Gauge Hartwell

12 January, 2021

CS427

Homework 3

1. We will show that tsss-L is equivalent to tsss-R for a 3-out-of-3 scheme with a hybrid proof.

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

$\underline{\text{SHARE}(m_L, m_R, U)\text{:}}$
$\quad if|U| \leq 3 : \text{return } err$
$\quad s_1 \leftarrow \{0,1\}^\ell$
$\quad s_2 \leftarrow \{0,1\}^\ell$
$\quad s_3 := s_1 \oplus s_2 \oplus m_L$
$\quad \text{return } \{s_i | i \in U\}$

$\underline{\text{RECONSTRUCT}(s_1, s_2, s_3)\text{:}}$
$\quad \text{return } \{s_1 \oplus s_2 \oplus s_3\}$

Starting with tsss-L showing our 3-out-of-3 scheme.

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

$\underline{\text{SHARE}(m_L, m_R, U)\text{:}}$
$\quad \text{if } |U| \leq 3 : \text{return } err$
$\quad \text{if } U = \{1\} :$
$\qquad s_1 \leftarrow \{0,1\}^\ell$
$\qquad s_2 \leftarrow \{0,1\}^\ell$
$\qquad s_3 := s_1 \oplus s_2 \oplus m_L$
$\qquad \text{return } \{s_1\}$
$\quad \text{elif } U = \{2\} :$
$\qquad s_1 \leftarrow \{0,1\}^\ell$
$\qquad s_2 \leftarrow \{0,1\}^\ell$
$\qquad s_3 := s_1 \oplus s_2 \oplus m_L$
$\qquad \text{return } \{s_2\}$
$\quad \text{elif } U = \{3\} :$
$\qquad s_1 \leftarrow \{0,1\}^\ell$
$\qquad s_2 \leftarrow \{0,1\}^\ell$
$\qquad s_3 := s_1 \oplus s_2 \oplus m_L$
$\qquad \text{return } \{s_3\}$
$\quad \text{elif } U = \{1,2\}$
$\qquad s_1 \leftarrow \{0,1\}^\ell$
$\qquad s_2 \leftarrow \{0,1\}^\ell$
$\qquad s_3 := s_1 \oplus s_2 \oplus m_L$
$\qquad \text{return } \{s_1, s_2\}$
$\quad \text{elif } U = \{1,3\}$
$\qquad s_1 \leftarrow \{0,1\}^\ell$
$\qquad s_2 \leftarrow \{0,1\}^\ell$
$\qquad s_3 := s_1 \oplus s_2 \oplus m_L$
$\qquad \text{return } \{s_1, s_3\}$
$\quad \text{elif } U = \{2,3\}$
$\qquad s_1 \leftarrow \{0,1\}^\ell$
$\qquad s_2 \leftarrow \{0,1\}^\ell$
$\qquad s_3 := s_1 \oplus s_2 \oplus m_L$
$\qquad \text{return } \{s_2, s_3\}$
$\quad \text{else return } \theta$

Next, we will duplicate the main body into separate branches of a new if-statement. The scheme will now generate s_1, s_2, and s_3 differently and separately. This has no effect on how the library operates.

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

$\underline{\text{SHARE}(m_L, m_R, U)\text{:}}$

  if $|U| \leq 3$: return err
  if $U = \{1\}$:
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus s_2 \oplus m_R$
    return $\{s_1\}$
  elif $U = \{2\}$:
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus s_2 \oplus m_R$
    return $\{s_2\}$
  elif $U = \{3\}$:
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus EAVESDROP(m_L, m_R)$
    return $\{s_3\}$
  elif $U = \{1,2\}$
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus s_2 \oplus m_R$
    return $\{s_1, s_2\}$
  elif $U = \{1,3\}$
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus EAVESDROP(m_L, m_R)$
    return $\{s_1, s_3\}$
  elif $U = \{2,3\}$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus EAVESDROP(m_L, m_R)$
    return $\{s_2, s_3\}$
  else return θ

$\diamond$

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

$\underline{\text{EAVESDROP}(m_L, m_R)\text{:}}$

  $k \leftarrow \{0,1\}^\ell$
  $c := k \oplus m_L$
  return c

The definition of S_2 has been factored into EAVESDROP and inlined to the definition of s_3 in the branches that have s_3 in their return statements, and s_3 has been changed to use mR in the statements that don't use s_3. This has no effect on the operation of the library.

