作业讲解 II

Anyi Cao

Nanjing University

Exercises 3.3

3.3 Say $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is such that for $k \in \{0,1\}^n$, algorithm Enc_k is only defined for messages of length at most $\ell(n)$ (for some polynomial ℓ). Construct a scheme satisfying Definition 3.8 even when the adversary is *not* restricted to outputting equal-length messages in $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$.

Solution:
Let Π =(Gen, Enc, Dec) be a scheme that is secure with respect to the original Definition 3.8 (for messages of equal length). Construct a scheme Π' =(Gen', Enc', Dec') as follows:
(a) Gen' is identical to Gen.
(b) Upon input a plaintext message m of length at most $l = l(n)$ (where n is the length of the key), Enc' first sets $m' := 0^{l-|m|}1||m$ and then encrypts m' using Enc. Note that m' is always exactly $l(n) + 1$ bits long.
(c) Dec' applies Dec to the ciphertext, and parses the result as $0^t1||m$ for $t \geq 0$. It outputs m. Next, we will show that the existence of an adversary breaking Π' with respect to the modified definition implies the existence of an adversary breaking Π with respect to Definition 3.8.

作业讲解 II - 1

Given an adversary $\mathcal{A}'$ who breaks Π',
$\Pr[PrivK^{eav}_{\mathcal{A}',\Pi'}(n) = 1] = \frac{1}{2} + \epsilon(n)$ where $\epsilon(n)$ is non-negligible.
We construct an adversary $\mathcal{A}$ to break Π by reduction.
When $\mathcal{A}'$ outputs a pair of plaintexts m_0, m_1, $\mathcal{A}$ pad them in the same of as Enc' would.
Then, it outputs the padded messages to be encrypted. Observe that $\mathcal{A}$ outputs equal-length messages, as required.
After getting c, $\mathcal{A}$ give the challenge ciphertext to $\mathcal{A}'$ and obtain output b'. Output 1 if $b' = 1$, and output 0 otherwise.
Thus, if $\mathcal{A}'$ can correctly guess b with probability non-negligibly greater than 1/2, then A guesses correctly with the same probability.
$\Pr[PrivK^{eav}_{\mathcal{A},\Pi}(n) = 1] = \Pr[PrivK^{eav}_{\mathcal{A}',\Pi'}(n) = 1] = \frac{1}{2} + \epsilon(n)$,
which contradicts with Π is secure.

Exercises 3.4

Prove the equivalence of Definition 3.8 and Definition 3.9.

DEFINITION 3.8 *A private-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *has* indistinguishable encryptions in the presence of an eavesdropper, *or is* EAV-secure, *if for all probabilistic polynomial-time adversaries* $\mathcal{A}$ *there is a negligible function* negl *such that, for all* n,

$$\Pr\left[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n).$$

The probability above is taken over the randomness used by $\mathcal{A}$ *and the randomness used in the experiment (for choosing the key and the bit* b*, as well as any randomness used by* Enc*).*

DEFINITION 3.9 *A private-key encryption scheme* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *has* indistinguishable encryptions in the presence of an eavesdropper *if for all* PPT *adversaries* $\mathcal{A}$ *there is a negligible function* negl *such that*

$$\left|\Pr[\mathsf{out}_{\mathcal{A}}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,0)) = 1] - \Pr[\mathsf{out}_{\mathcal{A}}(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n,1)) = 1]\right| \leq \mathsf{negl}(n).$$

$$
\begin{aligned}
&\Pr[PrivK^{eav}_{\mathcal{A},\Pi}(n)=1]=\Pr[out_{\mathcal{A}}(PrivK^{eav}_{\mathcal{A},\Pi}(n,b))=b]\\
=&\frac{1}{2}(\Pr[out_{\mathcal{A}}(PrivK^{eav}_{\mathcal{A},\Pi}(n,0))=0]+\Pr[out_{\mathcal{A}}(PrivK^{eav}_{\mathcal{A},\Pi}(n,1))=1])\\
=&\frac{1}{2}+\frac{1}{2}(\Pr[out_{\mathcal{A}}(PrivK^{eav}_{\mathcal{A},\Pi}(n,1))=1]-\Pr[out_{\mathcal{A}}(PrivK^{eav}_{\mathcal{A},\Pi}(n,0))=1])\\
=&\frac{1}{2}+\frac{1}{2}\epsilon(n)
\end{aligned}
$$

