作业讲解 IV

Anyi Cao

Nanjing University

Exercises 8.5

8.5 Let F be a (length-preserving) pseudorandom permutation.

(a) Show that the function $f(x, y) = F_x(y)$ is not one-way.

(b) Show that the function $f(y) = F_{0^n}(y)$ (where $n = |y|$) is not one-way.

(c) Prove that the function $f(x) = F_x(0^n)$ (where $n = |x|$) is one-way.

Solution:

(a) When receiving $f(x, y)$, pick x' randomly and compute $y' = F_{x'}^{-1}(f(x, y))$, there is $f(x', y') = F_{x'}(y') = f(x, y)$. Outputs (x', y').

(b) When receiving $f(y)$, compute $y' = F_{0^n}^{-1}(f(y))$ so that $f(y') = F(y)$. Outputs y'.

(c) To be solved, there're still some problems :(

That is, if we assume there is an adversary $\mathcal{A}$ can invert $f(x) = F_x(0^n)$ with a non-negligible probability $\epsilon(n)$, $\mathcal{A}$ will not care the value he received is from $F_k(\cdot)$ or a random permutation $g(\cdot)$. So when the oracle is $g(\cdot)$ and query it by 0^n to get a value $y = g(0^n)$, if there exists x that $F_x(0^n) = y$, $\mathcal{A}$ will return x with probability $\epsilon(n)$, which satisfies $F_x(0^n) = \mathcal{O}(0^n) = y$.

To sovle this problem we try to query another value unequal to 0^n, like 1^n, and compute whether $F_x(1^n) = \mathcal{O}(1^n)$. Then we meet another problem that, when the oracle is $F_k(\cdot)$, we may find a set $\{x_i\}$ that for each x_i, $F_{x_i}(0^n) = F_k(0^n)$, and $\mathcal{A}$ will return any of them with some probability distribution. When $\mathcal{A}$ return a $x \neq k$ while $F_x(0^n) = F_k(0^n)$, then the probability of second query passed, i.e. $F_x(1^n) = F_k(1^n)$, is only $\frac{1}{2^n}$.

When the oracle is F_k, the key k is sampled randomly, so that whatver the distribution $\mathcal{A}$ outputing $x \in \{x_i\}$ is, the total probability that $x = k$ is $\frac{\epsilon(n)}{|\{x_i\}|}$. Unfortunately, the size of $\{x_i\}$ may be a exponential value about n, like $2^{n/2}$, which leads to the final probability still a negligible value.

So above is my thoughts and problems, if you have any idea please discuss with me. (ORZ)

Exercises 8.8

8.8 Let f be a length-preserving one-way function. Is $g(x) \stackrel{\text{def}}{=} f(f(x))$ necessarily one-way? What about $g'(x) \stackrel{\text{def}}{=} f(x) \| f(f(x))$?

作业讲解 IV - 2

(a) $g(x) = f(f(x))$ is not necessarily one-way, we give a counterexample as follow. Let h be any length-preserving one-way function, we define f as follow: if $x_1 x_2 \cdots x_{n/2} = 0^{n/2}$ then $f(x) = 0^n$, else $f(x) = 0^n || h(x_{n/2} x_{n/2+1} \cdots x_n)$.

We first prove that f is one-way. Assume there is a probabilistic polynomial-timeadversary $\mathcal{A}$ that $\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] = \epsilon(n)$, then we can construct $\mathcal{A}'$ to invert h. $\mathcal{A}'$ receives $1^{n/2}$ and a value $y \in \{0,1\}^{n/2}$ and attempts to find a value $x \in h^{-1}(y)$. $\mathcal{A}'$ set $(1^n, 0^{n/2} || y)$ as the input of $\mathcal{A}$ and runs $\mathcal{A}$, finally ouputs the same with $\mathcal{A}$.

$$
\begin{aligned}
&\Pr_{x \xleftarrow{\$} \{0,1\}^n}[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x))] \\
= &\Pr_{x \xleftarrow{\$} \{0,1\}^n}[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x)) | x_{[1,n/2]=0^{n/2}}] \Pr[x_{[1,n/2]=0^{n/2}}] \\
+ &\Pr_{x \xleftarrow{\$} \{0,1\}^n}[\mathcal{A}(1^n, f(x)) \in f^{-1}(f(x)) | x_{[1,n/2]\neq 0^{n/2}}] \Pr[x_{[1,n/2]\neq 0^{n/2}}] \\
\leq &1 * \frac{1}{2^{n/2}} + \Pr_{x \xleftarrow{\$} \{0,1\}^{n/2}}[\mathcal{A}'(1^{n/2}, h(x)) \in h^{-1}(h(x))]
\end{aligned}
$$

