

In chapter 2, we proved

<div style="background-color: #f0f0f0; text-align: center; padding: 2px 5px;">$\mathcal{L}_{\text{OTPRReal}}$</div> <div style="border-top: 1px solid black; padding-top: 5px;"> $\text{EAVESDROP}(m \in \{\textcolor{red}{0}, \textcolor{red}{1}\}) :$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> $k \leftarrow \{\textcolor{red}{0}, \textcolor{red}{1}\}$ $c := k \oplus m$ return c </div>	\equiv	<div style="background-color: #f0f0f0; text-align: center; padding: 2px 5px;">$\mathcal{L}_{\text{OTPRand}}$</div> <div style="border-top: 1px solid black; padding-top: 5px;"> $\text{EAVESDROP}(m \in \{\textcolor{red}{0}, \textcolor{red}{1}\}) :$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> $c \leftarrow \{\textcolor{red}{0}, \textcolor{red}{1}\}$ return c </div>
---	----------	---

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

$\mathcal{A} \diamond$	<div style="background-color: #f0f0f0; text-align: center; padding: 2px 5px;">$\mathcal{L}_{\text{OTPRReal}}$</div> <div style="border-top: 1px solid black; padding-top: 5px;"> $\text{EAVESDROP}(m \in \{\textcolor{red}{0}, \textcolor{red}{1}\}) :$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> $k \leftarrow \{\textcolor{red}{0}, \textcolor{red}{1}\}$ $c := k \oplus m$ return c </div>
------------------------	---

reduces to the same program as

$\mathcal{A} \diamond$	<div style="background-color: #f0f0f0; text-align: center; padding: 2px 5px;">$\mathcal{L}_{\text{OTPRand}}$</div> <div style="border-top: 1px solid black; padding-top: 5px;"> $\text{EAVESDROP}(m \in \{\textcolor{red}{0}, \textcolor{red}{1}\}) :$ <hr style="border: 0; border-top: 1px solid black; margin: 2px 0;"/> $c \leftarrow \{\textcolor{red}{0}, \textcolor{red}{1}\}$ return c </div>
------------------------	---