☙ CS6222 Cryptography ❧

Topic: Public Key Encryption Date: Nov 26, 2024
Lecturer: Wei-Kai Lin (TA: Arup Sarker) Scriber: Yucheng Fu (zdp8uu)

1 Public Key Encryption

We begin with a setting that Alice has a private message $\mathbf{m}$ and wants to send it to Bob after encrypting it to $Enc(\mathbf{m}) = ct$. Then, Bob needs to decrypt it to $Dec(ct)$. Then the question is, Bob requires the key k sent from Alice. However, this key conveyance is not secure.

Alternatively, Bob can send a public key pk to Alice in advance. To make this secure, for $\forall$ NUPPT A and two message $\mathbf{m}_0$ and $\mathbf{m}$, we need

$$|\Pr[A(Enc_{pk}(\mathbf{m}_0), pk) = 1] - \Pr[A(Enc_{pk}(\mathbf{m}), pk) = 1]| \leq \epsilon(n)$$

We can use learning with errors (LWE) to implement an encryption scheme. Assuming

$$\mathbb{Z}_q = \{-\lfloor \frac{q-1}{2} \rfloor, \cdots, 0, \cdots, \lfloor \frac{q}{2} \rfloor\}.$$

We consider a matrix $A \in \mathbb{Z}_q^{m \times n}$ and vector $\vec{s} \in \mathbb{Z}_q^n$ such that $m \gg n$. There is an error vector $\vec{e} \in \phi^m$, which is from another distribution. The AWE assumption can be expressed as

$$(A, A\vec{s} + \vec{e}) \approx_c (A, \vec{U}),$$

where $\vec{U} \xleftarrow{uniform} \mathbb{Z}_q^m$.

In LWE, we assume the existence of many nodes, where some nodes represent α and others represent β. The task is to find a plate $\vec{s}$ to divide these two types of nodes. Such task can be formulated as

$$A\vec{s} + \vec{e} = \vec{b} \in \{\alpha,\ \beta\}^m$$
$$\min \vec{e} = \min\{\max |\vec{e}_i|\}$$

Then the assumption of LWE can be

$$(A, \vec{b}) \approx_c (A, \vec{U}), \quad \vec{U} \xleftarrow{uniform} \mathbb{Z}_q^m.$$

Then we give an example of LWE. Firstly we define:

1. Gen: $k = \vec{s} \in \mathbb{Z}_q^n$
2. $Enc_k(\mathbf{m})$: $ct = (\vec{a},\ \vec{a}^T\vec{s} + 2e + \mathbf{m})$, where $\vec{a}^T \in \mathbb{Z}_q^n$ is the parameter vector and $e \leftarrow \phi$ is a scalar.
3. $Dec_k(ct)$: For $ct = (\vec{a},\ b)$, calculate $\mathbf{m'} = (b - \vec{a}^T\vec{s})\ mod\ 2$.

2 Homomorphic Property of LWE

In the decryption step $(b - \vec{a}^T \vec{s})$ is equal to $2e + \mathbf{m}$. Therefore, mod 2 is equal to $\mathbf{m}$. There is a corollary that

Theorem 1. *If* $\gcd(q, 2) = 1$*, then LWE means*

$$(\vec{a},\ \vec{a}^T \vec{s} + 2e + \mathbf{m}) \approx_c (\vec{a},\ \vec{U})$$

Finally, we will introduce the homomorphic property of this encryption. Firstly, let

$$ct_1 = (\vec{a}_1,\ \vec{a}_1^T \vec{s} + 2e_1 + \mathbf{m}_1)$$

and

$$ct_2 = (\vec{a}_2,\ \vec{a}_2^T \vec{s} + 2e_2 + \mathbf{m}_2)$$

Then for a message $\mathbf{m}_3 = \mathbf{m}_1 + \mathbf{m}_2$ and $ct_3 = ct_1 + ct_2$, we have

$$ct_1 + ct_2 = (\vec{a}_1 + \vec{a}_2,\ (\vec{a}_1 + \vec{a}_2)^T \vec{s} + 2(e_1 + e_2) + (\mathbf{m}_1 + \mathbf{m}_2))$$

This means that $Dec(ct_3) = \mathbf{m}_1 + \mathbf{m}_2$, which is the linear homomorphic property.