Gauge Hartwell

19 February, 2021

CS427

Homework 11

1. Libraries:

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

$S := \emptyset$
$k \leftarrow \{0,1\}^{\lambda}$

$\underline{EAVESDROP(k, m_{L1}||...||m_{Li}, m_{R1}||...||m_{Ri}) :}$
  $r \leftarrow \{0,1\}^{\lambda}$
  $c_0 := r$
  for $i = 1$ to ℓ:
    $c_i := F(k,r) \oplus m_{Li}$
    $r := r + 1 \% 2^{blen}$
  $S := S \cup ((c_0||...||c_{\ell}))$
  return $c_0||...||c_{\ell}$

$\underline{Dec(k, c_0||...||c_{\ell})}$
  if $(c_0||...||c_{\ell}) \in S$
    return err
  $r := c_0$
  for $i = 1$ to ℓ:
    $m_i := F(k,r) \oplus c_i$
    $r := r + 1 \% 2^{blen}$
  if $m_{\ell} \neq H(m_1||...||m_{\ell-1})$
    return err
  return $m_1||...||m_{\ell-1}$

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

$S := \emptyset$
$k \leftarrow \{0,1\}^{\lambda}$

$\underline{EAVESDROP(k, m_{L1}||...||m_{Li}, m_{R1}||...||m_{Ri}) :}$
  $r \leftarrow \{0,1\}^{\lambda}$
  $c_0 := r$
  for $i = 1$ to ℓ:
    $c_i := F(k,r) \oplus m_{Ri}$
    $r := r + 1 \% 2^{blen}$
  $S := S \cup ((c_0||...||c_{\ell}))$
  return $c_0||...||c_{\ell}$

$\underline{Dec(k, c_0||...||c_{\ell})}$
  if $(c_0||...||c_{\ell}) \in S$
    return err
  $r := c_0$
  for $i = 1$ to ℓ:
    $m_i := F(k,r) \oplus c_i$
    $r := r + 1 \% 2^{blen}$
  if $m_{\ell} \neq H(m_1||...||m_{\ell-1})$
    return err
  return $m_1||...||m_{\ell-1}$

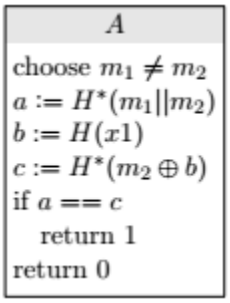
Calling Program:

A

choose $m \neq m'$
$x||y||z||w := EAVESDROP(m||H(m)||m', m'||H(m')||m$
$a := Dec(k, x||y||z)$
if $a \neq m$
  return 1
return 0

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

2.


A
choose $m_1 \neq m_2$
$a := H^*(m_1||m_2)$
$b := H(x1)$
$c := H^*(m_2 \oplus b)$
if $a == c$
return 1
return 0