Gauge Hartwell

17 February, 2021

CS427

Homework 10

1. Libraries:

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

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

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

$\underline{Dec((c_0||...||c_j)) :}$
  if $(c_0||...||c_j) \in S$:
    return err
  for i = 1 to ℓ:
    $m_i := F(k, c_0) \oplus c_i$
    $c_0 := (c_0 + 1)\%2^{blen}$
  $y := y(m_i||...||m_{L1})$
  if $y \neq m_i$:
    return err
  return $(m_i||...||m_{i-1})$

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

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

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

$\underline{Dec((c_0||...||c_j)) :}$
  if $(c_0||...||c_j) \in S$:
    return err
  for i = 1 to ℓ:
    $m_i := F(k, c_0) \oplus c_i$
    $c_0 := (c_0 + 1)\%2^{blen}$
  $y := y(m_i||...||m_{L1})$
  if $y \neq m_i$:
    return err
  return $(m_i||...||m_{i-1})$

Calling program:

A

choose $m \neq m'$
$r||x||t := EAVESDROP(m, m)$
$r'||x'||t' := EAVESDROP(m, m')$
$w||y||z := Dec(r||x||t)$
$a||b||c := Dec(r'||x'||t')$
if $(z \neq c)$:
  return 1
return 0

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

2. Libraries

$\mathcal{L}^{\Sigma}_{\text{mac-real}}$

$k \leftarrow \Sigma.KeyGen$

$\underline{GetTag(m \in \Sigma.\mathcal{M}):}$
$c_0 := 0^{\lambda}$
$t := 0^{\lambda}$
for $i = 1$ to ℓ:
$t := t \oplus (F(k, m_i \oplus c_{i-1}))$
return t

$\underline{CheckTag(m \in \Sigma.\mathcal{M}, t):}$
for $i = 1$ to ℓ:
if $(t == t \oplus (F(k, m_i \oplus c_{i-1})):$
return 1
return 0

$\mathcal{L}^{\Sigma}_{\text{mac-fake}}$

$k \leftarrow \Sigma.KeyGen$
$T := \emptyset$

$\underline{GetTag(m \in \Sigma.\mathcal{M}):}$
$c_0 := 0^{\lambda}$
$t := 0^{\lambda}$
for $i = 1$ to ℓ:
$t := t \oplus (F(k, m_i \oplus c_{i-1}))$
$T := T \cup \{(m, t)\}$
return t

$\underline{CheckTag(m \in \Sigma.\mathcal{M}, t):}$
if $((m, t) \in T):$
return 1
return 0

Calling program:

A

choose $m_1 || m_2 \leftarrow \{0,1\}^{2\lambda}$
$x := GetTag(m_1 || m_2)$
$z := GetTag(m_1)$
if $(CheckTag(m_1 || m_2 || m_2 \oplus x, z) == 1)$
return 1
return 0

Pr[A ◊ mac-real = 1] = 1
Pr[A ◊ mac-fake = 1] = 0
Advantage: 1-0 =1, non-negligible