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

Exercise Set 7

Due: April 29, 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: ABE Key Delegation [20 points]. Recall the lattice-based ABE scheme from class for attributes of length ℓ:

- The public key is $\mathsf{mpk} = (\mathbf{A}, \mathbf{B}, \mathbf{u})$ where $\mathbf{A} \xleftarrow{R} \mathbb{Z}_q^{n \times m}$, $\mathbf{B} \xleftarrow{R} \mathbb{Z}_q^{n \times m\ell}$ and $\mathbf{u} \xleftarrow{R} \mathbb{Z}_q^n$. The secret key is a trapdoor $\mathsf{msk} = \mathbf{T}$ for $\mathbf{A}$.
- A secret key for a function f is $\mathbf{z}_f \leftarrow [\mathbf{A} \mid \mathbf{B}_f]^{-1}(\mathbf{u})$, where $\mathbf{B}_f = \mathbf{B} \cdot \mathbf{H}_f$ and the trapdoor for $[\mathbf{A} \mid \mathbf{B}_f]$ is $\left[\begin{smallmatrix}\mathbf{T}\\ \mathbf{0}\end{smallmatrix}\right]$.
- An encryption of $\mu \in \{0,1\}$ with attribute $\mathbf{x} \in \{0,1\}^\ell$ is

$$\mathsf{ct} = \left(\mathbf{s}^\top \mathbf{A} + \mathbf{e}_1^\top \,,\, \mathbf{s}^\top (\mathbf{B} - \mathbf{x}^\top \otimes \mathbf{G}) + \mathbf{e}_1^\top \mathbf{R} \,,\, \mathbf{s}^\top \mathbf{u} + e' + \mu \cdot \lfloor q/2 \rceil \,,\, x\right),$$

  where $\mathbf{s} \xleftarrow{R} \mathbb{Z}_q^n$, $\mathbf{e}_1 \leftarrow \chi^m$, $e' \leftarrow \chi$, and $\mathbf{R} \xleftarrow{R} \{0,1\}^{m \times m\ell}$.
- To decrypt a ciphertext $\mathsf{ct} = (\mathbf{c}_1, \mathbf{c}_2, c_3, \mathbf{x})$, using a secret key $\mathsf{sk}_f = \mathbf{z}_f$, compute $c_3 - \left[\mathbf{c}_1^\top \mid \mathbf{c}_2^\top \mathbf{H}_{f,\mathbf{x}}\right]\mathbf{z}_f$ and round.

We say that an ABE scheme supports key delegation if the holder of a secret key sk_f can generate a key for the function $(f \wedge g)$ where $(f \wedge g)(\mathbf{x}) = 0$ if and only if $f(\mathbf{x}) = 0 = g(\mathbf{x})$. Formally, the key-delegation algorithm takes as input $(\mathsf{mpk}, \mathsf{sk}_f, g)$ and outputs $\mathsf{sk}_{f \wedge g}$. It does *not* know the master secret key. Security then says that ciphertexts encrypted to attributes $\mathbf{x}$ where either $f(\mathbf{x}) = 1$ or $g(\mathbf{x}) = 1$ should remain semantically secure even given $\mathsf{sk}_{f \wedge g}$.

Show how to modify the above ABE scheme to support key delegation. Specifically, you should modify the description of the key-generation algorithm and then show how you extend it to support key delegation. Then, you should explain how decryption works with delegated keys. Prove the correctness of your key-delegation procedure (i.e., show that the delegated key $\mathsf{sk}_{f \wedge g}$ correctly decrypts a ciphertext associated with an attribute $\mathbf{x}$ where $f(\mathbf{x}) = 0 = g(\mathbf{x})$). You do not need to give the precise error bounds needed for correctness, but you should explain (at a high level) why the relevant error terms are small (with a similar level of detail as proofs given in lecture). You do *not* need to prove the security of your resulting ABE scheme, but a strategy similar to the one from class should still apply. In particular, modifying the key-generation algorithm to give out msk or having the delegation algorithm give out sk_f would be trivially *insecure*.

Optional Feedback. Please answer the following *optional* questions to help us improve future iterations of this course. You do not need to answer these questions. However, we do encourage you to provide us feedback on how to improve the course experience for future semesters.

(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?

Challenge Problem: Ajtai Trapdoors [Optional]. Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ be a matrix. In class, we mentioned that that an Ajtai trapdoor for $\mathbf{A}$ is a matrix $\mathbf{T} \in \mathbb{Z}^{m \times m}$ where $\mathbf{AT} = \mathbf{0} \bmod q$, $\|\mathbf{T}\|_\infty$ is small, and $\mathbf{T}$ is full rank over the rational numbers (or the real numbers). Show the following:

(a) Given any vector $\mathbf{y} \in \mathbb{Z}_q^m$ in the image of $\mathbf{A}$, use $\mathbf{T}$ to construct a short vector $\mathbf{x}$ such that $\mathbf{Ax} = \mathbf{y}$. This shows that an Ajtai trapdoor can be used to obtain a gadget trapdoor (when $\mathbf{A}$ is full rank).

(b) Given a gadget trapdoor $\mathbf{R}$ for $\mathbf{A}$ (i.e., $\mathbf{AR} = \mathbf{G}$), show how to construct an Ajtai trapdoor for $\mathbf{A}$.