CS 355: Topics in Cryptography **Spring 2018**

Problem Set 1

Due: April 13, 2018 at 5pm (submit via Gradescope)

Instructions: You **must** typeset your solution in LaTeX using the provided template:

`https://crypto.stanford.edu/cs355/homework.tex`

Submission Instructions: You must submit your problem set via Gradescope. Please use course code **9KY4BB** to sign up. Note that Gradescope requires that the solution to each problem starts on a **new page**.

Problem 1: Key Leakage in PRFs [5 points]. Let F be a secure PRF defined over $(\mathcal{K}, \mathcal{X}, \mathcal{Y})$, where $\mathcal{K} = \mathcal{X} = \mathcal{Y} = \{0,1\}^n$. Let $\mathcal{K}_1 = \{0,1\}^{n+1}$. Construct a new PRF F_1, defined over $(\mathcal{K}_1, \mathcal{X}, \mathcal{Y})$, with the following property: the PRF F_1 is secure; however, if the adversary learns the last bit of the key then the PRF is no longer secure. This shows that leaking even a *single* bit of the secret key can completely destroy the PRF security property. [**Hint:** Try changing the value of F at a single point.]

Problem 2: Learning from a Noisy Oracle [10 points]. *(Problem courtesy of Dan Boneh.)*

(a) Suppose that for an $x \in \mathbb{Z}_2^n$ we have an efficient algorithm $\mathcal{A}_x$ such that $\Pr[\mathcal{A}_x(r) = \langle x, r\rangle]$ is at least $3/4 + \epsilon$, for some constant $\epsilon > 0$. The probability is over the uniformly random choice of r from $\mathbb{Z}_2^n$. Here, $\langle x, r\rangle$ denotes the inner product of x and r over $\mathbb{Z}_2^n$. Construct an efficient algorithm $\mathcal{B}$ that outputs x with probability at least $1/2$ by calling $\mathcal{A}_x$ at most $O(n \cdot \log n)$ times.

(b) **Extra Credit [5 points].** Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ be a one-way permutation. Let $\mathcal{D}$ be an efficient algorithm such that $\Pr[\mathcal{D}(f(x), r) = \langle x, r\rangle]$ is at least $3/4+\epsilon$, for some constant $\epsilon > 0$, and for a uniformly random choice of x and r from $\mathbb{Z}_2^n$. Give an efficient algorithm that uses oracle access to $\mathcal{D}$ to break the one-wayness of f.

Problem 3: Constructing PRFs from DDH [10 points].

(a) For a PRF $F \colon \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$, and an adversary $\mathcal{A}$, we define two experiments, Experiment 0 and Experiment 1. For $b \in \{0,1\}$, we define:

Experiment b:

(1) At the start of the experiment, the challenger samples a random key $k \xleftarrow{R} \mathcal{K}$.
(2) The adversary submits a *challenge query* $x^* \in \mathcal{X}$ to the challenger.
(3) If $b = 0$, the challenger replies with $y^* = F(k, x^*)$. If $b = 1$, the challenger replies with $y^* \xleftarrow{R} \mathcal{Y}$.
(4) The adversary can then makes any number of (adaptive) *evaluation queries*, each consisting of a value $x \in \mathcal{X}$, where $x \neq x^*$.
(5) For each evaluation query $x \neq x^*$, the challenger computes $y = F(k, x)$ and gives y to the adversary.
(6) At the end of the experiment, $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$.

For $b \in \{0,1\}$, let W_b be the event that $\mathcal{A}$ outputs 1 in Experiment b. We define $\mathcal{A}$'s advantage in the *single-challenge* security game as

$$\mathsf{SC\text{-}PRFAdv}[\mathcal{A}, F] := |\Pr[W_0] - \Pr[W_1]|$$

We say that a F is single-challenge secure if for all efficient efficient adversaries $\mathcal{A}$, the value $\mathsf{SC\text{-}PRFAdv}[\mathcal{A}, F]$ is negligible.

Show that if F is single-challenge secure, then F is a secure PRF.[1] In particular, show that if there is a PRF adversary $\mathcal{A}$, then there is a single-challenge PRF adversary $\mathcal{B}$ such that

$$\mathsf{PRFAdv}[\mathcal{A}, F] \le Q \cdot \mathsf{SC\text{-}PRFAdv}[\mathcal{B}, F],$$

where Q is the number of queries $\mathcal{A}$ makes in the PRF security game. [**Hint:** Try using a similar structure as that used in the security proof of the Blum-Micali construction from lecture.]

