CS442: Introduction to Cryptography Instructor: Aarushi Goel

Homework 5

Due: May 3; 2026 (11:59 PM)

Recall the decisional Diffie-Hellman assumption:

Decisional Deffie-Hellman (DDH) Assumption

Let $(\mathbb{G}, \cdot)$ be a cyclic group of prime order q with generator g and $x, y, z \xleftarrow{\$} \mathbb{Z}_q$, then the following distributions are computationally indistinguishable:

$$(\mathbb{G}, g, q, g^x, g^y, g^{xy}) \approx_c (\mathbb{G}, g, q, g^x, g^y, g^z)$$

1 Pseudorandom Generators

1. **(10 points)** Consider the following function $\mathsf{G} : \mathbb{Z}_q^2 \mapsto \mathbb{G}^3$.

$$\mathsf{G}(x, y) \coloneqq (g^x, g^y, g^{xy}),$$

where $x, y \xleftarrow{\$} \mathbb{Z}_q$ constitute the seed. Prove that the above construction is a secure **Pseudorandom Generator (PRG)**.

Hint: To show that G is a secure PRG, you must prove that its output is pseudorandom. That is, its output on a uniformly random seed is computationally indistinguishable from a uniformly random element of the output space $\mathbb{G}^2$.

2. Consider the following function $\mathsf{F} : \mathbb{Z}_q^3 \mapsto \mathbb{G}^5$.

$$\mathsf{F}(x, y_1, y_2) \coloneqq (g^x, g^{y_1}, g^{xy_1}, g^{y_2}, g^{xy_2}),$$

where $x, y_1, y_2 \xleftarrow{\$} \mathbb{Z}_q$ constitute the seed. We want to show that this is also a secure PRG.

Proof. To show that F is a PRG, we need to prove that its output is pseudorandom. Equivalently, we must show that the following distributions are computationally indistinguishable:

$$\{(g^x, g^{y_1}, g^{xy_1}, g^{y_2}, g^{xy_2});\ x, y_1, y_2 \xleftarrow{\$} \mathbb{Z}_q\} \approx_c \{(g^x, g^{y_1}, g^{r_1}, g^{y_2}, g^{r_2});\ x, y_1, y_2, r_1, r_2 \xleftarrow{\$} \mathbb{Z}_q\}$$

We prove this using a hybrid argument. Consider the hybrids:

- $\mathcal{H}_0 \coloneqq \{(g^x, g^{y_1}, g^{xy_1}, g^{y_2}, g^{xy_2});\ x, y_1, y_2 \xleftarrow{\$} \mathbb{Z}_q\}$
- $\mathcal{H}_1$
- $\mathcal{H}_2 \coloneqq \{(g^x, g^{y_1}, g^{r_1}, g^{y_2}, g^{r_2});\ x, y_1, y_2, r_1, r_2 \xleftarrow{\$} \mathbb{Z}_q\}$

By the hybrid lemma, it suffices to prove that

$$\mathcal{H}_0 \approx_c \mathcal{H}_1 \quad \text{and} \quad \mathcal{H}_1 \approx_c \mathcal{H}_2.$$

(a) **(5 points) Define $\mathcal{H}_1$.**

(b) **(5 points) Prove that $\mathcal{H}_0 \approx_c \mathcal{H}_1$.**

(c) **(5 points) Prove that $\mathcal{H}_1 \approx_c \mathcal{H}_2$.**

2 Key-Exchange

(10 points) Consider the following protocol between Alice and Bob:

- **Alice:** Samples $a \xleftarrow{\$} \{0,1\}^n$ and sends a to Bob.
- **Bob:** Samples $b \xleftarrow{\$} \{0,1\}^n$ and sends $c = a \oplus b$ to Alice. Outputs $\mathsf{key} = b$.
- **Alice:** Outputs $\mathsf{key} = c \oplus a$.

Is this a secure key-exchange protocol? If so, explain why. If not, describe an attack that an evesdropper can use to learn the final key.

3 Public-Key Encryption

1. Let us consider the following variant of El Gamal public key encryption for encrypting messages $m \in \{0,1\}$:

   - $\mathsf{KeyGen} \to (\mathsf{pk}, \mathsf{sk})$: Sample a cyclic group $(\mathbb{G}, \cdot)$ of prime order q with generator g. Sample $x \xleftarrow{\$} \mathbb{Z}_q$ and compute $h = g^x$. Output $\mathsf{pk} = (\mathbb{G}, q, g, h)$ and $\mathsf{sk} = (\mathsf{pk}, x)$.
   - $\mathsf{Enc}(\mathsf{pk}, m) \to c$:
     - If $m = 0$, then sample $y \xleftarrow{\$} \mathbb{Z}_q$ and output $c = (c_1, c_2) = (g^y, h^y)$.
     - If $m = 1$, then sample $y, z \xleftarrow{\$} \mathbb{Z}_q$ independently and output $c = (c_1, c_2) = (g^y, h^z)$.

   (a) **(5+10 points)** Describe a corresponding decryption algorithm $\mathsf{Dec}(\mathsf{sk}, c)$. Also prove that the resulting scheme achieves **correctness, except with negligible probability**. That is, prove that the following holds for $\forall m \in \{0,1\}$:

   $$\Pr\left[\ \mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, m)) = m \ \mid\ (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}\ \right] \leq 1 - \mathsf{negl}$$

   (b) **(10 points)** Assuming the DDH assumption holds, prove that the resulting scheme is a **one-message secure public-key encryption**.

2. Let $(\mathsf{KeyGen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $(\mathsf{KeyGen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two public-key encryption schemes. Only one of these schemes is secure, but we don't know which one is secure. Now consider the following scheme:

   - $\mathsf{KeyGen} \to (\mathsf{pk}, \mathsf{sk})$: Sample $(\mathsf{pk}_1, \mathsf{sk}_1) \leftarrow \mathsf{KeyGen}_1$ and $(\mathsf{pk}_2, \mathsf{sk}_2) \leftarrow \mathsf{KeyGen}_2$. Output $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$ and $\mathsf{sk} = (\mathsf{sk}_1, \mathsf{sk}_2)$.
   - $\mathsf{Enc}(\mathsf{pk}, m) \to c$: Parse $\mathsf{pk} = (\mathsf{pk}_1, \mathsf{pk}_2)$. Compute and output $c = \mathsf{Enc}_1(\mathsf{pk}_1, m) \oplus \mathsf{Enc}_2(\mathsf{pk}_2, m)$

(a) **(5 points)** Describe a corresponding decryption algorithm $\mathsf{Dec}(\mathsf{sk}, c)$.

(b) **(10 points)** Prove that this is a **one-message secure public-key encryption**.