# Homework - 1

September 15, 2022

**Notations used:**

- $y_b$ denotes the text the verifier chooses
- $b\!=\!0$ means that the verifier or challenger chose random text
- $b\!=\!1$ means that the verifier or challenger chose pseudo random text
- $b'\!=\!0$ means that the adversary says it is random
- $b'\!=\!1$ means that the adversary says it is pseudo random
- $PRGExp_1[A,G]$ is the experiment where adversary is sent pseudo random text
- $PRGExp_0[A,G]$ is the experiment where adversary is sent random text

**Lemma used (which is not in the book):**

- Closure property of Computational Indistinguishability
  - If we apply an efficient operation on distributions $X$ and $Y$, they remain computationally indistinguishable. i.e.$\forall$non uniform PPT $M$

    $X_n \approx Y_n \implies M(X_n) \approx M(Y_n)$

    Informal proof - Assume that there is an adversary $A'$which distinguishes $M(X_n)$ and $M(Y_n)$ with non-negligible probability, then we can construct an adversary $A$ which distinguishes $X_n$ ad $Y_n$. The adversary $A$ works by taking the $t_b$ given by the verifier where $t_b$ can either belong to $X_n$ or $Y_n$ distribution, applying the PPT algorithm on it, passing $M(t_b)$ to adversary $A'$ and returning whatever $A'$ outputs.

Reference - `https://www3.cs.stonybrook.edu/~omkant/S07.pdf`

1. **Question 1**
   (a) Yes it is perfectly secure, Let $\mathcal{M},\mathcal{C},\mathcal{K}$ be the message space, cipher text space and key space respectively where $\mathcal{M},\mathcal{C} \in \{0,1\}^n, \mathcal{K} \in \{0,1\}^{2n}$. It is given that

   $$Enc_k(m) = m \oplus k1 \oplus k2$$
   $$Dec_k(c) = c \oplus k1 \oplus k2$$

   Proof

   $$P\left(\frac{\mathbf{C}=c}{\mathbf{M}=m0}\right)$$
   $$= P(\mathbf{K1} \oplus \mathbf{K2} = c \oplus m0)$$
   $$= P(\mathbf{K1} \oplus \mathbf{K2} = z), \text{ Let } z = c \oplus m0$$
   $$= \prod_{i=1}^{n} P(\mathbf{K1}_i \oplus \mathbf{K2}_i = z_i)$$

   where $K1_i, K2_i$ and $z_i$ are the ith bits

   $$= \frac{1}{2^n} \text{ as K1 and K2 are chosen randomly and}$$
   $$P[K1_i \oplus K2_i = 1] = P[K1_i \oplus K2_i = 0] = \frac{1}{2}$$

   please see Table:1

   This proves that $P\left(\frac{\mathbf{C}=c}{\mathbf{M}=m}\right)$ is same for all $m \in \mathcal{M}$

| $K1_i$ | $K2_i$ | $K2_i \oplus K1_i$ |
|---|---|---|
| 1 | 1 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

Table 1: XOR of $K1_i$ and $K2_i$

(b) No it is still secure, It is equivalent to a one time pad with key $0^n$ and its probability of choosing such a key is

$$P[K1=K2]$$
$$=\prod_{i=1}^{n}\frac{1}{2}$$
$$=\frac{1}{2^n}$$

We cannot guess the message as $P(\frac{\mathbf{C}=m}{\mathbf{M}=m'})$is same for all messages $m'$

(c) No it is not perfectly secure.Given $K1=k'$ and $K2=k'\oplus\alpha. \Longrightarrow K1\oplus K2=\alpha$

We will choose $m0=\bar{\alpha}$ , $m1=\alpha$ and $c=0^{\alpha}$

$$P[\frac{C=c}{M=m1}]$$
$$=P[K=c\oplus m1]$$
$$=P[K=\alpha]$$
$$=P[K1\oplus K2=\alpha]$$
$$=P[\alpha=\alpha]$$
$$=1 \tag{1}$$

$$P[\frac{C=c}{M=mo}]$$
$$=P[K=c\oplus m0]$$
$$=P[K=\bar{\alpha}]$$
$$=P[K1\oplus K2=\bar{\alpha}]$$
$$=P[\alpha=\bar{\alpha}]$$
$$=0 \tag{2}$$

