Fundamentals of Cryptography Homework 3

周书予
2000013060@stu.pku.edu.cn

October 5, 2022

Problem 1

$\mathsf{Dec}(k,(r,c)) = F_k^{-1}(c) \oplus r$.

Denote $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as the encryption scheme mentioned in the problem, and $\tilde{\Pi} = (\widetilde{\mathsf{Gen}}, \widetilde{\mathsf{Enc}}, \widetilde{\mathsf{Dec}})$ exactly the same as Π, except that a truely random permutation f is used in place of F_k.

The proof is divided into two parts:

- In the first part we prove that for any PPT adversary $\mathcal{A}$, there is some negligible function $\varepsilon(n)$ such that

$$\left| \Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1\right] - \Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\tilde{\Pi}}(n) = 1\right] \right| < \varepsilon(n) \tag{1}$$

- In the second part we show that for any PPT adversary $\mathcal{A}$,

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\tilde{\Pi}}(n) = 1\right] \leqslant \frac{1}{2} + \frac{2q(n)}{2^n} \tag{2}$$

  for some polynomial $q(n)$.

When finished the proof of the two parts mentioned above, one can see that obviously $\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1\right] \leqslant \frac{1}{2} + \frac{q(n)}{2^n} + \varepsilon(n)$, which means Π is secure under CPA attack.

Proof of eq. (1)

For any PPT adversary $\mathcal{A}$, a PPT distinguisher $\mathcal{D}$ can be built, which has access to an oracle $\mathcal{O} : \{0,1\}^n \to \{0,1\}^n$ (here it refers to F_k or f) and interacts with $\mathcal{A}$ like this:

1. when $\mathcal{A}$ queries the ciphertext for message $m \in \{0,1\}^n$, choose uniformly random $r \in \{0,1\}^n$ and return $(r, \mathcal{O}(r \oplus m))$.
2. when $\mathcal{A}$ outputs m_0 and m_1, choose a random bit $b \in \{0,1\}$ and uniformly random $r \in \{0,1\}^n$, then return $(r, \mathcal{O}(r \oplus m_b))$.
3. continue answering $\mathcal{A}$'s queries until $\mathcal{A}$ outputs a bit b', then output $\mathbb{1}[b = b']$.

It is easy to see that

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)=1\right]=\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{D}^{F_k}(1^n)=1\right]$$
$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\tilde{\Pi}}(n)=1\right]=\Pr_{f\leftarrow\mathsf{Perm}_n}\left[\mathcal{D}^{f}(1^n)=1\right]$$

where Perm_n denotes the collection of all permutations over $\{0,1\}^n$.

Since F is a PRP, by definition we know that

$$\left|\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{D}^{F_k}(1^n)=1\right]-\Pr_{f\leftarrow\mathsf{Perm}_n}\left[\mathcal{D}^{f}(1^n)=1\right]\right|<\varepsilon(n)$$

for some negligible $\varepsilon(n)$, so eq. (1) is proved as desired.

Proof of eq. (2)

Notice that $\mathcal{A}$ runs in polynomial time, so it can only queries the ciphertext for polynomially many m, say, $q(n)$. Whenever $\mathcal{A}$ queries m it obtains $f(r\oplus m)$ where r is known to $\mathcal{A}$ and chosen uniformly random. That is, each query gives $\mathcal{A}$ a pair $(x,f(x))$ which is a point value of f, where $x=r\oplus m$ is chosen uniformly random.

When $\mathcal{A}$ outputs m_0,m_1 and receives $(r^*,f(r^*\oplus m_b))$, it checks out all the recordings from the interaction, and if the point value for $r^*\oplus m_0$ or $r^*\oplus m_1$ is found, it can break the encryption scheme with 100% confidence, otherwise it learns nothing about $f(r^*\oplus m_0)$ and $f(r^*\oplus m_1)$, and probability of outputing the correct answer is exactly $1/2$.

