CS-7810 Graduate Cryptography January 30, 2025

Problem Set 2

Lecturer: Daniel Wichs *Due: Feb 13, 2025*

Problem 1 (PRGs are OWFs) 10 pts

Show that if $G : \{\{0,1\}^n \to \{0,1\}^{2n}\}_{n\in\mathbb{N}}$ is a length-doubling pseudorandom generator (PRG) then G is a one-way function (OWF).

Optional (harder): does this hold if $G : \{\{0,1\}^n \to \{0,1\}^{n+1}\}_{n\in\mathbb{N}}$ *only outputs 1 extra bit?*

Problem 2 (Encryption and OWFs) 10 pts

Assume that $\mathsf{Enc}, \mathsf{Dec}$ is a one-time, computationally secure, deterministic encryption scheme with key size $\{0,1\}^n$ and message size $\{0,1\}^{n+1}$. Show how to construct a one-way function f using $\mathsf{Enc}, \mathsf{Dec}$.

Problem 3 (OWFs with Short Output Don't Exist) 5 pts

Let $f : \{0,1\}^* \to \{0,1\}^*$ be a function such that $|f(x)| \leq c \log |x|$ for all $x \in \{0,1\}^*$ and for some fixed constant $c > 0$. Show that f is not a one-way function.

Problem 4 (Shorten) 5 pts

Assume that $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way function (OWF). Show that $f'(x) = f(\mathit{short}(x))$ is also a OWF, where we define $\mathit{short}(x)$ denotes the first $\lceil n/2 \rceil$ bits of x.

What if we defined $\mathit{short}(x)$ to denote the first $\lceil \sqrt{n} \rceil$ bits of x? What if we define $\mathit{short}(x)$ to denote the firs $\lceil \log n \rceil$ bits of x? For what levels of "shortening" can you prove that the above holds?

Hint: it may be useful to rely on the above problem to solve some of the subsequent problems.

Problem 5 (OWF or Not?) 15 pts

Assume that $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way function (OWF). For each of the following candidate constructions f' argue whether it is also *necessarily* a OWF or not. If yes, give a proof else give a counter-example. For a counterexample, you should show that if OWFs exist then there is some function f which is one-way, but f' is not.

- $f'(x) = (f(x), x[1])$ where $x[1]$ is the first bit of x.
- $f'(x) = (f(x), x[1], \ldots, x[\lfloor n/2 \rfloor])$ where $n = |x|$ and $x[i]$ denotes the i'th bit of x.

- $f'(x) = f(x)||f(x+1)$ where $||$ denotes string concatenation and x is intepreted as an integer in binary with addition performed modulo 2^n for $|x| = n$.
- $f'(x) = f(G(x))$ where G is a pseudorandom generator.

Problem 6 (PRG or Not?) 15 pts

Assume that $G : \{\{0,1\}^n \to \{0,1\}^{2n}\}_{n\in\mathbb{N}}$ is a pseudorandom generator (PRG) with n-bit stretch. For each of the following candidate constructions argue whether it is also necessarily a PRG or not. If yes, give a proof else give a counter-example (showing that if PRGs exist then there exists some PRG G such that G' is not a PRF).

- $G'(x) = G(x+1)$ where addition is performed modulo 2^n for $x \in \{0,1\}^n$.
- $G'(x) = G(x||0)$ where $||$ denotes string concatenation.
- $G'(x) = G(x||G(x))$.
- $G'(x) = G(x) \oplus (0^n||x)$.
- $G'(x) = G(f(x))$ where f is a one-way function.

Problem 7 (PRF or Not?) 15 pts

Let F be a PRF family with n-bit key, n-bit input and n-bit output. For each of the following candidate constructions F' say whether F' is also necessarily a PRF. If so, give a proof else give a counter-example (showing that if PRFs exist then there exists some PRF F such that F' is not a PRF). Some of the candidates F' have different input/output lengths than F.

