CS 6222, Homework 3

Instructor: Wei-Kai Lin

Total points: 30. Points are noted after each problem.

Problem 1 (1pt each).

(a) Suppose that $g : \{0,1\}^n \to \{0,1\}^{n+1}$ for all n is a PRG. Prove that g is also a (strong) OWF.

(b) Why expansion is necessary for PRG? Provide a counterexample $g : \{0,1\}^n \to \{0,1\}^n$ for all n such that g is easy to compute and is pseudo-random, but g is also easy to invert.

Problem 2 (1pt). For any $n, m \in \mathbb{N}$, let $(u_i : u_i \leftarrow \{0,1\}^n)_{i \in [\log m]}$ be strings independently sampled uniformly at random (we abuse notation and round up $\log m$ to the next integer). Define strings r_I for each $I \subseteq [\log m]$ to be

$$r_I := \bigoplus_{i \in I} u_i.$$

Prove that the random variables $(r_1, r_2, ..., r_m)$ are pairwise independent, where r_j denotes r_I such that I is the j-th subset of $[\log m]$. That is, for all $j \neq j' \in [m]$, for all $x, y \in \{0,1\}^n$, show that

$$\Pr[r_j = x \cap r_{j'} = y] = \Pr[r_j = x] \cdot \Pr[r_{j'} = y].$$

Problem 3 (2pt each). Let g be a pseudorandom generator. In each of the following cases, say whether g' is necessarily a pseudorandom generator. If yes, give a proof; if not, show a counterexample. [KL, Exercise 3.6]

(a) Define $g'(s) := g(\bar{s})$, where $\bar{s}$ is the (bitwise) complement of s.

(b) Define $g'(s) := \overline{g(s)}$.

(c) Define $g'(s) := g(0^{|s|} \| s)$.

(d) Define $g'(s) := g(s) \| g(s+1)$.

Problem 4 (1, 2, 2pt each). Let X, Y be finite discrete random variables. Recall that Shannon entropy is defined to be

$$H(X) := \sum_x \Pr[X = x] \cdot \log \frac{1}{\Pr[X = x]},$$

which is the average amount of information obtained by observing (the value of) X. The *conditional Shannon entropy* is defined to be

$$H(Y|X) := \sum_{x,y} \Pr[Y = y \cap X = x] \cdot \log \frac{1}{\Pr[Y = y | X = x]},$$

which is the average amount of information obtained by observing (the value of) Y after X is known. (Both definitions follow the convention that divide-by-0 is skipped.)

(a) Suppose that X and Y are independent. Prove that $H(Y|X) = H(Y)$.

(b) Prove that $H(XY) = H(Y|X) + H(X)$ for (possibly) dependent (X, Y), where XY denotes the concatenated random variable of X and Y.

(c) For any function f, prove that $H(f(X)|X) = 0$. (Notice that means, for any $Y = f(X)$ that is determined by X, $H(Y|X) = 0$.)

Problem 5 (2pt)**.** Prove *unconditionally* the existence of a pseudorandom function

$$F = \left\{ f_s : \{0,1\}^{\log n} \to \{0,1\} \text{ such that } s \leftarrow \{0,1\}^n \right\}_{n\in\mathbb{N}}.$$

Notice that by unconditional, we mean the function is indistinguishable even for unbounded (including exponential time) algorithms, and it is sometimes called statistically secure. [KL, Exercise 3.10]

Problem 6 (2pt each)**.** Let $F = \{f_s : \{0,1\}^n \to \{0,1\}^n \mid s \in \{0,1\}^n\}_{n\in\mathbb{N}}$ be a length preserving pseudorandom function. For the following constructions of a keyed function f'_s, state whether $F' = \{f'_s : \{0,1\}^{n-1} \to \{0,1\}^{2n} \mid s \in \{0,1\}^n\}_{n\in\mathbb{N}}$ is a pseudorandom function. If yes, prove it; if not, show an attack. [KL, Exercise 3.11]

(a) $f'_s(x) := f_s(0\|x)\|f_s(0\|x)$.

(b) $f'_s(x) := f_s(0\|x)\|f_s(1\|x)$.

(c) $f'_s(x) := f_s(0\|x)\|f_s(x\|0)$.

(d) $f'_s(x) := f_s(0\|x)\|f_s(x\|1)$.

Problem 7 (2pt each)**.** For any function $g : \{0,1\}^n \to \{0,1\}^n$, define $g^{\$}(\cdot)$ to be a probabilistic oracle that, on input 1^n, chooses uniform $u \in \{0,1\}^n$ and returns the pair $(u, g(u))$. A family of keyed functions $F = \{f_s\}_{s\in\mathbb{N}}$ is a *weak pseudorandom function* if for all NUPPT algorithms D, there exists a negligible function ϵ such that

$$\left| \Pr[s \leftarrow \{0,1\}^n; D^{f_s^{\$}(\cdot)}(1^n) = 1] - \Pr[r \leftarrow \mathsf{RF}; D^{r^{\$}(\cdot)}(1^n) = 1] \right| \le \epsilon(n)$$

(a) Prove that if F is pseudorandom then it is weakly pseudorandom.

(b) Let $F' = \{f'_s : \{0,1\}^n \to \{0,1\}^n \mid s \in \{0,1\}^n\}_{n\in\mathbb{N}}$ be a family of pseudorandom function, and define

$$f_s(x) := \begin{cases} f'_s(x) & \text{if } x \text{ is even} \\ f'_s(x+1) & \text{if } x \text{ is odd,} \end{cases}$$

where $x \in \{0,1\}^n$ is interpreted as a n-bit non-negative integer for even, odd, and addition. Prove that $F = \{f_s \mid s \in \{0,1\}^n\}_{n\in\mathbb{N}}$ is weakly pseudorandom, but not pseudorandom.

[KL, Exercise 3.28]