CS 600.442 – Modern Cryptography Sep 14th

Lecture 2: One-way functions(Part II)

Instructor: Abhishek Jain *Scribe: Ke Wu*

1 Recall definitions from last lecture

Definition 1 *A function $f : \{0,1\}^* \to \{0,1\}^*$ is **one way function** if it satisfies:*

1. *$\exists$ a PPT algorithm $\mathcal{C}$ s.t. $\forall x \in \{0,1\}^*$, $Pr[\mathcal{C}(x) = f(x)] = 1$.*
2. *$\exists$ a negligible function $\mu : \mathbb{N} \to \mathbb{R}$ s.t. for every non-uniform PPT adversary $\mathcal{A}$ and $\forall n \in \mathbb{N}$: $Pr[x \xleftarrow{\$} \{0,1\}^n, x' \xleftarrow{\$} \mathcal{A}(1^n, f(x)) : f(x') = f(x)] \leq \mu(n)$.*

Definition 2 *A function $f : \{0,1\}^* \to \{0,1\}^*$ is a **weak one way function** if it satisfies:*

1. *$\exists$ a PPT algorithm $\mathcal{C}$ s.t. $\forall x \in \{0,1\}^*$, $Pr[\mathcal{C}(x) = f(x)] = 1$.*
2. *$\exists$ a noticeable function $\varepsilon : \mathbb{N} \to \mathbb{R}$ s.t. for every non-uniform PPT adversary $\mathcal{A}$ and $\forall n \in \mathbb{N}$: $Pr[x \xleftarrow{\$} \{0,1\}^n, x' \xleftarrow{\$} \mathcal{A}(1^n, f(x)) : f(x') \neq f(x)] \geq \varepsilon(n)$.*

2 $f_\times$ is a weak OWF

$f_\times : \mathbb{N}^2 \to \mathbb{N}$ is defined as:

$$f_\times = \begin{cases} \perp & if \quad x = 1 \vee y = 1 \\ x \cdot y & otherwise \end{cases}$$

Theorem 1 *$f_\times$ is a weak one way function.*

Proof.

Proof via definition: Let GOOD be the set of of input (x, y) that both x and y are prime. Then we have

$$\begin{aligned} &Pr[\mathcal{A} \text{ inverts } f_\times] \\ =&Pr[\mathcal{A} \text{ inverts } f_\times | (x,y) \in \mathsf{GOOD}] Pr[(x,y) \in \mathsf{GOOD}] \\ +&Pr[\mathcal{A} \text{ inverts } f_\times | (x,y) \notin \mathsf{GOOD}] Pr[(x,y) \notin \mathsf{GOOD}] \end{aligned}$$

Then according to the Factoring Assumption, when $(x, y) \in \mathsf{GOOD}$, $\mathcal{A}$ could invert $f_\times$ with a probability no more than a negligible function $\nu(n)$. Using Chebyshev' theorem, an n bit number is a prime number with probability $\frac{1}{2n}$, we can get

$$Pr[A] \leq \nu(n)\frac{1}{4n^2} + 1(1 - \frac{1}{4n^2}) = 1 - \frac{1}{4n^2}(1 - \nu(n))$$

Now we only need to prove that $\frac{1}{4n^2}(1 - \nu(n))$ is a noticeable function. Considering that $\forall c > 0, \nu(n) \leq \frac{1}{n^c}$, we can conclude that for $n \geq 2$, $1 - \nu(n) \geq \frac{1}{n}$. Thus $\frac{1}{4n^2}(1 - \nu(n)) \geq \frac{1}{4n^3}$ is noticeable. Hence $f_\times$ is a weak OWF.

Proof via reduction: Suppose that $f_\times$ is not a weak OWF, then we can construct an adversary breaking the factoring assumption. Assume that there exists a non-uniform PPT algorithm $\mathcal{A}$ inverting $f_\times$ with probability at leats $1-\frac{1}{8n^2}$. That is

$$Pr[(x,y) \xleftarrow{\$} \{0,1\}^n \times \{0,1\}^n, z = x \cdot y, \mathcal{A}(1^{2n}, z) \in f_\times^{-1}(z)] \geq 1 - \frac{1}{8n^2}$$

Now we construct a non-uniform adversary algorithm $\mathcal{B}$ on input z (which is a product of two random n-bit prime numbers) to break the factoring assumption. $\mathcal{B}$ runs as follows:

1. Pick (x,y) randomly from $\{0,1\}^n \times \{0,1\}^n$;
2. if x, y are both prime, let $z' = z$;
3. else, let $z' = xy$;
4. run $\omega = A(1^{2n}, z')$;
5. if x, y are both prime, return ω.

