CS 6222-Cryptography, Homework 2

Response by: Your Name, (computing id)

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

Directions. For each problem, typeset your solution in the `answer` environment, and if there are sub-problems, mark them clearly. Feel free to use as much space as you want to. Before you submit the PDF, update 1) "Your Name" and id on the above, and 2) the "Acknowledgement" box at the last page properly.

Policies. We re-iterate our policy. It is encouraged to think and discuss the problems before looking for ready-made solutions. You shall acknowledge and/or reference any discussion and published material except for lecture notes and resources of LaTeX. In any case, it is a violation if any of the following cases happens:

- You copied text directly (from any source).
- You used any material or discussion without acknowledgement or citation.
- You are unable to explain your work orally.

This homework reviews some concepts, including negligible, computational indistinguishability, and PRG. Problems 2 and 3 are facts in probability that will be used later in the course.

Problem 1 (Negligible functions, 1pt each)**.** True or False. Please provide a one-sentence explanation. All the functions below are defined over $n \in \mathbb{N}$.

(a) $2^{-n/4}$ is a negligible function.

(b) $2^{-100 \log n}$ is a negligible function.

(c) For any polynomial $a(n) \geq n$, $\left(1 - \frac{1}{a(n)}\right)^{a(n) \cdot n}$ is a negligible function.

(d) For any polynomial $a(n) \geq n$ and for any negligible function $\epsilon(n)$, $a(n) \cdot \epsilon(n)$ is a negligible function.

Problem 2 (Majority of random variables, 4pt each)**.** Let $\alpha > 0$ be a constant. Consider fixed strings x, y and a probabilistic polynomial-time algorithm A such that

$$\Pr_r[A(y; r) = x] \geq 1/2 + \alpha.$$

That is, $A(y; r)$ outputs x with probability at least $1/2 + \alpha$, where the probability is taken over the uniform random tape r used by A. Assume without loss of generality, the length of random tape $|r| = \ell(n)$ for some polynomial ℓ and $n := |y|$ is the input length. We want to amplify the probability of obtaining x by repeatedly running A using different random tapes. Consider the following procedure:

1. Let $r_1, r_2, ..., r_t$ be t random tapes for some fixed t; see below for the distribution of the random tapes.
2. Compute $z_i \leftarrow A(y; r_i)$ for all $i = 1, ..., t$ (thus z_i is a random variable depends on r_i).
3. Let z be the majority in the sequence $(z_1, ..., z_t)$ (that is, z is the string that appeared the maximal number of times in the sequence, and we break tie arbitrarily).

We sample the random tapes $(r_1, r_2, ..., r_t)$ from different distributions below, and then you are asked to provide an upper bound on the failure probability.

(a) Sample the random tapes independently and uniformly, i.e., $r_i \leftarrow \{0,1\}^\ell$ for all $i \in [t]$. Find an upper bound on $\Pr[z \neq x]$ using Chernoff's inequality (as a function of α, t).

(b) Sample the t random tapes $(r_1, r_2, ..., r_t)$ uniformly but only *pairwise independent*. Find an upper bound on $\Pr[z \neq x]$ using Chebyshev's inequality (as a function of α, t).

Remark: Notice that we can sample the pairwise independent random tapes using only $\ell \cdot \log t$ uniformly random bits, but the fully independent tapes take $\ell \cdot t$ uniformly random bits. The pairwise independence approach can be more efficient in the *number* of random bits.

Problem 3 (Statistically close distributions, 3pt)**.** For random variables X and Y taking values in U, their statistical difference (also known as variation distance) is

$$\Delta(X, Y) := \max_{T \subset U} |\Pr[X \in T] - \Pr[Y \in T]|.$$

Let $\mathcal{X} = (X_1, X_2, ...)$ and $\mathcal{Y} = \{Y_1, Y_2, ...\}$ be two ensembles of distributions. Suppose that there exists a function $\epsilon(n)$ such that for all $n \in \mathbb{N}$, $\Delta(X_n, Y_n) \leq \epsilon(n)$. Prove that for any deterministic algorithm D, for all $n \in \mathbb{N}$,

$$\left| \Pr_{t \leftarrow X_n}[D(t) = 1] - \Pr_{t \leftarrow Y_n}[D(t) = 1] \right| \leq \epsilon(n).$$

Remark: we say $\mathcal{X}$ and $\mathcal{Y}$ are *statistically close* iff ϵ is negligible. This proves that statistically close ensembles are always indistinguishable for even (non-uniform probabilistic) unbounded-time D.

Problem 4 (PRG, 3pt each)**.** Let g be a pseudorandom generator. In each of the following cases, prove that g' is also a pseudorandom generator, or provide a counterexample (that shows g' is not PRG even g is).

(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 $g'(s) := g(s \| 000)$, where $s \| s'$ denotes the concatenation of string s and s'.

(d) Define $g'(s) := g(s \| 0^{|s|})$, where $0^{|s|}$ denotes the $|s|$-bit and all 0 string.

Problem 5 (3pt)**.** Prove *unconditionally* the existence of a family of "pseudorandom" functions

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

such that F is oracle indistinguishable from the random functions of the same input/output length,

$$RF = \left\{ f : \{0,1\}^{\log n} \to \{0,1\} \right\}_{n \in \mathbb{N}}.$$

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

Acknowledgement

Replace this with your collaborators and resources like below (if you did not have any, replace this with *None*).

Problem 1 is inspired by a discussion with Jonathan, who explained Extended Euclidean Algorithm to me.

Problem 2: I used ChatGPT with the prompt "teach me DMT2" and obtained XXX.

Problem 3: Step X is followed by [KL21, Theorem Y, page Z].

References

[KL21] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. CRC Press, Massachusetts, 3 edition, 2021.