Gauge Hartwell

6 February, 2021

CS427

Homework 9

1. Libraries:

$\mathcal{L}^{\Sigma}_{\text{cca-L}}$

$k_1 \leftarrow \Sigma_1.KeyGen$
$k_2 \leftarrow \Sigma_2.KeyGen$
$S := \emptyset$

$\underline{EAVESDROP(m_L, m_R)}$
  if $|m_L| \neq |m_R|$
    return err
  $c_1 := \Sigma_1.Enc(k_1, m_L)$
  $c_2 := \Sigma_2.Enc(k_2, m_L)$
  $S := S \cup \{(c_1, c_2)\}$
  return (c_1, c_2)

$\underline{DEC((c_1, c_2))}$
  if $(c_1, c_2) \in S$
    return err
  $m_1 := \Sigma_1.Dec(k_1, c_1)$
  $m_2 := \Sigma_2.Dec(k_2, c_2)$
  if $(m_1 == m_2)$
    return m_1
  else return err

$\mathcal{L}^{\Sigma}_{\text{cca-R}}$

$k_1 \leftarrow \Sigma_1.KeyGen$
$k_2 \leftarrow \Sigma_2.KeyGen$
$S := \emptyset$

$\underline{EAVESDROP(m_L, m_R)}$
  if $|m_L| \neq |m_R|$
    return err
  $c_1 := \Sigma_1.Enc(k_1, m_R)$
  $c_2 := \Sigma_2.Enc(k_2, m_R)$
  $S := S \cup \{(c_1, c_2)\}$
  return (c_1, c_2)

$\underline{DEC((c_1, c_2))}$
  if $(c_1, c_2) \in S$
    return err
  $m_1 := \Sigma_1.Dec(k_1, c_1)$
  $m_2 := \Sigma_2.Dec(k_2, c_2)$
  if $(m_1 == m_2)$
    return m_1
  else return err

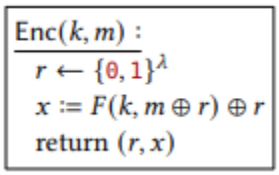
Calling Program:

A

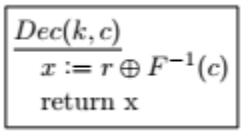
choose $m \neq m', t \neq 0^{\lambda}$
$x, y := EAVESDROP(m, m')$
$\hat{m} := DEC(x \oplus t, y)$
if $(\hat{m} == x \oplus t)$:
  return 1
else return 0

Pr[A ◊ cca-L = 1] = 1
Pr[A ◊ cca-R = 1] = 0
Advantage: 1 – 0 = 1

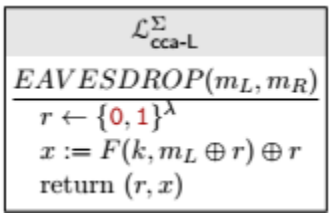
2. Encryption:

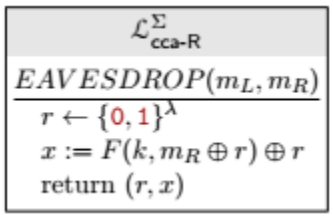


Decryption:

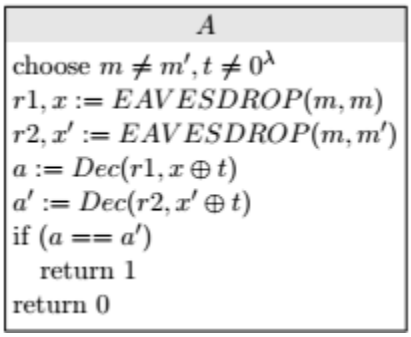


Libraries:





Calling Program:



Pr[A ◊ cca-L = 1] = 1

Pr[A ◊ cca-R = 1] = 0

Advantage: 1 – 0 = 1