CS 6501: Advanced Topics in Cryptography **Spring 2019**

Problem Set 5

Due: May 3, 2019 at 5pm (submit via Gradescope) **Instructor:** David Wu

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

https://www.cs.virginia.edu/dwu4/courses/sp19/static/homework.tex

Submission Instructions: You must submit your problem set via Gradescope. Please use course code **9YD875** to sign up. Note that Gradescope requires that the solution to each problem starts on a **new page**.

Problem 1: Conceptual Questions [30 points]. For each of the following questions, a brief explanation or proof will suffice. Note that your solution should still include the critical details (e.g., if you cite a theorem for the lecture notes, you should show that all of the stated conditions are indeed satisfied).

(a) In class, we discussed Lagrange interpolation over finite fields $\mathbb{F}_p$ (i.e., the integers modulo a prime p). It is critical that we work over a field. Show that if we work over a composite-order ring $\mathbb{Z}_n$ (e.g., the integers modulo $n = pq$ where p, q are prime), there exist two points $(x_1, y_1) \in \mathbb{Z}_n^2$ and $(x_2, y_2) \in \mathbb{Z}_n^2$ such that there is no degree-1 polynomial (i.e., a line) that interpolates those points.

(b) The version of Shamir secret sharing that we described in class allows a user to secret share a scalar $x \in \mathbb{F}_p$ to $n \leq p-1$ parties such that any subset with at least $t \leq n$ parties can decrypt. Suppose that instead of sharing a single scalar $x \in \mathbb{F}_p$, we want to secret-share a vector $x \in \mathbb{F}_p^k$. Suppose moreover that $k \leq t \leq n \leq p-k$. Describe a generalization of Shamir's secret sharing to this setting with the following properties:

- Any subset of t shares enables reconstruction of x.
- Any subset with at most $t-k$ shares perfectly hide x.

In your construction, each party's share should still consist of a single pair $(x_i, y_i) \in \mathbb{F}_p^2$.

(c) Let $\mathbb{G}$ be a group of order $p = 2^{\Omega(\lambda)}$. Let $t = 2\lceil \log p \rceil$. Sample $g_1, \ldots, g_t \xleftarrow{R} \mathbb{G}$ and set $\mathsf{pp} = (g_1, \ldots, g_t)$. Next, sample $x \xleftarrow{R} \{0,1\}^t \setminus \{0^t\}$, and $h \xleftarrow{R} \mathbb{G}$. Show that

$$\left(\mathsf{pp}, \prod_{i \in [t]} g_i^{x_i}\right) \overset{s}{\approx} (\mathsf{pp}, h).$$

This shows that a random subset product of group elements yields a uniformly random group element.

(d) An important property of a fully homomorphic encryption schemes is compactness: namely, if we homomorphically evaluate a circuit C on a ciphertext ct, the size of the resulting ciphertext ct' should be *sublinear* in the circuit size $|C|$. Show (by construction) that without this property, fully homomorphic encryption is trivial to construct: namely, any semantically-secure public-key encryption scheme implies a non-compact fully homomorphic encryption scheme.

(e) Recall that in the homomorphic signature scheme from class, a signature on $x \in \{0,1\}^t$ is a collection of short matrices $\mathbf{U}_1, \ldots, \mathbf{U}_t \in \mathbb{Z}_q^{m \times m}$ where $\mathbf{AU}_i = \mathbf{V}_i + x_i \cdot \mathbf{G}$, where $\mathbf{A}, \mathbf{V}_1, \ldots, \mathbf{V}_t \in \mathbb{Z}_q^{n \times m}$ are part of the public verification key. In class, we said that this was a *one-time* signature. Suppose an adversary obtains short matrices $\mathbf{U}_i$ and $\mathbf{U}_i' \in \mathbb{Z}_q^{m \times m}$ such that $\mathbf{AU}_i = \mathbf{V}_i$ and $\mathbf{AU}_i' = \mathbf{V}_i + \mathbf{G}$ (i.e., the adversary learns a signature on two messages x and x' where $x_i \neq x_i'$). Show that such an adversary can use this information to forge a signature on *any* message $y \in \{0,1\}^t$ (i.e., show that for all $y \in \{0,1\}^t$, the adversary can *efficiently* find *short* $\mathbf{U}_i \in \mathbb{Z}_q^{m \times m}$ where $\mathbf{V}_i = \mathbf{AU}_i + y_i \cdot \mathbf{G}$ for all $i \in [t]$).

