作业讲解 I

Anyi Cao

Nanjing University

作业讲解 I - 1

Exercises 2.1

Prove that, by redefining the key space, we may assume that the key-generation algorithm *Gen* chooses a uniform key from the key space, without changeing $\Pr[C = c|M = m]$ for any m, c.
Hint: Define the key space to be the set of all possible random bits used by the randomized algorith *Gen*.

Suppose *Gen* take a random seed $r \overset{\$}{\leftarrow} R$ as input, i.e $Gen(r) = k$, so we have scheme as follow:
Gen: $r \overset{\$}{\leftarrow} R$, $Gen(r) = k$, output k.
Enc: Output $c = Enc_k(m)$.
Dec: Output $m = Dec_k(c)$.

作业讲解 I - 1

Consider taking Gen and Enc as a new algorithm Enc' and the random seed r as Enc''s key, i.e. $Enc'_r(m) = c$.
Formally, we can define a scheme **(Gen', Enc' Dec')** as follow:

Gen': Output $r \xleftarrow{\$} R$.
Enc': $Gen(r) = k$, output $c = Enc_k(m)$.
Dec': $Gen(r) = k$, output $m = Dec_k(c)$.
Now the key of encryption scheme is chosen uniformly from R without changing $\Pr[C = c|M = m]$.

Exercises 2.3

Prove or refute: An encryption scheme with message space $\mathcal{M}$ is perfectly secret if and only if for every probability distribution over $\mathcal{M}$ and every $c_0, c_1 \in \mathcal{C}$ we have $\Pr[C = c_0] = \Pr[C = c_1]$.

Refute: For "only if" direction, we now give a counterexample of a perfectly secret scheme, where above condition does not hold.

1. $\mathcal{M} = \{0,1\}^1$, $\mathcal{K} = \{0,1\}^2$, $\mathcal{C} = \{0,1\}^2$.
2. **Gen:** $\Pr[K = 00] = \Pr[K = 10] = 1/6$ and $\Pr[K = 01] = \Pr[K = 11] = 1/3$.
3. **Enc**$_K$(M): $C = (M \oplus K[0])||K[1]$
4. **Dec**$_K$(C): $M = C[0] \oplus K[0]$

	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{3}$
K / M	00	01	10	11
0	00	01	10	11
1	10	11	00	01

作业讲解 I - 2

This encryption scheme is simply an extension to The One-Time Pad. For every c $\in \mathcal{C}$, we have $\Pr[C = c|M = 0] = \Pr[C = c|M = 1]$. For example, when c $= 00$, $\Pr[C = 00|M = 0] = \Pr[C = 00|M = 1] = 1/6$. Therefore, this scheme is perfectly secret.

However,
the ciphertext distribution is clearly not uniform.
$\Pr[C = 00] = 1/6$, while $\Pr[C = 01] = 1/3$
This contradicts the condition given in the exercise.

	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{3}$
M \ K	00	01	10	11
0	00	01	10	11
1	10	11	00	01

Proof Lemma 2.6

LEMMA 2.6 Encryption scheme Π is perfectly secret if and only if it is perfectly indistinguishable.

Proof:

"$\Rightarrow$": Assume Π is perfectly secret. Then for every $m_0, m_1 \in \mathcal{M}$ and every $c \in \mathcal{C}$, $\Pr[C = c|M = m_0] = \Pr[C = c|M = m_1]$.

We have:

$$
\begin{aligned}
& \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \\
= \; & \Pr[b = 0] \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1|b = 0] + \Pr[b = 1] \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1|b = 1] \\
= \; & \Pr[b = 0] \Pr[\mathcal{A} \textit{ outputs } 0|b = 0] + \Pr[b = 1] \Pr[\mathcal{A} \textit{ outputs } 1|b = 1] \\
= \; & \Pr[M = m_0] \Pr[\mathcal{A} \textit{ outputs } 0|M = m_0] + \Pr[M = m_1] \Pr[\mathcal{A} \textit{ outputs } 1|M = m_1] \\
= \; & \Pr[M = m_0] \sum_{c \in C} \Pr[C = c|M = m_0] \Pr[\mathcal{A} \textit{ outputs } 0|C = c] \\
& + \Pr[M = m_1] \sum_{c \in C} \Pr[C = c|M = m_1] \Pr[\mathcal{A} \textit{ outputs } 1|C = c]
\end{aligned}
$$