Let $\Pr[out_{\mathcal{A}}(PrivK^{eav}_{\mathcal{A},\Pi}(n,1))=1]-\Pr[out_{\mathcal{A}}(PrivK^{eav}_{\mathcal{A},\Pi}(n,0))=1]=\epsilon(n)$.
If Π satisfies definition 3.9, then $\epsilon(n)\leq negl(n)$, so
$\Pr[PrivK^{eav}_{\mathcal{A},\Pi}(n)=1]\leq\frac{1}{2}+\frac{1}{2}negl(n)$, which satisfies definition 3.8.

作业讲解 II - 2

If Π satisfies definition 3.8, then $\frac{1}{2} + \frac{1}{2}\epsilon(n) \leq \frac{1}{2} + negl(n)$, $\epsilon(n) \leq 2negl(n)$. We can construct $\mathcal{A}'$ that outputs the complement of $\mathcal{A}$, so

$$\begin{aligned}\Pr[PrivK^{eav}_{\mathcal{A}',\Pi}(n) = 1] =& 1 - \Pr[PrivK^{eav}_{\mathcal{A}',\Pi}(n) = 1] \\ =& \frac{1}{2} - \frac{1}{2}\epsilon(n)\end{aligned}$$

Therefore $-\epsilon(n) \leq 2negl(n)$.
So $|\Pr[out_{\mathcal{A}}(PrivK^{eav}_{\mathcal{A},\Pi}(n,1)) = 1] - \Pr[out_{\mathcal{A}}(PrivK^{eav}_{\mathcal{A},\Pi}(n,0)) = 1]| \leq \max\{\epsilon(n), -\epsilon(n)\} \leq 2negl(n) = negl'(n)$, which satisfies definition 3.9

Exercises 3.6

3.6 Let G be a pseudorandom generator. In each of the following cases, say whether G' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample.

(a) Define $G'(s) \stackrel{\text{def}}{=} G(\bar{s})$, where $\bar{s}$ is the complement of s.

(b) Define $G'(s) \stackrel{\text{def}}{=} \overline{G(s)}$.

(c) Define $G'(s) \stackrel{\text{def}}{=} G\left(0^{|s|} \| s\right)$.

(d) Define $G'(s) \stackrel{\text{def}}{=} G(s) \,\|\, G(s+1)$.

(a) Define $G'(s) \stackrel{\text{def}}{=} G(\bar{s})$, where $\bar{s}$ is the complement of s.

(b) Define $G'(s) \stackrel{\text{def}}{=} \overline{G(s)}$.

Lemma: If r is a uniformly random number, then $\bar{r}$ is also a uniformly random number.

(a) Yes, since $\bar{r}$ is also a random number, and the outputs of G using a random number as seed is pseudorandom.

(b) Yes, otherwise we can construct D using D' to distinguish $G(s)$ from r: when D receive a number t, it computes $\bar{t}$ and run D', outputs the same value with D'. Obviously we have $\Pr[D(G(s)) = 1] = \Pr[D'(G'(s)) = 1]$, $\Pr[D(r) = 1] = \Pr[D'(\bar{r}) = 1]$ (since $\bar{r}$ is also a uniformly random number). So if G is a PRG, then G' is also a PRG.

(c) Define $G'(s) \stackrel{\text{def}}{=} G\left(0^{|s|} \| s\right)$.

