CAS CS 538. Solutions to Problem Set 3

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

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 PRGadv$[\mathcal{A}, G]$.

Solution. In Experiment 0, $r = G(s)$ for a uniformly random $s \in \mathcal{S}$, and thus the probability that $\mathcal{A}$ outputs 1 is $\Pr[G(s) = G(t)] = \Pr[s = t] = 1/|\mathcal{S}|$ as G is injective; and in Experiment 1, $r \in \mathcal{R}$ is uniformly random and thus the probability that $\mathcal{A}$ outputs 1 is $\Pr[r = G(t)] = 1/|\mathcal{R}|$. Since $|\mathcal{R}| \geqslant |\mathcal{S}|$ by injectivity, we conclude that PRGadv$[\mathcal{A}, G] = \frac{1}{|\mathcal{S}|} - \frac{1}{|\mathcal{R}|}$.

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. We prove via reduction. Let $\mathcal{A}$ be an adversary that breaks the PRG game for G'. Construct an adversary $\mathcal{A}$ attacking the PRG game for G as follows:

- Upon receiving the value r from the challenger, delete every third bit and send the resulting string r' to $\mathcal{A}'$.
- Upon receiving back output b from $\mathcal{A}'$, output b.

Let p_0, p_1 be the probabilities that $\mathcal{A}'$ outputs 1 in Experiment 0 and Experiment 1 of PRG attack game for G' respectively. In experiment 0, the distribution of r' is uniform over the bit strings of length $\frac{4n}{3}$, which matches the distribution of strings a challenger for G' would produce in experiment 0. Therefore, $\mathcal{A}'$ outputs 1 with probability p_0. And since $\mathcal{A}$ outputs 1 iff $\mathcal{A}'$ outputs 1, we have $\Pr[\mathcal{A}(r') = 1] = p_0$. In experiment 1, $r = G(s)$ for some uniformly sampled seed s, and so the distribution of r' matches the distribution a challenger for G' would produce in experiment 1. By the same argument, $\Pr[\mathcal{A}(r') = 1] = p_1$.
Now we have that PRGadv$[\mathcal{A}, G] = |p_0 - p_1|$, which is non-negligible by assumption. We conclude via contrapositive that if G is a secure PRG, then G_B is a secure PRG.

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 $G_a(s) = G(s_1 s_2 \ldots s_n) \parallel s_{n+1}$, where $s_1 s_2 \ldots s_{n+1}$ is the bit decomposition of s. Show that G_a is a secure PRG assuming G is secure.

Solution. Let $\mathcal{A}_a$ be an adversary attacking G_a. We construct $\mathcal{A}(r)$ as follows: sample s_{n+1} uniformly from $\{0,1\}$ and output $\mathcal{A}_a(r \parallel s_{n+1})$.
Let $p_{a,0}, p_{a,1}$ be the probabilities that $\mathcal{A}_a$ outputs 1 in Experiment 0 and Experiment 1 of PRG attack

game for G_a respectively. In Experiment 0 of PRG attack game for G, $r = G(s)$ for a random s, so $\Pr[\mathcal{A}(r) = 1] = \Pr[\mathcal{A}_a(G(s) \parallel s_{n+1}) = 1] = \Pr[\mathcal{A}_a(G_a(s \parallel s_{n+1})) = 1] = p_{a,0}$; and in Experiment 1, r is drawn uniformly at random from $\mathcal{R}$, so $\Pr[\mathcal{A}(r) = 1] = \Pr[\mathcal{A}_a(r, s_{n+1}) = 1] = p_{a,1}$. Therefore, PRGadv$[\mathcal{A}_a, G_a] = |p_{a,0} - p_{a,1}| =$ PRGadv$[\mathcal{A}, G]$, which is negligible by security of G, and thus G_a is secure.

(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. We construct $\mathcal{A}_b$ to simply output the last bit of its input. In Experiment 0, $G_a(s_1 \dots s_n 0) = (G(s_1 \dots s_n), 0)$ is given to $\mathcal{A}_b$, and therefore $\mathcal{A}_b$ always outputs 0. In Experiment 1, a uniformly random element of $\mathcal{R} \times \{0,1\}$ is given $\mathcal{A}_b$; thus, the last bit of the value given to $\mathcal{A}_b$ is uniformly random and therefore $\mathcal{A}_b$ outputs 1 with probability $1/2$. Thus its advantage is $1/2$.

