Introduction to Cryptography
Courant, Fall 2016

Homework 8

Instructor: Oded Regev
Student: YOUR NAME HERE

Homework is due by **7am of Nov 21**. Send by email to both "regev" (under the cs.nyu.edu domain) and "avt237@nyu.edu" with subject line "CSCI-GA 3210 Homework 8" and name the attachment "YOUR NAME HERE HW8.tex/pdf". There is no need to print it. 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 are expected to read all the hints either before or after submission, but before the next class.

You may collaborate with others on this problem set and consult external sources. However, you must ***write your own solutions***. You must also ***list your collaborators/sources*** for each problem.

1. [1] Consider the following stateless SKE for a PRF family $\{f_k\}_k$. The secret key is a uniform $k \in \{0,1\}^n$. To encrypt $m \in \{0,1\}^n$ choose $r \in \{0,1\}^n$ uniformly and output the pair $(r, f_r(k) \oplus m)$.
   (a) (1 point) Describe a decryption procedure, and prove correctness.
   (b) (6 points) Is the scheme secure? (and under which definition?) Here is a small hint for half a point (ID 90015) A bigger hint for 2 points (ID 90016)

2. (CCA security)[2] Recall the PRF-based "XOR" stateless secret-key encryption scheme we had in class. The key is a uniform $k \in \{0,1\}^n$. To encrypt $m \in \{0,1\}^n$, choose a uniform $r \in \{0,1\}^n$ and output $(r, f_k(r) \oplus m)$. To decrypt (r, c), output $f_k(r) \oplus c$. We showed that this scheme is IND-CPA (chosen plaintext) secure. Here we consider two stronger security notions against *chosen ciphertext* attacks in which the adversary has access to the decryption oracle, $\mathrm{Dec}_k(\cdot)$ in addition to $\mathrm{Enc}_k(\cdot)$ and the challenge oracle. In the first one, called *lunch-time attack security* or IND-CCA1 security, the adversary can call only before calling the challenge oracle. In the second, IND-CCA2 security, he can also call it after calling the challenge oracle, but then, of course, he is not allowed to call the decryption oracle with the ciphertext returned to it by the challenge oracle (why?).
   (a) (4 points) Show that the XOR scheme is not IND-CCA2 secure.
   (b) (8 points) Prove that the XOR scheme is IND-CCA1 secure.
   (c) (4 points) (Extra Credit) Let $\{f_k : \{0,1\}^{2n} \to \{0,1\}^{2n}\}$ be a family of *strong PRPs* on $2n$ bits. Consider the scheme in which we encrypt a message $m \in \{0,1\}^n$ by choosing $r \in \{0,1\}^n$ randomly, and outputting $f_k(m|r)$. To decrypt c, output the first half of $f_k^{-1}(c)$. Prove that this scheme is IND-CCA2 secure.

3. (0 points) *(Expanding domain of PRF.♣)* Assume we have a PRF family $\{f_k : \{0,1\}^n \to \{0,1\}^n\}_k$. Let $H = \{h_k : \{0,1\}^N \to \{0,1\}^n\}$ be another family of functions for some large N, say $N = n^2$. What property does H need to satisfy so that the family $\{f_k(h_{k'}(\cdot)) : \{0,1\}^N \to \{0,1\}^n\}$ is a PRF family (where k and k' are chosen independently from the corresponding set of keys)? E.g., can we take H to consist of just the function that outputs the first n bits of its input?

[1] A question asked in the Fall 2013 class by Huxley Bennett
[2] From Dodis