Semantic Security
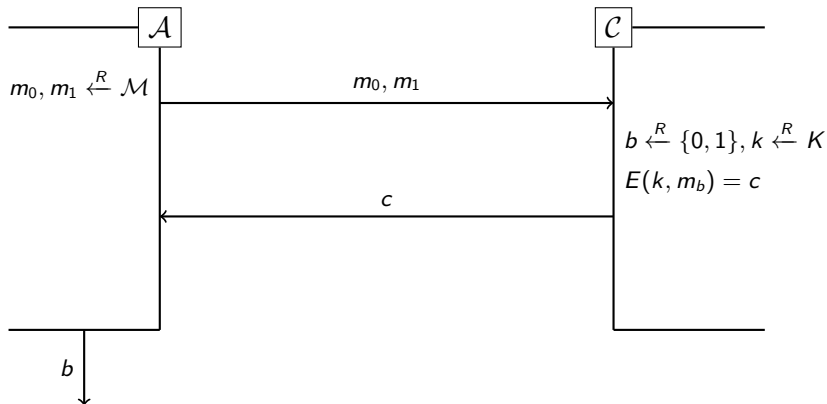
Rohit Musti

CUNY - Hunter College

February 18, 2022

One Time Pad Security Game: Semantic Security

$\mathcal{A}$

$\mathcal{C}$

$m_0, m_1 \xleftarrow{R} \mathcal{M}$

m_0, m_1

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

$E(k, m_b) = c$

c

b

Semantic Security: Message Recovery Game

$\mathcal{B}$

$m_0, m_1 \xleftarrow{R} \mathcal{M}$

$\mathcal{C}$

m_0, m_1

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

$E(k, m_b) = c$

c

$\mathcal{A}$

c

m'

$b = (m' == m_1)$