

Cryptography – Homework 2

冯诗伟 161220039

3.14

3.19

a

The encryption scheme is not EAV-secure. Because G is deterministic and publicly known, the adversary can get the plaintext just by compute $G(c_1) \oplus c_2 = G(r) \oplus G(r) \oplus m = m$ when obtaining the ciphertext $c = \langle c_1, c_2 \rangle$.

The encryption scheme is not CPA-secure for the reason mentioned above.

b

The encryption scheme is EAV-secure. Even if the input of F is fixed, the key k is uniform. So it is equivalent to OTP.

The encryption scheme is not CPA-secure. After the adversary produces m_0 and m_1 , he gets $m_b \oplus F_k(0^n)$. Then the adversary can send m_0 to the oracle and get $m_0 \oplus F_k(0^n)$ from the oracle. Since k is the same, the adversary now gets the value of $F_k(0^n)$. Thus he can directly compute the m_b and succeeds with the probability of 1.

c

The encryption scheme is both EAV-secure and CPA-secure.

Because m_0 and m_1 are independent and $F_k(r)$ and $F_k(r + 1)$ are independent, this is actually the same as Construction 3.30. Therefore, it is CPA-secure and we get that it is EAV-secure for free. (Actually, this scheme is CTR-mode.)

3.29

Construct the CPA-secure encryption scheme $\Pi^* = (Enc, Dec)$:

Enc: on input a message $m \in \{0, 1\}^n$, choose a uniform $r \in \{0, 1\}^n$ and output the ciphertext

$$c := \langle Enc_1(r), Enc_2(r \oplus m) \rangle$$

Dec: on input a ciphertext $c = \langle c_1, c_2 \rangle$, output the plaintext message

$$m := Dec_1(c_1) \oplus Dec_2(c_2)$$

Next I will show that Π^* is CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure.

1. If both Enc_1 and Enc_2 are CPA-secure, the adversary can get nothing about r or $r \oplus m$. So he cannot get any information about the plaintext.
2. If Enc_1 is CPA-secure while Enc_2 is not CPA-secure, the adversary can distinguish $r \oplus m_0$ from $r \oplus m_1$ with a probability significantly better than $\frac{1}{2}$. But r is uniform, the adversary cannot tell m_0 from m_1 .
3. If Enc_2 is CPA-secure while Enc_1 is not CPA-secure, the adversary can get some information about r . That is no help because the adversary can get nothing about $r \oplus m$.

In conclusion, Π^* is CPA-secure as long as at least one of Π_1 or Π_2 is CPA-secure.

Additional 3.26

a

If F is pseudorandom, we have

$$|Pr[D^{F_k(\cdot)}(1^n) = 1] - Pr[D^{f(\cdot)}(1^n) = 1]| \leq \text{negl}(n)$$

Since $f(\cdot)$ is originally uniform, $f^s(\cdot)$ is just the same as $f(\cdot)$.

$$Pr[D^{f(\cdot)}(1^n) = 1] = Pr[D^{f^s(\cdot)}(1^n) = 1]$$

Since F is pseudorandom, F with uniform k actually produces random strings. Thus F_k with uniform input produces random strings as well.

$$Pr[D^{F_k(\cdot)}(1^n) = 1] = Pr[D^{F_k^s(\cdot)}(1^n) = 1]$$

Therefore, we have

$$|Pr[D^{F_k^s(\cdot)}(1^n) = 1] - Pr[D^{f^s(\cdot)}(1^n) = 1]| \leq \text{negl}(n)$$

which means F is weakly pseudorandom.

b

Notice that whether the distinguisher D for F'_k can succeed is independent from the parity of x .

$$\begin{aligned} Pr[D^{F_k^s(\cdot)}(1^n) = 1] &= Pr[D^{F_k'^s(\cdot)}(1^n) = 1 \cap x \text{ is even}] + Pr[D^{F_k'^s(\cdot)}(1^n) = 1 \cap x \text{ is odd}] \\ &= \frac{1}{2}Pr[D^{F_k'^s(\cdot)}(1^n) = 1] + \frac{1}{2}Pr[D^{F_k'^s(\cdot)}(1^n) = 1] \\ &= Pr[D^{F_k'^s(\cdot)}(1^n) = 1] \end{aligned}$$

