Lecture 07 ()

1 Recap of Last 3-4 Lectures

1. $E = (keygen, enc, dec)$
2. Equivalence between bit-guessing and two world formulation
   - $P[\text{A wins}] \leq \frac{1}{2} + \mu(n)$
   - $p_0 - p_1 \leq \mu'(n)$
   - $\mu(n) = \frac{\mu'(n)}{2}$
3. PRG game

sir will write this in detail in the PDF notes

2 Given a Candidate G, Check that G is a (computationally) secure PRG

1. Prove security definition (not that easy, we don't know about all A)
2. Proving that inverse computation takes large amount of time (??)
3. Solving this will prove $P \neq NP$
4. We can rely on building blocks - we don't directly use them to build an encryption scheme since PRG is a clean object to build

xor is such an interesting function - can mangle data without destroying it

3 Proof of E_G being secure if G is secure

We assume that there exists an adversary A which breaks E_G. Now, we have $p_0 - p_1 = \delta$. We consider the two hybrid worlds where Hybrid-b encodes m_b with $r \in \{0,1\}^l$. For either case, p_h is the same since we are working on OTP (it should also work with a similar idea for a non OTP scheme).

4 Something More Fun (:eyes fun is sus)

sir gave some hints about this when I went to ask him the doubt(s)

$$G : \{0,1\}^n \to \{0,1\}^{n+1}$$

G is parameterised by $a_i \in [0, 2^{n+1} - 1], i \in \{1, 2, \dots, n\}$

$$G(x) = (\sum_{1 \le i \le n} a_i \cdot x_i) \mod 2^{n+1}$$

This is average case subset sum problem (average since it depends on choice of a_i's)

4.1 Question: can we extend Range to $\{0,1\}^l$

Inductively, yes:

$$G' : \{0,1\}^n \to \{0,1\}^{n+2}$$
$$y_1 y_2 \dots y_n y_{n+1} = G(x)$$
$$G'(x) = G(y_1 \dots y_n) y_{n+1}$$