

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 distinguish corresponding cipher to a message just by comparing the appended $H(m)$ part in the cipher. Hence this new modified encryption doesn't have indistinguishable encryptions 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 $t^* = F(K, m_1) || F(K, F(K, m_1)) = t_1^1 || t_1^2$. 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:

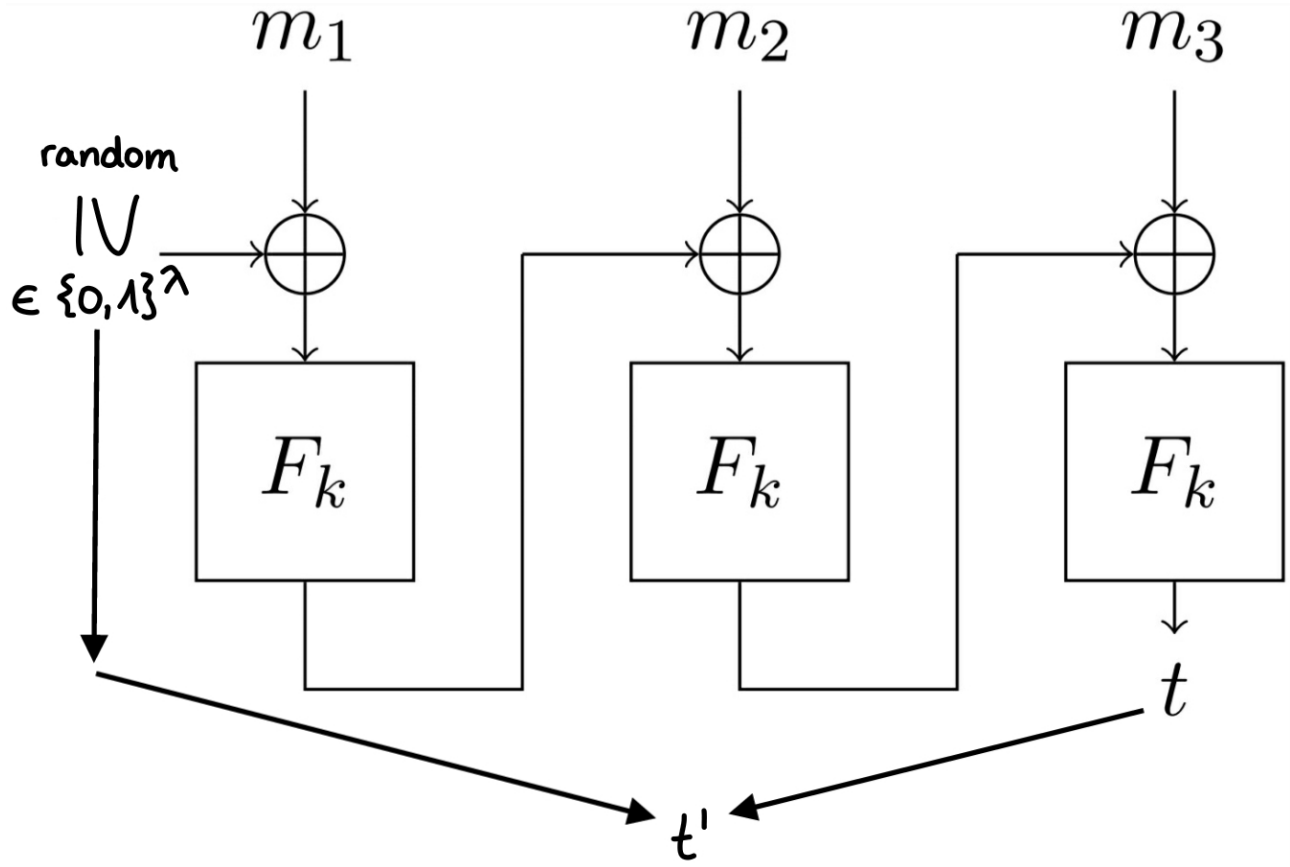
The adversary \mathcal{A} makes one query to the oracle:

$$m^1 = m_1 || m_2 \Rightarrow t^1 = (r \oplus (F(K, m_1) \oplus F(K, m_2)), r)$$

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 $\ell(\lambda) = l$
 $m^* = m_1^* \parallel \dots \parallel m_l^*$. We set $m_i^* = 0^\lambda$.
 We query m^* to our $\text{Mac}_k(\cdot)$ oracle and receive the tag $t^* = (IV^*, t^*)$. $IV^* \in \{0,1\}^\lambda$ is a randomly generated vector

$$\begin{aligned} c_1^* &= F_k(IV^* \oplus m_1^*) = F_k(IV^* \oplus 0^\lambda) = F_k(IV^*) \\ c_2^* &= F_k(c_1^* \oplus m_2^*) = F_k(F_k(IV^*) \oplus 0^\lambda) = F_k(F_k(IV^*)) \\ &\dots \\ c_l^* &= F_k(\dots F_k(IV^*) \dots) = t^* \end{aligned}$$

To break the security of the MAC the adversary \mathcal{A} can construct the following forgery:

$$m = 0^{\lambda-1}1 \parallel m_2^* \parallel \dots \parallel m_l^* \text{ with } IV = IV^* \oplus 0^{\lambda-1}1$$

meaning we flip the last bit of the first block of our message as well as the last bit of our IV^* .

