

In chapter 2, we proved

$$\begin{array}{c} \mathcal{L}_{\text{OTPR}_{\text{Real}}} \\ \hline \text{EAVESDROP}(m \in \{\textcolor{red}{0}, \textcolor{red}{1}\}) : \\ \hline k \leftarrow \{\textcolor{red}{0}, \textcolor{red}{1}\} \\ c := k \oplus m \\ \text{return } c \end{array} \equiv \begin{array}{c} \mathcal{L}_{\text{OTPR}_{\text{Rand}}} \\ \hline \text{EAVESDROP}(m \in \{\textcolor{red}{0}, \textcolor{red}{1}\}) : \\ \hline c \leftarrow \{\textcolor{red}{0}, \textcolor{red}{1}\} \\ \text{return } c \end{array}$$

With this fact, and from the definition of interchangability, we know that for all calling programs \mathcal{A}

$$\mathcal{A} \diamond \begin{array}{c} \mathcal{L}_{\text{OTPR}_{\text{Real}}} \\ \hline \text{EAVESDROP}(m \in \{\textcolor{red}{0}, \textcolor{red}{1}\}) : \\ \hline k \leftarrow \{\textcolor{red}{0}, \textcolor{red}{1}\} \\ c := k \oplus m \\ \text{return } c \end{array}$$

reduces to the same program as

$$\mathcal{A} \diamond \begin{array}{c} \mathcal{L}_{\text{OTPR}_{\text{Rand}}} \\ \hline \text{EAVESDROP}(m \in \{\textcolor{red}{0}, \textcolor{red}{1}\}) : \\ \hline c \leftarrow \{\textcolor{red}{0}, \textcolor{red}{1}\} \\ \text{return } c \end{array}$$