CS6115: Structure versus Hardness in Cryptography	Aug 12, 2021
Lecture 4 : Quadratic Fully Homomorphic Encryption from LWE	
Lecturer: *Shweta Agrawal*	Scribe: *Meenakshi*

In this lecture, we will be studying the quadratic homomorphic encryption (qFHE) in the secret key setting of [BV11].

1 Symmetric Key Encryption

Let n be the security parameter, q be the modulus and χ be the error distribution for the scheme. Let SKE = {keygen, enc, dec} be a symmetric key encryption scheme described below.

* $sk \leftarrow \mathsf{SKE.keygen}(1^n)$. On receiving the security parameter n as input, it samples $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and sets $sk = \mathbf{s}$.
* $(\mathbf{a}, b) \leftarrow \mathsf{SKE.enc}(sk, m)$. It takes input as a secret key sk, a message $m \in \{0,1\}$ and performs the following steps.
  1. sample $\mathbf{a} \in \mathbb{Z}_q^n$ and $e \in \chi$,
  2. compute $b =< \mathbf{a}, \mathbf{s} > +e + m(\frac{q+1}{2})$,
  3. output the ciphertext $ct = (\mathbf{a}, b)$.
* $m \leftarrow \mathsf{SKE.dec}(sk, ct)$. It computes $w = b- < \mathbf{a}, \mathbf{s} >$. Note that $\mathbf{s} = sk$.
  1. If $\frac{q}{2} \leq |w| \leq q$ then output 1.
  2. Otherwise output 0.

  Note that the correctness of this algorithm follows provided $|e| < \frac{q}{4}$. The security of SKE relies on the hardness of learning with errors problem.

Homomorphic Operations on the Above Symmetric Key Encryption SKE.

Let c_1, c_2 be two ciphertexts such that $c_i = (\mathbf{a}_i, b =< \mathbf{a}_i, \mathbf{s} > +e_i + m_i(\frac{q+1}{2}))$ for $i = 1, 2$.

- It is easy to see that the scheme is *additively homomorphic* as explained below.

  If we set $c = c_1 + c_2 \bmod q$ defined by

  $$c = (\mathbf{a}, b) = \Big(\mathbf{a}_1 + \mathbf{a}_2, < \mathbf{a}_1 + \mathbf{a}_2, \mathbf{s} > +(e_1 + e_2) + (m_1 + m_2)(\frac{q+1}{2})\Big)$$

  then

  $$b- < \mathbf{a}_1 + \mathbf{a}_2, \mathbf{s} >= (e_1 + e_2) + (m_1 + m_2)(\frac{q+1}{2}).$$

  Thus, if we set the parameters in such a way that the accumulated noise $e_1 + e_2$ remains bounded above by $\frac{q}{4}$ then we get a valid encryption of $m_1 + m_2$.

- We now understand the ideas of [BV11] to get the above scheme SKE to be *multiplicatively homomorphic*.

  If we look from the other way, we actually want is the encryption of $m_1 \cdot m_2$, given the encryption of m_1 and m_2. In other words, we want the encoding of $m_1 m_2(\frac{q+1}{2})$. We already have

  $$b_1- < \mathbf{a}_1, \mathbf{s} >\approx m_1(\frac{q+1}{2}),$$

$$b_2 - < \mathbf{a}_2, \mathbf{s} > \approx m_2\Big(\frac{q+1}{2}\Big).$$

That is $2(b_1 - < \mathbf{a}_1, \mathbf{s} >)(b_2 - < \mathbf{a}_2, \mathbf{s} >) \approx m_1 m_2(\frac{q+1}{2}) \bmod q$.

Let us recall the tensor product and the product of two inner products.

1. Let $\mathbf{w} = (w_1, w_2, \ldots, w_s) \in \mathbb{Z}^s$ and $\mathbf{z} = (z_1, z_2, \ldots, z_t) \in \mathbb{Z}^t$ then
$$\mathbf{w} \otimes \mathbf{z} = (w_i z_j)_{(i,j)\in[s][t]} \in \mathbb{Z}^{st}.$$
2. $< \mathbf{u}_1, \mathbf{v}_1 >< \mathbf{u}_2, \mathbf{v}_2 >=< \mathbf{u}_1 \otimes \mathbf{u}_2, \mathbf{v}_1 \otimes \mathbf{v}_2 >$.