Meanwhile,

$$
\begin{aligned}
& \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 0] \\
= \ & \Pr[b=0]\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 0 | b=0] + \Pr[b=1]\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 0 | b=1] \\
= \ & \Pr[b=0]\Pr[\mathcal{A} \ outputs \ 1 | b=0] + \Pr[b=1]\Pr[\mathcal{A} \ outputs \ 0 | b=1] \\
= \ & \Pr[M=m_0]\sum_{c\in C}\Pr[C=c|M=m_0]\Pr[\mathcal{A} \ outputs \ 1 | C=c] \\
& + \Pr[M=m_1]\sum_{c\in C}\Pr[C=c|M=m_1]\Pr[\mathcal{A} \ outputs \ 0 | C=c] \\
= \ & \Pr[M=m_1]\sum_{c\in C}\Pr[C=c|M=m_1]\Pr[\mathcal{A} \ outputs \ 1 | C=c] \\
& + \Pr[M=m_0]\sum_{c\in C}\Pr[C=c|M=m_0]\Pr[\mathcal{A} \ outputs \ 0 | C=c] \\
= \ & \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] = 1/2.
\end{aligned}
$$

Therefore, Π is perfectly indistinguishable.

作业讲解 I - 3

Another way

- Divide C into C_0 and C_1, s.t. $C_0 \cup C_1 = C$ and $C_0 \cap C_1 = \emptyset$
- Adversary outputs 0 if he received $c \in C_0$, and 1 if $c \in C_1$

$$
\begin{aligned}
& \sum_{c \in C} \Pr[C = c | M = m_0] \Pr[\mathcal{A} \textit{ outputs } 0 | C = c] \\
= & \sum_{c \in C_0} \Pr[C = c | M = m_0] \Pr[\mathcal{A} \textit{ outputs } 0 | C = c] \\
& + \sum_{c \in C_1} \Pr[C = c | M = m_0] \Pr[\mathcal{A} \textit{ outputs } 0 | C = c] \\
= & \sum_{c \in C_0} \Pr[C = c | M = m_0] * 1 + \sum_{c \in C_1} \Pr[C = c | M = m_0] * 0 \\
= & \sum_{c \in C_0} \Pr[C = c | M = m_0]
\end{aligned}
$$

So we have,

$$
\begin{aligned}
& \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \\
= \ & \Pr[M = m_0] \sum_{c \in C} \Pr[C = c | M = m_0] \Pr[\mathcal{A} \ outputs \ 0 | C = c] \\
& + \Pr[M = m_1] \sum_{c \in C} \Pr[C = c | M = m_1] \Pr[\mathcal{A} \ outputs \ 1 | C = c] \\
= \ & 1/2 (\sum_{c \in C_0} \Pr[C = c | M = m_0] + \sum_{c \in C_1} \Pr[C = c | M = m_1]) \\
= \ & 1/2 (\sum_{c \in C_0} \Pr[C = c | M = m_0] + \sum_{c \in C_1} \Pr[C = c | M = m_0]) \\
= \ & 1/2 (\sum_{c \in C} \Pr[C = c | M = m_0]) \\
= \ & 1/2
\end{aligned}
$$

Proof: "$\Leftarrow$": We try to prove the contrapositive of it.
Assume Π is not perfectly secret. There are $m'_0, m'_1 \in M$ and $c' \in C$ that $\Pr[C = c' | M = m'_0] \neq \Pr[C = c' | M = m'_1]$.
We construct an adversary $\mathcal{A}$ for which $\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \neq 1/2$.

1. Choose $m_0 = m'_0$ and $m_1 = m'_1$
2. Upon receiving the challenge ciphertext c, output $b = 0$ if $c = c'$, and randomly outputs 0 or 1 otherwise.

