Monash University
FIT 5124: Advanced Topics in Security
Week 5 Tutorial Sheet

Ron Steinfeld, 13 April 2015

This week's tutorial is related to the security of the Learning With Errors (LWE) problem and choosing parameters for LWE-based encryption given a desired security level and decryption error probability.

Problems

1 **LWE and cryptanalysis via reduction to SIS.** Consider the following decision LWE problem instance $(A, \boldsymbol{y})$ with parameters $m = 5, n = 3, q = 31$ and $\chi_{\alpha q}$ being the normal distribution with mean 0 and standard deviation αq rounded to integers, with $\alpha = 1/15$, the matrix A the one from Problem 1 of the week 4 tutorial, and with:

$$\boldsymbol{y} = \begin{bmatrix} 27 \\ 4 \\ 0 \\ 20 \\ 5 \end{bmatrix}$$

Suppose you have used a lattice reduction algorithm on the SIS lattice $L_q^{\perp}(A^T)$ to compute a short non-zero vector $\boldsymbol{v} = [-1, -1, 1, -1, -1]^T$ in $L_q^{\perp}(A^T)$.

a Verify that $\boldsymbol{v}$ indeed belongs to the SIS lattice $L_q^{\perp}(A^T)$.

b Apply the 'Decision LWE to SIS reduction' attack from the lecture to distinguish, using the vector $\boldsymbol{v}$, whether $(A, \boldsymbol{y})$ comes from the 'Real' LWE scenario, or the 'Random LWE' scenario. Based on the result of this distinguisher test, which scenario do you think the given $(A, \boldsymbol{y})$ above comes from?

c Estimate the distinguishing advantage of the distinguisher above and the probability that it made a mistake in deciding the scenario in (b).

2 **Choosing parameters for LWE-based encryption.** Based on the cryptanalysis algorithm via reduction to SIS above for security estimation, and the security estimation for SIS from previous lectures, choose parameters for Regev's basic encryption scheme (from lecture 3) at security level $T \geq 2^{80}$ enumeration 'nodes' (based on the state of the art SIS solvers from previous lectures), and decryption error probability $p_e \leq 10^{-3}$. How large is the public key, ciphertext, and ciphertext/plaintext expansion ratio? How many multiplications mod$q$ are needed for encryption and decryption?