Because F' is pseudorandom, F' is weakly pseudorandom.

$$|Pr[D^{F_k'^s(\cdot)}(1^n) = 1] - Pr[D^{f^s(\cdot)}(1^n) = 1]| \leq \text{negl}(n)$$

Notice that

$$Pr[D^{f(\cdot)}(1^n) = 1] = Pr[D^{f^s(\cdot)}(1^n) = 1], Pr[D^{F_k'^s(\cdot)}(1^n) = 1] = Pr[D^{F_k^s(\cdot)}(1^n) = 1]$$

$$\therefore |Pr[D^{F_k^s(\cdot)}(1^n) = 1] - Pr[D^{f^s(\cdot)}(1^n) = 1]| \leq \text{negl}(n)$$

which means F is weakly pseudorandom.

Next I will prove that F is not pseudorandom.

Construct the distinguisher D^* : D^* query the oracle with m_0 and m_1 where m_0 is even, m_1 is odd and $m_0 = m_1 + 1$.

D^* obtains $y_0 = \mathcal{O}(m_0)$ and $y_1 = \mathcal{O}(m_1)$ and outputs 1 if and only if $y_0 = y_1$.

If $\mathcal{O} = F_k$, D^* outputs 1 with probability of 1. If $\mathcal{O} = f$, D^* outputs 1 with probability of 2^{-n} .

$$\therefore |Pr[D^{F_k(\cdot)}(1^n) = 1] - Pr[D^{f(\cdot)}(1^n) = 1]| = 1 - 2^{-n}$$

So F_k is not pseudorandom.

c

CTR-mode encryption using a weak pseudorandom function is not necessarily CPA-secure.

Consider the weak pseudorandom function F_k in (b).

Construct the adversary \mathcal{A} . \mathcal{A} produces m_0 and m_1 where m_0 and m_1 are as long as three blocks.

$m_0 = m_{00} || m_{01} || m_{02}$, where $m_{00} = m_{01} = m_{02}$.

$m_1 = m_{10} || m_{11} || m_{12}$, where any two of m_{10}, m_{11}, m_{12} are different.

\mathcal{A} obtains the ciphertext $c = c_{b1} || c_{b2} || c_{b3}$ and can get the parity of ctr.

If ctr is odd, \mathcal{A} output 0 if and only if $c_{b1} = c_{b2}$.

If ctr is even, \mathcal{A} output 0 if and only if $c_{b1} = c_{b2}$.

Notice that when ctr is odd $c_{01} = m_{01} \oplus F_k(ctr + 3)$, $c_{02} = m_{02} \oplus F_k(ctr + 3)$, $c_{11} \neq c_{12}$, and when ctr is even $c_{00} = m_{00} \oplus F_k(ctr + 2)$, $c_{01} = m_{01} \oplus F_k(ctr + 2)$, $c_{00} \neq c_{01}$.

\mathcal{A} succeeds with a probability of 1.

In this case, CTR-mode encryption using a weak pseudorandom function is not CPA-secure.

CTR-mode encryption using a weak pseudorandom function is not necessarily EAV-secure.

Consider the weak pseudorandom function F_k in (b).

Construct the adversary \mathcal{A} . \mathcal{A} produces m_0 and m_1 where m_0 and m_1 are as long as three blocks.

$m_0 = m_{00} || m_{01} || m_{02}$, where $m_{00} = m_{01} = m_{02}$.

$m_1 = m_{10} || m_{11} || m_{12}$, where any two of m_{10}, m_{11}, m_{12} are different.

\mathcal{A} obtains the ciphertext $c = c_{b1} || c_{b2} || c_{b3}$ and can get the parity of ctr.

If ctr is odd, \mathcal{A} outputs 0 if and only if $c_{01} = c_{02}$.