(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.

Constrution of G_c. Let us view the seed s of G_c as an n-bit string s_0 followed by a single bit p. We construct $G_c(s_0 \parallel p)$ as follows:

- $s_1 = p \oplus (\text{parity}(s_0))$
- output $G_a(s_0 \parallel s_1)$

Proof of security of G_c Option 1: If $(s_0 \parallel p)$ is chosen uniformly, then so is $(s_0 \parallel s_1)$, because for every s_0, s_1 will be 0 with probability $1/2$ (when $p = \text{parity}(s_0)$) and 1 with probability $1/2$ (when $p \neq \text{parity}(s_0)$). So the output of G_c on a uniform seed has the same distribution as the output of G_a on a uniform seed. Since they have the same output distribution and G_a is secure, G_c is also secure.
Option 2: Alternatively, to show that G_c is secure, we can do essentially the same reduction as in part (a). In particular, let $\mathcal{A}_c$ be any adversary attacking G_c. We construct $\mathcal{A}(r)$ to output $\mathcal{A}_c(r, s_1)$ where s_1 is drawn uniformly at random. Let $p_{c,0}, p_{c,1}$ be the probabilities that $\mathcal{A}_c$ outputs 1 in Experiment 0 and Experiment 1 of PRG attack game for G_c respectively. In Experiment 0 of PRG attack game for G, $\Pr[\mathcal{A}(r) = 1] = \Pr[\mathcal{A}_c(G(s_0), s_1) = 1] = \Pr[\mathcal{A}_c(G_c(s_0 \parallel p)) = 1]$, where $p = s_1 \oplus \text{parity}(s_0)$ (because $G_c(s_0 \parallel p)$ will output $(G(s_0), p \oplus (\text{parity}(s_0)) = (G(s_0), s_1))$. Since s_1 is uniform for every s_0, so is p. This probability is $p_{c,0}$ by definition of $p_{c,0}$. In Experiment 1, r is drawn uniformly at random from $\mathcal{R}$, so $\Pr[\mathcal{A}(r) = 1] = \Pr[\mathcal{A}_c(r, s_1) = 1] = p_{c,1}$. Therefore, PRGadv$[\mathcal{A}_c, G_c] = |p_{c,0} - p_{c,1}| =$ PRGadv$[\mathcal{A}, G]$, which is negligible by security of G, and G_c is secure.

Proof of Insecurity When Parity of the Seed is 0. We now show that G_c is insecure if it's used only on seeds of 0 parity. We will show that $\mathcal{A}_b$ from part (b) breaks G_c under the distribution in question.

In Experiment 0, $G_c(s_0 \parallel b) = (G(s_0), \text{parity}(s_0) \oplus b) = (G(s_0), 0)$ is given to $\mathcal{A}_b$, and therefore it also always outputs 0. Experiment 1 is the same as in part (b). Therefore its advantage is still $1/2$.

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. Let G be G_a as defined in problem 3a. We construct $\mathcal{A}(r)$ as follows: split r into its constituent parts r_1 and r_2, and output 1 iff the final bit of r_1 and r_2 are the same. In experiment 0 of the PRG attack game, the challenger samples a seed s and we have $r_1 = G_a(s)$ and $r_2 = G_a(s+1)$. The last bit of r_1 and r_2 are the final bit of s and $s+1$ respectively. Since these values differ by 1, the last bit is always different, so $\mathcal{A}$ outputs 1 with probability 0.

In experiment 1, r is sampled uniformly at random, so the last bits of r_1 and r_2 are equal with probability $\frac{1}{2}$, making $\mathcal{A}$ output 1 with probability $\frac{1}{2}$. Therefore, $\text{PRGadv}[\mathcal{A}, G'] = |0 - \frac{1}{2}| = \frac{1}{2}$, which is non-negligible.