COMS E6261: Advanced Cryptography: Minimalist Cryptography.
Instructor: Prof. Tal Malkin

Problem Set 1

Due: Tuesday 2/9/16 by 10:10am (in class).

0. I highly recommend that you read the following proofs of theorems we gave in class. However, this reading assignment is not necessary for the rest of the problem set.

   (a) Universal OWF: [Ps, 2.13]

   (b) Goldreich-Levin theorem (hard-core predicates from every OWF): [Gol, 2.5.2]

   [Ps] is Pass-shelat textbook, and [Gold] is Goldreich's textbook (see the class webpage for complete references for these books).

1. (a) Let $b : \{0,1\}^n \rightarrow \{0,1\}$ be an efficiently computable predicate. Prove that if one-way functions exist, then there exists a one-way function f such that b is *not* a hard-core predicate for f.

   (b) The previous part proves that there is no universal hard-core predicate that works for every one-way function. Why does this not contradict the Goldreich-Levin theorem?

2. Here you will prove that a one-way function may leak information about every one of its input bits (namely no input bit is a hard-core bit for this function). In more detail:

   Prove that if there exist one-way functions, then there exists a one-way function f and a polynomial $p()$ such that for every i there exists a ppt algorithm A_i such that for all $n \geq i$,

   $$\mathrm{Prob}_{x=x_1,\ldots,x_n \leftarrow \{0,1\}^n}[A_i(f(x)) = x_i] \geq \frac{1}{2} + \frac{1}{p(n)}$$

3. Recall that $f : \{0,1\}^* \rightarrow \{0,1\}^*$ is a *worst-case one-way function* if f is efficiently computable, and for all ppt A

   $$\mathrm{Prob}_{x \leftarrow \{0,1\}^n, y=f(x)}[A(y) \in f^{-1}(y)] < 1$$

   (a) Prove that if $\mathcal{NP} \not\subseteq \mathcal{BPP}$, then there exists a worst-case one-way function.

   Guidance: take some $\mathcal{NP}$-complete language, and use it to define a function such that an algorithm to invert the function with probability 1 can be used to decide the language.

   (b) Prove that if there exists a worst-case one-way function, then $\mathcal{P} \neq \mathcal{NP}$.