6.876 Advanced Topics in Cryptography *Instructor: Vinod Vaikuntanathan*

Problem Set 1

Handed Out: October 30, 2017 *Due: November 20, 2017*

Notes

- This problem set is worth 100 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: Better Rate Encryption from LWE (25 points)

Recall our original public-key encryption scheme from LWE (see notes). It had a terrible rate, that is, the ratio of the bit-length of the ciphertext to that of the message it encrypts. In particular, every bit gets encrypted into a ciphertext of length $(n+1) \cdot \lceil \log q \rceil$, so the rate is $1/((n+1)\lceil \log q \rceil)$.

- Modify the scheme in section 3.2, lecture notes 1, to work with a plaintext space $\{0, 1, \ldots, p-1\}$ for a large enough p rather than $\{0, 1\}$. How large can you make $\log p / \log q$ asymptotically, assuming the hardness of LWE with a polynomial modulus-to-noise ratio?
- As a warmup to the next part, show that the many-many LWE problem is secure. That is, the following collection of elements is computationally indistinguishable from random under the LWE assumption:

$$\left(\mathbf{a}_i \leftarrow \mathbb{Z}_q^n;\ \mathbf{s}_j \leftarrow \mathbb{Z}_q^n;\ e_{ij} \leftarrow \chi;\ \text{output } (\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s}_j \rangle + e_{ij}) \right)$$

  where all computations are carried out in $\mathbb{Z}_q$.
- Modify the scheme from part 1 further to make the encryption rate $1 - \epsilon$ for any given constant $\epsilon > 0$.

Problem 2: Elementary Banaszczyk (25 points)

We used the Banaszczyk lemma in the proof of the worst-case to average-case reduction for SIS and LWE. That is, there is an absolute constant $C > 0$ such that for every $s \in \mathbb{R}^+$ and every lattice $\mathcal{L}$ with $\lambda_1(\mathcal{L}) > C \cdot s \cdot \sqrt{\frac{n}{2\pi}}$,

$$\sum_{y \in \mathcal{L} \setminus \{\mathbf{0}\}} \rho_s(\mathbf{y}) \leq 2^{-n}$$

where $\rho_s : \mathbb{R}^n \to \mathbb{R}$ is the Gaussian function defined as $\rho_s(\mathbf{y}) = e^{-\pi ||\mathbf{y}||^2 / s^2}$.

Your goal in this problem is to derive a (simple) proof of the lemma.

Hint: Derive first a packing bound that bounds the number of lattice points within a ball of radius R. The following trick might come in handy as well. For every bounded function $f : D \to \mathbb{R}$ where D is a countably infinite domain,

$$\sum_{d \in D} f(d) = \int_0^1 |\{d : f(d) \geq t\}| \ \ dt$$

Problem 3: Strange-(Ring)-LWE (25 points)

Consider the following two versions, the first of LWE and the second of Ring LWE. One of them is secure (as secure as LWE, resp. Ring-LWE) whereas the other one is insecure. Identify which is which and prove your claim.

- Sample $\mathbf{A} \in \mathbb{Z}^{n \times m}$ where $m = n^2$ and each entry is randomly 0 or 1. Pick a random $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ with $q = \mathsf{poly}(n)$, and an error vector $\mathbf{e} \leftarrow \chi^m$ where χ is the LWE error distribution (assume it is the Gaussian distribution if necessary). The strange-LWE assumption says that $(\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T)$ is computationally indistinguishable from the uniform distribution.
- Let $\mathcal{R}$ be a polynomial ring, say $\mathbb{Z}[x]/(x^n + 1)$ and $\mathcal{R}_q := \mathbb{Z}_q[x]/(x^n + 1)$. Sample $\mathbf{A} \in \mathcal{R}^{1\times 2}$ where each entry is a polynomial in $\mathcal{R}$ with each coefficient being either 0 or 1. Pick a uniformly random ring element $\mathbf{s} \leftarrow \mathcal{R}_q$ and an error vector $\mathbf{e} \leftarrow \mathcal{R}^{1\times 2}$ where χ is the Ring-LWE error distribution (assume it is the Gaussian distribution if necessary). The strange-Ring-LWE assumption says that $(\mathbf{A}, \mathbf{s}\mathbf{A} + \mathbf{e}^T)$ is computationally indistinguishable from the uniform distribution.

Which is true and which isn't? Prove your claims.

Problem 4: Circular Security (25 points)

- Given polynomially many LWE samples with secret $\mathbf{s} \in \mathbb{Z}_q^n$, and k linear functions $L_i : \mathbb{Z}_q^n \to \mathbb{Z}_q$, show how to generate "encryptions" of $L_i(\mathbf{s})$. That is,

$$\left(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s}\rangle + e_i + L_i(\mathbf{s})\right)_{i=1}^{k}$$

  where $\mathbf{a}_i$ is uniformly random in $\mathbb{Z}_q^n$ and e_i is distributed according to the LWE error distribution.
- Given polynomially many LWE samples with secret $\mathbf{s} \in \mathbb{Z}_q^n$, show how to generate encryptions of random quadatic functions $Q(\mathbf{s}) = \sum_{i,j} \alpha_{i,j} s_i s_j$ of the secret key. That is, generate a random such Q together with

$$\left(\mathbf{a}_i, \langle \mathbf{a}, \mathbf{s}\rangle + e + Q(\mathbf{s})\right)_{i=1}^{k}$$

  where $\mathbf{a}$ is uniformly random in $\mathbb{Z}_q^n$ and e is distributed according to the LWE error distribution. You may assume, if necessary, that the secrets/errors are chosen from the Gaussian distribution.