

1.

As a formal attack A :

```

(C1, C2) := EAV(0λ, 1λ)
choose arbitrary x ≠ 0λ
(C', C2') := EAV(0λ, 0λ).
m = DEC((k1, k2), (C1, C2')).
if m = 0λ return 1
else return 0.
    
```

So, in this attack.

$$\Pr[A \circ \mathcal{L}_{cca-L} = 1] = 1$$

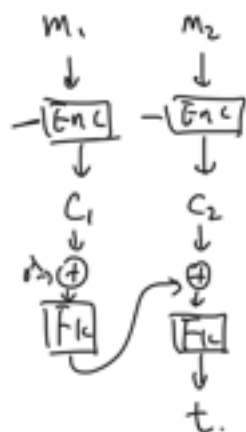
$$\Pr[A \circ \mathcal{L}_{cca-R} = 1] = 0$$

As we can see.

The possibilities of two attacks are distinguishable.

So, this security scheme does not under CCA-Secure.

2. Enc-then-DEC.



$\text{Enc}(k, k), m$:

```

(r, c) ← G.Enc(k, m)
t := M.MAC(k, c)
return (r, c, t)
    
```

```

DEC((k, k), (c, t)):
if t ≠ M.MAC(k, c):
return err
return E.DEC(k, c).
    
```

KeyGen:
 $k \leftarrow \mathcal{K}$
return k
Enc(k, m):

CBC-MAC^F(k, m₁ || m₂):

```

t := 0λ
t := Fk(m1 || t)
    
```

$r \leftarrow \{0,1\}^\lambda$
 $x := F(k, r) \oplus m$
 return (r, x) .
DEC(k, (r, x)):
 $m := F(k, r) \oplus x$
 return m

$t := F(k, m_1)$
 $= F(k, m_2 \oplus t)$
 $= F(k, m_2 \oplus F(k, m_1))$
 return t

Make an Attack A :

$(C_1, t_1) = \text{EAV}(0^\lambda, 1^\lambda)$
 $(C_2, t_2) = \text{EAV}(0^\lambda, 1^\lambda)$
 $m_1 || m_2 = \text{DEC}(C_1 || t_1 \oplus C_2, t_2)$
 if $m_1 = 0^\lambda$ return true.
 else return false

$\Pr[A \diamond \mathcal{L}_{\text{cca-L}} = \text{true}]$ and

$\Pr[A \diamond \mathcal{L}_{\text{cca-R}} = \text{true}]$

is Distinguishable,

So, this algorithm is not under security.

3. $H(k, m_1 || m_2 || m_3)$:
 $C_1 := F(k, m_1)$
 $C_2 := F(k, m_2 \oplus C_1)$
 $C_3 := F(k, m_3 \oplus C_2)$
 return C_3

$\mathcal{L}_{\text{cr-real}}$

$S \leftarrow \{0,1\}^\lambda$

$\mathcal{L}_{\text{cr-fake}}$

$S \leftarrow \{0,1\}^\lambda$

Return $S || t$:

GetSalt():

return s

TEST($x, x' \in \{0,1\}^*$):

if $x \neq x'$ and $H(s, x) = H(s, x')$ return true
return false

GetSalt():

return s

TEST($x, x' \in \{0,1\}^*$):

return false

Since for this hash function,
we know the public key k for F in PRP.

So, we construct an Attack A :

A

$a \leftarrow \{0,1\}^\lambda$

$b \leftarrow \{0,1\}^\lambda$

$k \leftarrow \text{arbitrary}$

$m_1 || m_2 || m_3 := a || F(k, a) || F(k, 0^\lambda)$

$m_1' || m_2' || m_3' := b || F(k, b) || F(k, 0^\lambda)$

if (TEST($m_1 || m_2 || m_3, m_1' || m_2' || m_3'$) == true)
return 1

else
return 0

$H(s, m_1 || m_2 || m_3):$

$C_1 = F(k, m_1)$

$C_2 = F(k, m_2 \oplus F(k, m_1))$
 $= F(k, 0^\lambda)$

$C_3 = F(k, m_3 \oplus F(k, 0^\lambda))$
 $= F(k, 0^\lambda)$

$H(s, m_1' || m_2' || m_3')::$

$C_1' = F(k, m_1')$

$C_2' = F(k, m_2' \oplus F(k, m_1'))$
 $= F(k, 0^\lambda)$

$C_3' = F(k, m_3' \oplus F(k, 0^\lambda))$
 $= F(k, 0^\lambda)$

So, $C_3 = C_3'$ for different a and b .

Which $\Pr[A \circ \mathcal{L}_{\text{cr-real}}^H \circ H = 1] = 1.$

$\Pr[A \circ \mathcal{L}_{\text{cr-fake}}^H \circ H = 1] = 1/2^\lambda$

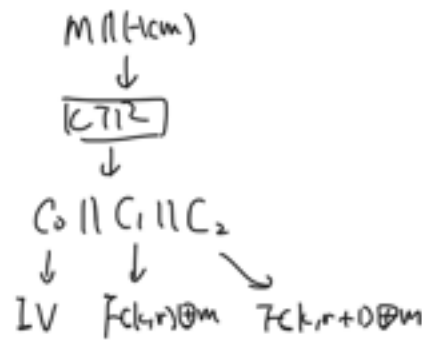
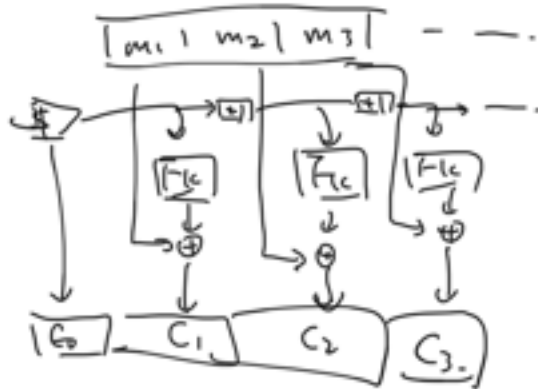
This Hash function does not have collision resistance

When the message looks like the structure

$m || F(k, m_1) || F(k, 0^\lambda)$ for arbitrary msg m_1

4. CTR($k, m, 1 \dots |m|$):

$r \leftarrow \$$
 $c_0 := r$
 for $i = 1 \dots t$.
 $c_i := F(k, r) \oplus m_i$
 $r := r + 1 \pmod{2^{\text{block}}}$
 return $c_0 || \dots || c_t$.



Since the Hash function is a plain hash.

A:

$C_0 || C_1 || C_2 := \text{EAV}(0^\lambda, 0^{\lambda-1} || 1).$

$C'_0 || C'_1 || C'_2 := \text{EAV}(0^{\lambda-1} || 1, 0^\lambda).$

$m := \text{DEC}(C_0 || C'_1 || C'_2).$

2f $t = m_L$ return 1

$t = m_R$ return 0.

$\Pr[A \circ \mathcal{L}_{\text{cca-L}} = 1] = 1$

$\Pr[A \circ \mathcal{L}_{\text{cca-R}} = 0] = 0 \rightarrow$ because all forms not look like $m || H(m)$ will be err.

So these two libraries are distinguishable.

So, this secure scheme does not under cca security.