

Fundamentals of Cryptography Homework 2

周书予

2000013060@stu.pku.edu.cn

September 24, 2022

Problem 1

We construct PRG G' like this: on input x of length n ,

1. G' first finds the largest m such that $m \leq n$ and $m \in \mathcal{I}$. If no such m exists, G' just simply outputs 0^{n+1} (an arbitrary string of length $n+1$).
2. Then it truncates x to m bits and stretches the input seed into length $n+1$ by repetitively replacing the last m bits (say x') with $G(x')$.

According to the second property of polynomial-time-enumerable set, $n = \text{poly}(m)$, which means any negligible function of m is also negligible of n . Thus the stretching procedure preserves pseudorandomness, which can be formally described as, for all PPT distinguisher D , there is a negligible function $\varepsilon(m) = \text{negl}(m)$, such that

$$\left| \Pr_{s \leftarrow \{0,1\}^m} [D(\text{STRETCH}(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{n+1}} [D(r) = 1] \right| \leq \varepsilon(m)$$

Notice that

$$\Pr_{s \leftarrow \{0,1\}^m} [D(\text{STRETCH}(s)) = 1] = \Pr_{s \leftarrow \{0,1\}^n} [D(G'(s)) = 1]$$

thus,

$$\left| \Pr_{s \leftarrow \{0,1\}^n} [D(G'(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{n+1}} [D(r) = 1] \right| \leq \varepsilon(m) = \varepsilon'(n)$$

which finish the prove that G' is a PRG of stretch $\ell(n) = n+1$.

Problem 2

Assume $|G(s)| = |G_0(s)| = |G_1(s)| = \ell(|s|)$.

Part A

G' is a PRG of stretch $\ell(n/2)$.

For any fixed PPT distinguisher D , define $\varepsilon : \mathbb{N} \rightarrow \mathbb{R}$ as

$$\varepsilon(n) = \left| \Pr_{s \leftarrow \{0,1\}^n} [D(G'(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{\ell(n/2)}} [D(r) = 1] \right|$$

By the definition of G' , we know that

$$\Pr_{s \leftarrow \{0,1\}^n} [D(G'(s)) = 1] = \Pr_{s \leftarrow \{0,1\}^{n/2}} [D(G(s)) = 1]$$

thus

$$\varepsilon(n) = \left| \Pr_{s \leftarrow \{0,1\}^{n/2}}[D(G(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{\ell(n/2)}}[D(r) = 1] \right| \leq \varepsilon'(n/2)$$

where ε' is a negligible function since G is assumed to be a secure PRG. $\varepsilon(n) \leq \varepsilon'(n/2)$ means ε is also negligible, thus G' is a PRG.

Part B

G' may not be a PRG.

Let H be a PRG of stretch $\ell(n)$, and let $G(s) = s_1 \| H(s_2, \dots, s_n)$. Obviously G is a PRG whose first bit of input and output are always the same.

When G' is constructed based on G , G' always outputs 0 as its first bit, which can be apparently distinguished from the uniform distribution over $\{0, 1\}^{\ell(n+1)}$.

Part C

G' may not be a PRG.

Let G be a PRG who ignores its last bit of input, and consider a PPT distinguisher D who examines whether the two halves of the output of G' are the same.

With probability $1/2$, the last bit of input s is 0, which indicates the output of $G(s)$ and $G(s+1)$ are totally the same. Thus,

$$\Pr_{s \leftarrow \{0,1\}^n}[D(G'(s)) = 1] \geq 1/2$$

meanwhile,

$$\Pr_{r \leftarrow \{0,1\}^{2\ell(n)}}[D(r) = 1] = 2^{-\ell(n)}$$

G' is not a PRG in this case.

Part D

G' is a PRG of stretch $\ell(n/2)$.

We will use a *hybird argument* to show this conclusion.

