

**Problem Set 2**

December 11, 2008

Due: Monday Dec 22 in class

## 1. [30 points]

- (a) Show that if there exist one way functions then  $P \neq NP$ .
- (b) Show that if there exist strong pseudorandom permutations then there exist one way functions.
- (c) Show that if there exist pseudorandom permutations then there exist pseudorandom permutations which are not strong pseudorandom permutations.

2. [30 points] The GGM construction was presented in class as a construction of an ensemble of function families, where the  $n$ th family consists of functions from  $\{0, 1\}^n$  to  $\{0, 1\}^n$ . We wish to construct pseudorandom function family ensembles where the domain of the function is  $\{0, 1\}^*$ . (That is, the adversary can ask queries of any length; but since the adversary is polynomial, it can only ask queries of polynomial length.)

- (a) The GGM construction naturally works for inputs of any length. Is the resulting ensemble (of families where the functions have domain  $\{0, 1\}^*$  and range  $\{0, 1\}^n$ ) pseudorandom?
- (b) If your answer to the previous question is negative, then show how to construct ensembles of pseudorandom function families with domain  $\{0, 1\}^*$  and range  $\{0, 1\}^n$ .
- (c) How can we extend the *range* of the functions in the families in the GGM construction, say double the length?

3. [30 points] A family of functions  $H = \{h_k : \{0, 1\}^n \rightarrow \{0, 1\}^m\}_{k \in \{0, 1\}^a}$  is called **pairwise independent** if for any  $\alpha, \beta \in \{0, 1\}^n$ ,  $\alpha \neq \beta$ ,  $\text{Prob}_{k \leftarrow \{0, 1\}^a} [h_k(\alpha) = h_k(\beta)] = 1/2^m$ . (That is, the probability that two fixed points in the domain collide under  $h_k$  is exactly the same as if  $h_k$  were a truly random function from  $\{0, 1\}^n$  to  $\{0, 1\}^m$ .) There are many combinatorial constructions of pairwise independent hash functions families with relatively short keys.

- (a) Show that the family  $\{h_{A,b}(x) = Ax + b\}_{A \in \mathcal{A}_{n \times m}, b \in \{0, 1\}^m}$ , where  $\mathcal{A}_{n \times m}$  is the set of  $n$  by  $m$  binary matrices, and the arithmetic is done in  $F_2$ , is pairwise independent.
- (b) An ensemble  $H = \{H_n\}_{n \in \mathbf{N}}$  of families of functions is pairwise independent with range  $m(n)$  if for each  $n \in \mathbf{N}$  the family  $H_n$  consists of functions from  $\{0, 1\}^n$  to  $\{0, 1\}^m$  and is pairwise independent.

Show how to modify the GGM construction of pseudorandom function families so that each evaluation of the function on inputs in  $\{0, 1\}^n$  will involve only  $O(\log^2(n))$  applications of the underlying length-doubling pseudorandom generator. (Here  $n$  is taken to be the security parameter.)

Hint: Use pairwise independent ensembles.

4. [30 points] **Key Exchange from Trapdoor Permutations.**

- (a) Show that if trapdoor permutations exist then there exist trapdoor permutations with a hard-core predicate.
- (b) Recall that a protocol  $P = (A, B)$  is a Key Exchange protocol for domain  $D = \{D_n\}_{n \in \mathbf{N}}$  if (using the notations from class):

**Agreement:** For any  $n \in N$  and any  $r_A, r_B$  we have  $P(1^n, r_A; 1^n, r_B) = (y_A, y_B)$  where  $y_A = y_B$ .

**Secrecy:**  $\{\text{OUT} + \text{COM}_P(1^n; 1^n)\}_{n \in \mathbf{N}} \approx_c \{\text{COM}_P(1^n; 1^n), y, y\}_{n \in \mathbf{N}}$  where  $y \leftarrow D_n$  (namely,  $y$  is taken uniformly at random from  $D_n$ ).

Show that if trapdoor permutations exist then there exist key exchange protocols for the domain  $\{\{0, 1\}^n\}_{n \in N}$ .