Introduction to Cryptography 1/25/18

Lecture 4: One Way Functions - II

Instructor: Vipul Goyal *Scribe: Rupal Nahar*

1 Terminology + Recap

Terminology:

1. $\xleftarrow{\$}$: sampling at random from some input space
2. **negl(n)**: notation for a negligible function (definition from last lecture) - very small
   Formally: A function ν is negligible if $\forall c \in \mathbb{N}, \exists n_0 \in \mathbb{N}$ such that $\forall n > n_0, \nu(n) \leq \frac{1}{n^c}$
3. **poly(n)**: notation for a function polynomial in n
4. **noticeable(n)**: $\frac{1}{poly(n)}$: not so close to 0.
   Formally: A function f is noticeable if $\exists$ c $\in \mathbb{R}$ and $N_c \in \mathbb{N}$ s.t. $\forall$ n $> N_c$. $f(n) \geq \frac{1}{n^c}$

Last class we saw the definition and motivation behind one-way functions. Today we will see how to construct one.
Two important definitions from last class:

1. **Strong one-way function**: A function f: $\{0,1\}^n \rightarrow \{0,1\}^m$ is called a strong one way function if it satisfies the following two conditions:
   - Easy to compute: $\exists$ PPT C, $\forall x$ s.t. Pr[C(x) = f(x)] = 1
   - Hard to Invert: $\forall$ non-uniform PPT adversaries A,
     Pr[x $\xleftarrow{\$}$ $\{0,1\}^n$, A(f(x)) = x' : f(x') = f(x)] $\leq$ negl(n)
2. **Weak One- Way Function**: A function f: $\{0,1\}^n \rightarrow \{0,1\}^m$ is called a weak one way function if it satisfies the following two conditions:
   - Easy to compute: $\exists$ PPT C, $\forall x$ s.t. Pr[C(x) = f(x)] = 1
   - Somewhat hard to invert: $\forall$ non-uniform PPT adversaries A,
     Pr[x $\xleftarrow{\$}$ $\{0,1\}^n$, A(f(x)) = x' : f(x') $\neq$ f(x)] $\geq$ noticeable(n)

2 Factoring

In this class we will construct one-way functions from factoring.

Definition 1 ***Factoring Assumption*** *- $\forall$ non-uniform PPT A, $\exists$ negl function $\mu(n)$ such that: Pr[$p_1 \xleftarrow{\$} \Pi_n$, $p_2 \xleftarrow{\$} \Pi_n$, $N=p_1 \cdot p_2$: A(N) = (p_1, p_2)] $\leq \mu(n)$*

Π_n = space of all n bit primes = all primes less than 2^n

So in words this is saying when the adversary is given input N, the probability of them outputting p_1 and p_2 is less than this negligible function applied on n.

3 Constructing One-Way Functions

Attempt 1: f: $\{0,1\}^{2n} \to \{0,1\}^{2n}$

$$f(x_1, x_2) = x_1 \cdot x_2 \text{ where } x_1 \text{ and } x_2 \text{ are both n-bits each}$$

Is this a one-way function?
No!

$$Pr[\text{one of them is even}] = \frac{3}{4}$$

This is a high probability and in this case, an adversary can output 2 factors one of which is 2, or in all cases always try dividing output by small numbers until finding 2 factors and with some noticeable probability adversary will succeed.

Remark 1 *The factoring assumption says only if we have a product of 2 prime numbers is it hard to factor. In this case we are just taking the product of 2 random numbers so it may not necessarily be hard to factor N.*

Could this be a weak one-way function?
Yes! Because with some (small) probability x_1 and x_2 could happen to be prime. In this case, because of the factoring assumption, the adversary is likely to fail. The probability of the adversary failing is roughly the same as the probability that x_1 and x_2 happen to be prime.

4 Example of a Reduction Based Security Proof

Note in proving the theorem 2 below we will need the following Chebystev's Theorem:

Theorem 1 *Chebystev Theorem: Probability of a random n-bit number being prime* $\geq \frac{1}{2n}$.

Theorem 2 *f (defined above as* $f(x_1, x_2) = x_1 \cdot x_2$*) is a weak OWF.*

What makes this a reduction based security proof? We have constructed a scheme, we have a complexity assumption which is the factoring assumption, and we will try to say that if one could break the security of this scheme, they could break the factoring assumption.

Proof. Assume for sake of contraction f is not weak.
So we have some adversary A such that A is successful in inverting OWF f with probability at least 1- negl(n) (so A succeeds almost all the time).

