Gauge Hartwell

1 February, 2021

CS427

Homework 7

1. A)

$Dec(k, m)$
$r \leftarrow \{0,1\}^{\lambda}$
$m := F(k, c \| r)$
return m

b) To show that the scheme has CPA$ security, we will start with the cpa-L library.

$\mathcal{L}_{\text{cpa-L}}$
$k \leftarrow KeyGen$

$EAVESDROP(m_L, m_R)$
$c := Enc(k, m_L)$
return c

First, we will factor out the call to Enc() into a subroutine, changing nothing about the operation of the library.

$EAVESDROP(m_L, m_R)$
$c := CTXT(m_L)$
return c
$\diamond$
$\mathcal{L}_{\text{cpa-real}}$
$k \leftarrow KeyGen$

$CTXT(m)$
$c := Enc(k, m)$
return c

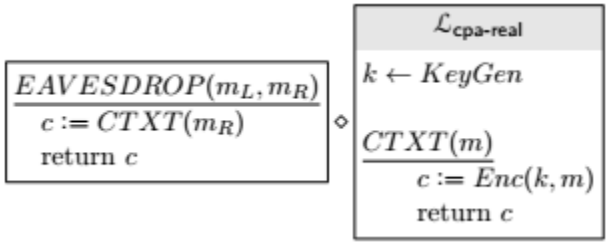
Second, we will replace cpa-real with cpa-rand. This change should be indistinguishable.

$EAVESDROP(m_L, m_R)$
$c := CTXT(m_L)$
return c
$\diamond$
$\mathcal{L}_{\text{cpa-rand}}$
$CTXT(m)$
$c := C$
return c

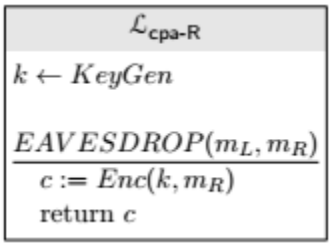
Next, we will change the argument that is passed into CTXT. This won't affect the operation of the library.

$EAVESDROP(m_L, m_R)$
$c := CTXT(m_R)$
return c
$\diamond$
$\mathcal{L}_{\text{cpa-rand}}$
$CTXT(m)$
$c := C$
return c

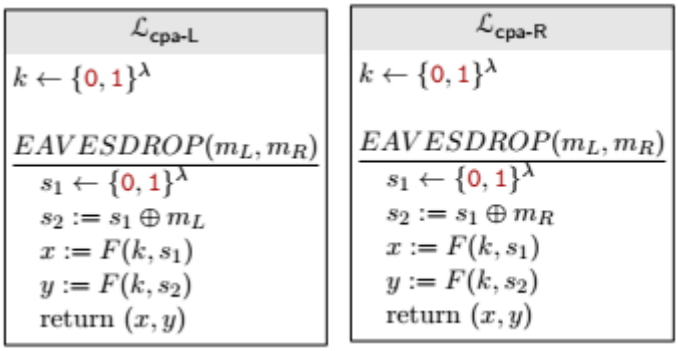
Now we can change cpa-rand back to cpa-real.



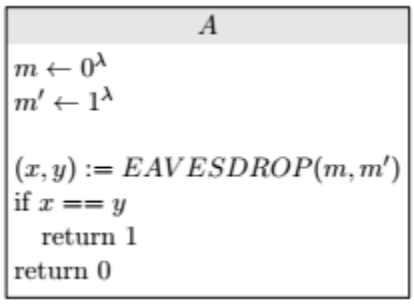
And finally, we can inline the cpa library.



2. Libraries:



Calling program:



Pr[A ◊ cpa-L = 1] = 1

Pr[A ◊ cpa-R = 1] = 0

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