CS 7810 Graduate Cryptography November 27th, 2017

Lecture 21: (Lattice Based) Homomorphic Encryption

Lecturer: Daniel Wichs *Scribe: Schuyler Rosefield*

1 Topic Covered

- Learning With Errors
- Encryption from LWE

2 Learning With Errors (LWE)

Choose a vector $\vec{s} \leftarrow \mathbb{Z}_q^n$. Assume we have a black box that computes the following
$\vec{a} \leftarrow \mathbb{Z}_q^n, \langle \vec{a}, \vec{s} \rangle$

The LWE problem is that of finding $\vec{s}$ given $\vec{a}_i$s and the inner products of $\vec{a}_i, \vec{s}$. This problem is simple to solve by constructing a matrix

$$A = \begin{bmatrix} | & & | \\ a_1 & \dots & a_n \\ | & & | \end{bmatrix}$$

and if A is a full rank matrix then it is easy to find $\vec{s}$ given $A, \vec{s}A$

In order to make this a hard problem we can instead change our blackbox to output the inner products with some small error. $\vec{a}, \langle \vec{a}, \vec{s} \rangle + e$ where $e \leftarrow \chi$ and $e \in \{-\beta, \dots, \beta\}$ with $\beta << \lfloor q/2 \rfloor$. The distribution χ is typically either gaussian or uniform.

This is now a non-trivial problem.

Definition 1 Search LWE Assumption (sLWE)
$\forall PPT \mathsf{A}$
$Pr[\mathsf{A}(A, \vec{s}A + \vec{e}) = \vec{s} : A \leftarrow \mathbb{Z}_q^{n \times m}, \vec{s} \leftarrow \mathbb{Z}_q^n, \vec{e} \leftarrow \chi^m] = negl(n)$

Definition 2 Decisional LWE Assumption (dLWE)
The distributions $(A, sA + e) \approx (A, b)$ are computationally indistringuishable where $A \leftarrow \mathbb{Z}_q^{n \times m}, s \leftarrow \mathbb{Z}_q^n, e \leftarrow \chi^m, b \leftarrow \mathbb{Z}_q^m$
There are a number of parameters here that can be tweaked

n : dimension
m : # of samples
q : modulus
χ : error distribution, β − bounded

Loosely to evaluate the hardness of the assumption based on the parameters,

n : larger $\Rightarrow$ harder

m : larger $\Rightarrow$ easier, but should still be hard for any $poly(n)$

β/q : larger $\Rightarrow$ harder, e.g. $q = 2^{\sqrt{n}}, \beta = n$

χ : Usually gaussian, but flexible

We expect this problem to be hard for a wide range of parameters.

Note 1 *Solving sLWE $\Rightarrow$ solving dLWE. We claim that the two distributions $(A, sA + e), (A, b)$ are statistically far.*

$$\begin{aligned} Pr[\exists s, e s.t. b = sA + e] &\leq \sum_{s,e} Pr_b[b = sA + e] \\ &= \frac{q^n (2\beta)^m}{q^m} \end{aligned}$$

So long as $2\beta < q$ then it is possible to choose m such that this probability is negligible. Therefore, if an adversary A can solve sLWE then there is a non-negligible probability that the output $\vec{s}$ matches the $(A, sA + e)$ distribution.

Note 2 *Given dLWE we can construct something akin to a pseudorandom generator. That is, we can start with $n \log q + m \log 2\beta$ random bits and output $m \log q$ pseudorandom bits.*

3 Public Key Cryptography from LWE

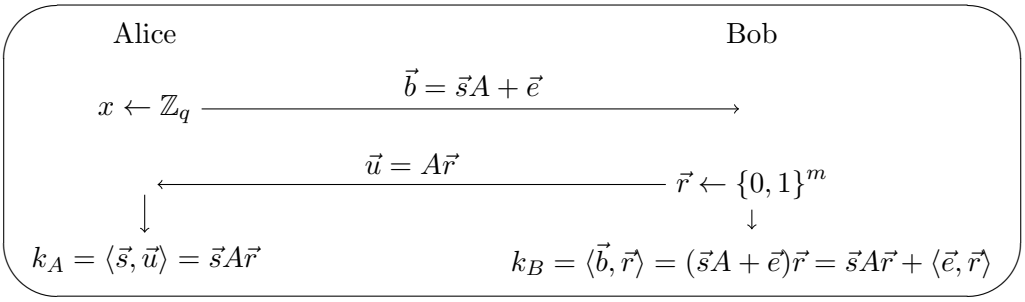
Over the last few years there has been a lot of research into crypto based onto this assumption. One of the largest motivators for this is that LWE appears to be resistant to quantum algorithms, unlike factoring or discrete log assumptions. As far as we know, there are no polynomial quantum algorithms that break these assumptions.

