Provable Security.

Take-Home Final.

Exercise 1 (20 points)**.** Show that indistinguishability is preserved under taking multiple independent (efficient) samples. That is, let X_1, X_2, Y_1, Y_2 be independent random variables where each is efficiently samplable by algorithm of running time t_s. If X_1 and Y_1 are (t,ε)-indistinguishable and so is X_2 and Y_2, i.e., for every probabilistic distinguisher D of running time t we have

$$|\Pr[\mathsf{D}(X_1)=1]-\Pr[\mathsf{D}(Y_1)=1]| \;\leq\; \varepsilon$$

$$|\Pr[\mathsf{D}(X_2)=1]-\Pr[\mathsf{D}(Y_2)=1]| \;\leq\; \varepsilon$$

Then, we must have that (X_1, X_2) and (Y_1, Y_2) are (t',ε')-indistinguishable, where t' and ε' are functions of t, t_s and ε.

Exercise 2 (20 points)**.** Suppose that $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private-key encryption scheme that has indistinguishable encryptions under a chosen-plaintext attack (i.e., CPA- secure) where by definition $\mathsf{Gen}(1^n)$ samples a key uniformly at random, i.e., $k \xleftarrow{\$} \{0,1\}^n$. Now if we replace Gen with Gen' that samples a key from a PRG $g : \{0,1\}^{n-1} \to \{0,1\}^n$, i.e., $k \leftarrow g(U_{n-1})$, then the resulting scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}, \mathsf{Dec})$ remains CPA-secure. Prove or disprove the argument.

Exercise 3 (20 points)**.** Let $\mathcal{G} = \{g : \{0,1\}^n \to \{0,1\}^{n-1}\}$ be a family of UOWHFs, prove or disprove that function f

$$f(g,x) \stackrel{\mathsf{def}}{=} (g, g(x)) \;,\; \text{where } g \xleftarrow{\$} \mathcal{G}, x \xleftarrow{\$} \{0,1\}^n$$

is a one-way function.
For simplicity, you can assume that every $g \in \mathcal{G}$ is a strictly 2-to-1 function and use the TCR2 property (instead of TCR).

Exercise 4 (20 points)**.** Let $f : \{0,1\}^n \to \{0,1\}^n$ be a (t,ε)-one-way permutation and for integer s define the following function

$$g(x, r^1, \ldots, r^s) \stackrel{\text{def}}{=} (f(x), r^1, \ldots, r^s, \mathsf{gl}(x, r^1), \ldots, \mathsf{gl}(x, r^s))$$

where $x, r^1, \ldots, r^s \in \{0,1\}^n$, and for every $j \in \{1, \ldots, s\}$: $\mathsf{gl}(x, r^j) = \bigoplus_{i=1}^n x_i \cdot r_i^j \pmod 2$, $x = x_1 \ldots x_n$ and $r^j = r_1^j \ldots r_n^j$.

1. Show that for appropriate value of s function g is a pseudorandom generator with stretch s (the case for $s = 1$ is given as Theorem 1 of Handout 4).
2. What is the upper bound on s to keep g a PRG (i.e., s cannot be too large as otherwise it will leak too much about x, and thus g is trivially broken)?

Hint: it suffices to show that for every $j \in \{1, \ldots, s\}$ function

$$f^{j-1}(x, r^1, \ldots, r^j) \stackrel{\text{def}}{=} (f(x), r^1, \ldots, r^j, \mathsf{gl}(x, r^1), \ldots, \mathsf{gl}(x, r^{j-1}))$$

is a one-way function (for some parameters related to ε, t and j) and thus $\mathsf{gl}(x, r^j)$ is a hard-core function of f^{j-1} (by Goldreich-Levin). Then we complete the proof for statement 1 by a hybrid argument. We can observe that the one-wayness of f^{j-1} deteriorates as the value of j increases, from which we can derive the upper bound on s.

Exercise 5 (20 points)**.** For a length-preserving function $f : \{0,1\}^n \to \{0,1\}^n$, denote by $f^{-1}(y) \stackrel{\text{def}}{=} \{x : f(x) = y\}$ the set of preimages that map to y under f. We say that f is regular if every $y = f(x)$ has the same number (say α) of preimages, i.e., $|f^{-1}(y)| = \alpha$. Show that if we pick a random f from the set of all functions mapping n bits to n bits $\{ \{0,1\}^n \to \{0,1\}^n \}$, then f is almost regular in the following sense: for some constant α and any $0 < \delta < 1$ we have

$$\Pr_{f \stackrel{\$}{\leftarrow} \{\{0,1\}^n \to \{0,1\}^n\},\ x \stackrel{\$}{\leftarrow} \{0,1\}^n} [\ \alpha \ \leq \ |f^{-1}(f(x))| \leq \ O(\alpha/\delta)\ ] \geq 1 - \delta$$

and what is the value of α.
Hint: f is a random function drawn from $\{ \{0,1\}^n \to \{0,1\}^n \}$ (which is a universal hash function family). Consider the collision probability of $f(U_n)$ given a random f, i.e.,

$$\mathsf{CP}(f(U_n)|f) \stackrel{\text{def}}{=} \mathbb{E}_{f \stackrel{\$}{\leftarrow} \{\{0,1\}^n \to \{0,1\}^n\}} \left[\sum_{y \in \{0,1\}^n} \Pr[f(U_n) = y]^2 \right]$$

and then try to find a connection to exercise 4 from homework 2 (see Handout 2).