Now,

$$\begin{aligned}
& \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \\
= \ & \Pr[b = 0] \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1 | b = 0] + \Pr[b = 1] \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1 | b = 1] \\
= \ & \Pr[b = 0] \Pr[\mathcal{A} \ outputs \ 0 | b = 0] + \Pr[b = 1] \Pr[\mathcal{A} \ outputs \ 1 | b = 1]
\end{aligned} \tag{1}$$

In addition,

$$
\begin{aligned}
& \Pr[\mathcal{A}\ outputs\ 0|b=0] \\
= & \Pr[C=c'|b=0]\Pr[\mathcal{A}\ outputs\ 0|b=0 \wedge C=c'] \\
& + \Pr[C \neq c'|b=0]\Pr[\mathcal{A}\ outputs\ 0|b=0 \wedge C \neq c'] \\
= & \Pr[C=c'|b=0] + 1/2\Pr[C \neq c'|b=0] \\
= & \Pr[C=c'|M=m_0'] + 1/2\Pr[C \neq c'|M=m_0']
\end{aligned} \tag{2}
$$

$$
\begin{aligned}
& \Pr[\mathcal{A}\ outputs\ 1|b=1] \\
= & \Pr[C=c'|b=1]\Pr[\mathcal{A}\ outputs\ 1|b=1 \wedge C=c'] \\
& + \Pr[C \neq c'|b=1]\Pr[\mathcal{A}\ outputs\ 1|b=1 \wedge C \neq c'] \\
= & 1/2\Pr[C \neq c'|b=1] \\
= & 1/2\Pr[C \neq c'|M=m_1']
\end{aligned} \tag{3}
$$

作业讲解 I - 3

Then substitute (2) and (3) into (1).

$$
\begin{aligned}
&\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \\
= {}& 1/2(\Pr[C = c' | M = m'_0] + 1/2 \Pr[C \neq c' | M = m'_0]) \\
&+ 1/2(1/2 \Pr[C \neq c' | M = m'_1]) \\
= {}& 1/2 \Pr[C = c' | M = m'_0] + 1/4(1 - \Pr[C = c' | M = m'_0]) \\
&+ 1/4(1 - \Pr[C = c' | M = m'_1]) \\
= {}& 1/2 + 1/4(\Pr[C = c' | M = m'_0] - \Pr[C = c' | M = m'_1]) \\
\neq {}& 1/2
\end{aligned}
$$

Therefore, Π is not perfectly indistinguishable.

In conclusion, the lemma is correct. □

Exercises 2.10

2.10 The following questions concern the message space $\mathcal{M} = \{0,1\}^{\leq \ell}$, the set of all nonempty binary strings of length at most ℓ.

(a) Consider the encryption scheme in which Gen chooses a uniform key from $\mathcal{K} = \{0,1\}^{\ell}$, and $\mathsf{Enc}_k(m)$ outputs $k_{|m|} \oplus m$, where k_t denotes the first t bits of k. Show that this scheme is not perfectly secret for message space $\mathcal{M}$.

(b) Design a perfectly secret encryption scheme for message space $\mathcal{M}$.

(a)
There are messages with different length in the message space M and this scheme don't protect this information.
The adversary can choose message $m_0 = 000, m_1 = 0001$ and output 0 if $|c| = 3$ and 1 if $|c| = 4$.
Obviously $\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] = 1$.
(b)
We can design a scheme that Gen' chooses a unifrom key from $K = \{0,1\}^{l+1}$, and $Enc'_k(m)$ first compute $m' = m||1||0^{l-|m|}$ and outputs $k \oplus m'$, and $Dec'_k(c)$ compute $m' = k \oplus c$ and remove all of 0 and the first 1 from tail and get m.

Exercises 2.18(a)(b)

2.18 Let $\varepsilon > 0$ be a constant. Say an encryption scheme is *ε-perfectly secret* if for every adversary $\mathcal{A}$ it holds that

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

(Compare to Definition 2.6.) Consider a variant of the one-time pad where $\mathcal{M} = \{0,1\}^\ell$ and the key is chosen uniformly from an arbitrary set $\mathcal{K} \subseteq \{0,1\}^\ell$ with $|\mathcal{K}| = (1-\varepsilon)\cdot 2^\ell$; encryption and decryption are otherwise the same.

(a) Prove that this scheme is ε-perfectly secret.

