1 1-out-of-2 OT

Let the two participants be P_1 and P_2, P_1 has two messages m_0, m_1, P_2 has a choice bit $b \in \{0, 1\}$.

Now P_1 wants P_2 knows one of the messages, but doesn't know the other one. And P_2 wants to receive the message with the choice bit b, and P_1 knows nothing about b.

1.1 method based on Discrete Logarithm Problem

Basic Setting. P_1 and P_2 both know an big integer g and a big prime number p.

Step1. P_1 generates random keys $s, r_0, r_1 \in_R \{0,1\}^\kappa$, and P_2 generates a random key $k \in_R \{0,1\}^\kappa$.

Step2. P_1 calculates g^s and send it to P_2.

Step3. P_2 calculates $L = \begin{cases} g^k, b = 0 \\ g^{s-k}, b = 1 \end{cases}$, and then send it to P_1.

Step4. P_1 calculates C_0 and C_1, in that $C_0 = (g^{r_0}, L^{r_0} \oplus m_0)$, $C_1 = (g^{r_1}, (g^s/L)^{r_1} \oplus m_1)$, and then P_0 sends C_0 and C_1 to P_2.

Step5. P_2 reconstructs the result based on received information:

$$m_b = C_b[0]^k \oplus C_b[1] \tag{1}$$