CS6222 Cryptography

Topic: One Way Function | Date: Sep 26, 2024
Lecturer: Wei-Kai Lin (TA: Arup Sarker) | Scriber: Kai Chen, Yucheng Fu

1 A Brief Recall

We first recall some important definition and theorem we mentioned in the last class.

Definition 1 (One way function). *For a function f, we call it one way function if it satisfies:*

1. *easy to compute: it can be calculated in a polynomial time;*
2. *hard to invert: for $\forall$ NUPPT A, $\exists$ a negligible $\epsilon(\cdot)$, such that*

$$\Pr_{x \leftarrow \{0,1\}^n} \left[A(1^n, y) \in f^{-1}(y) \mid y = f(x) \right] \leq \epsilon(n).$$

Theorem 1 (Chebychev). *There are two theorem for prime*

1. *Let $\pi(x)$ be the number primes that is less than x, then we have $\pi(x) \geq \frac{x}{2 \log x}$;*
2. $\Pr_{x \leftarrow \{0,1\}^n} [x \text{ is prime}] \geq \frac{1}{2n}$.

The first statement in theorem 1 is drawn from Chebychev theorem, and the second one can be directly obtained by the first statement.

2 Primes and Factoring Assumption

We first start from a obviously false assumption:

Assumption 1. *For $\forall p, q \in \Pi_n$, where $\Pi_n = \{prime < 2^n\}$, then there is no polynomial time algorithm A satisfies that $A(p, q) \in \{p, q\}$.*

This assumption is obviously false, because when p or q is very small, such as $2, 3, 5, \cdots$, the factoring is easy. Then we want to modify it into a more stringent version:

Assumption 2. *For $\forall p, q \in \Pi_n$, where $\Pi_n = \{2^{n-1} < prime < 2^n\}$, then there is no polynomial time algorithm A satisfies that $A(p, q) \in \{p, q\}$.*

Assumption 2 is a worst-case hardness, which means any input, even the worst input, is unable to be inverted. This is not what we want in the field of cryptography. This leads to a final version of assumption:

Assumption 3 (Factoring Assumption). *For $\forall p, q \in \Pi_n$, where $\Pi_n = \{prime < 2^n\}$, then for $\forall$ NUPPT A, $\exists$ a negligible $\epsilon(\cdot)$ such that*

$$\Pr_{p,q \leftarrow \Pi_n} [A(p, q) \in \{p, q\}] \leq \epsilon(n)$$

This kind of assumption is called average-case hardness, which means that under random input, it is averagely hard.

3 Mul Function

Let's start from the definition of *mul*.

Definition 2. *We define function mul as*

$$mul(x, y) = \begin{cases} 1, & \text{if } x = 1 \text{ or } y = 1 \\ xy, & \text{else} \end{cases}$$

First of all, we can easily prove that *mul* is not a OWF. Since when x is even (the probability of it is 1/2), $mul^{-1}(r) = \{2, r/2\}$. However, we want to introduce a weak version of OWF, and prove that *mul* is a weak OWF. The definition of weak OWF is given by

Definition 3 (Weak One Way Function)**.** *A function f is weak one way function if there exists a polynomial $q : \mathbb{N} \to \mathbb{N}$ such that for $\forall$ NUPPT adversary A, for sufficiently large $n \in \mathbb{N}$,*

$$\Pr_{x \leftarrow \{0,1\}^n} \left[A(1^n, y) \in f^{-1}(y) \mid y = f(x)\right] \leq 1 - \frac{1}{q(n)}.$$

Different from strong OWF, weak OWF only requires that there is a failure probability higher than $\frac{1}{q(n)}$, which therefore lead to the definition of "weak". Based on this definition, we will first give a proof that *mul* is weak OWF.

Theorem 2. *If assumption 3 is true, function mul is a weak OWF.*

Proof. Assume that for any polynomial q, there exists a NUPPT A contradicts the weak OWF. Then we define a adversary B to contradict the factoring assumption:

1. sample $x, y \leftarrow \{0,1\}^n$
2. if x, y are both prime, let $\bar{z} \leftarrow z$, else let $\bar{z} \leftarrow mul(x, y)$
3. Run A to get $\bar{x}, \bar{y} \leftarrow A(1^{2n}, \bar{z})$
4. return $\bar{x}, \bar{y}$ if x, y are both prime and $z = \bar{x}\bar{y}$

By theorem 1, we know that $\Pr[x, y \text{ are both primes}] = \frac{1}{4n^2}$. Then the probability that B fails to pass z to A (only when x, y are not prime neither) is at most $1 - \frac{1}{4n^2}$.

Furthermore, by our contradiction assumption, A fails to invert z with probability at most $\frac{1}{q(n)}$ for any poly q. We set $q(n) = 8n^2$. Therefore, the failure probability of B is

$$\begin{aligned} \Pr[B \text{ fails}] &= \Pr[B \text{ fails to transfer } z \text{ to } A, \text{ or } A \text{ fails}] \\ &\leq \Pr[B \text{ fails to transfer } z \text{ to } A] + \Pr[A \text{ fails}] \\ &= 1 - \frac{1}{4n^2} + \frac{1}{8n^2} = 1 - \frac{1}{8n^2} \end{aligned}$$

This contradicts the factoring assumption. Therefore *mul* is weak OWF.

Theorem 3. *Assuming $B'(M^*)$ repeat $B(M^*)$ for $r(n)$ times. If any output $\neq \perp$, output it. Then* $\Pr_{x,y \leftarrow \{0,1\}^n} [B'(1^n, M^*) = x, y \mid M^* = mul(x, y)] \leq \epsilon(n)$.

Proof Sketch. (1) *Good* prime set M^* is a large set. (2) Repeating working one *good* M^*.