For any PPT distinguisher D of G' , consider two distinguishers D_0 and D_1 , corresponding to G_0 and G_1 , respectively:

- D_0 takes input r_0 of length $\ell(n/2)$, randomly samples $r_1 \leftarrow \{0, 1\}^{\ell(n/2)}$, and then outputs $D(r_0 \oplus r_1)$.
- D_1 takes input r_1 of length $\ell(n/2)$, randomly samples $s_0 \leftarrow \{0, 1\}^{n/2}$, and then outputs $D(G_0(s_0) \oplus r_1)$.

Since G_0 and G_1 are both PRGs, there is two negligible functions $\varepsilon_0(n), \varepsilon_1(n)$ such that

$$\begin{aligned} \left| \Pr_{s_0 \leftarrow \{0,1\}^{n/2}}[D_0(G_0(s_0)) = 1] - \Pr_{r_0 \leftarrow \{0,1\}^{\ell(n/2)}}[D_0(r_0) = 1] \right| &\leq \varepsilon_0(n) \\ \left| \Pr_{s_1 \leftarrow \{0,1\}^{n/2}}[D_1(G_1(s_1)) = 1] - \Pr_{r_1 \leftarrow \{0,1\}^{\ell(n/2)}}[D_1(r_1) = 1] \right| &\leq \varepsilon_1(n) \end{aligned}$$

and notice that

$$\begin{aligned}
 \Pr_{s_1 \leftarrow \{0,1\}^{n/2}}[D_1(G_1(s_1)) = 1] &= \Pr_{\substack{s_0 \leftarrow \{0,1\}^{n/2} \\ s_1 \leftarrow \{0,1\}^{n/2}}}[D(G_0(s_0) \oplus G_1(s_1)) = 1] \\
 \Pr_{s_0 \leftarrow \{0,1\}^{n/2}}[D_0(G_0(s_0)) = 1] &= \Pr_{\substack{s_0 \leftarrow \{0,1\}^{n/2} \\ r_1 \leftarrow \{0,1\}^{\ell(n/2)}}}[D(G_0(s_0) \oplus r_1) = 1] \\
 \Pr_{r_1 \leftarrow \{0,1\}^{\ell(n/2)}}[D_1(r_1) = 1] &= \Pr_{\substack{s_0 \leftarrow \{0,1\}^{n/2} \\ r_1 \leftarrow \{0,1\}^{\ell(n/2)}}}[D(G_0(s_0) \oplus r_1) = 1] \\
 \Pr_{r_0 \leftarrow \{0,1\}^{\ell(n/2)}}[D_0(r_0) = 1] &= \Pr_{\substack{r_0 \leftarrow \{0,1\}^{\ell(n/2)} \\ r_1 \leftarrow \{0,1\}^{\ell(n/2)}}}[D(r_0 \oplus r_1) = 1]
 \end{aligned}$$

which indicates that

$$\left| \Pr_{\substack{s_0 \leftarrow \{0,1\}^{n/2} \\ s_1 \leftarrow \{0,1\}^{n/2}}}[D(G_0(s_0) \oplus G_1(s_1)) = 1] - \Pr_{\substack{r_0 \leftarrow \{0,1\}^{\ell(n/2)} \\ r_1 \leftarrow \{0,1\}^{\ell(n/2)}}}[D(r_0 \oplus r_1) = 1] \right| \leq \varepsilon_0(n) + \varepsilon_1(n)$$

The choice of distinguisher D is arbitrary, which means $G'(s) = G_0(s_0) \| G_1(s_1)$ is a PRG.

Part E

G' may not be a PRG.

By using the similar argument in **Part B**, we let G_0 be a PRG who has its first bit of output always equal to its first bit of input, and let G_1 be just the opposite, i.e. has its first bit of output always differ from its first bit of input.

We can find that $G'(s) = G_{s_1}(s)$ always outputs 0 as its first bit, which can be easily distinguished.

Part F

G' is a PRG of stretch $\ell(n-1) + 1$.

