COS 496: Cryptography	Due: Nov 8

Problem Set 3

Professor Amit Sahai

Please list everyone you collaborated with when solving the problems on this problem set. If you make use of outside material, make a note of that as well. Make sure you write up your solutions on your own.

Problem 1. Prove that the existence of pseudorandom generators implies the existence of one-way functions.

Problem 2. Prove that the existence of a pseudorandom function family $\{F_k\}$, where $f \in F_k$ maps $\{0,1\}^k$ to $\{0,1\}$, implies the existence of one-way functions. (Prove this directly. Do not use the fact that secure MAC's imply the existence of one-way functions.)

Problem 3. Assume pseudorandom generators exist. Give an example of a pseudorandom generator which outputs half of its input bits, and prove that it is still a pseudorandom generator. (This first part is easy!) Then give an example of a pseudorandom function family which allows you to recover half the secret bits, and prove that it remains a pseudorandom function family.

Problem 4. In class, we saw the following definition of security for a public-key encryption scheme (G, E, D), which we call *indistinguishability-security*:

For all PPT M, A, there exists a negligible function $\alpha(k)$ such that for all sufficiently large k, when we consider the following experiment:

$$\begin{aligned}
(PK, SK) &\leftarrow G(1^k) \\
(m_0, m_1, \sigma) &\leftarrow M(PK) \\
b &\leftarrow \{0,1\} \\
c &\leftarrow E(m_b, PK) \\
b' &\leftarrow A(c, PK, \sigma)
\end{aligned}$$

we have that $\Pr[b' = b] \leq \frac{1}{2} + \alpha(k)$.

Suppose that the key generation algorithm requires k^2 random bits, but you only have a source of k random bits. Prove that if you use a pseudorandom generator to generate the k^2 random bits required by the key generation algorithm, the encryption scheme will still remain secure.

Problem 5. Suppose $G_k : \{0,1\}^k \to \{0,1\}^{2k}$ is a family of pseudorandom generators. Suppose $\pi_k : \{0,1\}^k \to \{0,1\}^k$ and $\pi'_k : \{0,1\}^{2k} \to \{0,1\}^{2k}$ are families of (arbitrary, not-necessarily polynomial-time computable) permutations.

- Must the output of $\pi'(G(s))$, when s is chosen randomly, be computationally indistinguishable from uniform?
- Must the output of $G(\pi(s))$, when s is chosen randomly, be computationally indistinguishable from uniform? Does this imply that $G \circ \pi$ is always a pseudorandom generator? (Be careful!)

- Do your answers above change if π and π' are known to be polynomial-time computable?

Problem 6. Suppose $G_k : \{0,1\}^k \to \{0,1\}^{2k}$ is a family of pseudorandom generators. Define $H(s) = (G(s), G(\bar{s}))$, where $\bar{s}$ denotes the bit-wise complement of s. Is H always a pseudorandom generator?

Denote the output of $G_k(s)$ as $(g_1(s), g_2(s))$ where $|g_1(s)| = |g_2(s)| = k$. Let $H_k(s) = (G_{2k}(g_1(s)), G_{2k}(g_2(s)))$. Is H always a pseudorandom generator?