(d) Define $G'(s) \stackrel{\text{def}}{=} G(s) \| G(s+1)$.

Lemma: If G is a PRG with expanding factor $l(n) = kn$, then $G'(s) = G(s_{[1,m]}), m > n/k$ is also a PRG, where k is a constant and $s_{[1,m]}$ means the first m bits of s.

Explain: If s is a uniformly random value in $\{0,1\}^n$ then $s_{[1,m]}$ is also uniformly random in $\{0,1\}^m$ and the expanding factor of G' is $l'(n) = km > n$.

(c) No, we substitute G with $G''(s) = G(s_{[1,n/2]})$ and get $G'(s) = G''(0^{|s|}||s) = G(0^{|s|})$, which is a constant.

(d) No, we substitute G with $G''(s) = G(s_{[1,n-1]})$ and get $G'(s) = G''(s)||G''(s+1)$. If $s[n] = 0$ then $s_{[1,n-1]} = (s+1)_{[1,n-1]}$, and $G''(s) = G''(s+1)$.

Exercises 3.11

3.11 Let F be a length preserving pseudorandom function. For the following constructions of a keyed function $F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n}$, state whether F' is a pseudorandom function. If yes, prove it; if not, show an attack.

(a) $F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(0\|x)$.

(b) $F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(1\|x)$.

(c) $F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(x\|0)$.

(d) $F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(x\|1)$.

作业讲解 II - 4

$$\text{(a)}\ \ F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(0\|x).$$

(a) No. Because the first half is the same with the second hald, we can construct a distinguisher D that $D(r) = 1$ if $r_{[1,n]} = r_{[n+1,2n]}$.

(b) $F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(1\|x)$.

(b) Yes. We prove it by reduction.

Assume $F'_k(x)$ is not a PRF, i.e. there exists a PPT distinguisher D' can distinguish F'_k from a random function $f' : \{0,1\}^{n-1} \to \{0,1\}^{2n}$, that $|\Pr[D'^{F'_k(\cdot)}(1^{n-1}) = 1] - \Pr[D'^{f'(\cdot)}(1^{n-1}) = 1]| = \delta(n)$, where $\delta(n)$ is a non-negligible function. Then we can construct a distinguisher D by D' which can distinguish F_k from $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$.

D has access to the oracle $\mathcal{O}$ and simulates what D' does, i.e. when D' want to query x, D query $0||x, 1||x$ and get $\mathcal{O}(0||x), \mathcal{O}(1||x)$, then concat the result $\mathcal{O}(0||x)||\mathcal{O}(1||x)$ as the result of D''s query. Finally, D outputs the same as D'.

When D's oracle is F_k, the results of queries are the same with D', so we have

$$\Pr[D^{F_k(\cdot)}(1^{2n}) = 1] = \Pr[D'^{F'_k(\cdot)}(1^{n-1}) = 1]$$

When D's oracle is f, the answer of x is $f(0||x)||f(1||x)$. Suppose $q(n)$ is a polynomial bound of query. When D' is given an oracle f, the result of queries is $f'(x_1), f'(x_2), ..., f'(x_{q(n)})$. In the simulation of D, the results of queries is $f(0||x_1)||f(1||x_1), f(0||x_2)||f(1||x_2), ..., f(0||x_{q(n)})||f(1||x_{q(n)})$. Note that $x_i \neq x_j$ implies $(0||x_i) \neq (0||x_j)$ and $(0||x_i) \neq (1||x_j)$, the query is $2q(n)$ different points on f, so the distribution of probability is the same with D'.

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

So we have

$$\begin{aligned}
&|\Pr[D^{F_k(\cdot)}(1^{2n}) = 1] - \Pr[D^{f(\cdot)}(1^{2n}) = 1]| \\
=&|\Pr[D'^{F'_k(\cdot)}(1^{n-1}) = 1] - \Pr[D'^{f'(\cdot)}(1^{n-1}) = 1]| \\
=&\delta(n)
\end{aligned}$$

which contradict with that F_k is PRF. So F'_k is PRF.

