Monash University
FIT 5124: Advanced Topics in Security
Week 6 Tutorial Sheet

Ron Steinfeld, 16 April 2015

This week's tutorial is related to the security and practical aspects of efficient encryption schemes based on the Ring-LWE problem.

Problems

1 **Choosing parameters for Ring LWE-based encryption.** Based on the cryptanalysis algorithm via reduction to Ring-SIS from the Week 5 tutorial for security estimation, and the security estimation for SIS from previous lectures (assuming it is the same as for Ring-SIS), choose parameters for the Diffie-Hellman analogue Ring-LWE encryption scheme (from lecture 4) at security level $T \geq 2^{80}$ enumeration 'nodes', and decryption error probability $p_e \leq 10^{-3}$. How large is the public key, ciphertext, and ciphertext/plaintext expansion ratio? Compare with the LWE-based scheme parameters from week 5 tutorial.

2 **Importance of choice of polynomial ring in Ring-LWE.** Suppose we wanted to implement a ring-variant of Ajtai's collision-resistant hash function, using the ring $R_q^- = \mathbb{Z}_q[x]/(x^n - 1)$ (the original NTRU ring), instead of the usual ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ discussed in the lectures. Do you think the resulting hash function still collision-resistant? If not, how can a collision be found with non-negligible probability in this hash function?

3 **Importance of making noise not too small in LWE/Ring-LWE.** Suppose we wanted to use LWE (or Ring-LWE) with binary noise, rather than noise coefficients with standard deviation $> \sqrt{n}$ as in Regev's worst-case to average-case security reduction. Note that the noise coordinates e_i of the LWE instances all satisfy the quadratic equations $e_i \cdot (1 - e_i) = 0 \bmod q$. Explain how to use these equations to efficiently break the LWE problem when m exceeds about n^2, by reducing it to solving a linear system of n^2 equations in n^2 unknowns modulo q.

4 **Hardness of SSRing-LWE.** Prove that the SSRing-LWE from the lecture, with $m - 1$ samples (with a 'small' secret e chosen from the Ring-LWE noise distribution $\chi_{\alpha q}$) is as hard as the Ring-LWE (with a uniformly random secret $s \hookleftarrow U(R_q)$) with m samples. Hint: Given a Ring-LWE instance, use the first sample to solve for the secret s and eliminate s from the remaining samples by substitution.

5 **Implementation Experiments.** Experiment with the Ring-LWE oracle generator module in Sage (see online Sage documentation cryptography modules). Try to use it to implement and experiment with one of the Ring-LWE based encryption scheme, or to experiment with the the above algebraic attack of the distinguishing attack on Ring-LWE based on reduction to Ring-SIS.