USS: Introduction to mathematical cryptography
Monday August 1 problems

Continuous error distribution: A variation on Regev LWE

We present here is a variation on Regev's LWE scheme that uses errors e_i drawn from a *continuous* error distribution.

1. Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, and consider the ring homomorphism $\varphi\colon \mathbb{Z}/q\mathbb{Z} \to \mathbb{T}$ given by taking $\alpha \in \mathbb{Z}/q\mathbb{Z}$, lifting it to any representative in $\mathbb{Z}$, dividing by q, and then reducing modulo $\mathbb{Z}$. To make sure that you understand the map φ, compute the image of each of $0, 1, \ldots, q-1 \in \mathbb{Z}/q\mathbb{Z}$ in $\mathbb{T}$.

2. With this new map, the LWE pairs are created in this way: Fix q and n, and a secret vector $\vec{s} \in (\mathbb{Z}/q\mathbb{Z})^n$. Choose m vectors $\vec{a}_i \in (\mathbb{Z}/q\mathbb{Z})^n$ uniformly at random, and draw m values e_i from a probability distribution χ on $\mathbb{T}$. The LWE pairs are then of the form
$$(\vec{a}_i, b_i = \varphi(\vec{a}_i \cdot \vec{s}) + e_i) \in (\mathbb{Z}/q\mathbb{Z})^n \times \mathbb{T}.$$
Based on your knowledge of Regev's LWE scheme when the error is discrete, make your best guess as to what the encryption and decryption algorithms must be.

3. Explain in your own words why a distribution χ on $\mathbb{T}$ could be thought of a continuous error distribution for the LWE problem. If an error distribution on $\mathbb{T}$ with standard deviation σ is used, what would be the "equivalent" standard deviation for the discrete error distribution on $\mathbb{Z}/q\mathbb{Z}$?

A somewhat homomorphic encryption scheme

Recall the simple cipher over the integers which we studied last week on Tuesday. Show that this cipher supports at least one addition or one multiplication. (You can assume anything you want about the error growth so that decryption remains correct after one operation.)

BV LWE: a variation on Regev's LWE

We present here a variation on LWE inspired by Brakerski and Vaikuntanathan to illustrate different ways the same problem can be used to create a cipher. The algorithms are as follows:

- Key generation: Fix n, q, m and a distribution χ on $\mathbb{Z}/q\mathbb{Z}$ to draw the errors from, as well as a secret vector $\vec{s} \in (\mathbb{Z}/q\mathbb{Z})^n$, which is the secret key. Rather than "plain" LWE pairs, the public key contains m pairs of the form
$$(\vec{a}_i, b_i = \vec{a}_i \cdot \vec{s} + 2e_i),$$
for $\vec{a}_i \in (\mathbb{Z}/q\mathbb{Z})^n$ chosen uniformly at random.

- Encryption: To send a bit $x = 0$ or $x = 1$, choose a random set $T \subseteq \{1, 2, \ldots, m\}$, and send the pair $(\vec{a}, b)$, where $\vec{a} = \sum_{i \in T} \vec{a}_i$, but this time

$$b = x + \sum_{i \in T} b_i.$$

- Decryption: Compute $b - \vec{a} \cdot \vec{s}$ and lift to an integer in the set $\{0, 1, \ldots, q - 1\}$. The sent bit x is the parity of that integer with high probability.

1. Why is decryption described here only probably correct? What can go wrong? We note that the authors do have a fix for this, but it is technical (see Section 4.1 of their article *Efficient Fully Homomorphic Encryption from (Standard) LWE*, in the part explaining multiplication of ciphertexts).

2. Use the BV LWE pairs with $q = 17$

$$\begin{gathered} ((12, 11, 7, 13), 16), \\ ((12, 16, 11, 10), 0), \\ ((6, 16, 5, 3), 7), \\ ((13, 14, 15, 0), 13), \\ ((7, 11, 4, 14), 14), \\ ((12, 4, 1, 16), 7), \\ ((5, 2, 16, 8), 14) \end{gathered}$$

   to encrypt

   (a) $x = 0$,

   (b) $x = 1$.

3. Suppose that you have published a set of BV LWE pairs generated with $q = 17$ and $\vec{s} = (9, 0, 9, 2)$. You receive the ciphertext pair

$$((3, 13, 4, 9), 12).$$

   What was the bit (probably) sent to you?