For simplicity we will use P[A succeeds] to mean P[$x \leftarrow \{0,1\}^n$, $x' \leftarrow$A($f(x)$) : $f(x') = f(x)$]

$$\begin{aligned} Pr[\text{A succeeds}] = &(Pr[\text{A succeeds}|x_1, x_2 \text{ primes}] \cdot Pr[x_1, x_2 \text{ primes}])+ \\ &(Pr[\text{A succeeds}|\text{at least one of } x_1, x_2 \text{ not prime}]\cdot \\ &Pr[\text{at least one of } x_1, x_2 \text{ not prime}]) \end{aligned}$$

By Chebystev's theorem we know

$$Pr(x_1 \text{ prime}) = Pr(x_2 \text{ prime}) \geq \frac{1}{2n}$$

Furthermore, $Pr(x_1, x_2 \text{ prime}) \geq \frac{1}{4n^2}$, let's call this probability p

$$\begin{aligned} Pr[\text{A succeeds}] &\leq Pr[\text{A succeeds}|x_1, x_2 \text{ prime}]\Big(\frac{1}{p^2}\Big) + (1)\Big(1 - \frac{1}{p^2}\Big) \\ 1 - negl(n) &\leq Pr[\text{A succeeds}|x_1, x_2 \text{ prime}]\Big(\frac{1}{p^2}\Big) + \Big(1 - \frac{1}{p^2}\Big) \\ Pr[\text{A succeeds}|x_1, x_2 \text{ prime}] &\geq p^2\Big(\frac{1}{p^2} - negl(n)\Big) \\ &\geq 1 - negl(n) \cdot p^2 \\ &\geq 1 - negl(n) \end{aligned}$$

Remark 2 *The product of a negligible function and a polynomial is still a negligible function.*

The fact that Pr[A succeeds | x_1, x_2 prime] $\geq$ 1 - negl(n) is a direct contradiction to the factoring assumption. □

5 Yao's Hardness Amplification

Can we turn any weak one way function into a strong one way function?
Yes!

Theorem 3 *Yao's Hardness Amplification - Strong OWF exist iff weak OWF exist*

Given weak OWF f, strong OWF F is constructed as follows:

$$F(x_1, x_2, \ldots x_{n'}) = f(x_1) \,||\, f(x_2) \,||\, \ldots \,||\, f(x_{n'}) \text{ where n' } = \tfrac{n}{p_1}$$

where noticeable(n) $\leq p_1 = \Pr[x \xleftarrow{\$} \{0,1\}^n, A(f(x)) = x' : f(x') \neq f(x)]$
So F takes in a large input, the concatenation of x_1 through $x_{n'}$, and interprets the input as n' different strings each of length n.

Intuition:
The intuition here is that likely, inverting at least one of these outputs will be hard.
For the adversary to succeed in inverting the whole concatenated output, they have to invert each $f(x_1)$, $f(x_2)$, ... etc. so if we hit even at least one hard factoring instance (e.g. 2 large primes), then the function will be strong.

We will now go into more intuition for how the proof will go.
First we will assume for sake of contradiction, F is not strong.
$\implies \exists$ adversary which breaks F with probability $\geq p_2$ (where p_2 is some noticeable quantity).
We now construct an adversary B such that:

$$\Pr[\text{B inverts f}] > p_1.$$

Weak one-way functions guarantee that adversary fails to invert with probability at least p_1.
We aim to construct an adversary who succeeds with this probability (p_1) because that would mean our function was not a weak one way function to start with which would be a contradiction.
Adversary B takes as input N where N = $p_1 \cdot p_2$ (product of 2 primes).
A takes as input:"...,N,...."

$$\text{B(N), A(...,N,....)}$$

We then set:

$$\text{f}(x_i) = \text{N}$$

and sample rest of f(x_1) through f(x_n) at random and then compute.
With probability p_2, this adversary would succeed.
This is not good enough though, note:

$$(1\text{-}p_1) \text{ could be } >> p_2$$

From the original definition p_1 was the probability that adversary doesn't succeed.
So the adversary gets some input, let's call it y, and it's goal is to output inversion of y.
Adversary B runs the adversary A.
A puts 'y' in a random place and for every other place pick x_1, x_2, .. etc at random and put in f(x_1)... f($x_{n'}$).
So we have

$$\text{B(y) and A(f}(x_1), \text{ f}(x_2), .., \text{ y, ..., f}(x_{n'}).$$

For the adversary:

$$\Pr[\text{B inverts y}] \geq p_2.$$

Repeat A k times, then see if B succeeds or not.

$$\Pr(\text{B fails}) = \Pr(\text{A fails in all executions})$$

Since there are k executions,

$$\Pr(\text{A fails in all executions}) \leq (1 - p_2)^k = \text{negl}(\cdot)$$

as we increase k
So seems like we have constructed an adversary which is almost always successful in inverting.

