Introduction to Modern Cryptography
Theresa, Celine, Prisca, Saibaba
December 5, 2022

Solution of Exercisesheet 7

Exercise 7-1

This modified encryption does not achieve CPA security. Here $H(m)$ will not be random for every encryption because Hash is calculated only based on message. As an Adversary against CPA has access to encryption oracle, Adversary can atleast distuinguish correspoding cipher to a message just by comparing the appended $H(m)$ part in the cipher. Hence this new modified encryption doesnt have indistingushable enryptions and so not CPA secure.

Exercise 7-2

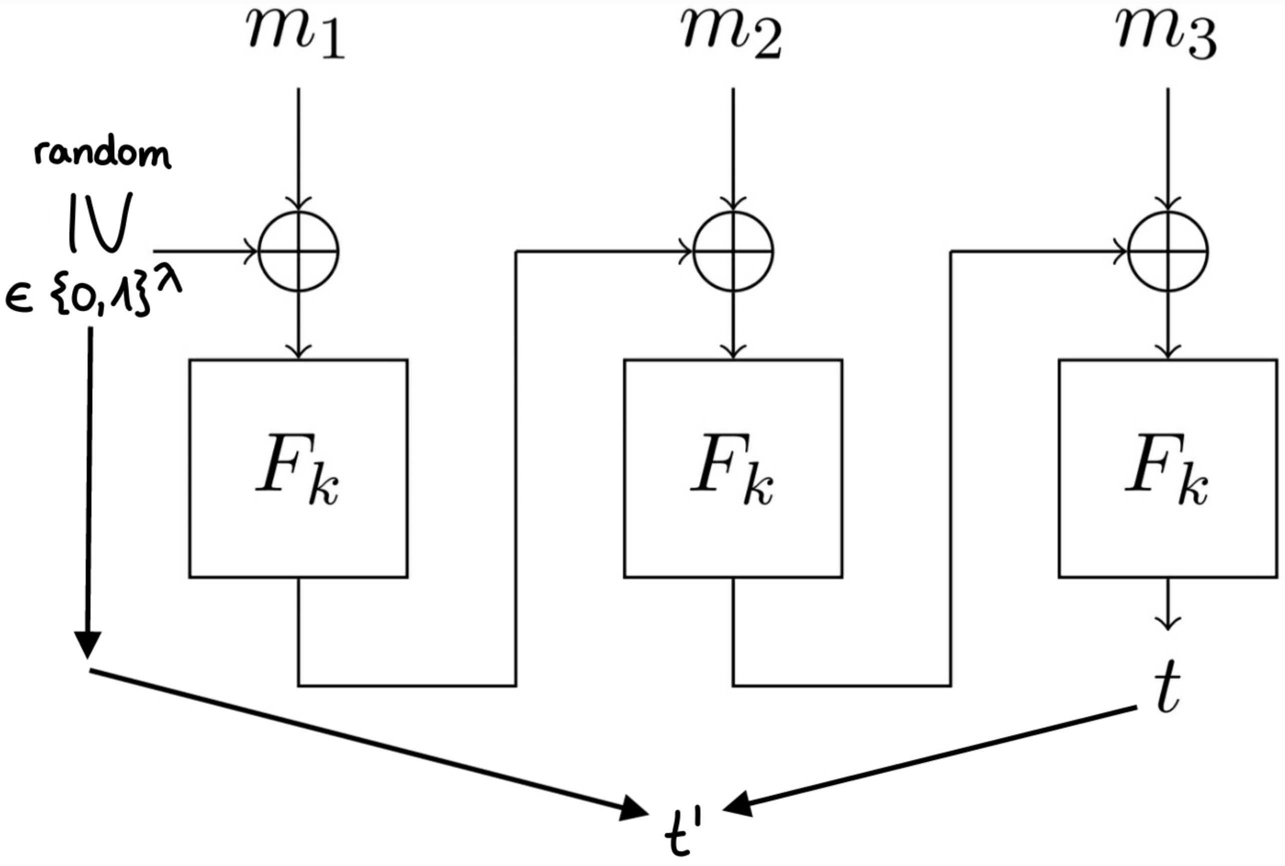
a not secure:
The adversary $\mathcal{A}$ makes two queries to the oracle:
$m^1 = m_1||m_2 \Rightarrow t^1 = t_1^1||t_2^1 = F(K, m_1)||F(K, F(K, m_2))$
$m^2 = F(K, m_1)||m_2 \Rightarrow t^2 = t_1^2||t_2^2 = F(K, F(K, m_1))||F(K, F(K, m_2))$
Then he knows the tag for the message $m^* = m_1||m_1$ which is $t^* = F(K, m1)||F(K, F(K, m1)) = t_1^1||t_1^2$. Because $m^* \neq m^1$ and $m^* \neq m^2$, (m^*, t^*) is a valid attack.