If ctr is even, \mathcal{A} outputs 0 if and only if $c_{00} = c_{01}$.

Notice that when ctr is odd $c_{01} = c_{02}$, $c_{11} \neq c_{12}$, and when ctr is even $c_{00} = c_{01}$, $c_{00} \neq c_{01}$.

\mathcal{A} succeeds with a probability of 1.

In this case, CTR-mode encryption using a weak pseudorandom function is not EAV-secure.

d

If F_k is weakly pseudorandom, we have

$$|Pr[D^{F_k^s(\cdot)}(1^n) = 1] - Pr[D^{f^s(\cdot)}(1^n) = 1]| \leq \text{negl}(n)$$

Let $\widetilde{\Pi} = (\widetilde{Gen}, \widetilde{Enc}, \widetilde{Dec})$ be an encryption scheme that is exactly the same as $\Pi = (Gen, Enc, Dec)$ from Construction 3.30, except that a truly random function is used in the place of F_k .

Let $\Pi^s = (Gen^s, Enc^s, Dec^s)$ be an encryption scheme that is exactly the same as $\Pi = (Gen, Enc, Dec)$ from Construction 3.30, except that a weakly pseudorandom function is used in the place of F_k .

Construct the distinguisher \mathcal{D} :

\mathcal{D} is given input 1^n and access to an oracle $\mathcal{O} : \{0, 1\}^n \rightarrow \{0, 1\}^n$.

1. Run $\mathcal{A}(1^n)$. Whenever \mathcal{A} queries its encryption oracle on a message $m \in \{0, 1\}^n$, answer this query in the following way:

- (a) Choose uniform $r \in \{0, 1\}^n$.
- (b) Return the ciphertext $\langle r, \mathcal{O}(r) \oplus m \rangle$ to \mathcal{A} .

2. When \mathcal{A} outputs messages $m_0, m_1 \in \{0, 1\}^n$, choose a uniform bit $b \in \{0, 1\}$ and then:

- (a) Choose uniform $r \in \{0, 1\}^n$.
- (b) Return the ciphertext $\langle r, \mathcal{O}(r) \oplus m \rangle$ to \mathcal{A} .

3. Continue answering the encryption-oracle queries of \mathcal{A} as before until \mathcal{A} outputs a bit b' . Output 1 if $b = b'$ and 0 otherwise.

If \mathcal{D} 's oracle is a random function,

$$Pr_{f \leftarrow Func_n} [D^{f(\cdot)}(1^n) = 1] = Pr[Privk_{\mathcal{A}, \widetilde{\Pi}}^{cpa}(n) = 1]$$

If \mathcal{D} 's oracle is a weakly pseudorandom function,

$$Pr_{k \leftarrow \{0, 1\}^n} [D^{F_k^s(\cdot)}(1^n) = 1] = Pr[Privk_{\mathcal{A}, \Pi^s}^{cpa}(n) = 1]$$

$$\therefore |Pr[D^{F_k^s(\cdot)}(1^n) = 1] - Pr[D^{f^s(\cdot)}(1^n) = 1]| \leq \text{negl}(n), \quad Pr[D^{f^s(\cdot)}(1^n) = 1] = Pr[D^{f(\cdot)}(1^n) = 1]$$

$$\therefore |Pr[Privk_{\mathcal{A}, \Pi^s}^{cpa}(n) = 1] - Pr[Privk_{\mathcal{A}, \widetilde{\Pi}}^{cpa}(n) = 1]| \leq \text{negl}(n)$$

Recall the inequation (3.11) in the textbook:

$$Pr[Privk_{\mathcal{A}, \widetilde{\Pi}}^{cpa}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n}$$

We now have

$$Pr[Privk_{\mathcal{A}, \Pi^s}^{cpa}(n) = 1] \leq \frac{1}{2} + \frac{q(n)}{2^n} + \text{negl}(n)$$

Since $q(n)$ is polynomial, $\frac{q(n)}{2^n}$ is negligible, which means Construction 3.30 is CPA-secure if F is a weak pseudorandom function.