Week 10 Friday Lec - 2.12.26

(1) we want show COMP.

(2) we can use Random Bit

(3) we can Pseudorandom bit generator.

$\longrightarrow$

$\Pr\left(x \leftarrow \{0,1\}^n : y \leftarrow f(x) \;\&\; x' \leftarrow B(1^n, 1^n, y) : f(x') = f(x)\right) \geq \frac{1}{poly(n)}$

$|\{f(x)\}_{x\in\{0,1\}^n}| \geq poly(n)$ Hard Primary.

$|\{x\}_{x\in\{0,1\}^n}| \geq poly(n)$ Hard Preimage.

Hard Together

Let f be a fnc.

f is mean p-wise fnc

if poly t, constants ε :

for any poly (n) $\Pr_{x_1, x_2, \ldots, x_t \leftarrow \{0,1\}^n}$

$\Pr\left(\{x_i \leftarrow \{0,1\}^n\}_{i=1}^{t} : \{f(x_i)\}_{i=1}^{t} = \{f(x_i)\}_{i=1}^{t}\right) \geq \frac{1}{f(n)}$

Strong. A Commitment with very hard.

weak. A Sprinkle with Random hard.

Let $F = \{F_n : n \in \mathbb{N}\}$ is a 2-wise Prf.

$F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$

$F_n : \{0,1\}^n \to \{0,1\}^n$

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

$m = 2^n \cdot 2(n)$

$\underbrace{y_1}_{2^n} \| \underbrace{y_2}_{2^n} \| \ldots \| \underbrace{y_{2(n)}}_{2^n}$

$= \underbrace{y_1}_{2^n} \| \underbrace{y_2}_{2^n} \| \ldots \| \underbrace{y_{2(n)}}_{2^n}$

$x_1 \in \{0,1\}^n$ $y_1 = G_n(x_1) \in \{0,1\}^n$

$x_2 \in \{0,1\}^n$ $y_2 = G_n(x_2) \in \{0,1\}^n$

Now, know y is $2^n \cdot 2(n)$

For the Random Good - assume that y is not a $2^n \cdot 2(n)$

$\left(\underbrace{y_1}_{2^n} \| \underbrace{y_2}_{2^n} \| \ldots \| \underbrace{y_{2(n)}}_{2^n}\right)$

$\longrightarrow \underbrace{y_1 \| y_2 \| \ldots \| y_{2(n)}}_{m}$

$\longrightarrow \underbrace{\{y_i\}_{i=1}^{2(n)}}_{m}$

if y is not $2^n \cdot 2(n)$

$\exists$ an i $\exists$ y_i & a poly t

$\Pr\left(x \leftarrow \{0,1\}^n : y_i = G_n(x) : x' \leftarrow A(1^n, t) : x' = x\right) \geq \frac{1}{2n(n)}$

$\geq \frac{1}{\frac{t}{poly}}$

$\neq \frac{1}{poly}$

A', $x \leftarrow \{0,1\}^n$, $y = G_n(x)$:

$A'(y)$

Repeat $4n^2 \cdot 2(n) \cdot t(n)$ times as follows:

For $i = 1$ to $2n \cdot f(n)$

Randomly choose

$i_1, i_2, \ldots, i_{2n}$ $i_j \in [1, 2n]$

$y_j = y_{i_j}$

If A successfully finds

$\{y_1, y_2, y_3, \ldots, y_{2n}\}$

output

$\{y_1, y_2 - y_1, y_3 - y_2, \ldots, y_{2n} - y_{2n-1}\}$

return x' & exit.

A (end) $\longrightarrow$ (in bits)

$2n \cdot f(n)$ triple $y \in \{0,1\}^n$

$m = 2^n \cdot 2(n)$

$\Pr\left(A(y) \text{ finds } y_i \in \{0,1\}^n\right) \geq \frac{1}{poly(n)}$

$\Pr\left(A(y) \text{ finds } y_i \in \{0,1\}^n\right) \geq \frac{1}{poly(n)}$

$\left(\underbrace{y_1 \| y_2 \| \ldots \| y_{2(n)}}_{2^n}\right)$

$\underbrace{y \in \{0,1\}^n}$ is find y_i

$\Pr\left(\text{Single iteration } y_i \text{ not finding } \{y_i\}_{i=1}^{2(n)}\right)$

$\leq \frac{1}{4 \cdot p(n) \cdot t(n)}$

Let $\Pr\left(x \leftarrow \{0,1\}^n : x \text{ does not } \text{input } y = f(x)\right)$

