CS276: Cryptography September 01, 2015

One-Way Functions II

Instructor: Alessandro Chiesa *Scribe: David Dinh*

Recall that a δ is defined as a *negligible* function if $\delta(k)^{-1}$ grows faster than any polynomial in k, and it is defined as *noticeable* if $\delta(k)^{-1}$ grows slower than some polynomial in k.

The sum of two negligible functions is also negligible. A negligible function subtracted to a noticeable or non-negligible function remains noticeable or non-neglible respectively.

Also recall that a one-way function is defined as follows: for all A (either uniform or nonuniform) adversaries in probabilistically polynomial time, $\delta_A(k) := \Pr[f_k(\hat{x}) = y | x \leftarrow \{0,1\}^{n(k)}, y \leftarrow f_k(x), \hat{x} \leftarrow A(1^k, y)]$ is negligible in k.

An α-weak one-way function is defined similarly, except instead of demanding that $\delta_A(k)$ be negligible, we require that $\delta_A(k) - \alpha(k)$ be negligible.

1 Fun with One-way Functions

Suppose we have a function $f_k : \{0,1\}^{n(k)} \to \{0,1\}^{m(k)}$, vectors $\vec{x} = (x_1, x_2, ...)$ for $x_k \in \{0,1\}^{n(k)}$ and $\vec{y} = (y_1, y_2, ...)$ for $y_k \in \{0,1\}^{m(k)}$. Let $g_k : \{0,1\}^{n(k)} \to \{0,1\}^{m(k)}$ be defined as y_k when $x = x_k$ and $f_k(x)$ otherwise.

Claim 1 *g is one-way if f is also one-way.*

Proof: Suppose for contradiction that g is not one-way but f is one-way, so there exists an A such that $\delta_A^{(g)}(k) := \Pr[g_k(\hat{x}) = y | x \leftarrow \{0,1\}^{n(k)}, y \leftarrow \{0,1\}^{m(k)}, \hat{x} \leftarrow A(1^k, y)]$ is non-negligible. Now suppose use that same adversary function on f. What's the probability that it works?

$$\begin{aligned}
\delta_A^{(f)}(k) &= \sum_{\hat{x}: f_k(\hat{x}) = y_k} \Pr[A \text{ inverts } g_k \text{on } \hat{x}] \Pr[x = \hat{x}] + \sum_{\hat{x}: g_k(\hat{x}) \neq y_k} \Pr[A \text{ inverts } g_k \text{on } \hat{x}] \Pr[x = \hat{x}] \\
&= \sum_{\hat{x}: f_k(\hat{x}) = y_k} \Pr[A \text{ inverts } g_k \text{on } \hat{x}] 2^{-n(k)} + \sum_{\hat{x}: g_k(\hat{x}) \neq y_k} \Pr[A \text{ inverts } g_k \text{on } \hat{x}] 2^{-n(k)} \\
&\leq \frac{\epsilon(k)}{2^{n(k)}} + \delta_A^{(f)}(k)
\end{aligned}$$

where we define $\epsilon_k = |\{x | g_k(x) = y_k\}| \geq 1$. Therefore, we have

$$\delta_A^{(f)}(k) \geq \delta_A^{(g)}(k) - \frac{\epsilon(k)}{2^{n(k)}}$$

We wish to show for contradiction that $\delta_A^{(f)}(k)$ is non negligible, so it suffices to show that $\frac{\epsilon(k)}{2^{n(k)}}$ is negligible. But remember that f is one-way, so there is some $\tilde{A}$ so that the probability that $\tilde{A}$ inverts f_k is $\epsilon(k)/2^n$ is negligible, as desired. □ If f is an one-way function, f^2 may not be. Here's an example: suppose we have $f = \{0,1\}^n \to \{0,1\}^n$, one-way. Define $g : \{0,1\}^{2n} \to \{0,1\}^{2n}$ so that $g(x_1, ..., x_{2n}\} = 0^n \| f(x_1, ..., x_n)$, and $h : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be defined as $h(x_1, ..., x_n) = 0^{2n}$ if $x_1, ..., x_n = 0^n$ and $g(x)$ otherwise. Since $h^2 = 0$, it's obviously not one-way.