Let $\mathbf{t} = (-\mathbf{s}, 1)$. There are two things that needs to be noted. Firstly,

$$< c_1, \mathbf{t} >< c_2, \mathbf{t} >= (< -\mathbf{a}_1, \mathbf{s} > +b_1)(< -\mathbf{a}_2, \mathbf{s} > +b_2) = (b_1 - < \mathbf{a}_1, s >)(b_2 - < \mathbf{a}_2, \mathbf{s} >).$$

Secondly, from the above definition we get $< c_1, \mathbf{t} >< c_2, \mathbf{t} >=< c_1 \otimes c_2, \mathbf{t} \otimes \mathbf{t} >$. Also,

$$\begin{aligned} 2 < c_1 \otimes c_2, \mathbf{t} \otimes \mathbf{t} > &= 2 < c_1, \mathbf{t} >< c_2, \mathbf{t} > \\ &= 2\Big(e_1 + m_1\big(\frac{q+1}{2}\big)\Big)\Big(e_2 + m_2\big(\frac{q+1}{2}\big)\Big) \\ &= 2e_1e_2 + (m_1e_2 + m_2e_1) + m_1m_2\big(\frac{q+1}{2}\big) \end{aligned} \quad (1)$$

Thus, $2 < c_1 \otimes c_2, \mathbf{t} \otimes \mathbf{t} >= 2 < c_1, \mathbf{t} >< c_2, \mathbf{t} >= m_1 m_2(\frac{q+1}{2}) + noise$.

The above explanation says that $2c_1 \otimes c_2$ is the new ciphertext w.r.t the new secret key $\mathbf{t} \otimes \mathbf{t}$. From the definition of tensor product, it is clear that the size of the ciphertext and noise grows rapidly. More specifically, dimension n changes to n^2. Following this way will limit the expressiveness of the multiplicative circuit. That is, if we take the multiplicative operation i times then the dimension increases to n^{2^i}. In other words, the max depth the multiplicative circuit can support is $\log\log n$. Also, if we look at Equation (1) we notice that the growth in the error is quadratic. Next, our job is to bring the dimension n^2 back to n. In [BV11], the technique of reducing the dimension is called DIMENSION REDUCTION.

Let $C_{mult} = 2c_1 \otimes c_2$ and the new secret key = $\mathbf{t} \otimes \mathbf{t}$.

Dimension Reduction

We want to reduce the complexity of the decryption without decreasing the homomorphic capacity. We therefore provide some "extra stuff" that lets us bring the dimension n^2 (after one multiplication) back down to n. The idea here is to apply a transformation $\mathbf{B} \in \mathbb{Z}^{n \times n^2}$ (publicly known) to C_{mult} such that the high dimension C_{mult} (wrt $\mathbf{t}_1 \otimes \mathbf{t}_1$) comes down to a low dimensional C_{new} (wrt $\mathbf{t}_2$). Roughly speaking we encrypt $\mathbf{t}_1 \otimes \mathbf{t}_1$ under $\mathbf{t}_2$ with a relatively larger modulus. We know that

$< \mathbf{t}_1 \otimes \mathbf{t}_1, 2c_1 \otimes c_2 > \approx m_1 m_2(\frac{q+1}{2})$ i.e., $(\mathbf{t}_1 \otimes \mathbf{t}_1)^T C_{mult} \approx m_1 m_2(\frac{q+1}{2})$. Let $\mathbf{B}^T \cdot \mathbf{t}_2 = \mathbf{t}_1 \otimes \mathbf{t}_1$ then $(\mathbf{B}^T \cdot \mathbf{t}_2)^T \cdot C_{mult} = \mathbf{t}_2^T \cdot C_{new}$ where $C_{new} = \mathbf{B} \cdot C_{mult}$.

Next, we need to specify the matrix $\mathbf{B}$ and the new secret key $\mathbf{t}_2$ such that $\mathbf{B}^T \mathbf{t}_2 \approx \mathbf{t}_1 \otimes \mathbf{t}_1$. Let us sample $\mathbf{s}_2 \leftarrow \mathbb{Z}_q^n$ and set $\mathbf{t}_2 = (-\mathbf{s}_2, 1)$. Let ψ_{ij} for all $i, j \in [n]$ be the columns of $\mathbf{B}$ such that

$$\psi_{ij} = \widetilde{Enc}(t_{1i}, t_{1j}) = (\mathbf{a}_{ij}, < \mathbf{a}_{ij}, \mathbf{s}_2 > +e_{ij} + t_{1i}t_{1j}).$$

Roughly speaking, the entries of the matrix $\mathbf{B}$ can be seen as the encryptions of old long key $\mathbf{s}_1 \otimes \mathbf{s}_1$ under the new short key $\mathbf{s}_2$. Observe that

$$< \psi_{ij}, \mathbf{t}_2 > \approx \mathbf{t}_{1i}\mathbf{t}_{1j} \quad (2)$$

Thus, the way we have specified ψ_{ij} and from Equation (2), we see that $\mathbf{B}^T \mathbf{t}_2 \approx \mathbf{t}_1 \otimes \mathbf{t}_1$.

In the next lecture, we will continue our discussion on dimension reduction techniques. Observe that $C_{new} = \mathbf{B} \cdot C_{mult}$ is low dimensional and decrypts correctly. However the noise grows hugely due to the large normed vector $2c_1 \otimes c_2$. In next class, we will see how the bit decomposition technique helps us to reduce the error growth and allows us to take the depth of the circuit to be $\log n$ which was $\log \log n$ earlier.

References

[BV11] Z. Brakerski and V. Vaikuntanathan, Efficient fully homomorphic encryption from (standard) LWE, Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on, 2011, pp. 97–106