One-way Functions

Debdeep Mukhopadhyay
IIT Kharagpur

Strong One-way

- Informally,
  - easy to compute
  - f can be inverted only with a negligible probability on a random input

    or, it is hard to invert on all but a negligible fraction of inputs

Strong One-way

A function $f:\{0,1\}^n \rightarrow \{0,1\}^n$ is (t,ε)-one way if
f is computable in poly(n) time and for all adversaries
A running in time bounded by t(n):
$\Pr_{x\in\{0,1\}^n}[A(f(x)) \in f^{-1}(f(x))] \leq \varepsilon(n)$

Consider $f_{mult}(M,N)=M*N$

- Consider the problem of finding non-trivial factors.
- The problem is easy when one of the inputs is even.
  - probability of the event=3/4 and is hence non-negligible.
  - thus there is a non-negligible fraction of the inputs for which f(x) is easy to invert.
  - these functions are not captured by our rather restrictive definition.

Weak One-way functions

- Informally,
  - easy to compute
  - *slightly* hard to invert for random inputs
  - f is easy to invert on some non-negligible fraction of the inputs.
  - Thus f_{mult} is weak one-way function.

Weak One way functions

A function $f:\{0,1\}^n \rightarrow \{0,1\}^n$ is weak one-way if f is computable in poly(n) time and for all adversaries A running in time bounded by t(n):

$$\Pr_{x\in\{0,1\}^n}[A(f(x)) \in f^{-1}(f(x))] < 1 - \frac{1}{q(n)}$$

Hardness Amplification

- How to build a strong one-way function from a weak one-way function?

Hardware Amplification

Let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a weak OWF. Then there exists a polynomial $m = t(n)$, such that for input length n, the following function:

$$g(x_1, x_2, ..., x_m) = f(x_1) f(x_2) ... f(x_m)$$

is a strong OWF.

The first step

Suppose there is a PPT algorithm A:

$\Pr_{x\in\{0,1\}^{mn}}[A(g(x)) \in g^{-1}(g(x))] > \frac{1}{p'(mn)}$

$or, \Pr[x_i \leftarrow \{0,1\}^n; A(g(x_1...x_m)) \in g^{-1}(g(x_1...x_m))] > \frac{1}{p(n)}$

Thus A takes $y_1...y_m$ as input and outputs $z_1...z_m$,

such that $f(z_i) = y_i$ for all i with probability $> \frac{1}{p(n)}$

Goal : To construct A' that uses A to invert f with

probability $\geq 1 - \frac{1}{q(n)}$ (that is violate the weak one-wayness

of f)

Adversary A'

A' repeats the following procedure $2nmp(n)$ times:

Procedure I

For i=1 to m

let $y_i = y$

for all $j \neq i$, pick $x_j = \{0,1\}^n$ and let $y_j = f(x_j)$

let $z_1...z_m = A(y_1...y_m)$

if $f(z_i) = y$, output z_i

else output fail

Define: $Good = \{x : \Pr[I(f(x) \in f^{-1}(f(x))] \geq \frac{1}{2mp(n)}$

other x is *Bad*

$Claim : \Pr[x_i \text{ is } Good] \geq 1 - \frac{1}{2q(n)}$

How do we prove? Contradict the claim…

Proof of the Claim

$\Pr[A(g(x_1 \ldots x_m) \text{ succeeds}] =$

$\Pr[A(g(x_1 \ldots x_m) \text{ succeeds} \wedge \exists \text{Bad } x_i] +$

$\Pr[A(g(x_1 \ldots x_m) \text{ succeeds} \wedge \forall i, x_i \text{ is Good}]$

$\Pr[A(g(x_1 \ldots x_m) \text{ succeeds} \wedge \exists \text{Bad } x_i]$

$\leq \sum_i \Pr[A(g(x_1 \ldots x_m) \text{ succeeds} \wedge \text{Bad } x_i]$

$\leq \sum_i \sum_{x \in Bad} \Pr[A(g(x_1 \ldots x_m) \text{ succeeds} \wedge x_i = x]$

$= \sum_i \sum_{x \in Bad} \Pr(x_i = x) \Pr[A(g(x_1 \ldots x_m) \text{ succeeds} \mid x_i = x]$

$\leq \sum_i \Pr_{\max}[A(g(x_1 \ldots x_m) \text{ succeeds when } x_i \text{ is Bad}]$

$\leq \sum_i \Pr_{\max}[\text{I succeeds in inverting } f(x_i) \text{ when } x_i \text{ is Bad}]$

$\leq m \frac{1}{2mp(n)} = \frac{1}{2p(n)}$

the second half…

$\Pr[A(g(x_1 \ldots x_m) \text{ succeeds} \wedge \forall i, x_i \text{ is Good}]$

$\leq \Pr[\forall i, x_i \text{ is Good}]$

$\leq (1-\frac{1}{2q(n)})^m$ [if we contradict the claim]

$=(1-\frac{1}{2q(n)})^{2nq(n)}$ [setting m=2nq(n)]

$\approx \frac{1}{e^n}$

$\therefore \Pr[A(g(x_1 \ldots x_m) \text{ succeeds}] \leq \frac{1}{2p(n)} + \frac{1}{e^n}$

This contradicts the fact that A is successful against g.

$\therefore \Pr[x_i \text{ is Good}] \geq 1-\frac{1}{2q(n)}$

and, $\Pr[x_i \text{ is Bad}] \leq \frac{1}{2q(n)}$

The final part

$\Pr[A'(f(x) \text{ fails}]$

$=\Pr[A'(f(x) \text{ fails}|x \text{ is Good}]\Pr[x \text{ is Good}]$

$+\Pr[A'(f(x) \text{ fails}|x \text{ is Bad}]\Pr[x \text{ is Bad}]$

$\leq \Pr[A'(f(x) \text{ fails}|x \text{ is Good}]+\Pr[x \text{ is Bad}]$

We know, $\Pr[x \text{ is Bad}] \leq \frac{1}{2q(n)}$

$\Pr[A'(f(x) \text{ fails}|x \text{ is Good}] \leq (1-\frac{1}{2mp(n)})^{2nmp(n)} \approx \frac{1}{e^n}$

$\Pr[A'(f(x) \text{ fails}] \leq \frac{1}{e^n} + \frac{1}{2q(n)} = \frac{1}{2q'(n)}$

$\therefore \Pr[A'(f(x) \text{ succeeds}] \geq 1-\frac{1}{2q'(n)}.$

This contradicts the weak one-wayness of $f(x)$.