2 Weak to Strong: Hardness Amplification

Also see Holenstein's lecture notes

Recall this theorem from last lecture:

Theorem 2 *Suppose f is a $(1-k^{-c})$-weak one-way function. Then there exists an one-way function g.*

Proof: Define the function $g : \{0,1\}^{rn} \to \{0,1\}^{rm}$ defined so that $g(\vec{x}) = (f(x_1), ..., f(x_r))$. It suffices to show that g is an OWF. Suppose for contradiction that it's not; that is, exists A such that $\delta_A^{(g)}(k)$ is non negligible. Now consider some adversary B targeted at f as follows:

$B_{(r,M)}(1^k, y)$ runs the following loop M times: set j to $[r]$, set $\vec{x}$ to $A(1^k, (f(x_1), ..., f(x_{j-1}), y, f(x_{j+1}), ..., f(x_r))$ where all the x_i's are chosen randomly from $\{0,1\}^n$, and if $f(x_j) = y$, output x.

Define $x \in \{0,1\}^n$ as *good* if Pr[1iteration succeeds for y=f(x)] $\geq d$ and S as the set of good Xs.

Then:

$$\begin{aligned}
\Pr[B\text{inverts } f(x)] &= \Pr[x \in S]\Pr[B\text{inverts } f(x)|x \in S] + \Pr[x \notin S]\Pr[B\text{inverts } f(x)|x \notin S] \\
&\geq \Pr[x \in S]\Pr[B\text{inverts } f(x)|x \in S] \\
&\geq \frac{|S|}{2^k}(1-(1-d)^M)
\end{aligned}$$

We want to get a bound on $|S|$. By assumption,

$$\begin{aligned}
\Pr[A\text{inverts } g] &= \Pr[\vec{y} = g(\vec{x}')|\vec{x} \leftarrow \{0,1\}^{rn}, \vec{y} \leftarrow g(\pi(\vec{x})), \vec{x}' \leftarrow A(1^*, \vec{y})] \\
&= \Pr[\text{above condition holds} \wedge \forall i : x_i \in S] + \Pr[\text{above condition holds} \wedge \exists i : x_i \notin S] \\
&\leq (\frac{|S|}{2^n})^r + \sum_{i=1}^{r} \Pr[\text{above condition holds} \wedge x_i \notin S] \\
&= (\frac{|S|}{2^n})^r + \sum_{i=1}^{r} \sum_{\hat{x} \notin S} \Pr[\text{above condition holds} \wedge x_i = \hat{x}]\Pr[x_i = \hat{x}] \\
&\leq (\frac{|S|}{2^n})^r + rd
\end{aligned}$$

Let's the probability that A inverts g be $\rho + \epsilon$ where ϵ is some error term. Now let $d = \epsilon/2r$ and $M = \frac{1}{d}\ln\frac{2}{d}$. Now $\rho + \epsilon \leq (|\delta|/2^n)^r + rd$ so $\rho + \epsilon/2 \leq (|S|/2^n)^r$ so $\frac{|S|}{2^n} \geq (\rho + \epsilon/2)^{1/r}$. Therefore:

$$
\begin{aligned}
\Pr[B \text{inverts } f(x)] &\geq \frac{|S|}{2^k}(1-(1-d)^M) \\
&\geq (\rho + \frac{\epsilon}{2})^{1/r}(1-e^{2dM}) \\
&= (\rho + \epsilon/2)^{1/4}(1-d/2) \\
&= (\rho + \epsilon/2)^{1/r}(1-\frac{\epsilon}{4r}) \\
&\geq \rho^{1/r}(1+\frac{\epsilon}{3r})(1-\frac{\epsilon}{4r}) \\
&= \rho^{1/r}(1+\frac{\epsilon}{24r})
\end{aligned}
$$

Now note that $r = k^{-(c+1)}$, and $\rho \approx k^{-d}$ so $\rho^{1/r} = (k^{-d})^{1/k^{c+1}} = e^{-\frac{d \ln k}{k^{c+1}}} \geq 1 - \frac{d \ln k}{k} = 1 - \frac{1}{k^c}\frac{d \ln k}{k} \geq 1 - \frac{1}{k^c}$. $\square$