For any PPT distinguisher D of G' , consider two distinguishers D_0 and D_1 , corresponding to G_0 and G_1 , respectively:

- D_0 takes input r of length $\ell(n-1)$ and outputs $D(0 \| r)$.
- D_1 takes input r of length $\ell(n-1)$ and outputs $D(1 \| r)$.

Since G_0 and G_1 are both PRGs, there is two negligible functions $\varepsilon_0(n), \varepsilon_1(n)$ such that

$$\begin{aligned}
 \left| \Pr_{s \leftarrow \{0,1\}^{n-1}}[D_0(G_0(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{\ell(n-1)}}[D_0(r) = 1] \right| &\leq \varepsilon_0(n) \\
 \left| \Pr_{s \leftarrow \{0,1\}^{n-1}}[D_1(G_1(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{\ell(n-1)}}[D_1(r) = 1] \right| &\leq \varepsilon_1(n)
 \end{aligned}$$

notice that

$$\begin{aligned}
 \Pr_{s \leftarrow \{0,1\}^n}[D(G'(s)) = 1] &= \frac{1}{2} (\Pr_{s \leftarrow \{0,1\}^{n-1}}[D_0(G_0(s)) = 1] + \Pr_{s \leftarrow \{0,1\}^{n-1}}[D_1(G_1(s)) = 1]) \\
 \Pr_{r \leftarrow \{0,1\}^{\ell(n-1)+1}}[D(r) = 1] &= \frac{1}{2} (\Pr_{r \leftarrow \{0,1\}^{\ell(n-1)}}[D_0(r) = 1] + \Pr_{r \leftarrow \{0,1\}^{\ell(n-1)}}[D_1(r) = 1])
 \end{aligned}$$

thus

$$\left| \Pr_{s \leftarrow \{0,1\}^n} [D(G'(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^{\ell(n-1)+1}} [D(r) = 1] \right| \leq \frac{\varepsilon_0(n) + \varepsilon_1(n)}{2}$$

which finish the proof that G' is a PRG.

Problem 5

Part A

f' is an OWF.

FSOC we assume PPT adversary \mathcal{A}' breaks f' as OWF, which means that

$$\Pr_{x \leftarrow \{0,1\}^n} [\mathcal{A}'(f(x) \| f(f(x))) \rightarrow x' : f(x) \| f(f(x)) = f(x') \| f(f(x'))] \geq \frac{1}{\text{poly}(n)}$$

then we can construct adversary \mathcal{A} which breaks f as OWF: on input y , call \mathcal{A}' with input $y \| f(y)$, and output whatever \mathcal{A}' outputs. It's clear that \mathcal{A} runs in poly-time, and

$$\Pr_{x \leftarrow \{0,1\}^n} [\mathcal{A}(f(x)) \rightarrow x' : f(x) = f(x')] \geq \frac{1}{\text{poly}(n)}$$

which indicates that f is not an OWF. A contradiction.

Part B

f' may not be an OWF.

Assume that there is a length-perserving OWF h , we construct f as $f(x_1 \| x_2) = 0^n h(x_1)$ where $|x_1| = |x_2| = n$. First we prove briefly that f is also a length-perserving OWF.

FSOC PPT adversary \mathcal{A} breaks f as OWF, which on input $0^n \| h(x_1)$ outputs $x'_1 \| x'_2$ such that $0^n \| h(x'_1) = 0^n \| h(x_1)$, with probability at least $\frac{1}{\text{poly}(n)}$. Then an adversary for h can be built, which simply concatenate 0^n before its input and then call \mathcal{A} , and outputs the first half of \mathcal{A} 's output.

By the construction of f' , $f'(x_1 \| x_2) = x_1 \| (x_2 \oplus h(x_1))$. An adversary \mathcal{A} , with $\mathcal{A}(y_1 \| y_2) = y_1 \| (y_2 \oplus h(y_1))$, runs in poly-time and breaks f as OWF.