$\Pr\left(x \leftarrow \{0,1\}^n : x \in GOOD\right)$

$+ \Pr\left(x \leftarrow \{0,1\}^n : x \notin GOOD\right)$

$\Pr\left(x \leftarrow \{0,1\}^n : x \notin GOOD\right)$

If $x \notin GOOD$ $x \in \{0,1\}^n$

$\Pr\left(\text{Single iteration } y_i \text{ not finding } \{y_i\}_{i=1}^{2(n)}\right) \leq \frac{1}{4 \cdot p(n) \cdot t(n)}$

$\Pr\left(\text{Single iteration } y_i \text{ not finding } \{y_i\}_{i=1}^{2(n)}\right) \leq 1 - \frac{1}{4 \cdot p(n) \cdot t(n)}$

$\Pr\left(x \in \{0,1\}^n, x \notin GOOD\right)$

$\leq \left(1 - \frac{1}{4 \cdot p(n) \cdot t(n)}\right)^{2 \cdot p(n) \cdot t(n)}$

$\leq e^{-n}$

$\left(1 - \frac{1}{n}\right)^n \leq e^{-1}$

$\left(1 - \frac{1}{n}\right)^{tn} \leq e^{-tn}$

Second term is $\leq e^{-n}$.

$= e^{-n}$

First term:

~~Probability of Good~~

$\Pr\left(x \leftarrow \{0,1\}^n : x \in GOOD\right) \geq 1$

$\cdot \Pr\left(x \in GOOD\right)$.

$\geq 3 \cdot \Pr\left(x \in GOOD\right) \geq \frac{1}{2 \cdot f(n)}$

$\Pr\left(x \in GOOD\right) \leq \frac{1}{2 \cdot f(n)}$

$\Pr\left(A \text{ does not input } y\right) \leq \underbrace{\frac{1}{2 \cdot f(n)}} + e^{-n}$

$< \frac{1}{2 \cdot f(n)} + \frac{1}{2 \cdot f(n)}$

$< \frac{1}{f(n)}$.

(That is a contradiction to f is hard.)

Thus, to complete the proof, we need to prove that $\Pr\left(x \in GOOD\right)$

Suppose $\Pr\left(x \in GOOD\right) > \frac{1}{2 \cdot f(n)}$

$\Pr\left(x \notin GOOD\right) \leq 1 - \frac{1}{2 \cdot f(n)}$

$\Pr\left(x_1 \notin GOOD\right) \leq \left(1 - \frac{1}{2 \cdot f(n)}\right)^{2n \cdot f(n)}$

$\forall \; i = 1, 2, \ldots, 2n \cdot f(n)$

$\leq e^{-n}$

Let $x \in \{0,1\}^n$ be the Random that a noncorrectly inverts $\underbrace{\exists}_{\exists} \; y \in \{0,1\}^n$.

(Recall that $\Pr\left(x \in GOOD\right) \geq \frac{1}{2 \cdot f(n)}$.)

$\Pr\left(x \in GOOD\right)$

$\Pr\left(\underbrace{A(1^n, 1^n)}_{x_1, x_2, \ldots, x_{2n \cdot f(n)}} \text{ not } x \in GOOD\right)$

$x_i \in \{0,1\}^n$

$= \Pr\left(\underbrace{A(1^n, 1^n)}_{x_1, x_2, \ldots, x_{2n \cdot f(n)}} \text{ not } x \in GOOD\right)$

$\cdot \Pr\left(\text{all bad } x_i \text{ } \forall \; x_1, \ldots, x_{2n \cdot f(n)}\right)$

$+ \Pr\left(\underbrace{A(1^n, 1^n)}_{x_1, x_2, \ldots, x_{2n \cdot f(n)}} \text{ not } x \in GOOD\right)$

$\Pr\left(\text{some } x_i \text{ } \forall \; x_1, \ldots, x_{2n \cdot f(n)}\right)$

$\Pr(x \in) = \Pr(x \in) \cdot \Pr(\text{all}) + \Pr(x \in) \cdot \Pr(\text{some})$

First part $\leq$ 1 (all bad $x_i \in GOOD$ $\forall \; x_1, \ldots, x_{2n \cdot f(n)}$)

$\leq \sum_{i=1}^{2n \cdot f(n)} \Pr\left(x_i \in GOOD\right)$.

$\leq \frac{2 \cdot n \cdot f(n)}{2 \cdot f(n)}$

$\leq \frac{1}{2 \cdot f(n)}$

Second term $\leq 1 \cdot e^{-n}$.

LHS $\leq \frac{1}{2 \cdot f(n)} + e^{-n}$

$< \frac{1}{2 \cdot f(n)} + \frac{1}{2 \cdot f(n)}$

$< \frac{1}{f(n)}$

Contradiction to f.

$X \geq \frac{1}{f(n)}$

$X \leq$ Term 1 + Term 2

$< \frac{1}{2 \cdot f(n)} + \frac{1}{2 \cdot f(n)}$

$= \frac{1}{f(n)}$

Contr.