

$A \rightarrow B$

$A_0 = A, A_2 = A'$

$B_0 = B, B_2 = B'$

A_1 | message

$\rightarrow B_0$

$B \rightarrow A$

$B_0 = B, B_2 = B'$

$A_0 = A, A_2 = A'$

B_1 | message

\rightarrow Alice

If Bob used A' then $A_1 = A'$ and $A_2 = \text{new } A'$

Else if Bob used A then $A_0 = A$ and $A_1 = A'$

$$A \rightarrow B$$

$$A_0 = A, A_1 = A'$$

$$B_0 = B, B_1 = B'$$

$$A \rightarrow B$$

$$A_0 = A, A_1 = A', A_2 = \text{new } A'$$

$$B_0 = B, B_1 = B'$$

$$B \rightarrow A$$

$$A_0 = A, A_1 = A', A_2 = \text{new } A'$$

$$B_0 = B, B_1 = B', B_2 = A_1$$

$$B \rightarrow A$$

$$A_0 = A, A_1 = A', A_2 = \text{new } A'$$

$$B_0 = B, B_1 = B', B_2 = A_1$$