Part C

f' may not be an OWF.

Assume h is a length-perserving OWF, we construct f as

$$f(x_1 \| x_2) = \begin{cases} x_1 \| h(x_2), & x_1 \text{ starts with } 0 \\ h(x_1) \| x_2, & x_1 \text{ starts with } 1 \end{cases}$$

First we prove that f is also an OWF: with adversary \mathcal{A}' which breaks f , one can construct \mathcal{A} , on input y it calls \mathcal{A}' with input $0^n \| y$ and outputs the second half of the output of \mathcal{A}' . Then \mathcal{A} breaks h as OWF, an contradiction.

Depending on the first bit of input, the output of $f(x_1\|x_2)$ must be in the form of either $x_1\|h(x_2)\|h(\overline{x_1})\|\overline{x_2}$ or $h(x_1)\|x_2\|\overline{x_1}\|h(\overline{x_2})$, so an adversary can be constructed, which on input $y_1\|y_2\|y_3\|y_4$, simply tries $y_1\|\overline{y_4}$ and $\overline{y_3}\|y_2$ as answers and outputs the correct one (if there is). So f' here is not a OWF.

Part D

f' is an OWF.

If f' is not an OWF, a.k.a. there exists adversary \mathcal{A}' such that

$$\Pr_{x \leftarrow \{0,1\}^n}[\mathcal{A}'(f(G(x))) \rightarrow x' : f(G(x')) = f(G(x))] \geq \frac{1}{\text{poly}(n)}$$

We construct a PPT distinguisher \mathcal{D} that breaks G as PRG using \mathcal{A}' : on input r , it outputs $\mathbb{1}[f(r) = f(G(\mathcal{A}'(f(r))))]$. We use the notation U_n to indicate the uniform distribution over $\{0,1\}^n$ in the following statement.

- When r is sampled from $G(U_n)$, by the assumption above \mathcal{D} outputs 1 with probability at least $\frac{1}{\text{poly}(n)}$.
- When r is sampled from U_{n+1} , recall that f is an OWF, so by definition, for the adversary $G \circ \mathcal{A}'$, we have

$$\Pr_{x \leftarrow \{0,1\}^{n+1}}[G \circ \mathcal{A}'(f(y)) \rightarrow y' : f(y') = f(y)] < \varepsilon(n)$$

which means that \mathcal{D} outputs 1 with probability less than $\varepsilon(n)$.

Thus \mathcal{D} breaks G as a PRG. A contradiction.

Part E

f' may not be an OWF.

Let f be the OWF mentioned in **Part B** ($f(x_1\|x_2) = 0^n\|h(x_2)$) and G be the PRG in **Problem 2 Part A** ($G(s) = G'(s_1, \dots, s_{n/2})$).

Now $f \circ G \equiv f(G(0^n))$ is constant, and is obviously not OWF.

Part F

f' is an OWF.

FSOC assume that adversary A breaks f' as OWF, which is, for some polynomial $p(n)$,

$$\Pr_{x \leftarrow \{0,1\}^n}[\mathcal{A}(f(x\|0^{\log n})) \rightarrow x' : f(x'\|0^{\log n}) = f(x\|0^{\log n})] \geq \frac{1}{p(n)}$$

We assert that \mathcal{A} is also an adversary which breaks f as OWF:

$$\begin{aligned}
 & \Pr_{x \leftarrow \{0,1\}^{n+\log n}} [\mathcal{A}(f(x)) \rightarrow x' : f(x') = f(x)] \\
 & \geq \Pr_{x \leftarrow \{0,1\}^{n+\log n}} [\mathcal{A}(f(x)) \rightarrow x' : f(x') = f(x) \wedge \text{last } \log n \text{ bits of } x \text{ are all 0s}] \\
 & = \Pr_{x \leftarrow \{0,1\}^n} [\mathcal{A}(f(x \| 0^{\log n})) \rightarrow x' : f(x' \| 0^{\log n}) = f(x \| 0^{\log n})] \cdot \frac{1}{2^{\log n}} \\
 & \geq \frac{1}{np(n)}
 \end{aligned}$$

$np(n)$ is also a polynomial, so \mathcal{A} breaks f as OWF, which causes a contradiction.