So we have $\Pr_{x \xleftarrow{\$} \{0,1\}^{n/2}}[\mathcal{A}'(1^{n/2}, h(x)) \in h^{-1}(h(x))] \geq \epsilon - \frac{1}{2^{n/2}}$, which is a non-negligible probability. By this way we prove that f is one-way.

Next we show that g is not one-way. Because the first half of $f(x)$ is always $0^{n/2}$, we have $g(x) = f(f(x)) = 0^n$ for any x, so the adversary can output any value as the inverted value.

(b) $g'(x) = f(x)||f(f(x))$ one-way, we prove it by reduction. Assume there is a probabilistic polynomial-timeadversary $\mathcal{A}$ that $\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(1^n, g'(x)) \in g'^{-1}(g'(x))] = \epsilon(n)$, then we can construct $\mathcal{A}'$ to invert f. When $\mathcal{A}'$ receives a value $y \in \{0,1\}^n$, he computes $y||f(y)$ and send it to $\mathcal{A}$, finally ouputs the same with $\mathcal{A}$. The ouputs of $\mathcal{A}$ satisfies that $f(x')||f(f(x')) = f(x)||f(f(x))$, which indicates that $f(x') = f(x)$. So that there is:

$$
\begin{aligned}
&\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}'(1^n, f(x)) \in f^{-1}(f(x))] \\
=&\Pr_{x \xleftarrow{\$} \{0,1\}^n} [\mathcal{A}(1^n, g'(x)) \in g'^{-1}(g'(x))] \\
=&\epsilon(n)
\end{aligned}
$$

So g' is one-way.

作业讲解 IV - 3

Exercises 9.4(b)

(b) Let p, q be relatively prime. Show that $\phi(pq) = \phi(p) \cdot \phi(q)$. (You may use the Chinese remainder theorem.)

When p, q are relatively prime, the Chinese remainder theorem says $\mathbb{Z}_{pq}^*$ is isomorphic to $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Then we can get
$\phi(pq) = |\mathbb{Z}_{pq}^*| = |\mathbb{Z}_p^*| \cdot |\mathbb{Z}_q^*| = \phi(p) \cdot \phi(q)$.

We provide another solution that does not use the Chinese remainder theorem. Let p and q be relatively prime. Consider the integers $\{1, \cdots, pq\}$ arranged in an array as follows:

$$\begin{array}{llll} 1 & p+1 & \cdots & (q-1)p+1 \\ 2 & p+2 & \cdots & (q-1)p+2 \\ \vdots & \vdots & \ldots & \vdots \\ p & 2p & \cdots & qp \end{array}$$

For any r having a factor in common with p, every element in the row

$$r \quad p+r \quad \cdots \quad (q-1)p+r$$

has a factor in common with p and hence also has a factor in common with pq. Eliminate those rows from consideration, and consider the remaining $\phi(p)$ rows.

Let

$$s \quad p+s \quad \cdots \quad (q-1)p+s$$

be such a row (i.e., $\gcd(s,p)=1$).
We claim that

$$[s \bmod q] \quad [p+s \bmod q] \quad \cdots \quad [(q-1)p+s \bmod q]$$

is a permutation of $\mathbb{Z}_q$.
From this it follows that each remaining row contains exactly $\phi(q)$ elements relatively prime to q.
The leaves a total of $\phi(p)\phi(q)$ elements relatively prime to pq.

Exercises 9.11

9.11 This question concerns the group $\mathbb{Z}_{21}^*$.

(a) How many elements are in this group? List the elements.

(b) What is $\phi(21)$?

(c) Compute $[11^{-1} \bmod 21]$.

(d) Compute $\left[2^{2403} \bmod 21\right]$ (by hand).

