

You can write your homework completely in HybLang! We are tasked to show that

$$\begin{array}{|c|} \hline \mathcal{L}_L \\ \hline \text{CTXT}(m \in \{\mathbf{0}, \mathbf{1}\}) : \\ \hline k \leftarrow \{\mathbf{0}, \mathbf{1}\} \\ c := k \oplus m \\ \text{return } c \& m \\ \hline \end{array} \equiv \begin{array}{|c|} \hline \mathcal{L}_R \\ \hline \text{CTXT}(m \in \{\mathbf{0}, \mathbf{1}\}) : \\ \hline c \leftarrow \{\mathbf{0}, \mathbf{1}\} \\ \text{return } c \\ \hline \end{array}$$

are interchangeable. This obviously not the case, since the distinguishing program

$$\begin{array}{|c|} \hline \mathcal{A} \\ \hline m := \mathbf{0} \\ c := \text{CTXT}(m) \\ \text{return } m \stackrel{?}{=} \mathbf{0} \\ \hline \end{array}$$

always returns true when linked to library L. Since we have

$$\begin{array}{|c|} \hline \mathcal{A} \\ \hline m := \mathbf{0} \\ c := \text{CTXT}(m) \\ \text{return } m \stackrel{?}{=} \mathbf{0} \\ \hline \end{array} \diamond \begin{array}{|c|} \hline \mathcal{L}_L \\ \hline \text{CTXT}(m \in \{\mathbf{0}, \mathbf{1}\}) : \\ \hline k \leftarrow \{\mathbf{0}, \mathbf{1}\} \\ c := k \oplus m \\ \text{return } c \& m \\ \hline \end{array} \implies \text{true}$$

and

$$\begin{array}{|c|} \hline \mathcal{A} \\ \hline m := \mathbf{0} \\ c := \text{CTXT}(m) \\ \text{return } m \stackrel{?}{=} \mathbf{0} \\ \hline \end{array} \diamond \begin{array}{|c|} \hline \mathcal{L}_R \\ \hline \text{CTXT}(m \in \{\mathbf{0}, \mathbf{1}\}) : \\ \hline c \leftarrow \{\mathbf{0}, \mathbf{1}\} \\ \text{return } c \\ \hline \end{array} \implies 1/2$$

so we know that

$$\begin{array}{|c|} \hline \mathcal{A} \\ \hline m := \mathbf{0} \\ c := \text{CTXT}(m) \\ \text{return } m \stackrel{?}{=} \mathbf{0} \\ \hline \end{array}$$

is a distinguishing program, so it is not the case that

$$\begin{array}{|c|} \hline \mathcal{L}_L \\ \hline \text{CTXT}(m \in \{\mathbf{0}, \mathbf{1}\}) : \\ \hline k \leftarrow \{\mathbf{0}, \mathbf{1}\} \\ c := k \oplus m \\ \text{return } c \& m \\ \hline \end{array} \text{ and } \begin{array}{|c|} \hline \mathcal{L}_R \\ \hline \text{CTXT}(m \in \{\mathbf{0}, \mathbf{1}\}) : \\ \hline c \leftarrow \{\mathbf{0}, \mathbf{1}\} \\ \text{return } c \\ \hline \end{array}$$

are interchangeable, thus proving a counterexample of the claim.