CAS CS 538. Solutions to Problem Set 3

Due electronically via gradescope, Monday February 9, 2026 11:59pm

Om Khadka, U51801771

Problems

Problem 1. (10 points) Suppose $\mathcal{A}$ in Attack Game 3.1 uses the following strategy. Choose a random $t \in \mathcal{S}$ and output 1 if and only if $G(t) = r$. Suppose G is injective. Compute $\text{PRGadv}[\mathcal{A}, G]$.

Solution. The definition of the game is just gonna be the game 3.1 layout from the book (Graduate Course in Applied Cryptography). From the given attack methodology, we're essentially computing for

$$\text{PRGadv}[\mathcal{A}, G] = |\Pr[W_0] - \Pr[W_1]|$$

Where W_b is just the chance that $\mathcal{A}$ returns 1 from any particular game.

$\exp 0$ **(Using G)**
In $\exp 0$, the following happens:

- Challenger picks $s \in^R \mathcal{S}$. Then, check if $r = G(s)$.
- Adversary $\mathcal{A}$ now gets r, chooses $t \in^R \mathcal{S}$, and outputs
  - 1 IFF $G(t) = r$
  - 0 otherwise

Firstly, note that $G(t) = r$ can also be thought of as $G(t) = G(s)$. And since G is one-to-one, $G(t)$ mapping out to $G(s)$ implies that $t = s$. Moreover, since s, t are determined independently and randomly from $\mathcal{S}$, we're essentially just checking if, upon randomly selecting 2 values from $\mathcal{S}$, that those 2 values end up being the same from $\mathcal{S}$, which equates to

$$\Pr[W_0] = \Pr[t = s] = \frac{1}{|\mathcal{S}|}$$

$\exp 1$ **(Using a rnd value)**
In $\exp 1$, the following happens:

- Challenger picks $r \in^R \mathcal{R}$.
- Adversary then gets r, chooses $t \in^R \mathcal{S}$, and then outputs
  - 1 IFF $G(t) = r$
  - 0 else

Now here, firstly note how r is independent from $t, \mathcal{S}$, and random from $\mathcal{R}$. Also since G is injective, this then means that this comparison is now just checking if some ranomly chosen seed, $G(t)$ happens to also be the same value as some truly random number, r. This equates to

$$\Pr[W_1] = \Pr[t = r] = \frac{1}{|\mathcal{R}|}$$

So plugging these values back into our OG equation:

$$\begin{aligned} \text{PRGadv}[\mathcal{A}, G] &= |\Pr[W_0] - \Pr[W_1]| \\ &= |\frac{1}{|\mathcal{S}|} - \frac{1}{|\mathcal{R}|}| \\ &= \frac{1}{|\mathcal{S}|} - \frac{1}{|\mathcal{R}|} \end{aligned}$$

Note: Since G is injective, there's no way that S can map out to more values than in $\mathcal{R}$. That's why I omitted those $||$'s

Problem 2. (20 points) Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a secure PRG. Let G' be a function where $G'(s)$ computes $G(s)$, deletes every third bit, and returns the result. Prove G' is a secure PRG.

Solution. Before solving this, I'll just say that, intuitively, the reason why G' is secure is because applying some random mathematical operation to an output won't meaningfuly change the message in such a way as to be recognizable (*Like adding 1 to all msgs x doesn't reveal anything meaningful.*)

I'll define the following:

- $G'(s) =$ the result of computing $y = G(s)$, and then removing every third bit in y.
- $L = 2n - [2n/3] =$ the length of output $G'(s)$.
- $G' : \{0,1\}^n \to \{0,1\}^L$.

Suppose, for the sake of contradiction, that G' isn't secure. I'll make a new adversary, $\mathcal{A}'$, that'll then use $G'(s)$ to distinguish games using random inputs from games using the problem's defined input. That is,

$$\text{PRGadv}[\mathcal{A}', G'] = |\Pr_{s \leftarrow \{0,1\}^n}[\mathcal{A}'(G'(s)) = 1] - \Pr_{r \leftarrow \{0,1\}^L}[\mathcal{A}'(r) = 1]|$$

is non-negligible.

