Monash University
FIT 5124: Advanced Topics in Security
Week 4 Tutorial Sheet

Ron Steinfeld, 26 March 2015

This week's tutorial will cover the Learning With Errors (LWE) problem and its application to building lattice-based encryption.

Problems

1 **Symmtric-Key Encryption from LWE.** Consider the following ciphertext $(A, \boldsymbol{c})$ for the LWE-based symmetric-key encryption scheme from the lecture, with parameters $q = 31$, $n = 3$, $\ell = 5$ (number of plaintext symbols per ciphertext), $t = 2$ (plaintext symbols from $\mathbb{Z}_2$), and noise distribution $\chi_{\alpha q}$ being the normal distribution with mean 0 and standard deviation αq rounded to integers, where $\alpha = 1/15$:

$$A = \begin{bmatrix} 17 & 8 & 12 \\ 3 & 28 & 21 \\ 14 & 19 & 5 \\ 24 & 2 & 11 \\ 1 & 12 & 23 \end{bmatrix}, \boldsymbol{c} = \begin{bmatrix} 3 \\ 27 \\ 7 \\ 27 \\ 30 \end{bmatrix}.$$

a Given that the secret key is $\boldsymbol{s} = [22, 27, 27]^T$, decrypt the ciphertext $(A, \boldsymbol{C})$ to recover the plaintext.
b Estimate the decryption error probability: the probability that your decrypted message is different from the encrypted message in one of the bit positions.

2 **Public-Key Encryption from LWE: Regev's encryption scheme.** Consider Regev's LWE-based public-key encryption scheme with parameters $q = 31, n = 3, m = 5, B_r = 3$ and $t = 2$ (plaintext symbols from $\mathbb{Z}_2$), and noise distribution $\chi_{\alpha q}$ being the normal distribution with mean 0 and standard deviation αq rounded to integers, where $\alpha = 1/15$.
a Generate a secret key $\boldsymbol{s}$ and corresponding public key pair $(A, \boldsymbol{p})$ for the system. For the matrix A, use the same matrix as in Problem 1.
b Encrypt the message bit $b = 1$ with the public key to get a ciphertext $(\boldsymbol{a}^T, c)$.
c Decrypt the message bit $b = 1$ with the secret key. Did your decryption succeed to recover b?
d Estimate the decryption error probability for your scheme. How would you change the parameters to lower this error probability?

3 **LWE and its Cryptanalysis.** 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, 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).