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

$\underline{\text{SHARE}(m_L, m_R, U)\text{:}}$

if $|U| \leq 3$: return err
if $U = \{1\}$:
  $s_1 \leftarrow \{0,1\}^\ell$
  $s_2 \leftarrow \{0,1\}^\ell$
  $s_3 := s_1 \oplus s_2 \oplus m_R$
  return $\{s_1\}$
elif $U = \{2\}$:
  $s_1 \leftarrow \{0,1\}^\ell$
  $s_2 \leftarrow \{0,1\}^\ell$
  $s_3 := s_1 \oplus s_2 \oplus m_R$
  return $\{s_2\}$
elif $U = \{3\}$:
  $s_1 \leftarrow \{0,1\}^\ell$
  $s_3 := s_1 \oplus EAVESDROP(m_L, m_R)$
  return $\{s_3\}$
elif $U = \{1,2\}$
  $s_1 \leftarrow \{0,1\}^\ell$
  $s_2 \leftarrow \{0,1\}^\ell$
  $s_3 := s_1 \oplus s_2 \oplus m_R$
  return $\{s_1, s_2\}$
elif $U = \{1,3\}$
  $s_1 \leftarrow \{0,1\}^\ell$
  $s_3 := s_1 \oplus EAVESDROP(m_L, m_R)$
  return $\{s_1, s_3\}$
elif $U = \{2,3\}$
  $s_2 \leftarrow \{0,1\}^\ell$
  $s_3 := s_1 \oplus EAVESDROP(m_L, m_R)$
  return $\{s_2, s_3\}$
else return θ

$\diamond$

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

$\underline{\text{EAVESDROP}(m_L, m_R)\text{:}}$

  $k \leftarrow \{0,1\}^\ell$
  $c := k \oplus m_R$
  return c

Next, we can swap ots-L for ots-R. This changes nothing about the operation of the library.

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

SHARE(m_L, m_R, U):
  if $|U| \leq 3$: return err
  if $U = \{1\}$:
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus s_2 \oplus m_R$
    return $\{s_1\}$
  elif $U = \{2\}$:
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus s_2 \oplus m_R$
    return $\{s_2\}$
  elif $U = \{3\}$:
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus s_2 \oplus m_R$
    return $\{s_3\}$
  elif $U = \{1,2\}$
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus s_2 \oplus m_R$
    return $\{s_1, s_2\}$
  elif $U = \{1,3\}$
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus s_2 \oplus m_R$
    return $\{s_1, s_3\}$
  elif $U = \{2,3\}$
    $s_1 \leftarrow \{0,1\}^\ell$
    $s_2 \leftarrow \{0,1\}^\ell$
    $s_3 := s_1 \oplus s_2 \oplus m_R$
    return $\{s_2, s_3\}$
  else return θ

The subroutine is inlined, changing nothing about how the library functions.

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

SHARE(m_L, m_R, U):
  $if |U| \leq 3$: return err
  $s_1 \leftarrow \{0,1\}^\ell$
  $s_2 \leftarrow \{0,1\}^\ell$
  $s_3 := s_1 \oplus s_2 \oplus m_R$
  return $\{s_i | i \in U\}$

Finally, the library can be simplified. The branches of the if-statement have been condensed and the library does not function any differently.

We showed that tsss-L is equivalent to hyb-1, which is equivalent to… hyb-4, which is equivalent to tsss-R, so this secret-sharing scheme is secure.

2. $X_1 = 4$, $y_1 = 6$
   $x_2 = 7$, $y_2 = 1$

   $L_1 = (x-7/(4-7)$, $L_2 = (x-4)/(7-4)$

   f(x) = (6((x-7)/(4-7)) + 1((x-4)/(7-4))) % 11
   = -5/3*x + 38/3
   = 2x + 9

   Secret is 9

   Other shares:
   f(1) = (2(1) + 9) % 11 = 0
   f(2) = (2(2) + 9) % 11 = 2
   f(3) = (2(3) + 9) % 11 = 4
   f(4) = (2(4) + 9) % 11 = 6
   f(5) = (2(5) + 9) % 11 = 8
   f(6) = (2(6) + 9) % 11 = 10
   f(7) = (2(7) + 9) % 11 = 1
   f(8) = (2(8) + 9) % 11 = 3
   f(9) = (2(9) + 9) % 11 = 5
   f(10) = (2(10) + 9) % 11 = 7