Computational Hardness & One-way Function

Worst-case one-way function

- A function $f : \{0,1\}^* \to \{0,1\}^*$ is worst-case one-way if:
    1. **Easy to compute.** There is a p.p.t (prob poly time) M such that $M(x) = f(x)$ on all x
    2. **Hard to Invert**. There is **no** p.p.t A such that for sufficiently large n, for all $x \in \{0,1\}^n$:

$$\Pr[y = f(x), x' \leftarrow A(1^n, y) : f(x') = y] = 1 \tag{1}$$

  Remark: According to 2, it is ok if only some special x is hard to invert.

  Remark: In fact, the existence of worst-case one-way function is equivalent to $NP \not\subseteq BPP$.

Strong One-way Function

- A function $f : \{0,1\}^* \to \{0,1\}^*$ is strong one-way if:
    1. **Easy to compute.** The same as above.
    2. **Hard to Invert**. For all p.p.t A, there is a negligible function ϵ s.t. for any input length n

$$\Pr[x \sim unif(\{0,1\}^n), y = f(x), x' = A(1^n, y) : f(x') = y)] \le \epsilon(n) \tag{2}$$

  Remark: Change negligible ϵ to $1 - \frac{1}{q(n)}$ for polynomial $q(n)$ gives **Weak** one-way function

Factoring as a one-way function

- Let $\Pi_n = \{p \text{ prime}, p < 2^n\}$
- $f_{mult} : \Pi_n \times \Pi_n \to \Pi_{2n}$, $f_{mult}(a, b) = ab$.
- Factoring Assumption: f_{mult} is a strong one-way function
- $|\Pi_n| = O(2^n/n)$