One other interesting facet is that we can speak more towards the hardness in the worst case. Typically for crypto assumptions we can say that it is hard in the average case, but we cannot prove that it is always hard. For example, for the factoring assumption with random p, q we cannot say that there does not exist an algorithm that can factor easier than the average case. However, for LWE, we can perform a worst case to average case reduction. That is, if LWE is hard for the average case it is hard in every case.

A third reason for studying LWE is that it allows the building of Fully Homomorphic Encryption (FHE) schemes.

Definition 3 Key Agreement from LWE

Public parameter $A \leftarrow \mathbb{Z}_q^{n \times m}$



Here we have $K_A - K_B = \langle \vec{e}, \vec{r} \rangle \leq m\beta$ so the two parties have keys that are "close enough". We can build two encryption schemes based on this idea.

Definition 4 Regev Encryption Scheme

$$\begin{aligned} Gen: & pk = \vec{b} = \vec{s}A + \vec{e} \\ & sk = \vec{s} \\ Enc_{PK}(\alpha): & \vec{r} \leftarrow \{0,1\}^m, \\ & \vec{u} = A\vec{r} \\ & Output(\vec{u}, \langle \vec{b}, \vec{r} \rangle + \alpha \cdot \lfloor q/2 \rfloor) \\ Dec_{SK}(ct = (\vec{u}, v)): & round(v - \langle \vec{s}, \vec{u} \rangle) \end{aligned}$$

Claim 1 $A \leftarrow \mathbb{Z}_q^{n \times m}, \vec{r} \leftarrow \{0,1\}^n, \vec{u} \leftarrow \mathbb{Z}_q^n$

$(A, A\vec{r}) \overset{stat}{\approx} (A, \vec{u})$

as long as $m > n \log q + n$

The proof follows from the leftover hash lemma.

$h_A : \{0,1\}^m \to \mathbb{Z}_q^n, h_A(\vec{r}) = A\vec{r}$ *is a universal hash function.* $\forall \vec{r} \neq \vec{r}', Pr_A[h_A(\vec{r}) = h_A(\vec{r}')] = \frac{1}{q^n}$ *since that is the probability that* $A\vec{r} = A\vec{r}' \Rightarrow A(\vec{r} - \vec{r}') = 0$.

Proof:

Correctness:

$$\begin{aligned} v - \langle \vec{s}, \vec{u} \rangle &= \langle \vec{b}, \vec{r} \rangle + \alpha \cdot \lfloor q/2 \rfloor - \langle \vec{s}, \vec{u} \rangle \\ &= \lfloor q/2 \rfloor \alpha + \langle \vec{e}, \vec{r} \rangle \end{aligned}$$

This is correct if $m\beta < q/4$

Security

goal: we want to find that $(\vec{b}, \vec{u}, v) \approx (U_{\mathbb{Z}_q^m}, U_{\mathbb{Z}_q^n}, U_{\mathbb{Z}_q})$

We construct the following hybrids

$$\begin{aligned} H_0: & (\vec{b}, \vec{u}, v) \\ & A, \vec{b} = \vec{s}A + \vec{e}, \vec{u} = A\vec{r}, v = \langle \vec{b}, \vec{r} \rangle + \alpha \cdot q/2 \\ H_1: & A, \vec{b} \leftarrow \mathbb{Z}_q^m, \vec{u} = A\vec{r}, v = \langle \vec{b}, \vec{r} \rangle + \alpha \cdot q/2 \\ H_2: & A, \vec{b} \leftarrow \mathbb{Z}_q^m, \vec{u} \leftarrow \mathbb{Z}_q^n, u' \leftarrow \mathbb{Z}_q, v = u' + \alpha \cdot q/2 \end{aligned}$$

$H_0 \approx H_1$ immediately from the dLWE assumption. Since $A, \vec{b}, \vec{r}$ are random, then $A\vec{r} \approx U_{\mathbb{Z}_q^n}$, and $\langle \vec{b}, \vec{r} \rangle \approx U_{\mathbb{Z}_q} \Rightarrow H_1 \approx H_2$.

□

DEFINITION 5 Dual Regev scheme

$$\begin{aligned} Gen: & pk = u = A\vec{r} \\ & sk = \vec{r} \\ Enc_{PK}(\alpha): & \vec{b} = \vec{s}A + \vec{e}, \\ & Output(\vec{b}, \langle \vec{s}, \vec{u} \rangle + \alpha \cdot \lfloor q/2 \rfloor + \vec{e}) \\ Dec_{SK}(ct = (\vec{b}, v)): & round(v - \langle \vec{b}, \vec{r} \rangle) \end{aligned}$$

The security proof is similar to the initial scheme