(b) Prove that this scheme is $\left(\frac{\varepsilon}{2(1-\varepsilon)}\right)$-perfectly secret when $\varepsilon \leq 1/2$. (Note that $\frac{\varepsilon}{2(1-\varepsilon)} \leq \varepsilon$ here, so this is an improvement over part (a).)

$$
\begin{aligned}
& \Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \\
= & \Pr[b=0]\Pr[\mathcal{A}\ outputs\ 0|b=0] + \Pr[b=1]\Pr[\mathcal{A}\ outputs\ 1|b=1] \\
= & \frac{1}{2}(\Pr[\mathcal{A}\ outputs\ 0|M=m_0] + \Pr[M=m_1]\Pr[\mathcal{A}\ outputs\ 1|M=m_1]) \\
= & \frac{1}{2}(\sum_{c\in C}\Pr[C=c|M=m_0]\Pr[\mathcal{A}\ outputs\ 0|C=c] \\
& + \sum_{c\in C}\Pr[C=c|M=m_1]\Pr[\mathcal{A}\ outputs\ 1|C=c])
\end{aligned}
$$

作业讲解 I - 5

Let $C_0(C_1)$ denote the ciphertext space of $m_0(m_1)$. Let $S = C_0 \cap C_1$ and $|S| = \delta|M|$. The best adversary will outputs $0(1)$ when $c \in C_0 - S(C_1 - S)$ and randomly outputs when $c \in S$.

$$\begin{aligned}
&\sum_{c \in C} \Pr[C = c | M = m_0] \Pr[\mathcal{A} \text{ outputs } 0 | C = c] \\
= &\sum_{c \in C_0 - S} \Pr[C = c | M = m_0] \Pr[\mathcal{A} \text{ outputs } 0 | C = c] \\
&+ \sum_{c \in S} \Pr[C = c | M = m_0] \Pr[\mathcal{A} \text{ outputs } 0 | C = c] \\
= &\sum_{c \in C_0 - S} \Pr[C = c | M = m_0] + \sum_{c \in S} \frac{1}{2} \Pr[C = c | M = m_0] \\
= &\frac{(1 - \epsilon - \delta)|M|}{(1 - \epsilon)|M|} + \frac{1}{2} \frac{(\delta)|M|}{(1 - \epsilon)|M|} \\
= &\frac{2 - 2\epsilon - \delta}{2(1 - \epsilon)}
\end{aligned}$$

作业讲解 I - 5

The same holds on for $\sum_{c \in C} \Pr[C = c | M = m_1] \Pr[\mathcal{A} \textit{ outputs } 1 | C = c]$, so we have

$$\begin{aligned}
&\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \\
= &\frac{1}{2}(\sum_{c \in C} \Pr[C = c | M = m_0] \Pr[\mathcal{A} \textit{ outputs } 0 | C = c] \\
&+ \sum_{c \in C} \Pr[C = c | M = m_1] \Pr[\mathcal{A} \textit{ outputs } 1 | C = c]) \\
= &\frac{1}{2}(\frac{2 - 2\epsilon - \delta}{2(1 - \epsilon)} + \frac{2 - 2\epsilon - \delta}{2(1 - \epsilon)}) \\
= &\frac{2 - 2\epsilon - \delta}{2(1 - \epsilon)}
\end{aligned}$$

So the smaller δ, the probability of adversary win higher. And $\delta \geq 2(1 - \epsilon) - 1 = 1 - 2\epsilon$.
So $\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \leq \frac{2 - 2\epsilon - 1 + 2\epsilon}{2(1 - \epsilon)} = \frac{1}{2(1 - \epsilon)} = \frac{1}{2} + \frac{\epsilon}{2(1 - \epsilon)}$

Exercises 2.18(c)

(c) Prove that any deterministic scheme that is ε-perfectly secret must have $|\mathcal{K}| \geq (1-2\varepsilon) \cdot |\mathcal{M}|$. (Note: It is an open question to prove a tight lower bound that also holds for randomized schemes.)

作业讲解 I - 5

Let $|K| = (1-\alpha)|M|$ and we want to prove $(1-\alpha) \geq (1-2\epsilon)$ if $\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \leq \frac{1}{2} + \epsilon$. And we try to prove the contrapositive of it that if $(1-\alpha) < (1-2\epsilon)$ then for every encryption shceme Π, there exists a PPT adversary A' that $\Pr[Privk^{eav}_{\mathcal{A}',\Pi} = 1] > \frac{1}{2} + \epsilon$.

For briefly we write $n = |M|$.Without loss of generality we can choose m_0 randomly and fix C_0. We denote $|C_0| = (1-\beta)n$ that $1-\beta \leq 1-\alpha$.

