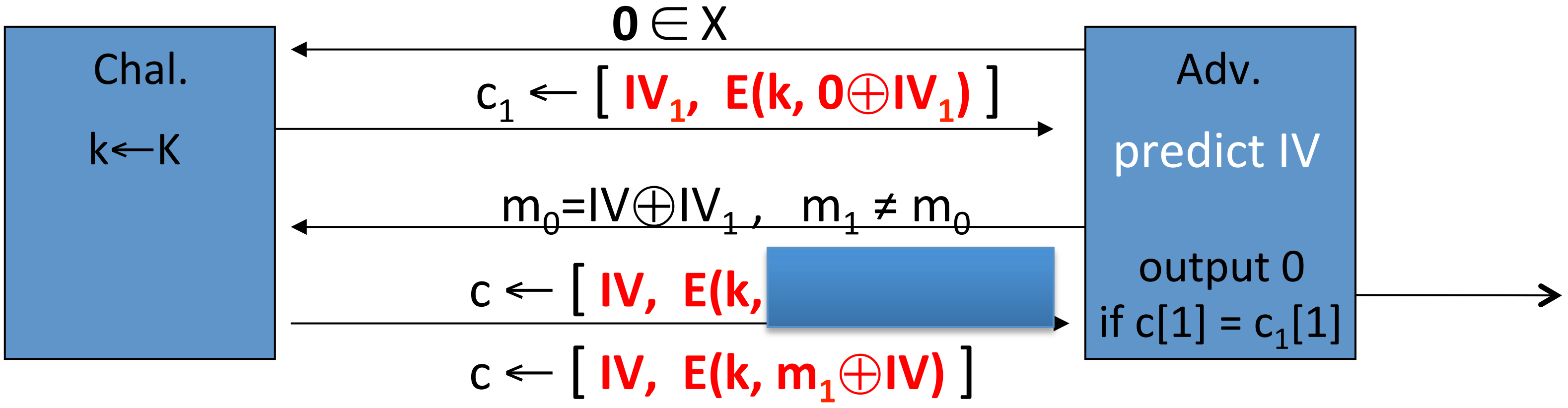
Suppose given $c \leftarrow E_{CBC}(k,m)$ can predict IV for next message



Chal.

$k \leftarrow K$

$\mathbf{0} \in X$

$c_1 \leftarrow [\ \mathbf{IV_1,\ E(k,\ 0 \oplus IV_1)}\ ]$

Adv.

predict IV

$m_0 = IV \oplus IV_1$, $m_1 \neq m_0$

$c \leftarrow [\ \mathbf{IV,\ E(k,}$ [redacted]

$c \leftarrow [\ \mathbf{IV,\ E(k,\ m_1 \oplus IV)}\ ]$

output 0
if $c[1] = c_1[1]$