The reason of randomly choosing (x,y) instead of passing the input directly to $\mathcal{A}$ is that, the input of $\mathcal{B}$ is a product of two random n-bit primes while that of $\mathcal{A}$ is the product of two random n-bit numbers. Passing the input directly to $\mathcal{A}$ would destroy the uniformly distribution of the input $\mathcal{A}$ expect.

Now we calculate the probability that $\mathcal{B}$ fails to break factoring assumption. We use notation as below:

$$\begin{aligned}
&Pr[\mathcal{B} \text{ fails to break factoring assumption}]\\
=&Pr[\mathcal{B} \text{ pass input to } \mathcal{A}]Pr[\mathcal{A} \text{ fails to invert } f_\times] + Pr[\mathcal{B} \text{ fails to pass input to } \mathcal{A}]\\
\leq&Pr[\mathcal{A} \text{ fails to invert } f_\times] + Pr[\mathcal{B} \text{ fails to pass input to } \mathcal{A}]\\
\leq&\frac{1}{8n^2} + (1 - \frac{1}{4n^2}) + \leq 1 - \frac{1}{8n^2}
\end{aligned}$$

Thus $\mathcal{B}$ breaks factoring assumption with a noticeable probability. And we get contraction.

3 Weak to strong OWF

Theorem 2 *For any weak OWF $f : \{0,1\}^n \rightarrow \{0,1\}^n$, $\exists$ polynomial $N(\cdot)$ s.t. $F : \{0,1\}^{nN(n)} \rightarrow \{0,1\}^{nN(n)} : F(x_1, ..., x_N(n)) = (f(x_1), ..., f(x_N))$ is a strong OWF.*

Proof.

Since f is weak OWF, then let $q : \mathbb{N} \rightarrow \mathbb{N}$ be a polynomial function, and for every non-uniform $\mathcal{A}$

$$Pr[x \xleftarrow{\$} \{0,1\}^n, y = f(x), \mathcal{A}(1^n, y) \in f^{-1}(y)] \leq 1 - \frac{1}{q(n)}$$

We want to find a N s.t. $(1 - \frac{1}{q(n)})^N$ tends to be very small. Thus we pick $N = 2nq(n)$, and $(1 - \frac{1}{q(n)})^N \sim e^{-2n}$.

Suppose that F is not a strong OWF. Then $\exists$ polynomial function $p(\cdot)$ and a non-uniform $\mathcal{A}'$ s.t.

$$Pr[(x_1, ..., x_N) \xleftarrow{\$} \{0,1\}^{nN}, (y_1, ..., y_N) = F(x_1, ..., x_N), \mathcal{A}'(1^{nN}, (y_1, ..., y_N)) \in F^{-1}(y_1, ..., y_N)] \geq \frac{1}{p(nN)}$$

Now we construct a non-uniform PPT $\mathcal{B}$ to break f with probability more than $1 - \frac{1}{q(n)}$.

First we construct $\mathcal{B}_0$ on input $y = f(x)$ for random $x \in \{0,1\}^n$ as follows:

1. Randomly pick $i \in [1, N]$
2. For $j \neq i$, randomly pick $x_j \xleftarrow{\$} \{0,1\}^n$, let $y_j = f(x_j)$. Let $y_i = y$.
3. Let $(z_1, ..., z_N) = \mathcal{A}'(1^{nN}, (y_1, ..., y_N))$.
4. If $f(z_i) = y$, output Z_i; otherwise, output $\perp$

To improve the chance of inverting f, we define $\mathcal{B} : \{0,1\}^n \to \{0,1\}^n \cup \perp$ on input y to run $B_0(y)$ for $2nNp(nN)$ times independently (to choose x_j independently and randomly each time). $\mathcal{B}$ outputs the first non-$\perp$ it receives. Otherwise $\mathcal{B}$ returns $\perp$.

