You can write your homework completely in HybLang! You can even put raw LaTeXin the annotations in HybLang! Is it just me or is

$$\pi \approx 3!$$

We are tasked to show that

$$\begin{array}{|l|}\hline \mathcal{L}_{\mathsf{L}} \\ \hline \underline{\text{CTXT}(m \in \{\mathtt{0},\mathtt{1}\}):} \\ \quad k \leftarrow \{\mathtt{0},\mathtt{1}\} \\ \quad c := k \oplus m \\ \quad \text{return } c\&m \\ \hline \end{array} \equiv \begin{array}{|l|}\hline \mathcal{L}_{\mathsf{R}} \\ \hline \underline{\text{CTXT}(m \in \{\mathtt{0},\mathtt{1}\}):} \\ \quad c \leftarrow \{\mathtt{0},\mathtt{1}\} \\ \quad \text{return } c \\ \hline \end{array}$$

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

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

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

$$\begin{array}{|l|}\hline \mathcal{A} \\ \hline m := \mathtt{0} \\ c := \text{CTXT}(m) \\ \text{return } m \stackrel{?}{=} \mathtt{0} \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}_{\mathsf{L}} \\ \hline \underline{\text{CTXT}(m \in \{\mathtt{0},\mathtt{1}\}):} \\ \quad k \leftarrow \{\mathtt{0},\mathtt{1}\} \\ \quad c := k \oplus m \\ \quad \text{return } c\&m \\ \hline \end{array} \Longrightarrow \text{true}$$

and

$$\begin{array}{|l|}\hline \mathcal{A} \\ \hline m := \mathtt{0} \\ c := \text{CTXT}(m) \\ \text{return } m \stackrel{?}{=} \mathtt{0} \\ \hline \end{array} \diamond \begin{array}{|l|}\hline \mathcal{L}_{\mathsf{R}} \\ \hline \underline{\text{CTXT}(m \in \{\mathtt{0},\mathtt{1}\}):} \\ \quad c \leftarrow \{\mathtt{0},\mathtt{1}\} \\ \quad \text{return } c \\ \hline \end{array} \Longrightarrow \frac{1}{2}$$

so we know that

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

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

$$\begin{array}{|l|}\hline \mathcal{L}_{\mathsf{L}} \\ \hline \underline{\text{CTXT}(m \in \{\mathtt{0},\mathtt{1}\}):} \\ \quad k \leftarrow \{\mathtt{0},\mathtt{1}\} \\ \quad c := k \oplus m \\ \quad \text{return } c\&m \\ \hline \end{array} \quad \text{and} \quad \begin{array}{|l|}\hline \mathcal{L}_{\mathsf{R}} \\ \hline \underline{\text{CTXT}(m \in \{\mathtt{0},\mathtt{1}\}):} \\ \quad c \leftarrow \{\mathtt{0},\mathtt{1}\} \\ \quad \text{return } c \\ \hline \end{array}$$

are interchangeable, thus proving a counterexample of the claim.