Based on (1) and (2) $P[\frac{C=c}{M=mo}]\neq P[\frac{C=c}{M=m1}] \Longrightarrow$ it is not perfectly secure

2. **Question 2**

(a) Given

$$g(n)=\frac{1}{p(n)} \text{ when } n\%100==0$$
$$=v(n) \text{ else}$$

Proof by contradiction

Let us assume the function $g(n)$ is a PRG, then for every polynomial $z(n)$ it should satisfy $g(n)<\frac{1}{z(n)}\forall n>N$ for some N.

Let us choose the polynomial as $z(n)=\frac{|p(n)|}{2}$ ,
then $\forall n>N: g(n)<\frac{1}{z(n)}=\frac{2}{|p(n)|}$

We choose a value $t=|N*100|>N$

$$t\%100==0 \tag{3}$$
$$\Longrightarrow g(t)=\frac{1}{p(t)} \tag{4}$$
$$\frac{1}{z(t)}=\frac{2}{|p(t)|} \tag{5}$$
$$\text{From (4) and (5) we can say that } g(t)>\frac{1}{z(t)} \tag{6}$$
$$\text{which is contradiction as } g(t) \text{ should be less than } \frac{1}{z(t)} \text{ given } t>N \tag{7}$$

(b) Yes, it is negligible. Given $f(n)=2^{\alpha}\times v(n)=c\times v(n)$ where $c=2^{\alpha}$. We will show that for every polynomial p(n) we can find an N such that $\forall n>N$ , $f(n)<\frac{1}{p(n)}$. Fix p(n), we know that since v(n) is negligible there exists an N1 such that $\forall n>N1, v(n)<\frac{1}{c\times p(n)}$ as $c\times p(n)$ is also a polynomial.
$\implies c\times v(n)<\frac{1}{p(n)}\forall n>N1$
$\implies f(n)<\frac{1}{p(n)}\forall n>N1$
So we found an $N=N1$ for the polynomial $p(n)$

3. **Question 3**

(a) It is not a pseudo random generator.
Adversary algorithm - Adversary will output 1 if the last $\alpha$ bits are $G(0^{\alpha})$.

Probability that the adversary wins =
Probability that verifier chooses pseudo random(PR) $\times$ Probability that adversary says it is PR
+
Probability that verifier chooses random $\times$ Probability that adversary says it is random.

i. Probability that verifier chooses pseudo random(PR) number = $\frac{1}{2}$

ii. Probability that verifier chooses random number = $\frac{1}{2}$
iii. Probability that adversary says it is PR when it is PR number = 1
iv. Probability that adversary says it is random number when it is random number = 1 - Probability that adversary says it is PR when it is random(He says it is PR when the output's last 3n bits exactly matches $G(0^{\alpha})$ = $1-\frac{1}{2^{3n}}$

Substituting in the equation, probability of adversary winning is:

$$=\frac{1}{2}\times 1+\frac{1}{2}\times(1-\frac{1}{2^{3n}}) \tag{8}$$
$$=1-\frac{1}{2^{3n+1}} \tag{9}$$
$$>\frac{3}{4} \tag{10}$$

which is significantly greater than $\frac{1}{2}$ hence it is not a PRG

(b) It is a PRG, we will prove by contradiction, assume $G'(s)$ is not a PRG, then we will prove that $G(s)$ is not a PRG.
Let's say $A'$ is an adversary which distinguishes $G'(s)$ . $A$ is an adversary which is trying to distinguish $G(s)$.

