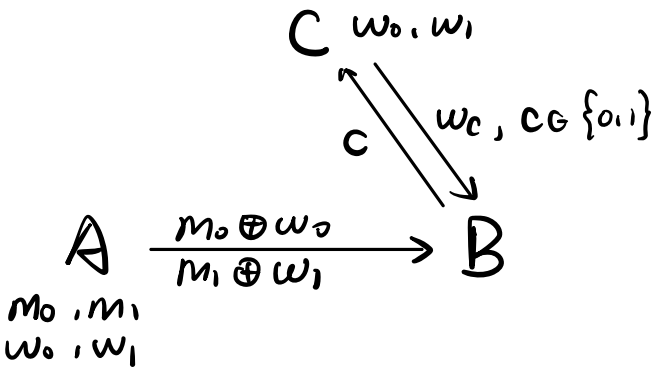
一、三方OT（实际为双方，第三方作为帮助者）

A为发送方

B为接收方

C为帮助者



①A与C共同产生2个 k比特的随机数 w_0, w_1

A与C都知道 w_0, w_1

A计算 $m_0 \oplus w_0, m_1 \oplus w_1$ ——发送——> B

B将自己的选择bit c发给C

C根据c $\xrightarrow[c \in \{0,1\}]{w_c}$ B

B根据 w_c 可通过 $w_c \oplus (m_c \oplus w_c)$ 解出 m_c

二、跨表示形式的子秘密计算 $(a[b]^B = [ab]^A)$

例：a为 Z_{2^k} 上的明文，而b为单比特

① b以 (b_1, b_2, b_3) 分享 $(b_1 \oplus b_2 \oplus b_3 = b)$

A (b_1, b_2)

B (b_2, b_3)

C (b_3, b_1)

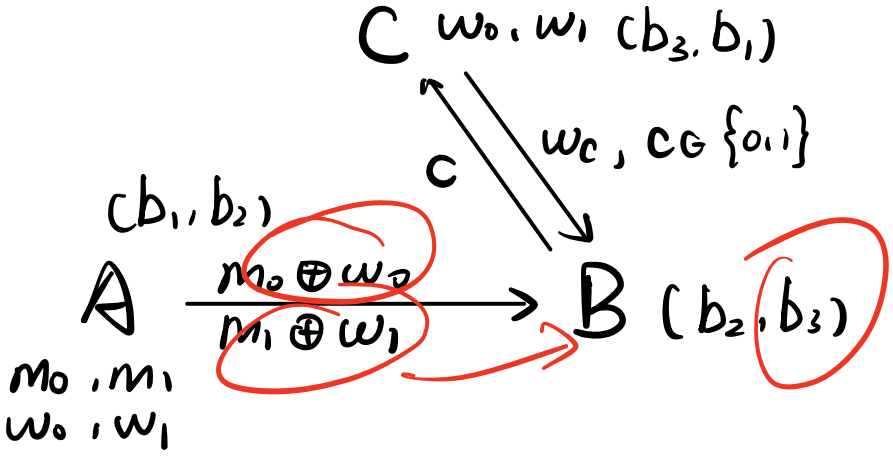
② A 生成一个随机数 r，

产生2个消息 $m_0 = (0 \oplus b_1 \oplus b_2)a - r$

$m_1 = (1 \oplus b_1 \oplus b_2)a - r$

B有 b_3，C有 b_3

③ 则可进行三方OT（如上）



B输入 b_3，获得 $m_{b_3} = (b_3 \oplus b_1 \oplus b_2)a - r = ba - r$

④ 计算 $[ab]^A$ （生成一三元组 (s_1, s_2, s_3)，使 $s_1 + s_2 + s_3 = 0$）

C
$(w_0, w_1)(s_2, s_1)$

A r (m_0, m_1) $(s_1, s_2)(w_0, w_1)$

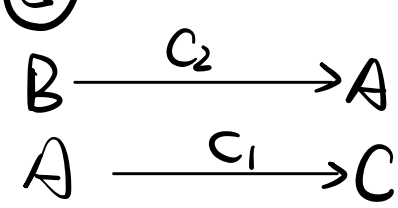
B $m_3 = ab - r$ (s_2, s_3)

A 本地计算 $c_1 = s_1 + r$

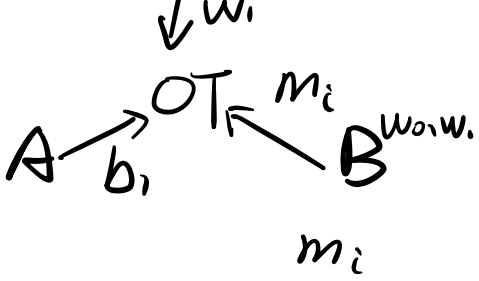
B： $c_2 = m_3 + s_3 = ab - r + s_2$

C： $c_3 = s_3$

⑤ C (w_0, w_1)



或再进行一个三方OT：



$= (i \oplus b_2 \oplus b_3)a - r + s_2$

则完成了 $[c]^A = [ab]^A$

$= (s_1 + r,\ ab - r + s_2,\ s_3)$

$$s_1 + r + ab - r + s_2 + s_3 = ab$$

Q:

多比特时怎么做？