The adversary, $\mathcal{A}$, will use $\mathcal{A}'$ to break G. G will just be the attack methodology from Game 3.1 from the book from before. That is,

- $\exp 0$ will guess from a pseudo-rnd seed s
- $\exp 1$ will guess from a truly random value y.

$\mathcal{A}$ construction:

- Get $y = \{0,1\}^{2n}$ from challenger.
- Compute $y' = y$ but with every third bit removed $(3, 6, ...)$.
- Run $\mathcal{A}'$ with y' to get b.
- Return b.

$\exp 0$**:**
Challenger will pick $s \leftarrow \{0,1\}^n$, and then sends $y = G(s)$. y' will then be $G'(s)$ by our defintion, otherwise meaning that:

$$\Pr[\mathcal{A}\text{outputs } 1|\exp 0] = \Pr_{s\leftarrow\{0,1\}^n}[\mathcal{A}'(G'(s)) = 1]$$

$\exp 1$**:**
The challenger will pick $y \leftarrow \{0,1\}^{2n}$ at random. I claim that y' is uniformly distributed over $\{0,1\}^L$. This holds since each bit of y is independent and random, and deleted fixed positions from these bits will still make it independent and random. In other words, I could say that the mapping of $f : \{0,1\}^{2n} \to \{0,1\}^L$ is surjective (onto), and that each $z \in \{0,1\}^L$ will have exxactly $2^{2n/3}$ elements.

Thusly, if y is uniform, then $y' = f(y)$ is also uniform over $\{0,1\}^L$, and therefore:

$$\Pr[\mathcal{A}\text{outputs } 1|\exp 1] = \Pr_{r\leftarrow\{0,1\}^L}[\mathcal{A}'(r) = 1].$$

The advantage of $\mathcal{A}$ in distinguishing between the G's will then be

$$\text{PRGadv}[\mathcal{A}, G] = |\Pr[\mathcal{A}\text{outputs } 1|\exp 0] - \Pr[\mathcal{A}\text{outputs } 1|\exp 1] = \text{PRGadv}[\mathcal{A}', G']$$

Basically, since $\mathcal{A}$ is efficent, $\mathcal{A}'$ should be able to also have some non-negligible advantge against G', making $\mathcal{A}$ also be non-negligible to G. But, G is a secure PRG, and thusly no efficent adversary could even crack this. This contradicts the point that $\mathcal{A}'$ coul exist, and thus it doesn't, also proving that G' is also secure.

Problem 3. In this problem you'll show that secure PRG $G : \{0,1\}^n \to \mathcal{R}$ can become insecure if the seed is not uniformly random in $\mathcal{S}$.

(a) (20 points) Consider PRG $G_a : \{0,1\}^{n+1} \to \mathcal{R} \times \{0,1\}$ defined as $G_a(s) = G(s_1 s_2 \dots s_n) \parallel s_{n+1}$, where $s_1 s_2 \dots s_{n+1}$ is the bit decomposition of s. Show that G_a is a secure PRG assuming G is secure.

Solution. Assuming that G is a secure PRG, I'll prove how G_a is also secure via reduction.

Let me define the following:

- $\mathcal{A} =$ efficent adversary against G_a

- $\text{PRGadv}[\mathcal{A}, G_a] = |\Pr_{s\leftarrow\{0,1\}^{n+1}}[\mathcal{A}(G_a(s)) = 1] - \Pr_{(r,b)\leftarrow\mathcal{R}\times\{0,1\}}[\mathcal{A}(r,b) = 1]|$.
- $\mathcal{B} =$ a new adversary against G with the following logic:
  - $\mathcal{B}$ gets $z \in \mathcal{R}$ from the challenger, where $z = G(x)$ for uniform $x \in \{0,1\}^n$ from $\exp 0$, or just uniform $z \in \mathcal{R}$ from $\exp 1$
  - $\mathcal{B}$ picks a uniform bit $b \leftarrow \{0,1\}$.
  - $\mathcal{B}$ outputs (z, b) to $\mathcal{A}$, an then outputs whatever $\mathcal{A}$ gives.