i. Challenger sends a message $y_b$ to adversary A.
ii. Adversary A computes $z_c=G(0^{\alpha})\oplus y_b$
iii. Adversary A sends the message $z_c$ to A'.
iv. Adversary A receives $c'$ from A'
v. Adversary A assigns $b'=c'$ and returns $b'$ to the Challenger

| **Verifier** | | **Adversary - A** | | **Adversary - A'** |
|---|---|---|---|---|
| randomly chooses either $b$=0,1 | | | | |
| | $\xrightarrow{y_b}$ | | | |
| | | calculates $z_c=G(0^{\alpha})\oplus y_b$ | | |
| | | | $\xrightarrow{z_c}$ | |
| | | | | distinguishes |
| | | | $\xleftarrow{c'}$ | |
| | | calculates $b'=c'$ | | |
| | $\xleftarrow{b'}$ | | | |
| finalize | | | | |

Proof

- Let's say b=1 i.e. the text sent by the challenger is pseudo random $y_b \leftarrow G(s) \implies z_c = G(0^\alpha) \oplus G(s)$ which is same as $G'(s)$. We simulated the experiment $PRGExp_1[A',G']$ for A'.
$$\implies P[\frac{b'=1}{b=1}] = P[\frac{c'=1}{c=1}] \text{ Where c'=1 denotes that adversary A' outputs pseudo random text}$$
- Let's say b=0 i.e. the text sent by the challenger is random $y_b \xleftarrow[R]{} \{0,1\}^n \implies z_c = G(0^\alpha) \oplus U_R^n$ where $U_R^n$ is a random message .We know that XOR of a constant($G(0^\alpha)$) with a random text is also a random text. We simulated the experiment $PRGExp_0[A',G']$ for A'.
$$\implies P[\frac{b'=1}{b=0}] = P[\frac{c'=1}{c=0}] \text{ Where c'=1 denotes that adversary A' outputs pseudo random text}$$
- From the above two equations we can say that
$$P[\frac{b'=1}{b=1}] - P[\frac{b'=1}{b=0}] = P[\frac{c'=1}{c=1}] - P[\frac{c'=1}{c=0}] = \epsilon \text{ which is non negligible}$$
$$\implies P[\frac{b'=1}{b=1}] - P[\frac{b'=1}{b=0}] = \epsilon$$

$\implies$ G is not a pseudo random, which is false. Hence G' is a pseudo random generator

(c) It is not a PRG, let's say the message is $y_b = t1||t2$.
Adversary algorithm - Adversary will return $b1=1$ i.e. it is PR if $t1=t2$
Proof:

$$P\left[\frac{b'=1}{b=1}\right] = 1 \text{ As b=1, it means the text is a PRG text, which means t1=t2 and adversary always outputs 1} \tag{11}$$
$$\tag{12}$$
$$P\left[\frac{b'=1}{b=0}\right] = P[t1=t2] \text{ as adversary outputs 1 only if t1=t2} \tag{13}$$
$$= \prod_{i=1}^{|t1|} \frac{1}{2} \tag{14}$$
$$= \frac{1}{2^{|t1|}} \qquad = \frac{1}{2^{3n}} \tag{15}$$
$$P\left[\frac{b'=1}{b=1}\right] - P\left[\frac{b'=1}{b=0}\right] = 1 - \frac{1}{2^{3n}} > \frac{1}{2} \text{ which is not negligible}$$

$\therefore$ It is not a PRG

(d) It is a PRG, we will prove by contradiction, assume $G'(s)$ is not a PRG, then we will prove that $G(s)$ is not a PRG.
Let's say $A'$ is an adversary which distinguishes $G'(s)$ . $A$ is an adversary which is trying to distinguish $G(s)$.

i. Challenger sends a message $y_b = x||y||z$ to adversary A.
ii. Adversary A truncates $y_b$ to $z_c = x||y$
iii. Adversary A sends the message $z_c$ to A'.
iv. Adversary A receives $c'$ from A'
v. Adversary A assigns $b' = c'$ and returns $b'$ to the Challenger

| **Verifier** | | **Adversary - A** | | **Adversary - A'** |
|---|---|---|---|---|
| randomly chooses either $b=0,1$ | | | | |
| | $\xrightarrow{y_b = x\|\|y\|\|z}$ | | | |
| | | truncates $y_b$ to $z_c = x\|\|y$ | | |
| | | | $\xrightarrow{z_c}$ | |
| | | | | distinguishes |
| | | | $\xleftarrow{c'}$ | |
| | | Assign $b' = c'$ | | |
| | $\xleftarrow{b'}$ | | | |
| finalize | | | | |