(c) $F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(x\|0)$.

(d) $F'_k(x) \stackrel{\text{def}}{=} F_k(0\|x) \,\|\, F_k(x\|1)$.

(c) No. Query $x = 0^{n-1}$ and if the oracle is F' it will get $F_k(0^n)||F_k(0^n)$.

(d) No. Query $x_1 = 0^{n-1}$ and $x_2 = 0^{n-2}1$. If the oracle is F', it will get $y_1 = F_k(0^n)||F_k(0^{n-1}1)$ and $y_2 = F_k(0^{n-1}1)||F_k(0^{n-2}11)$, that the second half of y_1 is the same as the first half of y_2.

Exercises 3.20

3.20 Let F be a length preserving pseudorandom function and G be a pseudorandom generator with expansion factor $\ell(n) = n+1$. For each of the following encryption schemes, state whether the scheme is EAV-secure and whether it is CPA-secure. (In each case, the shared key is a uniform $k \in \{0,1\}^n$.) Explain your answer in each case.

(a) To encrypt $m \in \{0,1\}^{n+1}$, choose uniform $r \in \{0,1\}^n$ and output the ciphertext $\langle r, G(r) \oplus m \rangle$.

(b) To encrypt $m \in \{0,1\}^n$, output the ciphertext $m \oplus F_k(0^n)$.

(c) To encrypt $m \in \{0,1\}^{2n}$, parse m as $m_1 \| m_2$ with $|m_1| = |m_2|$, then choose uniform $r \in \{0,1\}^n$ and send $\langle r, m_1 \oplus F_k(r), m_2 \oplus F_k(r+1) \rangle$.

(a) No. The ciphertext in this scheme doesn't depend on a key k and everyone can access to G, so everyone can decrypt the cipertext.

(b) The scheme has indistinguishable encryption in the presence of an eavesdropper, according to the indistinguishablity between PRF F_k and a random function f. But it is not CPA-secure because there's no randomness, adversary can compute $F_k(0^n) = c \oplus m$.

(c) The scheme is CPA-secure. The proof is the extension of the proof of Theorem 3.31 by query r and $r+1$ together. Assume in one query the adversary get $< u, F_k(u), F_k(u+1) >$, the condition that the adversary can get a non-negligible advantage is that $u \in \{r-1, r, r+1\}$. So by $q(n)$ query the adversary can succeed with probability less then $\frac{1}{2} + \frac{3q(n)}{2^n}$.

Exercises 3.19

3.19 Let F be a pseudorandom permutation, and define a fixed-length encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ as follows: On input a key $k \in \{0,1\}^n$ and message $m \in \{0,1\}^{n/2}$, algorithm Enc chooses a uniform string $r \in \{0,1\}^{n/2}$ and computes $c := F_k(r\|m)$.

Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $n/2$.

Dec: compute $F_k^{-1}(c)$ and output the second half.

Next we prove it is CPA-secure. We first introduce a scheme Π' using a truly random permutation instead of a pseudorandom permutation and prove Π' is CPA-secure. The proof is similar to the proof of Theorem 3.31. When adversary receive, he makes $q(n)$ queries for $m_1, m_2, \ldots, m_{q(n)}$. If $m_i \neq m$ then $r_i||m_i \neq r||m$, and the adversary get nothing since the result of query $r_i||m_i$ is a randomly value. If $m_i = m$, the adversary can get information only when $r_i = r$, in the condition he can win the game and the probability it happening is $\frac{1}{2^{n/2}}$. So the probability upper bound of adversary win the game is $\frac{1}{2} + \frac{q(n)}{2^{n/2}}$ when the adversary queries m for $q(n)$ times, which shows that Π' is CPA-secure.

So Π is CPA-secure, otherwise we can find a distinguisher to distinguish F_k with a truly random permutation f.

The End