(b) Let $\mathbb{G}$ be a group of prime order q, and let $H : \{0,1\}^n \to \mathbb{G}$ be a hash function that is modeled as a random oracle. Define a candidate PRF $F : \mathbb{Z}_q \times \{0,1\}^n \to \mathbb{G}$ as follows:

$$F(k, x) := H(x)^k.$$

Show that if the decisional Diffie-Hellman (DDH) assumption[2] holds in $\mathbb{G}$ and we model H as a random oracle, then F is single-challenge secure. In particular, show that if there is a single-challenge PRF adversary $\mathcal{A}$, then there exists a DDH distinguisher $\mathcal{B}$ such that

$$\mathsf{SC\text{-}PRFAdv}[\mathcal{A}, F] \le Q_{\mathrm{RO}} \cdot \mathsf{DDHAdv}[\mathcal{B}, \mathbb{G}],$$

where Q_{RO} is a bound on the number of random oracle queries $\mathcal{A}$ makes in the single-challenge PRF security game. Combined with the result from Part (a), this shows that F is a secure PRF under the DDH assumption. More precisely, if there exists a PRF adversary $\mathcal{A}$ (that makes Q queries and Q_{RO} random oracle queries), then there is a DDH distinguisher $\mathcal{B}$ such that

$$\mathsf{DDHAdv}[\mathcal{B}, \mathbb{G}] \ge \frac{1}{Q} \cdot \frac{1}{Q_{\mathrm{RO}}} \cdot \mathsf{PRFAdv}[\mathcal{A}, F].$$

We often refer to the $1/(Q \cdot Q_{\mathrm{RO}})$ factor as the "security loss" in the reduction. Intuitively, this statement says that the more queries $\mathcal{A}$ makes in the PRF security game, the smaller the distinguishing advantage of the DDH adversary $\mathcal{B}$. We say that such security reductions are *non-tight*.

(c) **Extra Credit [5 points].** Give a *tight* reduction of the security of F to the DDH assumption in the random oracle model. In particular, show that if there is a PRF adversary $\mathcal{A}$ for F, then there exists a DDH distinguisher $\mathcal{B}$ such that

$$\mathsf{DDHAdv}[\mathcal{B}, \mathbb{G}] \ge \mathsf{PRFAdv}[\mathcal{A}, F].$$

[**Hint:** Try reducing PRF security of F *directly* to the DDH assumption, without going through the single-challenge security game.]

[1] Definition 4.2 in Boneh-Shoup (pg. 131).

[2] Definition 10.8 in Boneh-Shoup (pg. 405).

Problem 4: Understanding Zero Knowledge [15 points].

(a) Let $\mathcal{L}$ be an (arbitrary) NP language (with associated NP relation $\mathcal{R}$). Moreover, assume that all instances $x \in \mathcal{L}$ have a *unique* witness: namely, for every $x \in \mathcal{L}$, there is a unique w where $\mathcal{R}(x, w) = 1$. Give an interactive proof system for $\mathcal{L}$ that is complete and sound but is zero knowledge *if and only if* there exists a probabilistic polynomial time algorithm M that on input $x \in \mathcal{L}$ outputs the (unique) NP witness w for the instance x. $\big($Namely, $\Pr[w \leftarrow M(x) : \mathcal{R}(x, w) = 1] \geq \frac{2}{3}\big)$.

(b) Suppose one-way functions exist. Give a language $\mathcal{L}$ and an interactive proof system for $\mathcal{L}$ that satisfies completeness, soundness, and honest-verifier zero knowledge, but *not* zero knowledge. [**Hint:** Recall from lecture that assuming one-way functions exist, the NP-complete language of graph 3-colorability has a zero-knowledge proof system. Modify this proof system so that the prover reveals additional information depending on the verifier's messages. To show that the resulting proof system is not zero-knowledge, show that the existence of a simulator (for a specific verifier) implies a decision algorithm for an NP-complete language. Use this to derive a contradiction.[3]]

Problem 5: Feedback [0 points]. Please answer the following questions to help us design future problem sets. You are not required to answer these questions, and if you would prefer to answer anonymously, please use this form. However, we do encourage you to provide us feedback on how to improve the course experience.

(a) Roughly how long did you spend on this problem set?

(b) What was your favorite problem on this problem set?

(c) What was your least favorite problem on this problem set?

(d) Any other feedback for this problem set?

[3] To formally show that a protocol is *not* zero-knowledge, you need to give a verifier V^* such that for *all* efficient simulators, the output distribution of the simulator is distinguishable from an interaction between the honest prover P and V^*.