Semantic Security

Rohit Musti

CUNY - Hunter College

February 18, 2022

PRG Security Game

$\boxed{\mathcal{A}}$

$\boxed{\mathcal{C}}$

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

if $b == 0$: $k \xleftarrow{R} K$, return k

if $b == 1$: $s \xleftarrow{R} S$, return $G(s)$

c

b