Problem 2: Hardness of Lattice Problems [20 points]. Throughout this problem, let $n, m, q, \beta \in \mathbb{N}$ be lattice parameters. Let $\mathsf{ISIS}_{n,m,q,\beta}$ denote the inhomogeneous SIS problem with parameters n, m, q, β. As in class, we define SIS and ISIS with respect to the ℓ_∞ norm.

(a) Show that if $\mathsf{SIS}_{n,m,q,\beta}$ is hard, then for all integers $0 < k < m$, $\mathsf{SIS}_{n,m-k,q,\beta}$ is also hard.

(b) Show that if $\mathsf{SIS}_{n,m+1,q,\beta}$ is hard, then $\mathsf{ISIS}_{n,m,q,\beta}$ is also hard.

(c) Show that if $\mathsf{ISIS}_{n,m,q,1}$ is hard, then $\mathsf{SIS}_{n,m+1,q,1}$ is also hard.

Problem 3: Key-Homomorphic PRFs from Lattices [30 points]. In this problem, we will study how to construction pseudorandom functions (in the random oracle model) from a "deterministic" variant of LWE called the learning with rounding (LWR) assumption.

(a) Let n, m, q be lattice parameters. For an integer $p < q$, define the modular "rounding" function $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$ as follows $\lfloor x \rceil_p = \lfloor p/q \cdot x \rceil$ where $\lfloor \cdot \rceil$ denotes the standard "rounding to the nearest integer" function over the real numbers (i.e., $\lfloor x \rceil_p$ first computes $p/q \cdot x$ over the real numbers and then rounds the result to the nearest integer). The $\mathsf{LWR}_{n,m,p,q}$ assumption states that for $\mathbf{A} \xleftarrow{R} \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \xleftarrow{R} \mathbb{Z}_q^n$, $\mathbf{u} \xleftarrow{R} \mathbb{Z}_p^m$

$$\left(\mathbf{A}, \left\lfloor \mathbf{s}^T \mathbf{A} \right\rceil_p\right) \overset{c}{\approx} (\mathbf{A}, \mathbf{u}).$$

Notably, the left distribution does not have any error terms. Suppose that the $\mathsf{LWE}_{n,m,q,\chi}$ assumption holds for a β-bounded error distribution χ: namely, $\Pr[x \leftarrow \chi : |x| < \beta] = 1$, and moreover, $\beta = \mathrm{poly}(n)$. Show that if $p/q = \mathrm{negl}(n)$ and $\mathsf{LWE}_{n,m,q,\chi}$ is hard, then $\mathsf{LWR}_{n,m,p,q}$ is also hard. [**Hint:** Use a hybrid argument.]

(b) Let $H : \{0,1\}^t \to \mathbb{Z}_q^n$ be a hash function, and define a function $F : \mathbb{Z}_q^n \times \{0,1\}^t \to \mathbb{Z}_p$ where $F(\mathbf{s}, x) := \left\lfloor \mathbf{s}^T H(x) \right\rceil_p$. Suppose that the $\mathsf{LWR}_{n,m,p,q}$ assumption holds and H is modeled as a random oracle. Show that F is a secure PRF against adversaries that make at most m queries (including both random oracle and PRF evaluation queries) to the distinguisher.

(c) Show that the PRF from Part (b) is *almost key-homomorphic*. Namely, the evaluation satisfies

$$F(\mathbf{s}_1 + \mathbf{s}_2, x) = F(\mathbf{s}_1, x) + F(\mathbf{s}_2, x) + e \in \mathbb{Z}_p,$$

where $|e| \leq 1$.

Problem 4: Time Spent [5 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 *optional* questions to help us design future problem sets. You do not need to answer these questions. 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?