6.876 Advanced Topics in Cryptography *Instructor: Vinod Vaikuntanathan*

Problem Set 2

Handed Out: November 25, 2018 *Due: December 12, 2018*

Notes

- This problem set is worth 75 points.
- Collaboration is allowed, *but you must write up the solutions by yourself without consulting to notes from the discussions.* You must also reference your sources.
- Grading is based on correctness as well as the clarity of the solutions. When writing proofs, it is generally a good idea to first explain the intuition behind your solution in words (wherever appropriate), before jumping in to the formalisms.
- *Notation:* $\mathbb{N}$ denotes the natural numbers, $\mathbb{Z}$ denotes the integers, $\mathbb{Q}$ denotes rational numbers and $\mathbb{R}$ the set of real numbers.

Problem 1: Another IBE Scheme (25 points)

In this problem, I will construct a new IBE scheme. Your goal is to show either that it is correct and (selectively) secure, or to break it.

- Setup generates $\ell + 1$ matrices $\mathbf{A}_0, \mathbf{A}_{1,0}, \mathbf{A}_{2,0}, \ldots, \mathbf{A}_{\ell,0}, \mathbf{A}_{1,1}, \mathbf{A}_{2,1}, \ldots, \mathbf{A}_{\ell,1} \in \mathbb{Z}_q^{n \times m}$, as usual, and a vector $\mathbf{y} \in \mathbb{Z}_q^n$ where n, q, m are picked "appropriately".
- KeyGen for an identity $id \in \{0,1\}^\ell$ generates a discrete Gaussian vector $\mathbf{r}$ such that

$$\left[\mathbf{A}_0 \middle\| \sum_i \mathbf{A}_{i,id_i}\right]\mathbf{r} = \mathbf{y} \bmod q$$

  where id_i denotes the i-th bit of the identity id.
- Enc for an identity id and message $m \in \{0,1\}$ works as follows. Choose a random $\mathbf{s} \in \mathbb{Z}_q^n$ and an LWE error $\mathbf{e} \in \chi^m, e' \in \chi$ and output

$$\left(\mathbf{s}^T \left[\mathbf{A}_0 \middle\| \sum_i \mathbf{A}_{i,id_i}\right] + \mathbf{e}^T, \mathbf{s}^T\mathbf{y} + e' + m\lfloor q/2 \rceil\right)$$

Hint: Try to solve the problem for $\ell = 2$. Techniques from the ABB IBE scheme may come in handy.

Problem 2: LWE with Leakage (25 points)

Suppose an adversary can, in addition to the LWE samples, receive k linear functions of the secret $\langle \mathbf{b}_1, \mathbf{s}\rangle, \ldots, \langle \mathbf{b}_k, \mathbf{s}\rangle$ (for $i = 1, \ldots, k$). Here, $\mathbf{b}_i$ are vectors that the adversary picked. Show that the adversary cannot break the decisional LWE assumption as long as $k \le (1-\epsilon)n$ for some absolute constant $\epsilon > 0$. That is, under the LWE assumption, prove that for any $\mathbf{b}_1, \ldots, \mathbf{b}_k \in \mathbb{Z}_q^n$:

$$\left(\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T, \langle \mathbf{b}_1, \mathbf{s}\rangle, \ldots, \langle \mathbf{b}_k, \mathbf{s}\rangle\right) \approx_c \left(\mathbf{A}, \mathbf{u}^T, \langle \mathbf{b}_1, \mathbf{s}\rangle, \ldots, \langle \mathbf{b}_k, \mathbf{s}\rangle\right)$$

where $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{e} \leftarrow \chi^m$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and $\mathbf{u} \leftarrow \mathbb{Z}_q^m$.

Problem 3: LWE in Disguise (25 points)

The notation $\mathbf{A}_\sigma^{-1}(\mathbf{u})$ for a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$ denotes a random variable $\mathbf{e} \in \mathbb{Z}^m$ distributed like the discrete Gaussian $D_{\mathbb{Z}^m,\sigma}$ subject to the condition that $\mathbf{A}\mathbf{e} = \mathbf{u} \pmod q$. We write this simply as $\mathbf{A}_\sigma^{-1}(\mathbf{u}) = \mathbf{e}$. Recall that coming up with such an $\mathbf{e}$ entails solving SIS which can be done efficiently given the trapdoor for $\mathbf{A}$.

Now on to the question. Show that for every $\mathbf{Z} \in \mathbb{Z}_q^{n\times \ell}$, the following distributions are computationally indistinguishable under the LWE assumption:

$$\mathbf{A}_\sigma^{-1}(\mathbf{Z} + \mathbf{E}) \approx_c \mathbf{U}$$

where $\mathbf{A}$ is uniformly random in $\mathbb{Z}_q^{n\times m}$, each column of $\mathbf{E} \in \mathbb{Z}^{n\times \ell}$ is chosen from the LWE error distribution χ^m, and each column of $\mathbf{U} \in \mathbb{Z}^{m\times \ell}$ is chosen from the discrete Gaussian distribution $D_{\mathbb{Z}^m,\sigma}$ (with no conditions attached).

(Note that the distinguisher is not given $\mathbf{A}$, and this is crucial.)