Exp 0:
In this case, $z = G(x)$ for uniform $x \in \{0,1\}^n$. The pair $(z, b) = (G(x), b)$ is distribute exactly as $G_a(s)$ for $s = (x, b)$, since x, b are both independent and random. Therefore,

$$\Pr[\mathcal{B} \text{ outputs } 1|\exp 0 \text{for } G] = \Pr_{s\leftarrow\{0,1\}^{n+1}}[\mathcal{A}(G_a(s)) = 1].$$

Exp 1:
In this case now, z is just chosen uniformly from $\mathcal{R}$. Since b is also uniform and independent from z, the pair (z, b) will then also be uniform over $\mathcal{R} \times \{0,1\}$. Therefore,

$$\Pr[\mathcal{B} \text{ outputs } 1|\exp 1 \text{for } G] = \Pr_{(r,b)\leftarrow\mathcal{R}\times\{0,1\}}[\mathcal{A}(r,b) = 1].$$

Therefore the PRG advantage is:

$$\text{PRGadv}[\mathcal{B}, G] = |\Pr[\mathcal{B} \text{ outputs} 1|\exp 0 \text{for } G] - \Pr[\mathcal{B} \text{ outputs } 1|\exp 1 \text{for } G]| = \text{PRGadv}[\mathcal{A}, G_a].$$

Since G is secure, $\text{PRGadv}[\mathcal{B}, G]$ will be negligible for any efficent $\mathcal{B}$. And since $\mathcal{B}$ is efficent (it esseentiall is only "flipping" a coin and then runs $\mathcal{A}$), $\text{PRGadv}[\mathcal{A}, G_a]$ will also be negligible. Therefore, no efficent adversary will be able to distinguish G_a from some random output, so $\therefore$ G_a is a secure PRG.

(b) (15 points) Show that G_a is insecure if its random seed is chosen so that its last bit is always 0. Demonstrate an adversary and compute its advantage.

Solution. In this part now, effectively what has changes is the seed value, s from G_a, as when it's chosen, a 0 is appended to the end, effectively reucing the seed space to $\{0,1\}^n \times \{0\}$.. For a seed $s = (x, 0)$, where $x \leftarrow \{0,1\}^n$ is uniform, then the output should be

$$G_a(x, 0) = G(x)||0$$

Basically just restating that the last bit of the output will always be 0.

For the contruction of $\mathcal{A}$, I will form the following:

- $\mathcal{A}$ gets a pair $(z, c) \in \mathcal{R} \times \{0,1\}$.
  - If $c = 0$, $\mathcal{A}$ returns 1 (or 'real')
  - Else, returns 0 (or just 'random')

Exp 0 (Real) Analysis
The challenger will pick $x \leftarrow \{0,1\}^n$, an then returns $(G(x), 0)$. The last bit c will then always be 0, so Therefore

$$\Pr[\mathcal{A} \text{ outputs } 1 | \exp 0] = 1.$$

Exp 1 (Random) Analysis
The challenger now will pick $(r, b) \leftarrow \mathcal{R} \times \{0,1\}$ uniformly. The last bit b is uniform from $\{0,1\}$, so therefore

$$\Pr[\mathcal{A} \Rightarrow 1 | \exp 1] = \Pr[b = 0] = 1/2.$$

So therefore, the advantage of $\mathcal{A}$ will be

$$\text{PRGadv}[\mathcal{A}, G_a] = |1 - \frac{1}{2}| = \frac{1}{2}.$$

This is a constant value (and a big one too), so the advantage is certainly non-negligible, making G_a insecure.