1. $F'_k(x) := F_k(x)||F_k(x+1)$ where $||$ denotes string concatenation and addition is modulo 2^n.
2. $F'_k(x) := F_k(x||0)||F_k(x||1)$ where $x \in \{0,1\}^{n-1}$.
3. $F'_k(x) := F_k(x) \oplus x$ where $\oplus$ denotes the bit-wise XOR operation.
4. $F'_k(x) := F_k(x) \oplus k$.
5. $F'_k(x) := F_x(k)$.

Problem 8 (One-Time Security: Alternate Definition) 10 pts

Our definition of one-time computationally secure encryption (see `https://www.khoury.northeastern.edu/home/wichs/class/crypto25/lecture4.pdf` section 5.1) considered two games $OneSec^b$ with $b = 0, 1$ which we required to be computationally indistinguishable. An alternate definition considers a single game $AltOneSec(n)$ which proceeds as follows:

- The adversary $A(n)$ chooses messages m_0, m_1 and gives them to the challenger

- The challenger chooses a uniformly random bit $b \leftarrow \{0,1\}$ and key $k \leftarrow \{0,1\}^n$. It encrypts the message m_b by setting $c = \mathsf{Enc}(k, m_b)$ and gives c to the adversary.
- The adversary outputs a "guess" b' and the game outputs 1 if $b = b'$ and 0 otherwise.

For an adversary A, we define $AltOneSec_A(n)$ to be a random variable denoting the output of the above game when played with A. An encryption scheme is then defined to be secure if for all PPT A there is some negligible ε such that $|\Pr[AltOneSec_A(n) = 1] - \frac{1}{2}| = \varepsilon(n)$.

Show that the alternate definition is equivalent to the one we gave in class, meaning that a scheme is secure according to one definition if and only if it is secure according to the other one.

Problem 9 (CPA Security - Alternate Definition) 10 pts

Let $(\mathsf{Enc}, \mathsf{Dec})$ be an symmetric-key encryption scheme with n-bit keys and $\ell(n)$-bit messages. In class (slides), we defined chosen plaintext attack (CPA) security for encrypting many messages as follows. For $b \in \{0,1\}$, define the algorithm $\mathsf{Enc}^b(k, m_0, m_1)$ to output $\mathsf{Enc}(k, m_b)$. Then for all PPT adversaries $\mathcal{A}$ we have:

$$\Pr[\mathcal{A}^{\mathsf{Enc}^0(k,\cdot,\cdot)}(1^n) = 1] - \Pr[\mathcal{A}^{\mathsf{Enc}^1(k,\cdot,\cdot)}(1^n) = 1] = negl(n)$$

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random. In other words, no PPT adversary can distinguish between having access to an oracle $\mathsf{Enc}^0(k,\cdot,\cdot)$ that, when given as input two message $m_0, m_1 \in \{0,1\}^{\ell(n)}$, always encrypts m_0 vs. an oracle $\mathsf{Enc}^1(k,\cdot,\cdot)$ that always encrypts m_1. The adversary $\mathcal{A}$ can call the oracle as many times as it wants.

In the lecture notes `https://www.ccs.neu.edu/home/wichs/class/crypto-fall17/lecture7.pdf` we gave a slightly different variant of the definitions where we defined an interactive game called $\mathsf{CPAGame}_b$ for $b = 0, 1$ and required that the two games are indistinguishable.

Show that the two definitions are equivalent, meaning that any scheme that satisfies one also necessarily satisfies the other.

Problem 10 (PRG Combiner) 10 pts

Two different PRG candidates, G_1 and G_2 are proposed. Everyone agrees that at least one of them is secure, but they disagree on which it is. Can you make everyone happy by constructing a PRG G^* out of G_1 and G_2 that is guaranteed to be secure assuming only that at least one of G_1 or G_2 is a PRG? Explicitly, you may assume that the candidates G_1 and G_2 is a polynomial-time computable functions expanding by one bit, and your goal is to come up with a PRG G^* that has any non-trivial stretch (even one bit is fine)