CS 6222-Cryptography, Homework 3

Response by: Your Name, (computing id)

Total points: 30. Points are noted after each problem.

Directions. For each problem, typeset your solution in the `answer` environment, and if there are sub-problems, mark them clearly. Feel free to use as much space as you want to. Before you submit the PDF, update 1) "Your Name" and id on the above, and 2) the "Acknowledgement" box at the last page properly.

Policies. We re-iterate our policy. It is encouraged to think and discuss the problems before looking for ready-made solutions. You shall acknowledge and/or reference any discussion and published material except for lecture notes and resources of LaTeX. In any case, it is a violation if any of the following cases happens:

- You copied text directly (from any source).
- You used any material or discussion without acknowledgement or citation.
- You are unable to explain your work orally.

This homework reviews the concepts of PRFs and OWFs. It also discusses the implication of OWF on complexity.

Problem 1 (PRFs, 3pt each)**.** Let $F = \{f_s : \{0,1\}^n \to \{0,1\}^n \mid s \in \{0,1\}^n\}_{n\in\mathbb{N}}$ be a length preserving pseudorandom function. For the following constructions of a keyed function f'_s, state whether $F' = \{f'_s : \{0,1\}^{n-1} \to \{0,1\}^{2n} \mid s \in \{0,1\}^n\}_{n\in\mathbb{N}}$ is a pseudorandom function. If yes, prove it; if not, show an attack. [KL, Exercise 3.11]

(a) $f'_s(x) := f_s(0\|x)\|f_s(0\|x)$.

(b) $f'_s(x) := f_s(0\|x)\|f_s(1\|x)$.

(c) $f'_s(x) := f_s(0\|x)\|f_s(x\|0)$.

(d) $f'_s(x) := f_s(0\|x)\|f_s(x\|1)$.

Answer.

(a)

(b)

(c)

(d)

□

Problem 2 (Encryption implies OWF, 2pt each)**.** Suppose that $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is a (symmetric-key) CPA-secure encryption scheme for the message space $\mathcal{M} = 2n$, where n is the key size and also the input to Gen. Additionally, suppose that each of Gen and Enc uses a random tape of $\ell(n)$ bits (think $\ell = n$). Recall that by $\mathsf{Gen}(1^n; r)$ and $\mathsf{Enc}_k(m; r)$, we mean that the random tape r is

used by the algorithms $\mathsf{Enc}, \mathsf{Gen}$. For each of the following function f, answer if f is a OWF (True or False), and explain briefly your reason (in 1 paragraph).

(a) $f(x) := \mathsf{Enc}_x(0; 1^\ell)$

(b) $f(x) := \mathsf{Enc}_{\mathsf{Gen}(1^n;x)}(0; 1^\ell)$

Answer.

(a)

(b)

□

Problem 3 (Complexity of OWFs, 2pt)**.** Prove that if OWF exists, then **NP** $\not\subseteq$ **BPP**. (Note: **BPP** is defined as follows, and we have **P** $\subseteq$ **BPP**.)

The class **BPP** is the set of all decision problems solvable by a probabilistic Turing machine in polynomial time with an error probability bounded by $1/3$ for all instances. That is, a language L is in **BPP** if and only if there exists a probabilistic Turing machine M, such that

- M runs for polynomial time on all inputs $x \in \{0,1\}^*$ and $M(x) \in \{0,1\}$, and
- for all $x \in L$, $\Pr[M(x) = 1] \geq 2/3$, and
- for all $x \notin L$, $\Pr[M(x) = 0] \leq 1/3$.

Answer.

□

Problem 4 (OWFs, 3pt each)**.** Let $f_1, f_2 : \{\{0,1\}^n \to \{0,1\}^n\}_{n\in\mathbb{N}}$ be one-way functions. Prove or disprove each of the following function g is a OWF (there are 4 subproblems).

(a) $g(x) := f_1(x) \| (000\ldots0)$

(b) $g(x) := f_1(x) \oplus f_2(x)$

(c) $g(x) := f_1(x)[1, ..., \lfloor |x|/2 \rfloor]$

(d) $g(x) := f_1(f_2(x))$

Answer.

(a)

(b)

(c)

(d)

□

Acknowledgement

Replace this with your collaborators and resources like below (if you did not have any, replace this with *None*).

Problem 1 is inspired by a discussion with Jonathan, who explained Extended Euclidean Algorithm to me.

Problem 2: I used ChatGPT with the prompt "teach me DMT2" and obtained XXX.

Problem 3: Step X is followed by [KL21, Theorem Y, page Z].

References

[KL21] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. CRC Press, Massachusetts, 3 edition, 2021.