CS 355: Topics in Cryptography **Spring 2019**

Problem Set 1

Due: April 12, 2019 at 5pm (submit via Gradescope)

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

`https://crypto.stanford.edu/cs355/19sp/homework.tex`

Submission Instructions: You must submit your problem set via Gradescope. Please use course code **M2BJ5P** to sign up. Note that Gradescope requires that the solution to each problem starts on a **new page**.

Bugs: We make mistakes! If it looks like there might be a mistake in the statement of a problem, please ask a clarifying question on Piazza.

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: Merkle Puzzles [15 points]. In lecture, you saw Merkle's key-exchange protocol. That protocol uses a hash function $H \colon \mathbb{Z}_{\lambda^2} \to \{0,1\}^{\log^2 \lambda}$, where $\lambda \in \mathbb{Z}^+$ is the security parameter. We model H as a random oracle.

Merkle's key-exchange protocol works as follows:

1. Alice picks integers $a_1, \dots, a_\lambda \xleftarrow{R} \mathbb{Z}_{\lambda^2}$ and publishes $H(a_1), \dots, H(a_\lambda)$.
2. Bob picks integers $b_1, \dots, b_\lambda \xleftarrow{R} \mathbb{Z}_{\lambda^2}$ and publishes $H(b_1), \dots, H(b_\lambda)$.
3. Alice and Bob find the least $i, j \in \{1, \dots, \lambda\}$ such that $H(a_i) = H(b_j)$. If no such pair exists, output "fail."
4. Alice outputs a_i as her shared secret with Bob. Bob outputs b_j as his shared secret with Alice.

While Alice and Bob each make λ queries to H, we argued in class that any successful eavesdropping attacker must make $\Omega(\lambda^2)$ queries to H.

(a) There is some chance that Alice and Bob agree on indices i and j in Step 3 such that $H(a_i) = H(b_j)$ but $a_i \neq b_j$. First, explain why this is problematic in the context of a key-agreement protocol. Next, show that the probability of this bad event is negligible.

(b) Prove that Alice and Bob successfully agree on a shared secret with probability at least $1/100$. Make sure that your argument accounts for the failure event from part (a).
[**Hint:** You may use the "Birthday Bound" in Appendix B.1 of the Boneh-Shoup book.]

(c) Show that it is possible to reduce the failure probability to some quantity *negligible* in λ while still keeping the total communication between Alice and Bob $\widetilde{O}(\lambda)$. (Recall that $\widetilde{O}(\lambda)$ is notation for $\lambda \cdot \text{polylog}(\lambda)$.)

(d) As described, Merkle's scheme requires total communication $2\lambda \log^2 \lambda$ bits. Describe how to reduce the total communication to $\lambda \log^2 \lambda + o(\lambda)$ bits, without changing the protocol's failure probability or security properties.

(e) **Extra credit [4 points].** Generalize Merkle's protocol to work with three parties. That is, construct a protocol in which: Alice, Bob, and Carol each publish one message of length $\widetilde{O}(\lambda)$, the three parties agree on a common shared secret with constant probability, and the best attack runs in time $\Omega(\lambda^{1+\epsilon})$ for some constant $\epsilon > 0$. You should sketch why your protocol is correct and secure, but you need not provide a formal security argument.

(f) **Research problem [+100 points].** If we take $\lambda \approx 2^{30}$ to get security against attackers running in time $\lambda^2 \approx 2^{60}$, then Merkle's protocol requires a huge amount of communication—around ten *gigabytes*. Show that it is possible to reduce the communication of Merkle's scheme to $\widetilde{O}(1)$ while: (a) Alice and Bob still run in time $\widetilde{O}(\lambda)$ and (b) the protocol maintains security against attackers running in time $o(\lambda^2)$. Even constructing a scheme with communication complexity $\widetilde{O}(\lambda^\epsilon)$ for any $\epsilon < 1$ would be very interesting. Your solution must somehow skirt the known impossibility results.

(g) **Research problem [+1000 points].** Construct a key-agreement protocol from a one-way function (e.g., AES) in which Alice and Bob run in time λ and the best attack runs in time *super-polynomial* in λ. We have no idea how to construct such a protocol, but we also have no way to rule out the existence of such a protocol either. A famous result of Impagliazzo and Rudich implies that any such protocol would likely not make "black-box" use of the one-way function.

Problem 4: Understanding Interactive Proofs [15 points]. *(Problems from "The Foundations of Cryptography - Volume 1, Basic Techniques" by Oded Goldreich)*

(a) *The role of verifier randomness:* Let L be a language with an interactive proof system where the verifier V is deterministic. Show that $L \in \mathsf{NP}$.

(b) *The role of prover randomness:* Let L be a language with an interactive proof system. Show that there exists an interactive proof system for L for which the prover P is deterministic.
[**Hint:** Use the fact that P is unbounded.]

(c) *The role of errors:* Let L be a language with an interactive proof system with perfect soundness, that is if $x \notin L$, the verifier *never* accepts (not even with negligible probability). Show that $L \in \mathsf{NP}$.

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?