(c) (15 points) Construct a secure PRG $G_c : \{0,1\}^{n+1} \to \mathcal{R} \times \{0,1\}$ that becomes insecure if its seed s is chosen so that the *parity* of the bits in s is always 0 (where parity is defined as the XOR of all the bits). Hint: a small change to G_a is all you need here. Note that you will need to prove two separate facts: that G_c is secure when its seed is uniform, and that G_c is insecure when when the parity of the bits of s is 0. Both of these proofs can use the previous parts, even if you have not solved them.

Solution. Firstly, let me just construct and define G_c as the following:

For $s = s_1 \dots s_{n+1} \in \{0,1\}^{n+1}$, let

$$G_c(s) = G(s_1 \dots s_n) || (\bigoplus_{i=1}^{n+1} s_i).$$

where $G : \{0,1\}^n \to \mathcal{R}$ is a secure PRG, and the XOR symbol just being XOR from bottom to top. This equation is basically saying that G_c with reutnr a pseudornd string, $G(s_1 \dots s_n)$, with a single parity bit appended to the end of the seed.

Now, asuppose G is a secure PRG, then I can prove that G_c is also secure with this problem's seed, $s \in^R \{0,1\}^{n+1}$.

Let $\mathcal{A}$ be our efficent adversary for G_c. Then, $\mathcal{B}$ will be our other efficent adversary for G, where

- $\mathcal{B}$ gets a string $z \in^R \mathcal{R}$ from the challenger ($z = G(x)$, for a uniform x if it's $\exp 0$, or just random z for $\exp 1$).
- $\mathcal{B}$ then chooses an independent uniform bit, $p \leftarrow \{0,1\}$.
- $\mathcal{B}$ will then output (z, p) to $\mathcal{A}$, and then return the output of $\mathcal{A}$.

Exp 0
In this case, $z = G(x)$ for uniform $x \in^R \{0,1\}^n$. Then, (z, p) will then be distributed in the same manner to $G_c(s)$, for a uniform s. This is because, I coul write $s = (x, s_{n+1})$ with x being uniform an s_{n+1} being both uniform and independent. Then, the parity bit will be , $\bigoplus_{i=1}^{n+1} s_i = (\bigoplus_{i=1}^{n} x_i) \oplus s_{n+1}$.
Given x, this bit is uniform since s_{n+1} is also uniform. Morever, the parity bit is independent of x (since for any fixe x, it's also uniform). So then therefore, the pair, $(G(x), \text{parity})$, will then have to have the same distribution as $(G(x), p)$, where p is independent and uniform. Thus, the Pr of this case is

$$\Pr_{s \leftarrow \{0,1\}^{n+1}}[\mathcal{A}(G_c(s)) = 1].$$

Exp 1
In this case, z is just uniform over $\mathcal{R}$, and p is both uniform and independent. So, (z, p) are both uniform over $\mathcal{R} \times \{0,1\}$. And thus,

$$\Pr[\mathcal{B} \text{ outputs } 1 | \exp 1] = \Pr_{(r,b) \leftarrow \mathcal{R} \times \{0,1\}}[\mathcal{A}(r, b) = 1].$$

So then therefore, the PRGadv will be

$$\text{PRGadv}[\mathcal{B}, G] = |\Pr[\mathcal{B} \text{ outputs } 1 | \exp 0] - \Pr[\mathcal{B} \text{ outputs } 1 | \exp 1] = \text{PRGadv}[\mathcal{A}, G_c].$$

And since G is secure, PRGadv$[\mathcal{B}, G]$ will be negligible, thus showing that PRGadv$[\mathcal{A}, G_c]$ also being neglibigle for efficent $\mathcal{A}$, so then $\therefore$ G_c is secure, **But only if we're using uniform seeds.**

Consider the case now where the seed, s is chosen uniform from the set, such that

$$\{s \in \{0,1\}^{n+1} : \bigoplus_{i=1}^{n+1} s_i = 0\}.$$

For any such s, the parity bit (being the last bit for $G_c(s)$) will then ALWAYS be 0. Therefore, $G_c(s) = (G(s_1 \dots s_n), 0)$.

