CSE 594 : Modern Cryptography 05/02/2017

Lecture 4: One Way Functions - II

Instructor: Omkant Pandey *Scribe: Bharathkrishna G Murali, Swarnima Shrivastava*

1 Weak to Strong OWFs

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

Proof. Let $GOOD$ be the set of inputs (x, y) to $f_\times$ such that both x and y are prime numbers. When $(x, y) \in GOOD$, the adversary cannot invert the multiplication function $f_\times(x, y)$ because of hardness of factoring.

Suppose adversary inverts with probability 1 when $(x, y) \notin GOOD$. But if $Pr[(x, y) \in GOOD]$ is noticeable, then overall, the adversary can only invert with a bounded noticeable probability.
Let us consider a certain input of length $2n$. By Chebyshev's theorem, a random input pair (x,y) will be two primes with a probability $1/4n^2$, and in this case, the function should be hard to invert except with negligible probability.
Let $q(n) = 8n^2$. We need to prove that no non-uniform PPT adversary can invert $f_\times$ with a probability greater than $1 - 1/q(n)$.

Goal: Given an adversary A that breaks weak one-wayness of $f_\times$ with probability of at least $1 - 1/q(n)$, we will construct an adversary B that breaks the factoring assumption with a non-negligible probability.

Algorithm 1 Adversary B(z): Breaking the factoring assumption

1: Sample $x, y \leftarrow \{0, 1\}^n$
2: **if** x and y are both prime **then**
3: $z' \leftarrow z$
4: **else**
5: $z' \leftarrow xy$
6: **end if**
7: $w \leftarrow A(1^n, z')$
8: Output W if x and y are both prime.

1.1 Analysis of B

Since the primality testing can be done in polynomial time, and since A is a non-uniform PPT, B is also a non-uniform PPT. Suppose we now feed A the product of a pair of random n-bit primes, z. A fails to invert with a probability of at most $1/q(n) = 1/8n^2$.

By Chebychev's Theorem, B fails to pass z to A with probability of at most $1 - 1/4n^2$. So we have 2 cases where B fails:
1. it does not hit the GOOD set, the probability for this is at most $1 - 1/4n^2$.
2. A fails to invert, even if B hits the GOOD set. The probability for this is at most $1/8n^2$.

Using the union bound, we conclude that

$$\boxed{B \text{ fails with probability at most } (1 - 1/4n^2) + (1/8n^2) \leq (1 - 1/8n^2)} \quad (1)$$

This means that B succeeds with probability of at least $1/8n^2$. In other words, there does not exist a negligible function that bounds the success probability of B, which contradicts the factoring assumption.

2 Hardness amplification: Equivalence of weak and strong OWFs

Hardness Amplification means to convert a somewhat hard problem into a really hard problem. Here, this is done by running the weak-one way function f on enough random inputs such that it produces a list of elements which contains at least one item which is hard to invert. It provides an efficient way to transform any weak one-way function to a strong one. Hardness amplification shows that the existence of weak one-way functions is equivalent to the existence of strong one-way functions.

Every weak function has a core set of hard inputs where every adversary fails. The intuition of hardness amplification is to use the Weak OWF many times so that it becomes a strong OWF.

Q: Is f(f(....f(x))) a good idea ?
It will not be good if f is not injective. Also, the function could end up in the actual input. Hence, f could behave strangely on special inputs.

Let us assume GOOD to be the set of inputs hard to invert and BAD to be the set of inputs easy to invert. An OWF is weak when the fraction of BAD inputs is noticeable. An OWF is strong when the fraction of BAD inputs is negligible. To convert weak OWF to strong, we can use the weak OWF on many (say N) inputs independently.

In this case, to successfully invert the new OWF, adversary must invert ALL the N outputs of the weak OWF. If N is sufficiently large and the inputs are chosen independently at random, we will hit one of the 'hard to invert' inputs with a high probability. This implies that the probability of inverting all of them will be very small.

Theorem 2 (Yao) *For any weak one-way function $f : \{0,1\}^n \to \{0,1\}^n$, there exists a polynomial N(.) such that the function $F : \{0,1\}^{(n.N(n))} \to \{0,1\}^{(n.N(n))}$ defined as*

$$F(x1, ..., x_N(n)) = (f(x1), ..., f(x_N(n))) \text{ is a strong one-way function.}$$

Proof. Since f is weakly one-way, there exists a polynomial $q(.)$ such that every efficient A fails to invert f with at least $1/q(n)$ probability.

$$\boxed{\Pr_x[\ A fails\ on\ f(x)\ ]\ \geq\ 1/q(n)]} \quad (2)$$

Let $\Pr_x[\ A fails\ on\ f(x)\ ]$ be denoted as $\alpha := \alpha(n)$
Let $q(n)$ be denoted as $q := q(n)$

Hence, the above equation (2) becomes :

$$\boxed{\alpha \geq 1/q} \tag{3}$$

The main idea is that large N should almost always hit a "hard to invert x".
Choose N such that $(1 - \alpha^N) = (1 - 1/q)^N$ is small.

