Recall that a \( \delta \) 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-negligible respectively.

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

An \( \alpha \)-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 \( f_k : \{0,1\}^n \to \{0,1\}^m \), vectors \( \vec{x} = (x_1, x_2, \ldots) \) for \( x_k \in \{0,1\}^n \) and \( \vec{y} = (y_1, y_2, \ldots) \) for \( y_k \in \{0,1\}^m \). Let \( g_k : \{0,1\}^n \to \{0,1\}^m \) 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 \( \delta_{g}^{(f)}(k) := \Pr[g_k(\hat{x}) = y|x \leftarrow \{0,1\}^n, y \leftarrow \{0,1\}^m, \hat{x} \leftarrow A(1^k, y)] \) is non-negligible. Now suppose use that same adversary function on \( f \). What’s the probability that it works?

\[
\delta_{f}^{(f)}(k) = \sum_{\hat{x} : f_k(\hat{x}) = y_k} \Pr[A \text{ inverts } g_k \mid x = \hat{x}] \Pr[x = \hat{x}] + \sum_{\hat{x} : f_k(\hat{x}) \neq y_k} \Pr[A \text{ inverts } g_k \mid \hat{x}] \Pr[\hat{x} = \hat{x}]
\]

\[
= \sum_{\hat{x} : f_k(\hat{x}) = y_k} \Pr[A \text{ inverts } g_k \mid \hat{x}] 2^{-n(k)} + \sum_{\hat{x} : f_k(\hat{x}) \neq y_k} \Pr[A \text{ inverts } g_k \mid \hat{x}] 2^{-n(k)}
\]

\[
\leq \frac{\epsilon(k)}{2^{n(k)}} + \delta_{A}(f)(k)
\]

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

\[
\delta_{f}^{(f)}(k) \geq \delta_{A}(g)^{(f)}(k) - \frac{\epsilon(k)}{2^{n(k)}}
\]

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 \( A \) so that the probability that \( A \) inverts \( f_k \) is \( \epsilon(k)/2^n \) is negligible, as desired. \( \square \) 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 \( g(x_1, ..., x_{2n}) = 0^n \iff f(x_1, ..., x_n) \) 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.

\[ \text{2 Weak to Strong: Hardness Amplification} \]

Also see Holenstein’s lecture notes

Recall this theorem from last lecture:

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

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

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

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

Then:

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

We want to get a bound on \( |S| \). By assumption,

\[ \Pr[\text{inverts } g] = \Pr[\bar{y} = g(\bar{x})]|\bar{x} \leftarrow \{0, 1\}^{rn}, \bar{y} \leftarrow g(\pi(\bar{x})), \bar{x} \leftarrow A(1^*, \bar{y})] = \Pr[\text{above condition holds } \land x_i \in S] + \Pr[\text{above condition holds } \land x_i \notin S] \leq (\frac{|S|}{2^n})^r + \sum_{i=1}^{r} \Pr[\text{above condition holds } \land x_i \notin S] = (\frac{|S|}{2^n})^r + \sum_{i=1}^{r} \sum_{\bar{x} \notin S} \Pr[\text{above condition holds } \land x_i = \hat{x}] \Pr[x_i = \hat{x}] \leq (\frac{|S|}{2^n})^r + rd \]

Let’s the probability that \( A \) inverts \( g \) be \( \rho + \epsilon \) where \( \epsilon \) 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:
\[ \Pr[\text{Binverts } f(x)] \geq \frac{|S|}{2^e} (1 - (1 - d)^M) \]
\[ \geq (\rho + \frac{\epsilon}{2})^{1/r} (1 - e^{2dM}) \]
\[ = (\rho + \epsilon/2)^{1/4}(1 - d/2) \]
\[ = (\rho + \epsilon/2)^{1/r}(1 - \frac{\epsilon}{4r}) \]
\[ \geq \rho^{1/r}(1 + \frac{\epsilon}{3r})(1 - \frac{\epsilon}{4r}) \]
\[ = \rho^{1/r}(1 + \frac{\epsilon}{24r}) \]

Now note that \( r = k^{-(c+1)} \), and \( \rho \approx k^{-d} \) so \( \rho^{1/r} = (k^{-d})^{1/k^{c+1}} = e^{-\frac{\ln k}{k^{c+1}}} \geq 1 - \frac{\ln k}{k} = 1 - \frac{1}{k^{c}} \frac{\ln k}{k} \geq \frac{1}{k^{2c}} \).