(a) $\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}, |\mathbb{Z}_{21}^*| = 12.$

(b) $\phi(21) = \phi(3)\phi(7) = 2 * 6 = 12$

(c) By CRT we know $\mathbb{Z}_{21}^*$ is isomorphic to $\mathbb{Z}_3^* \times \mathbb{Z}_7^*$, so that $11 \leftrightarrow (11 \bmod 3, 11 \bmod 7) = (2, 4)$, and $[2^{-1} \bmod 3] = 2, [4^{-1} \bmod 7] = 2$. So $[11^{-1} \bmod 21] \leftrightarrow (2, 2) \leftrightarrow 2$.
Another way by using use the extended Euclidean algorithm to compute $11X + 21Y = 1 \bmod 21$, set $Y = -1$ and get $X = 2$, so $[11^{-1} \bmod 21] = 2$.

(d) By Fermat-Euler Theorem we know $a^{\phi(N)} = 1 \bmod N$. So that $2^{2403} \bmod 21 = 2^{2403 \bmod \phi(21)} \bmod 21 = 2^{2403 \bmod 12} \bmod 21 = 2^3 \bmod 21 = 8$.

Exercises 9.18

9.18 Fix N, e with $\gcd(e, \phi(N)) = 1$, and assume there is an adversary $\mathcal{A}$ running in time t for which

$$\Pr\left[\mathcal{A}\left([x^e \bmod N]\right) = x\right] = 0.01,$$

where the probability is taken over uniform choice of $x \in \mathbb{Z}_N^*$. Show that it is possible to construct an adversary $\mathcal{A}'$ for which

$$\Pr\left[\mathcal{A}'\left([x^e \bmod N]\right) = x\right] = 0.99$$

for *all* x. The running time t' of $\mathcal{A}'$ should be polynomial in t and $\|N\|$.

Hint: Use the fact that $y^{1/e} \cdot r = (y \cdot r^e)^{1/e} \bmod N$.

Solution: Let s be a parameter, fixed later. Construct $\mathcal{A}'$as follows:

On input N, y, e do:
for $i = 1$ *to* s **do**
  Chooser $i \leftarrow \mathbb{Z}_N^*$.
  Run $\mathcal{A}([(r_i)^e \cdot y \bmod N])$ to obtain x_i.
  If $(x_i)^e = (r_i)^e \cdot y \bmod N$ then output $[x_i/r_i \bmod N]$ and terminate.
end
If the algorithm has not yet terminated, output fail.

Algorithm 1: $\mathcal{A}'$

Let y be arbitrary. In every iteration, A is run on a uniform element of $\mathbb{Z}_N^*$, irrespective of how y is distributed. This is so since r_i is uniform, hence $[(r_i)^e \bmod N]$ is uniform (since raising to eth powers is a permutation), and thus $[(r_i)^e \cdot y \bmod N]$ is uniform.
Furthermore, if $\mathcal{A}$ ever correctly computes an eth root in any iteration, then $\mathcal{A}'$ outputs the eth root of y because $(x_i)^e = (r_i)^e \cdot y \bmod N$ implies $(x_i/r_i)^e = y \bmod N$.

Combining the observations above and setting $s = 100 \ln 100$, we seethat the probability that $\mathcal{A}'$ fails to output an inverse is

$$(1 - \frac{1}{100})^{100 \ln 100} = ((1 - \frac{1}{100})^{100})^{\ln 100} \leq e^{-\ln 100} = \frac{1}{100}$$

The running time of $\mathcal{A}'$ is $O(t \cdot poly(\|N\|))$

Exercises 11.4

11.4 Consider the following key-exchange protocol:

(a) Alice chooses uniform $k, r \in \{0,1\}^n$, and sends $s := k \oplus r$ to Bob.

(b) Bob chooses uniform $t \in \{0,1\}^n$, and sends $u := s \oplus t$ to Alice.

(c) Alice computes $w := u \oplus r$ and sends w to Bob.

(d) Alice outputs k and Bob outputs $w \oplus t$.

Show that Alice and Bob output the same key. Analyze the security of this protocol against a passive eavesdropper.

Solution: Alice ouputs k and Bob outputs $w \oplus t$.

$$w \oplus t = u \oplus r \oplus t = s \oplus t \oplus r \oplus t = s \oplus r = k \oplus r \oplus r = k$$

The scheme is not secure against a passive eavesdropper because if an adversary can get message (s, u, w) they exchanged, he can compute

$$s \oplus u \oplus w = s \oplus s \oplus t \oplus w = t \oplus w = k$$

to get the key they used.

The End