# Solution of Exercisesheet 5

## Exercise 5-1

Given $\{F_k\}_{k\in K}$ is a family of bit permutations.

Adversary $A$ can choose two inputs $x_1$ and $x_2$. Then the corresponding bit permutation with key $k$ be $F_k(x_1)$ and $F_k(x_2)$.

Let's take an example, $F_k$ as the function that swaps the first two bits of its input. For this function, the distinguisher can easily distinguish between $F_k(x_1)$ and $F_k(x_2)$ with a function, $f$ that also swaps first two bits of the output. Or this can also be easily distinguished just comparing the bits other than first two bits.

Similarly, for any such bit permutation function there exists a function $f$ which can easily distuingush the between the inputs of a bit permutation $F_k$. Hence these family of bit permutations cannot be a pseudorandom permutation.

## Exercise 5-2

Assume n $= 3$
The Adversary $\mathcal{A}$ can choose the two messages $m_0 = 001\ 001$ and $m_1 = 110\ 011$
The challenger encrypted one of the messages.
Since f is a pseudorandom permutation, f is deterministic and has a reverse operation.

If $m_0$ is encrypted:
$Enc(m_0) = Enc(m_0^0 \,||\, m_0^1) = Enc(001\ 001) = f(m_0^0) \,||\, f(m_0^1) = f(001) \,||\, f(001) = c^0 \,||\, c^1$
$\Rightarrow c^0 = c^1$

If $m_1$ is encrypted:
$Enc(m_1) = Enc(m_1^0 \,||\, m_1^1) = Enc(110\ 011) = f(m_1^0) \,||\, f(m_1^1) = f(110) \,||\, f(011) = c^0 \,||\, c^1$
$\Rightarrow c^0 \neq c^1$

If b $= 0$: $c_b = c^0 \,||\, c^1$, $c^0 = c^1$
If b $= 1$: $c_b = c^0 \,||\, c^1$, $c^0 \neq c^1$
This shows that even when the adversary can't break the encryption of the pseudorandom permutation the adversary can distinguish what message was encrypted with a probability of $100\%$
$\Rightarrow$ ECB mode is not EAU-secure

## Exercise 5-3

1. To show: If $f$ is pseudorandom, than $\Pi_{CTR}$ is CPA-secure.
Proof by contradiction. We assume there exists an adversary $\mathcal{A}$, which can break $\Pi_{CTR}$ with a non-negligible propability. Then we construct the distinguisher $\mathcal{B}$, who can distinguish $f$ from a truly random function and invokes $\mathcal{A}$ as follows:
$\mathcal{B}$ has access to an oracle $\mathcal{O}_B$ that runs either the pseudorandom permutation function $f$ or a randomly choosen permutation function $f^*$. $\mathcal{B}$ has to give $\mathcal{A}$ access to an encryption oracle $\mathcal{O}_{Enc}$.

