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

Problem Set 2

Due: April 26, 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: Conceptual Questions [10 points]. For each of the following statements, say whether it is TRUE or FALSE. Write *at most one sentence* to justify your answer.

(a) If there exists a PRG with 1-bit stretch, there exists a PRG with n^{800}-bit stretch (where n is the length of the PRG seed).

(b) If $\mathsf{P} = \mathsf{NP}$, then PRFs exist.

(c) If an interactive proof system has soundness error greater than $1/3$, then it cannot be a proof of knowledge with knowledge error less than $1/3$.

(d) Consider a modified version of Schnorr's signature in which the signing nonce r is computed as $r \leftarrow H(m)$, where $H : \{0,1\}^* \to \mathbb{Z}_q$ is a hash function, m is the message to be signed, and q is the order of the group used for the signature scheme. This deterministic version of Schnorr's signature scheme is secure.

(e) Any pair of points $(x_1, y_1), (x_2, y_2) \in \mathbb{Z}_6^2$, where $x_1 \neq x_2$ defines a polynomial of degree at most 1 over $\mathbb{Z}_6$. (Note: "6" is not a prime.)

Problem 2: Understanding Fiat-Shamir [10 points]. Let Σ be a Sigma protocol.

(a) Show that if Σ has soundness error $1/2$, then applying the Fiat-Shamir transform *directly* to Σ yields a non-interactive zero-knowledge proof (NIZK) that is unsound. In particular, demonstrate an efficient attack that breaks the soundness of this NIZK.

(b) Use Σ to construct a Sigma protocol Σ' that has negligible soundness error, and prove that its soundness error is negligible. Then explain how to apply the Fiat-Shamir transform to this protocol.

(c) The standard Fiat-Shamir transform applies to Sigma protocols, which are three-message protocols in which the verifier sends a single message. We can consider a generalized version of the Fiat-Shamir transform that applies to protocols with many more rounds of interaction. In this generalized Fiat-Shamir transform, we replace each of V's messages with a hash of V's view in the protocol so far.

Show that this generalized Fiat-Shamir transform is unsound. In particular, give an example of a public-coin interactive proof system (P, V) such that:

(i) (P, V) is complete, has negligible soundness error, and is honest-verifier zero-knowledge, and

(ii) applying the generalized Fiat-Shamir transform to (P, V) yields a NIZK that is unsound. In other words, show an efficient attack that breaks the soundness of the resulting NIZK.

(d) **Extra Credit [5 points].** In class we saw that applying Fiat-Shamir to Schnorr's identification protocol yields a secure signature scheme. To get a signature on a message m from an identification protocol with public key $X = g^x$, we apply Fiat-Shamir using the hash function:

$$H_{X,m}(r) := \text{SHA256}(X, m, r).$$

As an optimization, you could imagine using a simpler construction that does not hash in the signer's public key X:

$$H^{\text{bad}}_m(r) := \text{SHA256}(m, r).$$

Show that if you instantiate Schnorr signatures with H^{bad}_m, then given a valid signature on message m under public key X, it's possible to produce a valid signature on m under a public key $X' = g^{x'}$ (where $x \neq x'$) *without* knowing the corresponding secret key x'.

This is one reason why, when using the Fiat-Shamir transform, it is important to hash not only the prover's first message but also the statement/instance itself (which is X in this case).

Interlude: A Refresher on Commitment Schemes. The next two problems use cryptographic commitment schemes. We defined and used these informally in class, and make things more precise here. See also CS 255 HW3 Problem 4 and Boneh-Shoup, Chapter 3.12.

Definition (Commitments)**.** An efficiently computable function $\mathsf{Commit} : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$ is a (perfectly binding) commitment scheme if it satisfies the following two properties:

- **(Computational) Hiding**: For all $m_0, m_1 \in \mathcal{M}$,

$$\{\mathsf{Commit}(m_0, r) : r \xleftarrow{R} \mathcal{R}\} \approx_c \{\mathsf{Commit}(m_1, r) : r \xleftarrow{R} \mathcal{R}\} . \tag{1}$$

- **(Perfect) Binding**: For all $m_0, m_1 \in \mathcal{M}$, $r_0, r_1 \in \mathcal{R}$, if $m_0 \neq m_1$, then

$$\mathsf{Commit}(m_0, r_0) \neq \mathsf{Commit}(m_1, r_1) .$$

Conversely, we can define commitment schemes that are perfectly hiding and computationally binding. Perfect hiding means that the distributions in Equation (1) are identical. Computational binding means that no efficient adversary $\mathcal{A}$ can find $m_0, m_1 \in \mathcal{M}, r_0, r_1 \in \mathcal{R}$ such that $m_0 \neq m_1$ and $\mathsf{Commit}(m_0, r_0) = \mathsf{Commit}(m_1, r_1)$.

You can think about why a commitment scheme cannot be both perfectly hiding and perfectly binding. The proof is fairly simple.

