CS 395T: Topics in Cryptography **Spring 2024**

Exercise Set 5

Due: April 3, 2024 at 11:59pm (Submit on Gradescope) **Instructor:** David Wu

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

https://www.cs.utexas.edu/~dwu4/courses/sp24/static/homework.tex

You must submit your problem set via Gradescope (accessible through Canvas).

Collaboration Policy. You may discuss your general approach with other students, but you may not share written documents. You should not search online for solutions to these problems. If you do consult external sources, you must cite them in your submission. You must include the names of all of your collaborators with your submission. Refer to the official course policies for the full details.

Problem 1: SIS and Inhomogeneous SIS [20 points]. Let n, q, β be lattice parameters where q is prime and $m, \beta = \text{poly}(n)$. In this problem, we will explore implications between the hardness of $\mathsf{SIS}_{n,m+1,q,\beta}$ and the hardness of $\mathsf{ISIS}_{n,m,q,\beta'}$. Formally show the following (i.e., give an explicit reduction and analyze the advantage):

(a) Hardness of $\mathsf{SIS}_{n,m+1,q,\beta}$ implies hardness of $\mathsf{ISIS}_{n,m,q,\beta'}$ whenever $\beta \geq \sqrt{1+(\beta')^2}$; and

(b) Hardness of $\mathsf{ISIS}_{n,m,q,\beta'}$ implies hardness of $\mathsf{SIS}_{n,m+1,q,\beta}$ whenever $\beta' \geq \beta$.

You may treat the lattice dimension n as the security parameter. For this problem, both SIS and ISIS are defined with respect to the ℓ_2 norm: for a vector $\mathbf{v} = [v_1, \ldots, v_n] \in \mathbb{Z}^n$, $\|\mathbf{v}\|_2 = \sqrt{\sum_{i \in [n]} v_i^2}$.

Optional Feedback. Please answer the following *optional* questions to help design future exercise 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) How long did you spend on this exercise set?

(b) Do you have any feedback for this exercise set?

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

(d) Are there specific topics that you are interested in seeing in this course?

Challenge Problem: GPV Signatures [Optional]. Recall the general structure of the Gentry-Peikert-Vaikuntanathan signature scheme from lecture:

- The verification key is a matrix $\mathbf{A} \xleftarrow{R} \mathbb{Z}_q^{n \times m}$ and a norm bound β. The signing key is a trapdoor $\mathsf{td}_{\mathbf{A}}$ for $\mathbf{A}$.
- To sign a message $\mu \in \{0,1\}^*$, compute $\mathbf{y} = H(\mu) \in \mathbb{Z}_q^n$, where $H\colon \{0,1\}^* \to \mathbb{Z}_q^n$ is modeled as a random oracle. Using $\mathsf{td}_{\mathbf{A}}$, sample $\mathbf{x} \leftarrow \mathbf{A}^{-1}(\mathbf{y})$. Output the signature $\mathbf{x} \in \mathbb{Z}_q^m$. Recall that the notation $\mathbf{x} \leftarrow \mathbf{A}^{-1}(\mathbf{y})$ denotes sampling $\mathbf{x}$ from a discrete Gaussian distribution over $\mathbb{Z}^m$ conditioned on $\mathbf{A}\mathbf{x} = \mathbf{y}$.
- To verify a signature $\mathbf{x}$ on the message μ, check that $\|\mathbf{x}\| \leq \beta$ and $\mathbf{A}\mathbf{x} = H(\mu)$.

(a) Show that the above signature scheme is *insecure* as described. Specifically, give an efficient attack that breaks unforgeability of the signature scheme.

(b) Describe how to modify the scheme and obtain a secure signature scheme. Your modification should be a simple modification to the above construction (there are multiple correct approaches).