Let N = 2nq

This gives :

$$\boxed{(1 - 1/q)^{2nq} \approx e^{-2n}} \tag{4}$$

Now let us assume by contradiction that F is not a strong OWF.
For an efficient adversary B and a polynomial p(.) such that

$$\boxed{\Pr_{x_1,....x_N}[B \; inverts \; F(x_1, ...x_N)] \; \geq \; 1/p(n.N)} \tag{5}$$

Let $pr(x_1, ...x_N)$ $[B \; inverts \; F(x_1, ...x_N)]$ be denoted as $\beta := \beta(n.N)$.
Let $p(n.N)$ be denoted as $p := p(n.N)$.
Hence, the equation (5) above becomes :

$$\boxed{\beta \; \geq \; 1/p} \tag{6}$$

In order to contradict that f is a weak one-way function, we build an adversary A_0 using B to break f with probability

$$\boxed{\alpha < 1/q} \tag{7}$$

We should keep in mind that α is a function of n and β is a function of (n.N). We are just not writing this in the equations for mathematical convenience of representation.
Let such an adversary A_0 be as follows:

Algorithm 2 Adversary $A_0(y)$:

1: Choose $i \xleftarrow{\$} [N]$ and set $y_i = y$
2: $\forall j \neq i$, sample $x_j \in \{0,1\}^N$ and set $y_j = f(x_j)$
3: Let $(z_1, ...z_N) \leftarrow B(y_1, ..., y_n)$
4: If $f(z_i) = y$, output z_i, else output $\perp$

Q: Is feeding $(y, y....y)$ to B in above algorithm a good idea ?
Since input is not random in nature so it is not good enough to give $\alpha < 1/q$.
Q: Is it a good idea to feed B with $(y, y_2, y_3....y_N)$ where y is fixed but every other $y_i = f(x_i)$ for a random x_i?
This introduces randomness to the input but y is still fixed. To further improve, feed y in a random

location i to balance out probabilities.
Q: Can we do better?
The idea here is to run A_0 many times to improve chances of inverting y!
For this purpose, say we have main adversary A that runs A_0 multiple times to invert y as below:

Algorithm 3 Main Adversary A:

1: Run $A_0(y)$ for $T := T(n)$ times $= 4n^2 * q(n) * p(n.N)$
2: Output the first non-$\perp$ answer

2.1 Analysis of A_0

Q: Why isn't A_0 good enough?

Because for some values of y, B will have very low chances of inverting f. There can be many such $y's$ but now we will prove that there wouldn't be too many.Let us suppose BAD be the set of those input values x such that A_0 has low chances of inverting $f(x)$.

$$\boxed{BAD := \{x \mid \Pr_{A_0}[A_0 \; inverts \; f(x)] < low\}} \tag{8}$$

Here, lower the RHS, less will be the size of set BAD
To prove $Eq(6)$, we need set BAD such that:

$$\boxed{\Pr_x[\; x \in BAD] \; < \; 1/2q} \tag{9}$$

Let us prove it using contradiction.

Proof. Suppose, $\Pr_x[\ x \in BAD] \ \geq \ 1/2q$

$$
\begin{aligned}
\beta &= \Pr_{(x_1,x_2,...x_N)}[B \ inverts \ F(x_1,x_2,...,x_N)] \\
&= \Pr_{(x_1,x_2,...x_N)}[B \ inverts \ F(x_1,x_2,...,x_N) \wedge (\forall i \ : \ x_i \notin BAD)] \\
&+ \Pr_{(x_1,x_2,...x_N)}[B \ inverts \ F(x_1,x_2,...,x_N) \wedge (\exists i \ : \ x_i \in BAD)] \\
&\leq \Pr_{(x_1,x_2,...x_N)}[\forall i \ : \ x_i \ \notin BAD] \\
&+ \sum_i \Pr_{(x_1,x_2,...x_N)}[B \ inverts \ F(x_1,x_2,...,x_N) \wedge (x_i \in BAD)] \\
&\leq (1 \ - \ \frac{1}{2q})^N \ + \ N \cdot \Pr_{(x_1,x_2,...x_N)}[B \ inverts \ F(x_1,x_2,...,x_N) \wedge (x_i \in BAD)] \\
&\leq (1 \ - \ \frac{1}{2q})^{2nq} \ + \ N \cdot \Pr_{(x \xleftarrow{\$} \{0.1\}^n, B)}[A_0 \ inverts \ f(x) \wedge (x \in BAD)] \\
&\leq \ e^{-n} \ + \ N \cdot \ \Pr[x \in BAD] \cdot \Pr_{(x \xleftarrow{\$} \{0.1\}^n, B)}[A_0 \ inverts \ f(x) | x \in BAD] \\
&\leq e^{-n} + 2nq \cdot 1 \cdot \frac{1}{4npq} \\
&= e^{-n} + \frac{1}{2p} \\
&< \frac{1}{2p} + \frac{1}{2p} \\
\Rightarrow \beta &< \frac{1}{p}. \ \ (Contradicts(6)). \quad (QED)
\end{aligned}
$$

2.2 Analysis of Main Adversary A

Let us calculate the failure probability of main adversary A that runs A_0 N times.
Proof.

$$
\begin{aligned}
\alpha &= \Pr_{(x \xleftarrow{\$} \{0.1\}^n)}[A \ fails \ to \ invert \ f(x)] \\
&= \Pr_x[x \in BAD] \ \cdot \ \Pr_x[A \ fails \ to \ invert \ f(x) \mid x \in BAD] \\
&+ \Pr_x[x \notin BAD] \ \cdot \ \Pr_x[A \ fails \ to \ invert \ f(x) \mid x \notin BAD] \\
&\leq \ \frac{1}{2q} \cdot 1 + 1 \cdot (\Pr_x[A \ fails \ to \ invert \ f(x) \mid x \notin BAD])^T \\
&\leq \ \frac{1}{2q} + (1 \ - \ \frac{1}{4npq})^{4pqn^2} \\
&\leq \ \frac{1}{2q} + e^{-n} < 1/q. \quad (Contradicts(3)) \quad QED.
\end{aligned}
$$

Therefore, we can say that if F is not a strong one-way function then f can't be a weak one-way function.