Let BAD be the set that $\mathcal{B}_0$ inverts f with a probability at least $\frac{1}{2Np(nN)}$ if $x \in \mathsf{BAD}$.

$$\mathsf{BAD} = \{x \in \{0,1\}^n | Pr[\mathcal{B}_0(1^n, f(x)) \in f^{-1}(f(x))] \geq \frac{1}{2Np(nN)}\}$$

Then the probability that $\mathcal{B}$ fails to invert f on BAD set is $(1 - \frac{1}{2Np(nN)})^{2nNp(nN)} \sim e^{-n}$, which is extremely small.

Now we prove that the fraction of BAD set is noticeable.

Lemma 3 $Pr[x \in \mathsf{BAD}] \geq 1 - \frac{1}{2q(n)}$.

Proof of [lemma 3]

If $Pr[x \in \mathsf{BAD}] < 1 - \frac{1}{2q(n)}$, then we can prove that $\mathcal{A}'$ is unable to break F with probability more than $\frac{1}{p(nN)}$. To prove this, we use the notations below:

E_1 is the event that $\mathcal{A}'$ successfully inverts F on input $(y_1, ..., y_N)$.

E_2 is the event that $\mathcal{B}_0$ successfully inverts f on input y. $\bar{E}_2$ is that $\mathcal{B}_0$ fails.

$$\begin{aligned} Pr[E_1 | x \in \mathsf{BAD}] &= Pr[E_1 | (E_2 \wedge x \in \mathsf{BAD})] Pr[E_2 \wedge x \in \mathsf{BAD}] + Pr[E_1 | \bar{E}_2 \wedge x \in \mathsf{BAD}] Pr[\bar{E}_2 \wedge x \in BAD] \\ &= Pr[E_1 | E_2 \wedge x \in \mathsf{BAD}] Pr[E_2 \wedge x \in \mathsf{BAD}] \leq Pr[E_2 \wedge x \in \mathsf{BAD}] \end{aligned}$$

Thus now we can compute the probability of $Pr[E_1]$.

$$
\begin{aligned}
Pr[E_1] &= Pr[E_1|x \in \mathsf{BAD}]Pr[x \in \mathsf{BAD}] + Pr[E_1|x \notin \mathsf{BAD}]Pr[x \in \mathsf{BAD}] \\
&= Pr[E_1|x_i \in \mathsf{BAD}, \forall i]Pr[x_i \in \mathsf{BAD}, \forall i] + Pr[E_1|\exists j, x_j \notin \mathsf{BAD}]Pr[\exists j, x_j \notin \mathsf{BAD}] \\
&\leq Pr[E_1|x_i \in \mathsf{BAD}, \forall i]Pr[x_i \in \mathsf{BAD}, \forall i] + \sum_j Pr[E_1|x_j \notin \mathsf{BAD}]Pr[\exists j, x_j \notin \mathsf{BAD}] \\
&\leq Pr[E_1|x_i \in \mathsf{BAD}, \forall i]Pr[x_i \in \mathsf{BAD}, \forall i] + NPr[E_2|x_j \in \mathsf{BAD}]Pr[\exists j, x_j \notin \mathsf{BAD}] \\
&\leq Pr[x_i \in \mathsf{BAD}, \forall i] + N\frac{1}{2Np(nN)} \\
&\leq (1 - \frac{1}{2q(n)})^{2nq(n)} + \frac{1}{2p(nN)} \\
&\leq e^{-n} + \frac{1}{2p(nN)} \\
&\leq \frac{1}{p(nN)}
\end{aligned}
$$

And this means that $\mathcal{A}'$ is unable to break F with probability more than $\frac{1}{p(nN)}$. And we get contradiction. ■

Now that we know $Pr[x \in \mathsf{BAD}] \geq 1 - \frac{1}{2q(n)}$, we can compute the probability that $\mathcal{B}$ fails to invert f. We denote this event as $\bar{E}_B$.

$$
\begin{aligned}
Pr[\bar{E}_B] &= Pr[\bar{E}_B|x \in \mathsf{BAD}]Pr[x \in \mathsf{BAD}] + Pr[\bar{E}_B|x \notin \mathsf{BAD}]Pr[x \notin \mathsf{BAD}] \\
&\leq e^{-n}Pr[x \in \mathsf{BAD}] + \Pr[x \notin \mathsf{BAD}] \\
&\leq (1 - \frac{1}{2q(n)}) + \frac{1}{2q(n)} \\
&\leq \frac{1}{q(n)}
\end{aligned}
$$

which is contradict with the condition that f is weak OWF. Thus F is a strong OWF.