

$$\begin{array}{c}
 \xrightarrow{* \quad H(R||m)} \\
 \xrightarrow{* \quad R'||m'} \\
 H(R||m) \stackrel{?}{=} H(R'||m')
 \end{array}$$

$$\begin{array}{c}
 \xrightarrow{* \quad g^a \bmod p} \\
 \xleftarrow{* \quad g^b \bmod p} \\
 (g^a)^b \bmod p = (g^b)^a \bmod p
 \end{array}$$

$$\begin{array}{c}
 \xrightarrow{* \quad c = H(R||m)} \\
 \xrightarrow{* \quad R'||m'} \\
 c \stackrel{?}{=} H(R'||m')
 \end{array}$$

$$\begin{array}{c}
 \xrightarrow{* \quad g^a} \\
 \xleftarrow{* \quad g^b} \\
 (g^a)^b = (g^b)^a
 \end{array}$$

$$\begin{array}{c}
 \xrightarrow{* \quad c = H(r \parallel m)} \\
 \xrightarrow{* \quad \bar{r} \parallel \bar{m}} \\
 c \stackrel{?}{=} H(\bar{r} \parallel \bar{m})
 \end{array}$$

$$\begin{array}{c}
 \xrightarrow{* \quad A = g^a} \\
 \xleftarrow{* \quad B = g^b} \\
 A^b = B^a
 \end{array}$$

$$\begin{array}{c}
 \xrightarrow{* \quad c = H(r \parallel m)} \\
 \xrightarrow{* \quad r \parallel m} \\
 c \stackrel{?}{=} H(r \parallel m)
 \end{array}$$

$$\begin{array}{c}
 \xrightarrow{* \quad A = g^a} \\
 \xleftarrow{* \quad B = g^b} \\
 A^b = B^a
 \end{array}$$