

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 , S , and random from \mathcal{R} . Also since G is injective, this then means that this comparison is now just checking if some randomly 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:

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

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 $G : \{0, 1\}^n \rightarrow \{0, 1\}^{2n}$ 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 meaningfully 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 .
- $L = 2n - \lceil 2n/3 \rceil$ = the length of output $G'(s)$.
- $G' : \{0, 1\}^n \rightarrow \{0, 1\}^L$.

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,

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

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 definition, otherwise meaning that:

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

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 $f : \{0, 1\}^{2n} \rightarrow \{0, 1\}^L$ is surjective (onto), and that each $z \in \{0, 1\}^L$ will have exactly $2^{2n/3}$ elements.

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

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

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

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

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

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

(a) (20 points) Consider PRG $G_a : \{0, 1\}^{n+1} \rightarrow \mathcal{R} \times \{0, 1\}$ 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} = efficient 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} , and 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 distributed exactly as $G_a(s)$ for $s = (x,b)$, since x,b are both independent and random. Therefore,

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

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,

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

Therefore the PRG advantage is:

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

Since G is secure, $\text{PRGadv}[\mathcal{B}, G]$ will be negligible for any efficient \mathcal{B} . And since \mathcal{B} is efficient (it essentially is only "flipping" a coin and then runs \mathcal{A}), $\text{PRGadv}[\mathcal{A}, G_a]$ will also be negligible. Therefore, no efficient 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 changed is the seed value, s from G_a , as when it's chosen, a 0 is appended to the end, effectively reducing 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

$$G_a(x,0) = G(x) \parallel 0$$

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

For the construction 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 $x \leftarrow \{0, 1\}^n$, and then returns $(G(x), 0)$. The last bit c will then always be 0, so Therefore

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

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

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

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 $G_c : \{0, 1\}^{n+1} \rightarrow \mathcal{R} \times \{0, 1\}$ 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 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. Your solution goes here

Problem 4. (20 points)

Let $G : \{0, 1\}^n \rightarrow \mathcal{R}$ 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. Your solution goes here