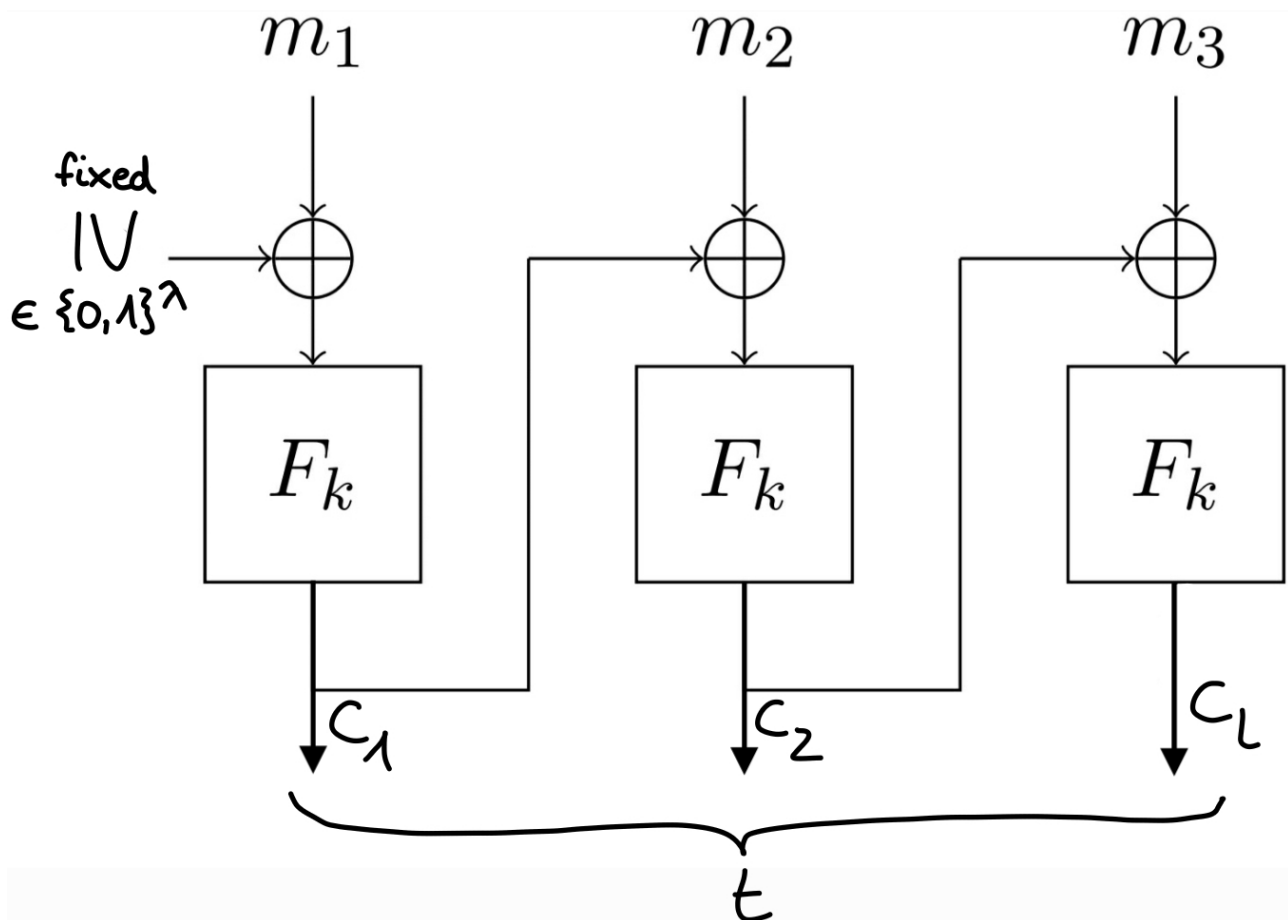
This causes that $IV^* \oplus m_1^* = IV \oplus m_1$ and therefore

$$c_1^* = F_k(IV^* \oplus m_1^*) = F_k(IV \oplus m_1) = c_1 \text{ as well as all other } c_i^* = c_i \text{ of the chain for } i \in \{2, l\}.$$

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 unforgeability 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 $m^1 = m_1^1 \parallel \dots \parallel m_l^1$ and $m^2 = m_1^2 \parallel \dots \parallel m_l^2$ with $m_i^1 = m_i^2 = 0^\lambda$ for $2 \leq i \leq l$.

$$c_1^i = F_k(IV \oplus m_1^i) \text{ with } IV^* \in \{0,1\}^\lambda \text{ as a fixed vector}$$

$$c_2^i = F_k(c_1^i \oplus m_2^i)$$

...

$$c_l^i = F_k(\dots F_k(IV \oplus m_1^i) \dots)$$

$$t = (c_1^i, \dots, c_l^i) \text{ for } i \in \{1,2\}$$

To break the security of the MAC the adversary \mathcal{A} can construct the following forgery:

$$m^* = m_1^2 \parallel m_2^* \parallel m_3^1 \parallel \dots \parallel m_l^1$$

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 $c_2^1 = F_k(c_1^1 \oplus m_2^1) = F_k(c_1^2 \oplus m_2^*) = c_2^2$ and $c_i^1 = c_i^2$ for $i \in \{3,l\}$.

Therefore the adversary \mathcal{A} can create the valid forgery $t = (c_1^2, c_2^1, \dots, c_l^1)$ for m^* which has not been queried before and can break the unforgability of the Mac.



SOLUTION OF EXERCISESHEET 7

Exercise 7-4