More formally:
Proof. (Description of B remains the same)
B(y) works as follows: (where y = f(x))

- Phase 1
  - Choose random i, set y_i = y
  - $\forall$ j $\neq$ i, set y_j = f(x_j), $x_j \xleftarrow{\$} \{0,1\}^n$
  - Run A(y_1, y_2, ..., y_i, ..., $y_{n'}$)

- Phase 2
  - Get output x_1, .., x_i, ..., $x_{n'}$
  - output x_i

If A was successful then B is done.
If A was unsuccessful (meaning f(x_i) $\neq$ y), repeat phase 1 with fresh randomness $\frac{n^2 \cdot p_1}{p_2}$ times.

Definition 2 *BAD* $= \{x|$ $Pr_{coins\ of\ B}$*[B inverts f(x) in a single iteration]* $< \frac{p_1 \cdot p_2}{2n}\}$

Lemma 4 *Fraction of BAD inputs, x, is at most* $\frac{p_1}{2}$*. In other words,* $Pr[x \in BAD] \leq \frac{p_1}{2}$

This will be useful in the proof of lemma 4:

Remark 3 *Union Bound (suppose the events have the same probability):*

$$Pr(A_1 \cup A_2 \cup ... \cup A_m) \leq P(A_1) + ... + P(A_m) = mP(A_i)$$

For the sake of convenience, we define $Pr((x_1, ..., x_{n'}) \leftarrow \{0,1\}^{nn'}, (x'_1, ..., x'_{n'}) \leftarrow A(F(x_1, ..., x_{n'})) : F(x'_1, ..., x'_{n'}) = F(x_1, ..., x_{n'})) = Pr$(A succeeds) and Pr(A fails) $= 1 - Pr$(A succeeds). Similarly, $Pr(x \leftarrow \{0,1\}^n, x' \leftarrow B(f(x)) : f(x) = f(x')) = Pr$(B succeeds) and Pr(B fails) $= 1 - Pr$(B succees)
Proof of Lemma 4: Assume for sake of contradiction this lemma is not true:

$$\begin{aligned}
Pr[\text{A succeeding in inverting } (x_1, x_2, ..., x_{n'})] =& Pr[\text{A succ...}|\forall i, x_i \notin BAD] \cdot Pr[\forall i, x_i \notin BAD] + \\
& Pr[\text{A succ...}|\text{for some } i, x_i \in BAD] \cdot Pr[\exists i, x_i \in BAD] \\
p_2 \leq& 1 \cdot \left(1 - \frac{p_1}{2}\right)^{n'} + \Bigg(n' \cdot Pr[\text{A succ...}|\text{for specific } i, x_i \in BAD] \\
& \cdot Pr[\exists i, x_i \in BAD]\Bigg) \text{ by union bound} \\
p_2 \leq& 1 \cdot \left(1 - \frac{p_1}{2}\right)^{n'} + \frac{n}{p_1} \cdot \frac{p_1 \cdot p_2}{2n} \cdot 1 \\
p_2 \leq& 1 \cdot negl(n) + \frac{p_2}{2} \\
\frac{p_2}{2} \leq& negl(n)
\end{aligned}$$

This is a contradiction to the fact that there exists an adversary which can break it with noticeable probability. □

Remark 4 $(1 - \frac{p_1}{2})^{n'}$ *is negligible because this will converge to* e^{-cn} *and that is a negligible function.*

Now looking at failure probability of main adversary B that runs A $\frac{n^2 \cdot p_1}{p_2}$ times:

$$\begin{aligned}
Pr[\text{B fails to invert f(x)}] =& Pr[x \in BAD] \cdot Pr[\text{B fails to invert} | x \in BAD] + \\
& Pr[x \notin BAD] \cdot Pr[\text{B fails to invert} | x \notin BAD] \\
\leq & \frac{p_1}{2} \cdot 1 + 1 \cdot (Pr[\text{A fails to invert f(x)} | x \notin BAD])^k \\
\leq & \frac{p_1}{2} + (1 - \frac{p1 \cdot p2}{2n})^{\frac{n^2 \cdot p_1}{p_2}} \\
\leq & \frac{p_1}{2} + e^{-cn} \text{ for all large enough n}
\end{aligned}$$

This means f is not weak and that is a contradiction to our assumption.
Therefore, we conclude that F is a One Way Function. □