# Solution of Exercisesheet 5

$\mathcal{O}_{Enc}$ is realised by answering with $Enc_k(m)$ on the input $m$, where $f_k$ is replaced with the oracle $\mathcal{O}_B$. Thus, $c$ looks like $c = (IV, m \oplus s)$, where $s = \mathcal{O}_B(IV)||\mathcal{O}_B(IV+1)||...||\mathcal{O}_B\left(IV + \left\lceil \frac{|m|}{n} \right\rceil\right)$ with the last bits truncated so $|s| = |m|$.
$\mathcal{A}$ then askes for the encryption of one of the two messages $m_0$ and $m_1$ with $|m_0| = |m_1|$. $\mathcal{B}$ then samples a bit $b \leftarrow \$\{0,1\}$ and forwards $c_b \leftarrow Enc_k(m_b)$ to $\mathcal{A}$, where $Enc_k(m_b)$ is realised like in the encryption oracle. $\mathcal{B}$ then outputs the same bit $b'$ which $\mathcal{A}$ outputs.
$\mathcal{B}$ is efficient, because he only forwards or concatenate messages or truncates bits from a message, which all can be done in constant time and invokes $\mathcal{A}$ which is efficient.
To analyse the success distuiguish two cases: If $\mathcal{O}_B$ runs a pseudorandom permutation function $f$ then $\mathcal{B}$ perfectly simulates $\Pi_{CTR}$ to $\mathcal{A}$. $\Rightarrow Pr[\mathcal{B}^{f(\cdot)}(1^\lambda) = 1] = Pr[PrivK^{CPA}_{\Pi^{CTR},\mathcal{A}} = 1] = \frac{1}{2} + non - negl(\lambda)$, because $\mathcal{A}$ is an efficient adversary against die CPA-security of $\Pi_{CTR}$
If the oracle runs a randomly choosen function $f^*$ and $\mathcal{A}$ queries the encryption oracle at least q times we have $Pr[\mathcal{B}^{f^*(\cdot)}(1^\lambda) = 1] = \frac{1}{2} + \frac{q(\lambda)}{2^\lambda}$.
Now we subtract those two cases:
$|Pr[\mathcal{B}^{f(\cdot)}(1^\lambda) = 1] - Pr[\mathcal{B}^{f^*(\cdot)}(1^\lambda) = 1]| = \left|\frac{1}{2} + non - negl(\lambda) - \frac{1}{2} - \frac{q(\lambda)}{2^\lambda}\right| = non - negl(\lambda) - \frac{q(\lambda)}{2^\lambda} = non - negl(\lambda)$. So the distinguisher $\mathcal{B}$ can distinguish between $f$ and $f^*$ with a non-negligible gap which is a contradiction to the pseudorandomness of $f$. Therefore such an adversary $\mathcal{A}$ against the CPA-security of $\Pi_{CTR4}$ cannot exist.

2. To show: $\Pi_{CTR}$ is not CCA-secure.
In the game for CCA-security the adversary $\mathcal{A}$ has access to an encryption oracle $\mathcal{O}_{Enc}$ and a decryption oracle $\mathcal{O}_{Dec}$.
$\mathcal{A}$ gives the challenger the two messages $m_0 = 0^\lambda$ and $m_1 = 1^\lambda$ and gets the ciphertext $c_b = (IV, c'_b)$ back. Then $\mathcal{A}$ askes the decryption oracle $\mathcal{O}_{Dec}$ for the decoding of $c^*_b = (IV, c'^*_b)$, where $c'^*_b$ is $c'_b$ with the last bit flipped. Since $c^*_b$ is not equals to $c_b$, $\mathcal{O}_{Dec}$ will answer the query. The result is than either $0^{\lambda-1}1$ or $1^{\lambda-1}0$, because the only difference to computation of $c'_b \oplus s = m$ is the last bit of $c'_b$. If the result is $0^{\lambda-1}1$ the adversary returns $b' = 0$, if the result is $1^{\lambda-1}0$ $b' = 1$.

## Exercise 5-4

The scheme is CCA1-secure.
An adversary can use an encryption and decryption oracle before receiving the challenge ciphertext c.
The encryption and decryption oracle allows the adversary to relate a ciphertext $c := (c_1, c_2) = (r, F_k(r) \oplus m)$ to a message $m := F_k(c_1) \oplus c_2 = F_k(r) \oplus (F_k(r) \oplus m)$
After using the oracles, the adversary receives the challenge ciphertext $c = (r_c, F_k(r_c) \oplus m_c)$. The only possibility for the adversary to efficiently know from which of two messages the challenge ciphertext originates from, is when $r_c$ was used by the encryption oracle to answer at least one of the adversary's queries or when the adversary coincidentally used $r_c$ as input to the decryption oracle.
In these cases, the adversary may easily determine which of its messages was encrypted.
Whenever the encryption oracle returns a ciphertext $c := (r, s)$ in a response to encrypt the message

# Solution of Exercisesheet 5

m, the adversary learns the value of $F_k(r)$ since $F_k(r) = s \oplus m$. But the adversary can query at most a polynomial number of messages and each query has the probability of $\frac{1}{2^n}$ that the selected value for $r = r_c$ what is negligible.
The scheme is therefore CCA1-secure.