

Challenger

Adversary

$$k \xleftarrow{R} K, b \xleftarrow{R} \{0, 1\}$$

$$c^{(1)} = E(k, m_b^{(1)})$$

\vdots

$$c^{(n)} = E(k, m_b^{(n)})$$

$$m_0^{(1)}, m_1^{(1)}$$

$$c^{(1)}$$

\vdots

$$m_0^{(n)}, m_1^{(n)}$$

$$c^{(n)}$$

Choose $m_0^{(1)}, m_1^{(1)}$

\vdots

Choose $m_0^{(n)}, m_1^{(n)}$

Guess b as b'

b'