Part G

咋做啊

Problem 6

Part A

$$\begin{aligned}
 & \Pr[f(\hat{x}_1) = f(x_1), \dots, f(\hat{x}_m) = f(x_m)] \\
 & = \Pr[f(\hat{x}_1) = f(x_1), \dots, f(\hat{x}_m) = f(x_m) \wedge \text{some } x_i \text{ is bad}] \\
 & \quad + \Pr[f(\hat{x}_1) = f(x_1), \dots, f(\hat{x}_m) = f(x_m) \wedge \text{all } x_i \text{ are good}] \\
 & \leq \sum_{j=1}^m \Pr[f(\hat{x}_1) = f(x_1), \dots, f(\hat{x}_m) = f(x_m) \wedge x_j \text{ is bad}] + (\Pr[x \text{ is good}])^m \\
 & \leq \sum_{j=1}^m \Pr[f(\hat{x}_1) = f(x_1), \dots, f(\hat{x}_m) = f(x_m) | x_j \text{ is bad}] + (\Pr[x \text{ is good}])^m \\
 & \leq \sum_{j=1}^m m \cdot \Pr[\mathcal{A}(f(x_j)) \rightarrow x' : f(x') = f(x_j) | x_j \text{ is bad}] + (\Pr[x \text{ is good}])^m \\
 & < \frac{m^2}{r(n)} + (\Pr[x \text{ is good}])^m
 \end{aligned}$$

Part B

Let $m(n) = 2nq(n)$ and $r(n) = 2m(n)^2p(n)$.

From **Part A** we know that

$$\frac{1}{p(n)} < \frac{m(n)^2}{r(n)} + (\Pr[x \text{ is good}])^m \Rightarrow (\Pr[x \text{ is good}])^m > \frac{1}{2p(n)}$$

which implies $\Pr[x \text{ is good}] \geq 1 - \frac{1}{2q(n)}$ since otherwise we have

$$\frac{1}{2p(n)} < (\Pr[x \text{ is good}])^m < \left(1 - \frac{1}{2q(n)}\right)^{2nq(n)} \approx \exp(-n)$$

RHS of this inequility is negligible while LHS is non-negligible, which shows a contradiction.

So $\Pr[x \text{ is good}] \geq 1 - \frac{1}{2q(n)}$ and $\Pr[x \text{ is bad}] \leq \frac{1}{2q(n)}$.

Part C

We show that $\mathcal{A}_{\text{repeat}}$ breaks f as weak-OWF.

$$\begin{aligned}
 & \Pr[\mathcal{A}_{\text{repeat}}(f(x)) \rightarrow x' : f(x') \neq f(x)] \\
 &= \Pr[\mathcal{A}_{\text{repeat}}(f(x)) \rightarrow x' : f(x') \neq f(x) \wedge x \text{ is good}] \\
 & \quad + \Pr[\mathcal{A}_{\text{repeat}}(f(x)) \rightarrow x' : f(x') \neq f(x) \wedge x \text{ is bad}] \\
 &\leq \Pr[\mathcal{A}_{\text{repeat}}(f(x)) \rightarrow x' : f(x') \neq f(x) | x \text{ is good}] + \Pr[x \text{ is bad}] \\
 &\leq \left(1 - \frac{1}{r(n)}\right)^{n \cdot r(n)} + \frac{1}{2q(n)} \\
 &\approx \exp(-n) + \frac{1}{2q(n)} \\
 &< \frac{1}{q(n)}
 \end{aligned}$$

which violates the definition ($q(n)$ -weakness) of f .

So we have already finished the proof that f' is an OWF.