Provable Security.

Take-Home Final. Submission deadline: June 30, 2018. E-mail address: yuyu@cs.sjtu.edu.cn

Exercise 1 (20 points)**.** Show that indistinguishability is preserved under taking multiple independent (efficient) samples. That is, let X_1, X_2, Y_1, Y_2 be independent random variables where each is efficiently samplable by algorithm of running time t_s. If X_1 and Y_1 are (t,ε)-indistinguishable and so is X_2 and Y_2, i.e., for every probabilistic distinguisher D of running time t we have

$$|\Pr[\mathsf{D}(X_1)=1]-\Pr[\mathsf{D}(Y_1)=1]| \;\leq\; \varepsilon$$

$$|\Pr[\mathsf{D}(X_2)=1]-\Pr[\mathsf{D}(Y_2)=1]| \;\leq\; \varepsilon$$

Then, we must have that (X_1, X_2) and (Y_1, Y_2) are (t',ε')-indistinguishable, where t' and ε' are functions of t, t_s and ε.

Exercise 2 (20 points)**.** Suppose that $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a private-key encryption scheme that has indistinguishable encryptions under a chosen-plaintext attack (i.e., CPA- secure) where by definition $\mathsf{Gen}(1^n)$ samples a key uniformly at random, i.e., $k \xleftarrow{\$} \{0,1\}^n$. Now if we replace Gen with Gen' that samples a key from a PRG $g : \{0,1\}^{n-1} \to \{0,1\}^n$, i.e., $k \leftarrow g(U_{n-1})$, then the resulting scheme $\Pi' = (\mathsf{Gen}', \mathsf{Enc}, \mathsf{Dec})$ remains CPA-secure. Prove or disprove the argument.

Exercise 3 (20 points)**.** Design an attack (with as much efficiency as possible) against the LPN problem with secret size n and noise rate $\mu = o(1)$, assuming you can obtain as many samples as needed. Analyze the time complexity of the attack you propose.
Notice: the noise rate is subconstant so the BKW algorithm may not be the best choice.

Exercise 4 (20 points)**.** Let $f : \{0,1\}^n \to \{0,1\}^n$ be a (t,ε)-one-way permutation and for integer s define the following function

$$g(x, r^1, \ldots, r^s) \stackrel{\text{def}}{=} (f(x), r^1, \ldots, r^s, \mathsf{gl}(x, r^1), \ldots, \mathsf{gl}(x, r^s))$$

where $x, r^1, \ldots, r^s \in \{0,1\}^n$, and for every $j \in \{1, \ldots, s\}$: $\mathsf{gl}(x, r^j) = \bigoplus_{i=1}^n x_i \cdot r_i^j \pmod 2$, $x = x_1 \ldots x_n$ and $r^j = r_1^j \ldots r_n^j$.

1. Show that for appropriate value of s function g is a pseudorandom generator with stretch s (the case for $s = 1$ is given as Theorem 1 of Handout 4).

2. What is the upper bound on s to keep g a PRG (i.e., s cannot be too large as otherwise it will leak too much about x, and thus g is trivially broken)?

Hint: it suffices to show that for every $j \in \{1, \ldots, s\}$ function

$$f^{j-1}(x, r^1, \ldots, r^j) \stackrel{\text{def}}{=} (f(x), r^1, \ldots, r^j, \mathsf{gl}(x, r^1), \ldots, \mathsf{gl}(x, r^{j-1}))$$

is a one-way function (for some parameters related to ε, t and j) and thus $\mathsf{gl}(x, r^j)$ is a hard-core function of f^{j-1} (by Goldreich-Levin). Then we complete the proof for statement 1 by a hybrid argument. We can observe that the one-wayness of f^{j-1} deteriorates as the value of j increases, from which we can derive the upper bound on s.

Exercise 5 (20 points)**.** Design secure multiparty computation protocols for the following scenarios, and justify the security.

1. Two parties P_1 and P_2 who want to compute the XOR sum of their respective inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ in the semi-honest adversary model.

2. t parties P_1, $\cdots$, P_t, who want to compute the (modulo p) sum of their respective values x_1,$\cdots$,x_t all over Z_p (for prime p) in the semi-honest adversary model.

3. assume there are t parties P_1, $\cdots$, P_t with respective inputs x_1, $\cdots$, x_t, and two semi-honest servers S_1 and S_2, where all parties and servers can communicate with each other securely. Design an efficient way to reduce the problem of multiparty computation of function $f(x_1, \cdots, x_t)$ among P_1, $\cdots$, P_t to that of two-party computation between S_1 and S_2, both in the semi-honest adversary model.