Problem 3: Sigma Protocol for Circuit Satisfiability [10 points]. Let circuit-SAT be the language of satisfiable Boolean circuits[1] :

$$\mathsf{circuit\text{-}SAT} = \left\{C \colon \{0,1\}^n \to \{0,1\} \mid n \in \mathbb{N}, \exists (x_1, \ldots, x_n) \in \{0,1\}^n \text{ such that } C(x_1, \ldots, x_n) = 1\right\} .$$

[1] You can assume without loss of generality that a Boolean circuit consists of only XOR and AND gates.

Let $\mathsf{Commit}\colon \{0,1\} \times \mathcal{R} \to \mathcal{C}$ be a perfectly-binding and computationally-hiding commitment scheme with message space $\{0,1\}$, randomness space $\mathcal{R}$, and commitment space $\mathcal{C}$. Suppose that there exist Sigma protocols $\langle P_{\text{XOR}}, V_{\text{XOR}} \rangle$ and $\langle P_{\text{AND}}, V_{\text{AND}} \rangle$ for languages $\mathcal{L}_{\text{XOR}}$ and $\mathcal{L}_{\text{AND}}$, respectively, where:

$$\mathcal{L}_{\text{XOR}} = \left\{ (c_1, c_2, c_3) \in \mathcal{C}^3 \;\middle|\; \begin{array}{c} \exists (m_1, m_2, m_3) \in \{0,1\}^3, (r_1, r_2, r_3) \in \mathcal{R}^3 \text{ such that} \\ \forall\, i \in \{1,2,3\}\ \ c_i = \mathsf{Commit}(m_i; r_i) \text{ and } m_1 \oplus m_2 = m_3 \end{array} \right\}$$

$$\mathcal{L}_{\text{AND}} = \left\{ (c_1, c_2, c_3) \in \mathcal{C}^3 \;\middle|\; \begin{array}{c} \exists (m_1, m_2, m_3) \in \{0,1\}^3, (r_1, r_2, r_3) \in \mathcal{R}^3 \text{ such that} \\ \forall\, i \in \{1,2,3\}\ \ c_i = \mathsf{Commit}(m_i; r_i) \text{ and } m_1 \wedge m_2 = m_3 \end{array} \right\}.$$

Give a Sigma protocol for circuit-SAT. In addition to describing a protocol, you will also need to show that your protocol satisfies completeness, soundness, and honest-verifier zero-knowledge. [**Hint:** When showing that your protocol is honest-verifier zero-knowledge, you may want to use a hybrid argument. One of your hybrids might rely on the commitment scheme being computationally hiding, and the other hybrid might rely on the underlying Sigma protocols being honest-verifier zero-knowledge.]

Problem 4: Secret Sharing [10 points]. Consider a dealer who wants to share a secret s between n shareholders using a (t, n) secret-sharing scheme where $t < n$. The shareholders suspect that the dealer secretly holds a grudge against one of them and has given that person an invalid share, inconsistent with the rest of the shares. (In this problem, we assume that all shareholders are honest.)

(a) Show that if they are willing to reveal all their shares, the shareholders can detect if one of them has indeed been given an invalid share.

We would like the shareholders to be able to detect an invalid share *without having to reveal their shares*. To do this, consider the following modification to Shamir's secret-sharing scheme:

1. The dealer chooses $r, a_1, b_1, \ldots, a_{t-1}, b_{t-1} \in \mathbb{F}_q$ independently at random, and constructs the polynomials $u(x) = s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$ and $v(x) = r + b_1 x + b_2 x^2 + \cdots + b_{t-1} x^{t-1}$ over $\mathbb{F}_q$.

2. The dealer creates t Pedersen commitments $c_0, c_1, \ldots, c_{t-1} \in \mathbb{G}$ where $c_o = \mathsf{Commit}(s; r) = g^s h^r$ and $c_j = \mathsf{Commit}(a_j; b_j) = g^{a_j} h^{b_j}$ for $j \in [t-1]$. (See CS 255 HW3 Problem 4 for a refresher on Pedersen commitments.) The dealer publicly broadcasts all the commitments to all the shareholders.

3. The dealer creates n shares $\{(i, s_i, r_i)\}_{i=1}^n$, where $s_i = u(i)$ and $r_i = v(i)$ are computed over $\mathbb{F}_q$. The dealer privately sends each of the n shareholders her own share.

(b) Describe a verification routine that allows the shareholders to jointly verify that all the shares given to them are valid without having to reveal them.

(c) Prove that the protocol preserves the secrecy of the secret s against any coalition of fewer than t shareholders. [**Hint:** Show that the view of any coalition of $t-1$ shareholders is distributed independently of the secret s.]

(d) **Extra Credit [5 points].** Prove that if a dealer can trick the shareholders into accepting an invalid set of shares it can solve the disrete log of h with respect to g.

Problem 5: Time Spent [3 points for answering]. How long did you spend on this problem set? This is for calibration purposes, and the response you provide will not affect your score.

Optional Feedback [0 points]. Please answer the following questions to help us design future problem sets. You do not need 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) What was your favorite problem on this problem set? Why?

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

(c) Do you have any other feedback for this problem set?

(d) Do you have any other feedback on the course so far?