Homework is due by **noon of Sep 23**. Send by email to Oded with subject line "CSCI-GA 3210 Homework 2" and name the attachment "YOUR NAME.tex/pdf". Please also bring a printed copy to class. Start early!

Instructions. Solutions must be typeset in LaTeX (a template for this homework is available on the course web page). Your work will be graded on *correctness*, *clarity*, and *conciseness*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea. You may collaborate with others on this problem set and consult external sources. However, you must ***write your own solutions*** and ***list your collaborators/sources*** for each problem.

1. *(Weak vs strong one-way functions.*♣*)* Try to complete the proof from class, showing that the existence of weak one-way functions implies the existence of strong one-way functions. At the very least, formally write what needs to be proven, and suggest ways to prove it, or explain attempts that do not work.

2. *(Fun with one-way functions.)*

   (a) (2 points) Assume we modify the definition of a one-way function by allowing the adversary to output a *list* of supposed preimages, and he wins if at least one of them is a valid preimage (and as before the winning probability of any efficient adversary should be negligible). How does this modified definition compare with the original one? Formally prove your answer.

   (b) (2 points) [2] For a security parameter n, define $f : \{2^{n-1}, \ldots, 2^n\} \to \{1, \ldots, 2^{2n}\}$ by $f(x) = x^2$ (over the integers). Is it a one-way function? (Rabin's function is similar, except it's done in $\mathbb{Z}_N$)

   (c) (4 points) [3] Suppose that $f : \{0,1\}^* \to \{0,1\}^*$ is such that $|f(x)| \le c \log |x|$ for every $x \in \{0,1\}^*$, where $c > 0$ is some fixed constant. (Here $|\cdot|$ denotes the length of a string.) Prove that f is *not* a one-way function. (You may use a *non-uniform* inverter in your solution; for one bonus point, use a uniform one.)

   (d) (5 points) [2] Assume $g : \{0,1\}^n \to \{0,1\}^n$ is a one-way function. Is the function $f : \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined by $f(x_1, x_2) = (g(x_1), g(x_1 \oplus x_2))$ necessarily also a one-way function?

   (e) (3 points) (bonus[4]) Show that there exists a one-way function $f : \{0,1\}^n \to \{0,1\}^n$ for which the function $f'(x) := f(x) \oplus x$ is *not* one-way. You can assume the existence of a one-way function $g : \{0,1\}^n \to \{0,1\}^n$ for all n.

3. (6 points) *(Worst-case to average-case reduction.[3])* Let N be the product of two distinct n-bit primes, and suppose there is an efficient algorithm $\mathcal{A}$ that computes square roots on a noticeable fraction of quadratic residues mod N:

   $$\Pr_{y \leftarrow \mathbb{QR}_N^*}[\mathcal{A}(N, y) \in \sqrt{y} \bmod N] = \delta \ge 1/\operatorname{poly}(n).$$

   Construct an efficient algorithm $\mathcal{B}$ that, using $\mathcal{A}$ as an oracle, computes the square root of *any* $y \in \mathbb{QR}_N$ with *overwhelming* probability (solely over the random coins of $\mathcal{A}$ and $\mathcal{B}$). That is, for every $y \in \mathbb{QR}_N$, it should be the case that

   $$\Pr[\mathcal{B}^{\mathcal{A}}(N, y) \in \sqrt{y} \bmod N] = 1 - \operatorname{negl}(n).$$

   Explain in your own words why such reductions are known as worst-case to average-case reductions.

♣Again, this is a question meant to encourage you to think; you are not required to solve it fully, but you are required to demonstrate that you thought about it seriously.

[2]A question from Dodis's class

[3]A question from Peikert's class

[4]By Bao Feng, as appears in Goldreich's book