.
$\mathcal{R} \leftarrow \boldsymbol{m_b} \in \mathbb{Z}_2^{\xi\times\ell\times\kappa}$, the chosen message.

```
$\mathcal{S}$.Round1()$\dashrightarrow(A)$
  Sample $a \overset{\$}{\leftarrow} \mathbb{Z}_q$                                  $(KA.R)$
  $A \leftarrow a \cdot G$                                          $(KA.msg_1)$
  Send$(A) \rightarrow \mathcal{R}$
$\mathcal{R}$.Round2$(A \in \mathbb{G}, \boldsymbol{b})\dashrightarrow(\boldsymbol{m_x}, \boldsymbol{\phi})$
  for $\forall i \in [\xi]\ \ \forall l \in [\ell]$ do
      Sample $\beta \overset{\$}{\leftarrow} \mathbb{Z}_q$                          $(KA.R)$
      $m_R \leftarrow \beta \cdot G$                                $(KA.msg_2)$
      $m_{b(i,l)} \leftarrow \mathsf{H}(\beta \cdot A, i \mid\mid b_{(i)})$                 $(KA.key_2)$
      Sample $\phi_{i,l,1-b_{(i)}} \overset{\$}{\leftarrow} \mathbb{G}$                  $(POPF.Program)$
      $\phi_{i,l,b_{(i)}} \leftarrow m_R - \mathsf{H}_{b_{(i)}}(\phi_{i,l,1-b_{(i)}})$          $(POPF.Program)$
  Send$(\boldsymbol{\phi_0} = \{\{\phi_{i,l,0}\}_{l\in[\ell]}\}_{i\in[\xi]},\ \boldsymbol{\phi_1} = \{\{\phi_{i,l,1}\}_{l\in[\ell]}\}_{i\in[\xi]}) \rightarrow \mathcal{S}$
  return $(\boldsymbol{m_b} = \{\{m_{b(i,l)}\}_{l\in[\ell]}\}_{i\in[\xi]})$
$\mathcal{S}$.Round3$(\boldsymbol{\phi_0}, \boldsymbol{\phi_1} \in \mathbb{G}^{\xi\times\ell})\dashrightarrow \boldsymbol{m_0}, \boldsymbol{m_1}$
  for $\forall i \in [\xi]\ \ \forall l \in [\ell]\ \ \forall j \in \{0,1\}$ do
      $P \leftarrow \phi_{j\,(i,l)} + \mathsf{H}_j(\phi_{1-j\,(i,l)})$                 $(POPF.Eval)$
      $m_{j\,(i,l)} \leftarrow \mathsf{H}(a \cdot P, i \mid\mid j)$                    $(KA.key_1)$
  return $\boldsymbol{m_0} = \{\{m_{0\,(i,l)}\}_{l\in[\ell]}\}_{i\in[\xi]},\ \boldsymbol{m_1} = \{\{m_{1\,(i,l)}\}_{l\in[\ell]}\}_{i\in[\xi]}$
```

References

[MRR21] Ian McQuoid, Mike Rosulek, and Lawrence Roy. Batching base oblivious transfers. In *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part III 27*, pages 281–310. Springer, 2021.