CS-7810 Graduate Cryptography September 27, 2017

Problem Set 2

Lecturer: Daniel Wichs *Due: Oct. 9, 2017*

Problem 1 (PRGs are OWFs) 8 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 (hard): 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 $f'(x) = f(short(x))$ is also a OWF, where we define $short(x)$ denotes the first $\lceil n/2 \rceil$ bits of x.

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

If G is a PRG, for which levels of "shortening" is $G'(x) = G(short(x))$ also a PRG?

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.

- $G'(x) = G(x+1)$ 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. 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 (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.

We give an alternate definition of security which we call AltCPA security 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 $\mathcal{A}$ 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.

Show that the original definition of CPA security that we defined in class also implies AltCPA security (any scheme that satisfies the former must also satisfy the latter).

Optional: show that the two definitions are actually equivalent, by also showing that the alternate definition implies the original.