Foundations of Cryptography (CS60088)

Spring 2026

Tutorial 2: Computational secrecy and pseudorandom objects

1. Let G be a pseudorandom generator (PRG) that stretches n-bit strings to $2n$-bit strings. For $s \in \{0,1\}^n$, write
$$G(s) = G_0(s) \,\|\, G_1(s),$$
where $G_0(s)$ denotes the first n bits of $G(s)$ and $G_1(s)$ denotes the last n bits. Define a new generator G' that stretches n-bit strings to $4n$-bit strings as
$$G'(s) = G(G_0(s)) \,\|\, G(G_1(s)).$$
Prove or disprove that if G is a secure PRG, then G' is also a secure PRG.

2. Suppose G_1 and G_2 are PRGs mapping $\{0,1\}^n$ to $\{0,1\}^\ell$. Define a new generator
$$G : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^\ell$$
by
$$G(s_1, s_2) = G_1(s_1) \oplus G_2(s_2).$$
Show that if either G_1 or G_2 is secure (we may not know which one), then G is a secure PRG.

3. (a) Formally define (using a security game) the notion of *perfect secrecy under chosen-plaintext attacks*, also called *perfect IND-CPA security*, for symmetric encryption schemes. Your definition should be analogous to perfect secrecy in the presence of an eavesdropper.
   (b) Show that there cannot exist an encryption scheme that achieves perfect IND-CPA security.

4. Let $E_1 = (\mathsf{Gen}_1, \mathsf{Enc}_1, \mathsf{Dec}_1)$ and $E_2 = (\mathsf{Gen}_2, \mathsf{Enc}_2, \mathsf{Dec}_2)$ be two symmetric encryption schemes over message spaces $\mathcal{M}_1, \mathcal{M}_2$, key spaces $\mathcal{K}_1, \mathcal{K}_2$, and ciphertext spaces $\mathcal{C}_1, \mathcal{C}_2$, respectively. You are given that exactly one of E_1 or E_2 is IND-CPA-secure, but you do not know which one.
   Assume $\mathcal{M}_1 = \mathcal{M}_2 = \{0,1\}^n$. Construct an encryption scheme
$$E = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$$
from E_1 and E_2 that is guaranteed to be IND-CPA-secure. Prove that your construction is indeed IND-CPA-secure.

5. Let $G : \{0,1\}^n \to \{0,1\}^\ell$ be a pseudorandom generator, and define $G'(s)$ to be the first n bits of $G(s)$. Consider the keyed function $F_k : \{0,1\}^n \to \{0,1\}^n$ defined by
$$F_k(x) = G'(k) \oplus x,$$
where $k \in \{0,1\}^n$. Is the family $\{F_k\}$ pseudorandom? Justify your answer.

6. Let $\mathcal{F} = \{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^n}$ be a pseudorandom function family, and let G be a pseudorandom generator with input length n and output length $\ell = n + 1$. In each of the following schemes, the shared key k is chosen as $k \xleftarrow{U} \{0,1\}^n$.

   For each scheme, state whether it is IND-EAV-secure and whether it is IND-CPA-secure. Justify your answer.

   (a) To encrypt $m \in \{0,1\}^{2n+2}$, parse m as $m_1 \,\|\, m_2$ with $|m_1| = |m_2|$, and output

   $$\langle G(k) \oplus m_1,\ G(k+1) \oplus m_2 \rangle.$$

   (b) For $m \in \{0,1\}^{n+1}$, choose $r \xleftarrow{U} \{0,1\}^n$ and output

   $$\langle r,\ G(r) \oplus m \rangle.$$

   (c) Encrypt $m \in \{0,1\}^n$ as

   $$m \oplus F_k(0^n).$$

   (d) Parse $m \in \{0,1\}^{2n}$ as $m_1 \,\|\, m_2$ with $|m_1| = |m_2|$, choose $r \xleftarrow{U} \{0,1\}^n$, and output

   $$\langle r,\ m_1 \oplus F_k(r),\ m_2 \oplus F_k(r+1) \rangle.$$

7. Let F be a length-preserving pseudorandom function. For each of the following constructions of a keyed function

   $$F' : \{0,1\}^n \times \{0,1\}^{n-1} \to \{0,1\}^{2n},$$

   state whether F' is a pseudorandom function. If it is, prove it; otherwise, describe an explicit attack.

   (a) $F'_k(x) \stackrel{\text{def}}{=} F_k(0 \,\|\, x) \,\|\, F_k(1 \,\|\, x)$.

   (b) $F'_k(x) \stackrel{\text{def}}{=} F_k(0 \,\|\, x) \,\|\, F_k(x \,\|\, 1)$.

8. Prove unconditionally the existence of a pseudorandom function

   $$F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$$

   with key length $\ell_{\text{key}}(n) = n$ and input length $\ell_{\text{in}}(n) = O(\log n)$. *Hint:* Implement a uniform function with logarithmic input length.

9. Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$. In each of the following cases, determine whether the function G' is *necessarily* a pseudorandom generator. If yes, give a proof; if not, provide a counterexample.

   (a) Define

   $$G'(s) \stackrel{\text{def}}{=} G\big(s_1 \cdots s_{\lceil n/2 \rceil}\big),$$

   where $s = s_1 s_2 \cdots s_n \in \{0,1\}^n$.

(b) Define

$$G'(s) \stackrel{\text{def}}{=} G\Big(0^{|s|} \,\|\, s\Big)\,.$$

(c) Define

$$G'(s) \stackrel{\text{def}}{=} G(s) \,\|\, G(s+1),$$

where $s+1$ denotes addition modulo 2^n.