Now we consider the "number of ciphertexts without considering repeation", denote as γ. Formally for a ciphertext c, $\gamma(c) = |\{(m,k)|Enc_k(m) = c\}|$.

For the correctness of decryption there are at most $(1-\alpha)n$ messages can be encrypted to one ciphertext, i.e. $\gamma(c) \leq (1-\alpha)n$, so $\gamma(C_0) = \sum_{c \in C_0} \gamma(c) \leq (1-\alpha)(1-\beta)n^2$.

Let $\{m_1, m_2, ..., m_{n-1}\} = M - \{m_0\}$ and let
$\delta_i \cdot n = |\{k | Enc_k(m_i) \in C_i \cap C_0\}|$, $\sum_{c \in C_i \cap C_0} \Pr[C = c | M = m_i] = \frac{\delta_i}{1-\alpha}$.

Then $\gamma(C_0)$ is greater than or equal to the results that adding up all of $\delta_i \cdot n$ and plusing the size of C_0, i.e. $\gamma(C_0) \geq (1-\beta)n + \sum_{i=1}^{n-1} \delta_i \cdot n$.

$\sum_{i=1}^{n-1} \delta_i \cdot n \leq \gamma(C_0) - (1-\beta)n \leq (1-\alpha)(1-\beta)n^2 - (1-\beta)n < (1-\alpha)(1-\beta)(n^2 - n)$.

$(n-1)\delta_{\min} \leq \sum_{i=1}^{n-1} \delta_i < (1-\alpha)(1-\beta)(n-1)$.

So there exists m_j that $\delta_j = \delta_{\min} < (1-\alpha)(1-\beta)$, let m_j be another message.

For $c \in C_0 \cap C_j$, adversary guess 0 if $\Pr[C = c|M = m_0] \geq \Pr[C = c|M = m_j]$ and 1 otherwise.

Notice that $\sum_{c \in C_i \cap C_0} \Pr[C = c|M = m_i] = \frac{\delta_i}{1-\alpha}$, and similarly we difine $\sum_{c \in C_i \cap C_0} \Pr[C = c|M = m_0] = \frac{\delta_0}{1-\alpha}$.

$$
\begin{aligned}
& \Pr[C = c|M = m_0] \Pr[\mathcal{A} \ \mathit{outputs} \ 0|C = c] \\
& + \Pr[C = c|M = m_j] \Pr[\mathcal{A} \ \mathit{outputs} \ 1|C = c] \\
= \ & \max\{\Pr[C = c|M = m_0], \Pr[C = c|M = m_j]\}
\end{aligned}
$$

$$
\begin{aligned}
& \sum_{c \in C_0 \cap C_j} (\Pr[C = c|M = m_0] \Pr[\mathcal{A} \ \mathit{outputs} \ 0|C = c] \\
+ \ & \Pr[C = c|M = m_j] \Pr[\mathcal{A} \ \mathit{outputs} \ 1|C = c]) \\
\geq \ & \frac{\max\{\delta_0, \delta_j\}}{1 - \alpha}
\end{aligned}
$$

作业讲解 I - 5

$$
\begin{aligned}
&\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] \\
&= \frac{1}{2}(\sum_{c\in C} \Pr[C = c|M = m_0] \Pr[\mathcal{A}\ outputs\ 0|C = c] \\
&\quad + \sum_{c\in C} \Pr[C = c|M = m_1] \Pr[\mathcal{A}\ outputs\ 1|C = c]) \\
&\geq \frac{1}{2}(\frac{1-\alpha-\delta_0}{1-\alpha} + \frac{1-\alpha-\delta_j}{1-\alpha} + \frac{\max\{\delta_0,\delta_j\}}{1-\alpha}) \\
&= \frac{1}{2}(2 - \frac{\min\{\delta_0,\delta_j\}}{1-\alpha}) > \ 1 - \frac{(1-\alpha)(1-\beta)}{2(1-\alpha)} \\
&= 1 - \frac{1-\beta}{2} > \ 1 - \frac{1-\alpha}{2} \\
&> 1 - \frac{1-2\epsilon}{2} = \ \frac{1}{2} + \epsilon
\end{aligned}
$$

So if $(1-\alpha) < (1-2\epsilon)$, we can always find messages m_0, m_j making $\Pr[Privk^{eav}_{\mathcal{A},\Pi} = 1] > \frac{1}{2} + \epsilon$.

The End