0368-4162-01: Foundation of Cryptography, Fall 2010
Instructors: Ran Canetti and Iftach Haitner

Problem Set 1

November 16, 2010 Due: Nov 22 in class

We let poly denote the set of all polynomial p. Given $x \in \{0,1\}^*$, we let $|x|$ denote its length and let $x[i]$, for $1 \leq i \leq |x|$, stands for the i'th bit of x. Recall that $[n] := \{1, \cdots, n\}$ and that U_n is a random variable uniformly distributed over $\{0,1\}^n$. Given a random variable X, by $x \leftarrow X$ we mean that x is sampled according to X (uniformly from X, if X is a set). Given a function f, we let $f(X)$ denote the random variable induced by applying f to a random sample from X. Given a set T, the shorthand $\Pr_X[T]$ stands for $\Pr_{x \leftarrow X}[x \in T]$ (stands for $\Pr_{x \leftarrow X}[x = T]$, if T is an element). Finally, everything is stated (and should be answered) in the uniform model, i.e., adversaries are uniform algorithms.

1. **An alternative definition of statistical distance :** Recall that the statistical distance between two distributions X and Y over a universe $\mathcal{U}$ is defined as

$$\mathrm{SD}(X,Y) := \max_{\mathcal{S} \subseteq \mathcal{U}} |\Pr_X[\mathcal{S}] - \Pr_Y[\mathcal{S}]|.$$

   (a) (15 points) Prove that for any such two distributions it holds that

$$\mathrm{SD}(X,Y) = \frac{1}{2} \cdot \sum_{u \in \mathcal{U}} \left| \Pr_X[u] - \Pr_Y[u] \right|.$$

   (b) (10 points) Show that for any such two distributions, there always exists an algorithm A such that

$$\mathrm{SD}(X,Y) = \Delta^A(X,Y) := \Pr_{u \leftarrow X}[A(u) = 1] - \Pr_{u \leftarrow Y}[A(u) = 1].$$

2. (15 points) **Hardcore bit for one-way functions:** Let $f \colon \{0,1\}^n \mapsto \{0,1\}^n$ be a one-way function. Prove that for any PPT (probabilistic polynomial-time algorithm) A and large enough n it holds that

$$\Pr_{x \leftarrow \{0,1\}^n, i \leftarrow [n]}[A(f(x), i) = x[i]] \leq 1 - \frac{1}{2n^2}.$$

3. (15 points) **Failing sets:** Let $\delta : \mathbb{N} \mapsto [0,1]$ and let $f \colon \{0,1\}^n \mapsto \{0,1\}^n$ be a $(1-\delta(n))$-one-way function (i.e., for any PPT A and large enough n, it holds that $\Pr_{y \leftarrow f(U_n)}[A(y) \in f^{-1}(y)] \leq 1 - \delta(n)$). Prove that for any PPT A, $p \in$ poly and large enough n, there exists a set $\mathcal{S}_n \subseteq \{0,1\}^n$ such that the following hold:

(a) $\Pr_{f(U_n)}[\mathcal{S}_n] \geq \delta(n)/2$, and

(b) $\Pr[A(y) \in f^{-1}(y)] \leq \frac{1}{p(n)}$, for any $y \in \mathcal{S}_n$.

4. (15 points) **Hardness amplification via iterations:** Prove or disprove: let $q \in \text{poly}$ and let $f \colon \{0,1\}^n \mapsto \{0,1\}^n$ be a $(1 - \frac{1}{q(n)})$-one-way permutation. Let $f^1(x) := f(x)$ and for $i \in \mathbb{N}$ let $f^{i+1}(x) := f(f^i(x))$. Then there exists $p \in \text{poly}$ such that the function $f_p : \{0,1\}^n \mapsto \{0,1\}^n$, defined by $f_p(x) = f^{p(|x|)}(x)$, is one way.

5. (15 points) **Hardness of the Discrete Log function:** Let $\mathrm{P} = \{(p_n, g_n)\}_{n\in\mathbb{N}}$ be such that $2^n < p_n < 2^{n+1}$ is a prime and g_n is a generator of the group $Z^*_{p_n}$. Further, assume that p_n and g_n can be computed in polynomial time from 1^n. The Discrete Log function $\mathrm{DL}_\mathrm{P} \colon \mathbb{Z}^*_{p_n} \mapsto \mathbb{Z}^*_{p_n}$ is defined as $\mathrm{DL}_\mathrm{P}(x) := g_n^x \bmod p_n$, where $n = |x|$. Prove that DL_P is one way iff it is $(1 - \frac{1}{p(n)})$-one way for some (positive) $p \in \text{poly}$.

6. (15 points) **Distinguishing to predicting:** Let X_n be a distribution ensemble over $\{0,1\}$, let $\varepsilon : \mathbb{N} \mapsto [0,1]$ and let A be a PPT such that

$$\Pr[A(1^n) = X_n] \geq \frac{1}{2} + \varepsilon(n),$$

for every n. Prove that there exists a PPT B such that the following holds (for every n):

$$\Pr[B(1^n, X_n) = 1] - \Pr[B(1^n, U_1) = 1] \geq \varepsilon(n)$$