

1.

As a formal attack A :

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

choose arbitrary $x \neq 0^\lambda$

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

$$m = \text{DEC}((k_1, k_2), (C_1, C'_2)).$$

if $m = 0^\lambda$ return 1

else return 0.

So, in this attack,

$$\Pr[A \diamond \text{Lcca-L}] = 1$$

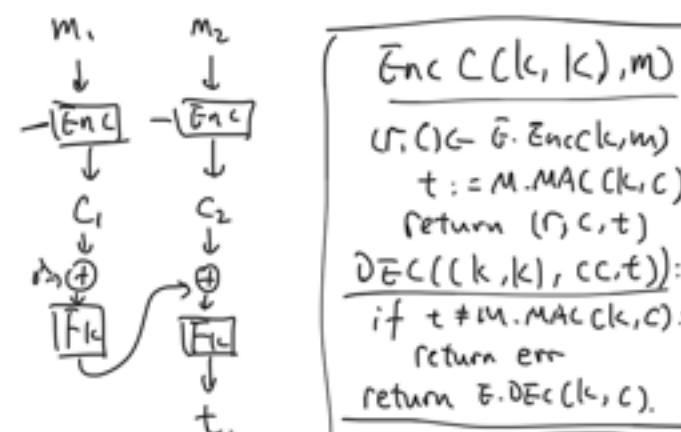
$$\Pr[A \diamond \text{Lcca-R}] = 0$$

As we can see,

The possibilities of two attacks are distinguishable.

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

2. Enc-then-DEC -



KeyGen:
 $k \leftarrow \mathbb{G} \leftarrow 1^\lambda$
 return k

Enc(k, m):

Enc($C(k, k), m$):

$(r, c) \leftarrow G \cdot \text{Enc}(k, m)$

$t := M \cdot \text{MAC}(k, c)$

return (r, c, t)

DEC($(k, k), cc, t$):

if $t \neq M \cdot \text{MAC}(k, c)$:

return err

return $E \cdot \text{DEC}(k, c)$.

CBC-MAC^F($k, m_1 || m_2$):

$t := 0^\lambda$

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

\vdots

$P \leftarrow S_0, 1^{\lambda}$	$= F(k, m_1)$
$x := F(k, r) \oplus M$	$t := F(k, m_2 \oplus t)$
return (r, x) .	$= F(k, m_2 \oplus F(k, m_1))$
$\text{DEC}(k, (r, x)) :=$	return t
$m := F(k, r) \oplus x$	
return m	

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

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

$\Pr[A \diamond L_{\text{cca-R}} = \text{true}]$

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

$L_{\text{or-real}}$

$S \subseteq S_0, 1^{\lambda}$

$L_{\text{cr-false}}$

$S \subseteq S_0, 1^{\lambda}$

Get s.t.:

GetSalt():
 returns

TEST(x, x ∈ {0,1}^*):

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

TEST(x, x ∈ {0,1}^*):
 returns

TEST(x, x ∈ {0,1}^*):

 return false

Since for this hash function,
we know the public key k for FinPRP.

So, we construct an Attack A:

A

$a \leftarrow s_0, \{0,1\}^\lambda$

$b \leftarrow s_0, \{0,1\}^\lambda$

$k \leftarrow \text{arbitrary}$

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

$m'_1 || m'_2 || m'_3 := b || F(k, b) || F(k, 0^\lambda)$

if ($\text{TEST}(m_1 || m_2 || m_3, m'_1 || m'_2 || m'_3) == \text{true}$)
 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 $\Pr[A \odot \mathbb{1}_{\text{cr-real}}^H \odot H = 1] = 1$.

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

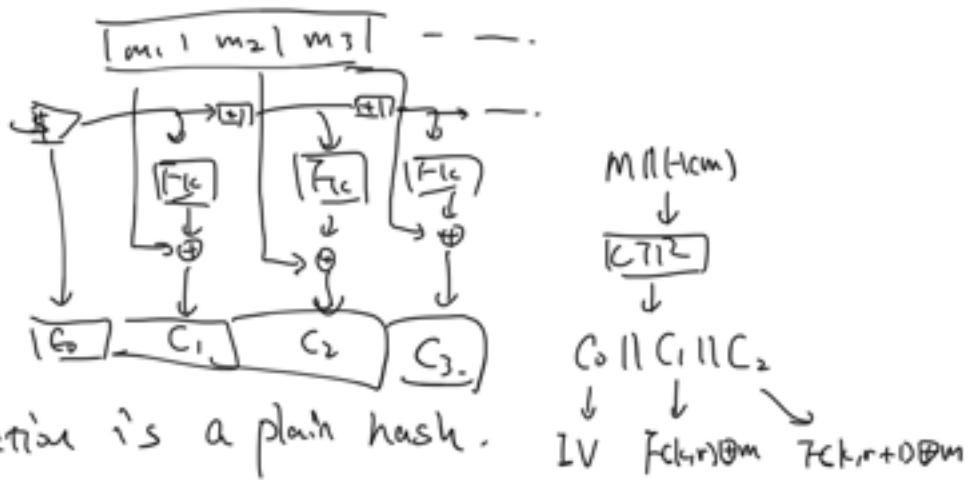
This Hash function does not have collision resistance

when the message looks like the structure

$m_1 || F_{k,m_1} || F_{k,0^\lambda}$, for arbitrary msg m_1

4. CTR($k, m_1 \dots m_L$):

```
r ← $  
c₀ := r  
for i = 1 to L:  
    cᵢ := Fₖ(r) ⊕ mᵢ  
    r := r + 1 % 2^{λm}  
return c₀ || ... || c_L.
```



Since the Hash function is a plain hash.

A:

```
C₀||C₁||C₂ := EAV(0^λ, 0^{λ-1}||1).  
(₀||C₁'||C₂') := EAV(0^{λ-1}||1, 0^λ).  
m := DEC(C₀||C₁'||C₂').  
If t = M_L return 1  
t = M_R return 0.
```

$\Pr[A \odot \mathbb{1}_{\text{cc-a}} = 1] = 1$

$\Pr[A \odot \mathbb{1}_{\text{cc-R}} = 0] = 0 \rightarrow$ because all form not look like $m||H(m)$ will be err.

So these two libraries are distinguishable.

∴ this secure scheme does not under CCA security.