Lecture 8.1: HW1 Discussion

Question 1

- Consider $f(x) = x_1 \dots x_m$, where $m \leqslant \log^c n$
- These functions are hard to invert because an adversary takes $n \geqslant 2^{m^{1/c}}$ time to write down the pre-image

Question 2

- $\nu(\cdot)$ is negligible if: $\forall$ polynomial $p(\cdot)$, $\exists n_0 \in \mathbb{N}$ such that $\forall\ n \geqslant n_0$ we have: $\nu(n) \leqslant 1/p(n)$
- $\nu(\cdot)$ is non-negligible if: $\exists$ polynomial $p(\cdot)$ such that $\forall n_0 \in \mathbb{N}$ there exists $n \geqslant n_0$ such that: $\nu(n) > 1/p(n)$
- "Eventually" operator: $\exists n_0 \in \mathbb{N}$ such that $\forall\ n \geqslant n_0$
- "Infinitely often" operator: $\forall n_0 \in \mathbb{N}$ there exists $n \geqslant n_0$
- Think: Contrapositive of statements in security proofs and the use of "non-negligible" functions

Question 3

- Since we do not know how to efficiently enumerate primes, we define $f(x, y) = x \cdot y$
- Use the fact that Π_n (the set of all primes with n-bit representations) is *dense* in $\{0,1\}^n$
- See: Theorem 33.5 in lecture notes by Pass-Shelat

Question 4

- Think: How two-repetition of a weak one-way function makes it harder to invert
- Intuition: To invert $g(x_1, \ldots, x_m) = f(x_1) \ldots f(x_m)$ we need to invert all
- See: Theorem 35.1 in lecture notes by Pass-Shelat

Question 5

- Levin's OWF
- If there exists a OWF then there exists a OWF with *small* running time
- Levin's OWF: $f^*(M, x)$ outputs the execution of $M(x)$ if it has small running time; otherwise 0

Question 6

- Setting:
  - How to prove: "Some Cryptographic Primitive" implies OWF?
  - We shall show the contrapositive: not-OWF implies not-"Some Cryptographic Primitive"
  - [Impagliazzo-Luby-89,Impagliazzo-Thesis-90] showed: not-OWF implies not-distributionally-OWF
  - Suffices: not-distributionally-OWF implies not-"Some Cryptographic Primitive"
- Uniform Generation Problem for NP [Jerrum-Valiant-Vazirani-86,Bellar-Goldreich-Petrank-00]: Uniformly reverse sample x such that $f(x) = y$
- not-distributionally-OWF: Uniformly reverse sample x such that $f(x) = y$, where $y = f(U_n)$ and the distortion is arbitrary "1/poly" small
- Former is "worst-case" while the latter is "average-case" notion