Now let $\mathcal{A}$ be a distinguisher G_c from random values with a non-negligible advantage. It would work as such:

- $\mathcal{A}$ gets pair $(z, b) \in \mathcal{R} \times \{0,1\}$.
- If $b = 0$, output 1 ("real")
- If not, output 0 ("random")

For **Exp 0**, The challenger will pick s uniformly from seeds with parity 0, and then return that, $G_c(s) = (G(x), 0)$, where x are the first n bits. Thus, the last bit is ALWAYS 0, meaning that $\mathcal{A}$ will always output 1 (probability 1).

For **Exp 1**, The challenge will then pick (r, b) uniformly over $\mathcal{R} \times \{0,1\}$. Thusly, $\Pr[b = 0] = \frac{1}{2}$, so $\mathcal{A}$ will output 1 with a probability of just $\frac{1}{2}$.

Therefore the PRGAdv becomes

$$\text{PRGadv}[\mathcal{A}, G_c] = |1 - \frac{1}{2}| = \frac{1}{2},$$

Which is like again a non-negligible (const) advantage, meaning that G_c would then become insecure **if the seeds are forced to be of parity 0.**

Problem 4. (20 points)
Let $G : \{0,1\}^n \to \mathcal{R}$ be a secure PRG, and consider G' defined as $G'(s) = G(s) \parallel G(s+1)$. Prove that G' is not necessarily a secure PRG. *(Hint: Use problem 3a.)*

Solution. Suppose the following *counterexample*: a specific secure PRG G such that G' is insecure.

Let $H : \{0,1\}^{n-1} \to \mathcal{R}_0$ be a secure PRG (this type of PRG should be valid). Then we can define $G : \{0,1\}^n \to \mathcal{R}_0 \times \{0,1\}$ to be

$$G(s) = H(s_1 \dots s_{n-1}) \parallel s_n,$$

where $s = s_1 \dots s_n$. From the previous Problem, 3(a), G it's already been proven that this is a secure PRG.

Now consider $G'(s) = G(s) \parallel G(s+1)$, where $s+1$ denotes incrementing s as an n-bit integer modulo 2^n. Then I could write $s = x \parallel b$ with $x \in \{0,1\}^{n-1}$ and $b \in \{0,1\}$.

- If $b = 0 : s = x0$, so $s + 1 = x1$. Then

$$G(s) = H(x) \parallel 0, \quad G(s+1) = H(x) \parallel 1.$$

- If $b = 1 : s = x_1$, so $s + 1 = (x+1)0$. Then

$$G(s) = H(x) \parallel 1, \quad G(s+1) = H(x+1) \parallel 0.$$

Thus, in $G'(s) = G(s) \parallel G(s+1)$, the last bit of the first half (all the way to $L+1$, where L is the length of the output, H) equals b, and the last bit of the second half (to $2(L+1)$) equals $1 - b$. Basically, these two bits are always different.

Now let's make an adversary $\mathcal{A}$ for G' as follows. For the input of $y \in \{0,1\}^{2(L+1)}$:

1. Let a be the bit at position $L+1$ (the last bit of the first half).
2. Let a' be the bit at position $2(L+1)$ (the last bit of the second half).
3. If $a \neq a'$, output 1 (guess "real"); otherwise output 0 (guess "random").

Comparing the 2 experiments:

- **Experiment 0 (real):** The challenger will pick $s \leftarrow \{0,1\}^n$, and then return $y = G'(s)$. Since a and a' are always different, $\mathcal{A}$ outputs 1 always (probability 1).
- **Experiment 1 (random):** Now the challenger will pick $y \leftarrow \{0,1\}^{2(L+1)}$ uniformly. Then a and a' are independent uniform bits, so then $\Pr[a \neq a'] = \frac{1}{2}$. Therefore, $\mathcal{A}$ probability to output 1 will be $\frac{1}{2}$.

Therefore,

$$\mathrm{PRGadv}[\mathcal{A}, G'] = \left|1 - \frac{1}{2}\right| = \frac{1}{2},$$

which is non-negligible (a const like again). Thus, G' is not a secure PRG.