CSC 2414 Problem Set 3

Due: December 22, 2011

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.
- There is no deadline for the extra credit problem. You can turn in a solution any time until the last class.
- **Notation:** If X is a probability distribution, then $x \in_R X$ means that x is drawn randomly according to the probability distribution X. If S is a finite set, then $x \in_R S$ means that x is drawn from the uniform probability distribution over S.

Problem 1: LWE with a Short Secret (65 points)

Define the "short secret LWE" problem ssLWE as follows. Let n and $q \geq 2$ be natural numbers and χ be a probability distribution over $\mathbb{Z}_q = \{0, \ldots, q-1\}$, and let χ^n denote a probability distribution on $\mathbb{Z}_q^n$ where each component is drawn independently from χ.

$\mathsf{ssLWE}_{n,q,\chi}$: Given access to an oracle that produces samples of the form $(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i)$ where $\mathbf{a}_i \in_R \mathbb{Z}_q^n$, $x_i \in_R \chi$ and $\mathbf{s} \in_R \chi^n$, find $\mathbf{s}$.

Note that the only difference between LWE and ssLWE is in the distribution of the secret $\mathbf{s}$ – in LWE, the secret is drawn from the uniform distribution over $\mathbb{Z}_q^n$ whereas in ssLWE, it is drawn from χ^n.

Prove that ssLWE and LWE are equivalent. Namely,

- (5 points) Show that if there is an algorithm that solves LWE with m samples, then there is an algorithm that solves ssLWE with m samples as well.
- (60 points) Show that if there is an algorithm that solves ssLWE, then there is an algorithm that solves LWE. Your LWE algorithm can use up more samples than the ssLWE algorithm – try to make do with $m + O(n)$ samples.

  [Hint: Observe that given (say) n ssLWE samples written compactly as $(\mathbf{A}, \mathbf{A}^T\mathbf{s} + \mathbf{e})$, one can write down a linear relation between the LWE secret $\mathbf{s}$ and the error $\mathbf{e}$.]

Problem 2: Modulus Reduction Lemma (35 points)

The modulus reduction procedure works as follows:

1. **Input:** A ciphertext of the form $\mathbf{c} := (\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s} \rangle + 2e + \mu) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ where $\mathbf{a} \in_R \mathbb{Z}_q^n$, $\mathbf{s} \in_R \chi^n$, $e \in_R \chi$, and the message $\mu \in \{0, 1\}$. A natural number p.

2. **Procedure:**

   - Scaling: Compute $\mathbf{c}_f = (\frac{p}{q} \cdot \mathbf{a}, \frac{p}{q} \cdot b) \in \mathbb{Q}^n \times \mathbb{Q}$.
   - Special Rounding: Round $\mathbf{c}_f$ to the nearest integer vector $\mathbf{c}' \in \mathbb{Z}^n \times \mathbb{Z}$ such that $\mathbf{c}' = \mathbf{c} \pmod 2$. Namely, apply the special rounding operation to each coefficient of $\mathbf{c}_f$ separately.

3. **Output:** The output is the vector $\mathbf{c}' = (\mathbf{a}', b')$, considered as an element of $\mathbb{Z}_p^n \times \mathbb{Z}_p$.

Your goal is to prove that $\mathbf{c}'$ is an encryption of μ modulo p. Namely,

- Prove that $\left| b' - \langle \mathbf{a}', \mathbf{s} \rangle \right| \leq \frac{p}{q} \cdot \left| b - \langle \mathbf{a}, \mathbf{s} \rangle \right| + \sum_{i=1}^{n} |s_i| = \frac{p}{q} \cdot \left| b - \langle \mathbf{a}, \mathbf{s} \rangle \right| + \ell_1(\mathbf{s})$, where $\ell_1(\mathbf{s})$ denotes the ℓ_1 norm of the vector $\mathbf{s}$.
- Assume that $p < q$ and that χ is a B-bounded distribution where $B < \frac{p(q/2-1)}{2p+nq}$.
  Define $\mathsf{Dec}_{\mathbf{s}}(\mathbf{a}', b') = (b' - \langle \mathbf{a}', \mathbf{s} \rangle \pmod p) \pmod 2$. Prove that the output of Dec is μ.