Proof

- Let's say b=1 i.e. the text sent by the challenger is pseudo random $y_b \leftarrow G(s) \implies z_c = x||y$ which is same as $G'(s)$. We simulated the experiment $PRGExp_1[A',G']$ for A'.

  $\implies P[\frac{b'=1}{b=1}] = P[\frac{c'=1}{c=1}]$ Where c'=1 denotes that adversary A' outputs pseudo random text
- Let's say b=0 i.e. the text sent by the challenger is random $y_b \underset{R}{\leftarrow} \{0,1\}^{3n} \implies z_c =$ first 2n characters of $U_R^{3n}$ where $U_R^{3n}$ is a random message of size 3n .We know that substring of any random text is also a random text. $\therefore z_c \underset{R}{\leftarrow} U^{2n}$. We simulated the experiment $PRGExp_0[A',G']$ for A'.

  $\implies P[\frac{b'=1}{b=0}] = P[\frac{c'=1}{c=0}]$ Where c'=1 denotes that adversary A' outputs pseudo random text
- From the above two equations we can say that

  $P[\frac{b'=1}{b=1}] - P[\frac{b'=1}{b=0}] = P[\frac{c'=1}{c=1}] - P[\frac{c'=1}{c=0}] = \epsilon$ which is non negligible

  $\implies P[\frac{b'=1}{b=1}] - P[\frac{b'=1}{b=0}] = \epsilon$

  $\implies$ G is not a pseudo random, which is false. Hence G' is a pseudo random generator

4. **Question 4**

   G*(s) is a PRG. We will be using the closure property of indistinguishability lemma
   Based on indistinguishably property we can say that $G(s) \approx U_{2n} \to$ **(1)**
   where $U_{2n}$ stands for uniform distribution over strings of length 2n.

   - We describe the PPT algorithm $M : \{0,1\}^{2n} \to \{0,1\}^n$ as
     - For an input $s$ of length $2n$
     - Pick bits from i to i+n-1 from s i.e. $o = s_i, s_{i+1}, ... s_{i+n-1}$
     - Calculate G(o)

     Since M is a PPT, apply it on either side of the above equation (1)

   $\therefore M(G(s)) \approx M(U^{2n})$
   - Simplify
     - $M(G(s))$ is same as the algorithm for $G^*(s)$
     - $\therefore M(G(s)) = G^*(s) \to$ **(2)**
     - Consider $M(U^{2n}) = G($pick n bits from $i^{\text{th}}$ index in $U^{2n})$
     - We know that substring of any random string is also random, hence n bits from $i^{\text{th}}$ index in $U^{2n}$ is $U^n$
     - $\therefore M(U^{2n}) = G(U^n) = G(s) \to$ **(3)**
     - From (2) and (3) we can say that $G^*(s) \approx G(s) \to$ **(4)**
   - From equations **(4)** and **(1)** we can say that
     - $G(s) \approx U_{2n}$
     - $G^*(s) \approx G(s)$
     - Using hybrid lemma we can say that $G^*(s) \approx U_{2n}$
     - $\therefore$ **G*(s) is a PRG as it is indistinguishable from U**$^{2n}$

5. **Question 5**

   (a) For this question $b=0$ means the message sent by challenger is $m_0$
   (b) For this question $b=1$ means the message sent by challenger is $m_1$
   (c) For this question $b'=0$ means the message guessed by adversary is $m_0$
   (d) For this question $b'=1$ means the message guessed by adversary is $m_1$
   (e) LHS: $P[Priv^{coa}_{\mathcal{A},\pi}(n) = 1]$ = probability that adversary wins = $\frac{1}{2} \times P\left[\frac{b'=0}{b=0}\right] + \frac{1}{2} \times P\left[\frac{b1=1}{b=1}\right] <= \frac{1}{2} + negl(n)$

