1 From R-OT to 1-out-of-2 OT

Sender: $m_0, m_1$. Receiver has $b$. Receiver wants to get $m_b$

They run R-OT, sender gets $r_0, r_1$, receiver gets $c \in \{0, 1\}$ and $r_c$.

...We want the sender to encrypt $m_b$ with $r_c$

$R \rightarrow S : x := b \oplus c$

$S \rightarrow R : \{m_0\}_{r_x}, \{m_1\}_{r_{\neg x}}$

Simulating receiver’s view (input $b$, output $M$): $c, r, \{M\}_r, \square$
2 Corrupt sender in HE-based OT

- $\mathcal{A}$ tells $\text{Sim}$ that sender is corrupt. $\text{Sim}$ tells it to $\mathcal{I}$
- $\mathcal{E}$ gives $m_0, m_1$ and $b$ to $\mathcal{I}$
- $\mathcal{I}$ gives $m_0, m_1$ to $\text{Sim}$. $\text{Sim}$ gives them to $\mathcal{A}$
- $\mathcal{A}$ gives changed $m'_0, m'_1$ to $\text{Sim}$

- Things that have to happen now, in some order:
  - $\text{Sim}$ generates keypair $(sk, pk)$ and a random bit $b^*$, tells $\mathcal{A}$ that he as the Sender got $pk, \mathcal{E}_{pk}(b^*)$, and a ZK proof that the ciphertext contains a bit
  - $\text{Sim}$ receives from $\mathcal{A}$ the second message $\mathcal{E}_{pk}(m^*)$, which Sender is expected to send to Receiver
  - $\text{Sim}$ adjusts $(m_0, m_1)$ in $\mathcal{I}$ as $(m^*, m^*)$ and tells $\mathcal{I}$ to compute
3 Corrupt Receiver in B-M OT

- $A$ tells $Sim$ that Receiver is corrupt. $Sim$ tells it to $I$
- $Z$ gives $m_0, m_1$ and $b$ to $I$
- $I$ gives $b$ to $Sim$. $Sim$ gives $b$ to $A$. $A$ adjusts $b$ to $b^*$
- 1st msg.: $Sim$ generates a random $c$, gives it to $A$ as message $S \rightarrow R$
- 2nd msg.: $A$ gives $h_0, h_1$ to $Sim$ (such that $h_0 \cdot h_1 = c$)
- $Sim$ gives $b^*$ to $I$ and tells it to do the computation. $I$ computes $M = \text{choose}(b^*; m_0, m_1)$ and gives $M$ to $Sim$
- 3rd msg.: $Sim$ generates $r_0, r_1$, gives

$$g^{r_0}, M \oplus H(h_0^{r_0}), g^{r_1}, M \oplus H(h_1^{r_1})$$

to $A$ as message $S \rightarrow R$
- $Sim$ tells $I$ to give $M$ to Receiver
• Whenever \( A \) queries \( H(x) \): \( Sim \) answers with random values...
  
  – If a query is repeated, give the same answer
4 Corrupt Sender in B-M OT

- $A$ tells $Sim$ that sender is corrupt. $Sim$ tells it to $I$
- $Z$ gives $m_0, m_1$ and $b$ to $I$
- $I$ gives $m_0, m_1$ to $Sim$. $Sim$ gives them to $A$
- $A$ gives changed $m'_0, m'_1$ to $Sim$
- 1st msg: $A$ gives $c$ to $Sim$
- 2nd msg: $Sim$ creates random $h_0, h_1$, s.t. $h_0 h_1 = c$
- 3rd msg: $A$ gives $g_0, R_0, g_1, R_1$
- $Sim$ finds $m''_0 = R_0 \oplus H_{smth}$, where $smth$ was queried by $A$ to $H$
- $Sim$ tells $I$ to adjust $(m_0, m_1) := (\ldots, \ldots)$ and tells $I$ to compute
- queries $H(x)$: record all $x$-s when answering the queries