b not secure:
The adversary $\mathcal{A}$ makes one query to the oracle:
$m^1 = m_1||m_2 \Rightarrow t^1 = F(K, m_1) \oplus F(K, m_2)$
Then he knows the tag for the message $m^* = m_2||m_1$ which is $t^* = F(K, m_2) \oplus F(K, m_1) = F(K, m_1) \oplus F(K, m_2) = t^1$. Because $m^* \neq m^1$, (m^*, t^*) is a valid attack.

c not secure:
The adversary $\mathcal{A}$ makes one query to the oracle:
$m^1 = m_1||m_2 \Rightarrow t^1 = (r \oplus (F(K, m_1) \oplus F(K, m_2)), r)$
Then he knows the tag for the message $m^* = m_2||m_1$ which is $t^* = (r \oplus (F(K, m_2) \oplus F(K, m_1)), r) = (r \oplus (F(K, m_1) \oplus F(K, m_2)), r) = t^1$. Because $m^* \neq m^1$, (m^*, t^*) is a valid attack.

Solution of Exercisesheet 7

Exercise 7-3



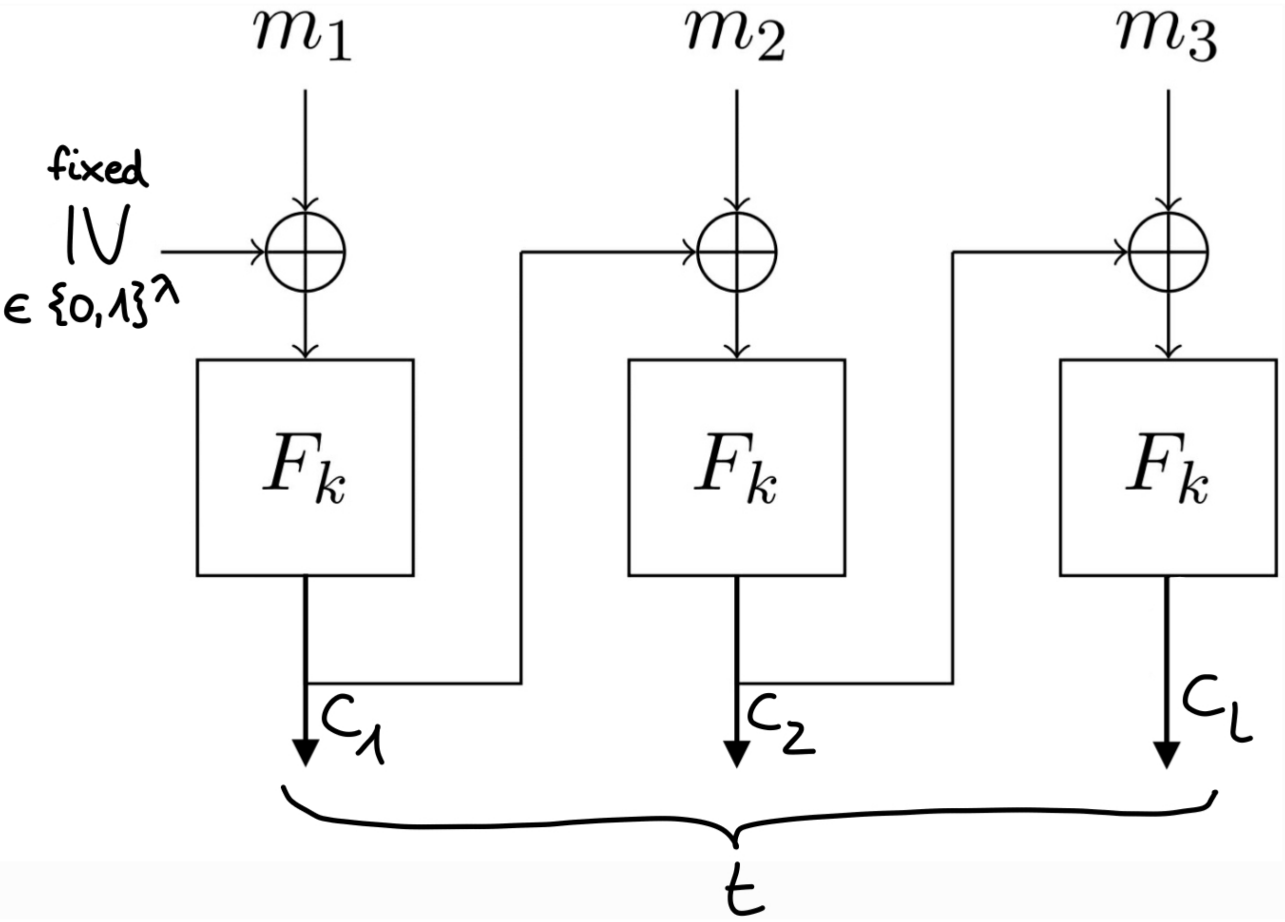
(a) The adversary $\mathcal{A}$ can choose the message m* of length $\ell(\lambda) \cdot \lambda$. We set $\ell(\lambda) =$ l
m* = m$_1^*$ || ... || m$_l^*$. We set m$_i^*$ = 0^λ.
We query m* to our Mac$_k(\cdot)$ oracle and recieve the tag t$^{*‘}$ = (IV*, t*). IV$^* \in \{0,1\}^\lambda$ is a randomly generated vector

