Fully Homomorphic Encryption – Problem Set

Lecture 1

Vulnerabilities of the Verifiability Protocol. Recall the verifiability protocol that we saw in class. Our goal here is to show why it is important that the precomputed values c_0, z_0 remain hidden.

1. Consider the first protocol without the outer layer of encryption. Namely the verifier sends c_0, c_x to the prover. Show that in this case, if the prover knows c_0 or z_0 then it can convince the verifier of a false statement.

2. Show that the attack above can be executed even in the case where there are two non-communicating provers: One operating only on c_0 and one operating only on c_x (without knowing which is which, of course).

3. Recall that in homomorphic encryption, if $c' = \mathsf{Enc}(m)$ then $\mathsf{Eval}(f, c')$ is an encryption of $f(m)$. How would you launch the above attack when c_0 and c_x are encrypted under another layer of homomorphic encryption?

Lecture 2

Regev's Encryption Scheme. In this exercise, we will try to reconstruct Regev's public key encryption scheme. We let n be some natural number, and $q \gg n$ be some natural number to be used as modulus. **All arithmetic operations in this exercise are performed modulo q.** We start with (a special case of) the famous "Leftover Hash Lemma" (Impagliazzo-Levin-Luby).

Lemma 1. *Let $\mathbf{A}$ be a uniform matrix in $\mathbb{Z}_q^{m \times n}$, for $m \geq n \log q + 2n$. Let $\mathbf{r}$ be a uniform vector in $\{0,1\}^m$. Then the distribution $(\mathbf{A}, \mathbf{r}^T\mathbf{A})$ is within statistical distance 2^{-n} from uniform over $\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$.*

Assume that we can generate a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{s} \in \mathbb{Z}_q^n$ such that $\mathbf{As} = \mathbf{e}$ for $\|\mathbf{e}\| \ll q$. Assume furthermore that $\mathbf{A}$ is computationally indistinguishable from being uniform. In other words, any efficient adversary that sees $\mathbf{A}$ without seeing $\mathbf{s}$ cannot distinguish $\mathbf{A}$ from a completely uniform matrix. Consider an encryption scheme where $\mathbf{A}$ is the public key and $\mathbf{s}$ is the secret key.

1. Show that an adversary that only has access to the public-key, cannot distinguish between a vector of the form $\mathbf{r}^T\mathbf{A}$ and a uniform vector $\mathbf{u}^T \in \mathbb{Z}_q^n$, where $\mathbf{r} \in \{0,1\}^m$ is as above.

2. Consider an adversary as above and let $\mathbf{v} \in \mathbb{Z}_q^n$ be a vector that is known to the adversary. Show that the adversary cannot distinguish between $(\mathbf{r}^T\mathbf{A} + \mathbf{v}^T)$ and $\mathbf{u}^T$. (Hint: Think about $(\mathbf{u} + \mathbf{v})^T$ as an intermediate value. What is the distribution of this value?)

3. Prove that if $\mathbf{r} \in \{0,1\}^m$, and if $\mathbf{e} \in \mathbb{Z}^m$ is such that $\|\mathbf{e}\| \ll q/m$, then $\langle \mathbf{r}, \mathbf{e} \rangle \ll q$.

4. Show that given the secret key $\mathbf{s}$ and given $\mathbf{r}^T\mathbf{A} + \mathbf{v}^T$, it is possible to find an *estimate* of the value $\mathbf{v}^T \cdot \mathbf{s} = \langle \mathbf{v}, \mathbf{s} \rangle$.

5. If the first entry of $\mathbf{s}$ always equals to $q/2$, and the vector $\mathbf{v}$ is of the form $[m, 0, \ldots, 0]$, for $m \in \{0,1\}$. Show that it is possible to *find* the value of m using $\mathbf{s}$.

Lecture 3

Back to Hybrid Encryption. Recall that in hybrid encryption, there is a public key homomorphic scheme HE with keys (pk, evk, sk) and a symmetric scheme SYM with key $symsk$. We create an evaluation key $evk' = (evk, c^*)$ for $c^* = \mathsf{HE.Enc}_{pk}(symsk)$, and perform encryption using $symsk$.

1. Consider a ciphertext $c = \mathsf{SYM.Enc}_{symsk}(m)$. Consider the function $C_c(x) = \mathsf{SYM.Dec}_x(c)$. What is the value of $C_c(symsk)$?
2. What is the output of $\mathsf{Eval}_{evk}(C_c, c^*)$? Recall that the output of Eval is a ciphertext. What does this ciphertext encode? Under which key?
3. Show that the hybrid scheme defined by encrypting with $symsk$, evaluating with evk' and decrypting with sk, is homomorphic.
4. Assume that HE is homomorphic for all depth d circuits, and let d' be the depth of the circuit C_c. What is the homomorphic capacity of the hybrid scheme?
5. Try to think what happens if instead of SYM we use an additional homomorphic scheme. Try to think what happens if we do a hybrid of more than two schemes of this sort.

Lecture 4

Generic Bootstrapping. We saw in class how bootstrapping can be used to reduce the noise in ciphertexts, but bootstrapping is in fact a more general technique that can be applied to any bounded depth HE.

1. Let D be the decryption circuit of an encryption scheme. Namely, $D(sk, c) = m$. Let d be the depth of this circuit.

   Consider the circuit $C(sk, c_1, c_2)$, defined as

   $$C(sk, c_1, c_2) = \big(D(sk, c_1)\ \mathbf{NAND}\ D(sk, c_2)\big).$$

   What is the depth of the circuit C?
2. Let c_1 be an encryption of a bit m_1 and c_2 be an encryption of a bit m_2. What is the result of $C(sk, c_1, c_2)$?
3. Given some c_1, c_2, we define the circuit $C'_{c_1,c_2}(sk) = C(sk, c_1, c_2)$ (note that in C'_{c_1,c_2}, the values c_1, c_2 are hard-coded and are not a part of the input). What is the output of $C'_{c_1,c_2}(sk)$?
4. If our scheme is homomorphic, and letting $c^* = \mathsf{Enc}_{pk}(sk)$ be *an encryption of the secret key* sk. what is the output of $\mathsf{Eval}(C'_{c_1,c_2}, c^*)$? Recall that the output of homomorphic evaluation is always a ciphertext. What does this ciphertext encode?
5. Show that if the scheme is homomorphic only for depth $d + 1$ circuits, and c^* is given, then any circuit can be evaluated homomorphically. Recall that any circuit can be written using only **NAND** gates.