CS 4501-Cryptography, Homework 4

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 one-way functions and the hard-core lemma (actually all but Problem 2 are related to hard-core predicate). The the problems are ordered roughly by the difficulty level.

Problem 1 (5pt)**.** Show that if an efficiently computable one-to-one function f has a hard-core predicate, then f is one-way. [KL, Exercise 8.13]

Answer.

□

Problem 2 (8pts)**.** Let $f_1, f_2 : \{0,1\}^n \to \{0,1\}^n$ be one-way functions for all $n \in \mathbb{N}$. Prove or disprove each of the following function g is a OWF.

(a) $g(x) := f_1(x) \oplus 1^n$

(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)

□

Problem 3 (7pt)**.** For $x \in \{0,1\}^n$, represent $x = x_1...x_n$. Prove that if there exists a one-way function, then there exists a one-way function f such that for every i there is an algorithm A_i such that

$$\Pr_{x \leftarrow \{0,1\}^n}[A_i(f(x)) = x_i] \geq \frac{1}{2} + \frac{1}{2n}.$$

[KL, Exercise 8.12] (It could be tempting to think that any one-way function hides at least one *specific* bit of the input. This exercise demonstrates that is impossible.)

Answer.

□

Theorem 1 (Goldreich-Levin)**.** *Let $n, m \in \mathbb{N}$, let Q be a distribution over $\{0,1\}^n \times \{0,1\}^m$, and let D be an algorithm such that*

$$\Pr_{\substack{(x,y)\leftarrow Q \\ r\leftarrow\{0,1\}^n}}[D(y,r,x\odot r)=1] - \Pr_{\substack{(x,y)\leftarrow Q \\ r\leftarrow\{0,1\}^n \\ U\leftarrow\{0,1\}}}[D(y,r,U)=1] \geq \alpha$$

for some α. Then there exists a PPT $A^{D(\cdot)}$ (that means, A runs in polynomial time and queries D as an oracle for polynomial number of times) such that

$$\Pr_{(x,y)\leftarrow Q}\left[A^{D(\cdot)}(1^n, 1^{\lceil 1/\alpha \rceil}, y) = x\right] \geq \alpha^3/8n.$$

Problem 4 (5pt each)**.** This problem aims to extend the number of hard-core bits. Use Theorem 1 if you can. Suppose $f : \{0,1\}^n \to \{0,1\}^n$ is a one-way permutation for all $n \in \mathbb{N}$. In the following, x and r_i are n-bit for all i.

(a) Define g to be the following function:

$$g(x, r_1, r_2) := f(x)\|r_1\|x \odot r_1\|r_2\|x \odot r_2.$$

Prove that g is a PRG.

(b) Following the previous, g is PRG. Argue that

$$g'(x, r_1, r_2) := f(x)\|r_1\|r_2\|x \odot r_1\|x \odot r_2$$

is also a PRG.

(c) (Bonus, 5pt) Now, consider the integer $c := \lceil \log n \rceil$. Define

$$g(x, r_1, r_2, ..., r_c) := f(x)\|r_1\|r_2\|...\|r_c\|x \odot r_1\|x \odot r_2\|...\|x \odot r_c,$$

where $x, r_1, r_2, ..., r_c \in \{0,1\}^n$. Argue that g is still a PRG.

Answer.

(a)

(b)

(c)

□

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