c$_1^*$ = F$_k$(IV* $\oplus$ m$_1^*$) = F$_k$(IV* $\oplus$ 0^λ) = F$_k$(IV*)
c$_2^*$ = F$_k$(c$_1^*$ $\oplus$ m$_2^*$) = F$_k$(F$_k$(IV*) $\oplus$ 0^λ) = F$_k$(F$_k$(IV*))
...
c$_l^*$ = F$_k$(... F$_k$(IV*) ...) = t*

To break the security of the MAC the adversary $\mathcal{A}$ can construct the following forgery:
m = $0^{\lambda-1}1$ || m$_2^*$) || ... || m$_l^*$) with IV = IV* $\oplus$ $0^{\lambda-1}1$
meaning we flip the last bit of the first block of our message as well as the last bit of our IV*.
This causes that IV* $\oplus$ m$_1^*$ = IV $\oplus$ m$_1$ and therefore
c$_1^*$ = F$_k$(IV* $\oplus$ m$_1^*$) = F$_k$(IV $\oplus$ m$_1$) = c$_1$ as well as all other c$_i^*$ = c$_i$ of the chain for i ℓ {2,l}.

We can conclude that t* = t but m* $\neq$ m and therefore m was not queried to Mac$_k$ before.
$\Rightarrow$ The adversary $\mathcal{A}$ can now create the valid forgery t$^‘$ = (IV, t) and can break the unforgability of the Mac.

Solution of Exercisesheet 7



(b) The adversary $\mathcal{A}$ can choose the messages m of length $\ell(\lambda) \cdot \lambda$. We set $\ell(\lambda)$ = l. We choose
$m^1 = m_1^1$ || ... || m_l^1 and
$m^2 = m_1^2$ || ... || m_l^2
with $m_i^1 = m_i^2 = 0^\lambda$ for $2 \leq i \leq l$.

$c_1^i = F_k(IV \oplus m_1^i)$ with IV $^* \in \{0,1\}^\lambda$ as a random but fixed vector
$c_2^i = F_k(c_1^i \oplus m_2^i)$
...
$c_l^i = F_k($ ... $F_k(IV \oplus m_1^i)$ ...$)$
t = $(c_1^i$, ..., $c_l^i)$ for i $\in \{1,2\}$

To break the security of the MAC the adversary $\mathcal{A}$ can construct the following forgery:
$m^* = m_1^2$ || m_2^* || m_3^1 || ... || m_l^1
with $m_2^* = c_1^1 \oplus m_2^1 \oplus c_1^2$ which generates a vector that satisfies the following equation:
$\Rightarrow c_1^1 \oplus m_2^1 = c_1^2 \oplus m_2^*$
This helps us construct m^* such that $c_2^1 = F_k(c_1^1 \oplus m_2^1) = F_k(c_1^2 \oplus m_2^*) = c_2^*$ and $c_i^1 = c_i^*$ for i $\in \{3,l\}$.
Therefore the adversary $\mathcal{A}$ can create the valid forgery t = $(c_1^2, c_2^1,$ ... , $c_l^1)$ for m^* which has not been queried before and can break the unforgability of the Mac.

Solution of Exercisesheet 7

Exercise 7-4