The probability that the point value for $r^*\oplus m_0$ or $r^*\oplus m_1$ can be found equals to the probability of finding out two specific items among 2^n during $q(n)$ times of random choosing, which by union bound is not greater than $2q(n)/2^n$. Thus,

$$\Pr\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\tilde{\Pi}}(n)=1\right]\leqslant\frac{2q(n)}{2^n}\cdot 1+\left(1-\frac{2q(n)}{2^n}\right)\cdot\frac{1}{2}=\frac{1}{2}+\frac{2q(n)}{2^n}$$

Problem 2

Part A: F' is a PRF

First we show that for any PPT distinguisher $\mathcal{D}$,

$$\left|\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{D}^{g\circ F_k}(1^n)\right]-\Pr_{f\leftarrow\mathsf{Func}_n}\left[\mathcal{D}^{g\circ f}(1^n)\right]\right|<\mathsf{negl}(n) \tag{3}$$

(here $f_1\circ f_2$ denotes the composition of function f_1 and f_2.)

This can be done by constructing another distinguisher $\mathcal{D}'$, which always queries the same message m as $\mathcal{D}$ does except that the oracle used here is F_k or f instead of $g\circ F_k$ or $g\circ f$, and outputs the same as $\mathcal{D}$ does.

It is easy to see that

$$\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{D}^{g\circ F_k}(1^n)\right]=\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{D}'^{F_k}(1^n)\right]$$
$$\Pr_{f\leftarrow\mathsf{Func}_n}\left[\mathcal{D}^{g\circ f}(1^n)\right]=\Pr_{f\leftarrow\mathsf{Func}_n}\left[\mathcal{D}'^{f}(1^n)\right]$$

Since F is a PRF, from its definition it is clear to see that eq. (3) can be proved.

Then we can show that for any PPT distinguisher $\mathcal{D}$,

$$\left|\Pr_{f\leftarrow \mathsf{Func}_n}\left[\mathcal{D}^{g\circ f}(1^n)\right] - \Pr_{h\leftarrow \mathsf{Func}_{n,2n}}\left[\mathcal{D}^{h}(1^n)\right]\right| < \mathsf{negl}(n) \tag{4}$$

(here $\mathsf{Func}_{n,2n}$ is defined as $\{h : \{0,1\}^n \to \{0,1\}^{2n}\}$.)

This can be done by using hybird argument: assume $\mathcal{D}$ interacts with oracle for $p(n)$ rounds and, WLOG, we assume $\mathcal{D}$ never queries for the same x for encryption (that is obviously suboptimal). Based on $\mathcal{D}$, distinguisher $\mathcal{D}'$ can be built, which on input $r \in \{0,1\}^{2n}$ works as follows:

- randomly sample t from $\{1, 2, \cdots, p(n)\}$, and randomly fix some $f \leftarrow \mathsf{Func}_n$ and $h \leftarrow \mathsf{Func}_{n,2n}$. ($f$ and h do not need to be fully stored.)
- interact with $\mathcal{D}$. Whenever queried with x in round i, return $\begin{cases} g(f(x)), & i < t \\ r, & i = t \\ h(x), & i > t \end{cases}$.
- output the same as $\mathcal{D}$ does.

From this construction we know that

$$\begin{aligned}&\Pr_{s\leftarrow\{0,1\}^n}\left[\mathcal{D}'(g(s)) = 1\right] - \Pr_{r\leftarrow\{0,1\}^{2n}}\left[\mathcal{D}'(r) = 1\right] \\ &\qquad = \frac{1}{p(n)}\left(\Pr_{f\leftarrow \mathsf{Func}_n}\left[\mathcal{D}^{g\circ f}(1^n)\right] - \Pr_{h\leftarrow \mathsf{Func}_{n,2n}}\left[\mathcal{D}^{h}(1^n)\right]\right)\end{aligned}$$

Since g is a PRG, both sides of the equation are negligible, and eq. (4) is proved as desired.

From eq. (3) and eq. (4) one can draw that

$$\left|\Pr_{k\leftarrow\{0,1\}^n}\left[\mathcal{D}^{g\circ F_k}(1^n)\right] - \Pr_{h\leftarrow \mathsf{Func}_{n,2n}}\left[\mathcal{D}^{h}(1^n)\right]\right| < \mathsf{negl}(n) \tag{5}$$

which suggests that $F'_k = g \circ F_k$ is a PRF.

Part B: F' may not be a PRF

Let g be a PRG which drops its first bit of input. It is easy to see that such PRG exists.

Then for any $x \in \{0,1\}^{n-1}$, $F'_k(0\|x) = F_k(g(0\|x)) = F_k(g(1\|x)) = F'_k(1\|x)$, which suggests that F'_k is not that "random" and can be easily distinguished from a truely random function.

Problem 3

Part A: F' may not be a strong PRP

Part B: F' is a PRF

Problem 4