My Hybrid Proof

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

```
$\mathcal{L}_{\mathsf{L}}$
CTXT($m \in \{0,1\}$):
  $k \leftarrow \{0,1\}$
  $c := k \oplus m$
  return $c\&m$
```

$$\equiv$$

```
$\mathcal{L}_{\mathsf{R}}$
CTXT($m \in \{0,1\}$):
  $c \leftarrow \{0,1\}$
  return $c$
```

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

```
$\mathcal{A}$
$m := 0$
$c :=$ CTXT($m$)
return $m \overset{?}{=} 0$
```

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

```
$\mathcal{A}$
$m := 0$
$c :=$ CTXT($m$)
return $m \overset{?}{=} 0$
```

$$\diamond$$

```
$\mathcal{L}_{\mathsf{L}}$
CTXT($m \in \{0,1\}$):
  $k \leftarrow \{0,1\}$
  $c := k \oplus m$
  return $c\&m$
```

$$\implies \text{true}$$

and

```
$\mathcal{A}$
$m := 0$
$c :=$ CTXT($m$)
return $m \overset{?}{=} 0$
```

$$\diamond$$

```
$\mathcal{L}_{\mathsf{R}}$
CTXT($m \in \{0,1\}$):
  $c \leftarrow \{0,1\}$
  return $c$
```

$$\implies \frac{1}{2}$$

so we know that

```
$\mathcal{A}$
$m := 0$
$c :=$ CTXT($m$)
return $m \overset{?}{=} 0$
```

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

```
$\mathcal{L}_{\mathsf{L}}$
CTXT($m \in \{0,1\}$):
  $k \leftarrow \{0,1\}$
  $c := k \oplus m$
  return $c\&m$
```

and

```
$\mathcal{L}_{\mathsf{R}}$
CTXT($m \in \{0,1\}$):
  $c \leftarrow \{0,1\}$
  return $c$
```

are interchangeable, thus proving a counterexample of the claim.