   RHS: $|P[\frac{b'=1}{b=0}] - P[\frac{b'=1}{b=1}]| <= negl(n)$

- Proof for RHS $\implies$ LHS.
  LHS = Probability that adversary wins

$$
\begin{aligned}
&= \frac{1}{2} \times P\left[\frac{b'=0}{b=0}\right] + \frac{1}{2} \times P\left[\frac{b1=1}{b=1}\right] \\
&= \frac{1}{2} \times \left(1 - P\left[\frac{b'=1}{b=0}\right]\right) + \frac{1}{2} \times P\left[\frac{b1=1}{b=1}\right] \\
&= \frac{1}{2} + \frac{1}{2}\left(P\left[\frac{b'=1}{b=1}\right] - P\left[\frac{b'=1}{b=0}\right]\right) \\
&= \frac{1}{2} + \frac{1}{2} \times negl(n) \textbf{ using RHS} \\
&= \frac{1}{2} + negl(n)
\end{aligned}
$$

- Proof for LHS $\implies$ RHS.

  We know that probability that adversary wins is $\frac{1}{2}$+negligible

$$
\begin{aligned}
\text{LHS} &= \frac{1}{2} \times P\left[\frac{b'=0}{b=0}\right] + \frac{1}{2} \times P\left[\frac{b1=1}{b=1}\right] <= \frac{1}{2} + negl(n) \\
&\implies \frac{1}{2} \times [1 - P\left[\frac{b'=1}{b=0}\right]] + \frac{1}{2} \times P\left[\frac{b1=1}{b=1}\right] <= \frac{1}{2} + negl(n) \\
&\implies 1 - P\left[\frac{b'=1}{b=0}\right] + P\left[\frac{b1=1}{b=1}\right] <= 1 + 2 \times negl(n) \\
&\implies \left| P\left[\frac{b'=1}{b=1}\right] - P\left[\frac{b1=1}{b=0}\right] \right| <= negl'(n) \\
&\implies \left| P\left[\frac{b'=1}{b=0}\right] - P\left[\frac{b1=1}{b=1}\right] \right| <= negl'(n) \text{ which is RHS}
\end{aligned}
$$

(f)
- Let n be the length of the key
- Consider an input $\mathbf{m0}=1$ to the Encryption algorithm, since the encryption is a polynomial time algorithm in the input size = $\max(|K|,|M|)=n \implies$ the cipher text can't exceed a polynomial $q(n) \forall$ keys $k \in \{0,1\}^n$
- Let $X=q(n)$
- Number of cipher texts of length less than or equal X $= \prod_{i=1}^{X} 2^i = 2^{X+1} - 2 \leq 2^{X+1}$
- Each cipher text can map to at most $2^n$ messages as there are $2^n$ keys.
- $\therefore$ Maximum number of distinct messages which can map to cipher texts with size less than X are $2^n \times 2^{X+1} = 2^{X+1+n}$ **- (1)**
- Now consider all messages with size $X+n+2$ , there are $2^{X+n+2}$ messages **- (2)**
- From (1) and (2) we can conclude there will be atleast one message of size $X+n+2$ which doesn't map to any cipher text of size less than or equal to X, let that message be **m1** - (3)
- Now we have two messages $m0$ and $m1$ , the max size for cipher text with input $m0$ is $X$, the size of cipher text with input $m1 > X$
- Now we can construct an adversary which passes $m0$ and $m1$ as input to the adversary, and predicts the message selected by the verifier based on whether

$$m = m1 \text{ If } |c| > |X| \tag{16}$$

$$m = m0 \text{ If } |c| \leq |X| \tag{17}$$

  where c is cipher text sent by the verifier, and the adversary wins this game with probability 1, so it is not perfectly secure.