CS 600.442 – Modern Cryptography September 2, 2015

Lecture 2: One Way Functions

Instructor: Abhishek Jain *Scribe: Howard Huang and Gijs Van Laer*

1 One Way Functions

Intuition. Let us start by recalling the intuition for one-way functions. A function f is one way if it satisfies the following two (informal) properties:

1. **Easy to compute:** Given any input x, it should be possible to compute $f(x)$ in polynomial time.
2. **Hard to invert:** Any polynomial time adversary should fail in recovering x given $f(x)$. In other words, the probability of inverting $f(x)$ should be "small."

Let us now attempt to formalize the above two properties. Here is a first attempt at a semi-formal definition.

Definition 1 (Strong One-Way Functions: Attempt 1) *A function $f : \{0,1\}^n \to \{0,1\}^m$ is a strong one-way function if:*

1. **Easy to compute:** *$\exists$ a PPT algorithm C that computes $f(x)$ on all inputs $x \in \{0,1\}^n$.*
2. **Hard to invert:** *For every non-uniform PPT adversary A,*

$$Pr\left[x \overset{\$}{\leftarrow} \{0,1\}^n, y \leftarrow f(x) : f\left(A\left(y\right)\right) = y\right] \leq \text{"small"}$$

Is this a good definition of one-way functions? There are two problems: first, we need to formalize what "small" means. There is, in fact, another problem with this definition. But we will visit it later. Let us first address the issue of formalizing "small." Informally speaking, we want to define a "fast" decaying function that decays asymptotically faster than any inverse polynomial. We will call such a function *negligible*.

1.1 Negligible Functions

Definition 2 (Negligible Functions) *A function $\mu(.)$ is negligible if:*

$$\forall c \in \mathbb{N}, \underbrace{\exists n_0 \in \mathbb{N} \text{ such that } \forall n > n_0}_{\text{"eventually"}}, \mu(n) \leq \frac{1}{n^c}$$

The above definition captures the intuition that a negligible function **eventually** decays faster than any inverse polynomial. An exponentially decaying function (e.g., 2^{-n}) is obviously negligible. Other examples are $n^{-log(n)}$, and more generally, $n^{-\omega(1)}$.

Often, we will also use the opposite of negligible functions, which we refer to as *non-negligible functions*. Intuitively, a function $\mu(\cdot)$ is non-negligible if there is at least one polynomial $q(\cdot)$ such $\mu(\cdot)$ is infinitely often larger than $1/q(\cdot)$.

Definition 3 (Non-negligible Functions) *A function $\mu(.)$ is non-negligible if $\exists c \in \mathbb{N}$ such that for infinitely many $n \in \mathbb{N}, \mu(n) \geq \frac{1}{n^c}$.*

Can we Amplify Negligible Functions? Recall that we plan to use negligible functions to capture the success probability of PPT adversaries when defining security of a cryptographic system. The following theorem establishes that a PPT adversary cannot "amplify" his success probability from negligible to non-negligible.

Theorem 1 (Negligible functions do not amplify) *The sum of polynomially many negligible functions is also a negligible function.*

We now prove the theorem for the special case where we consider the sum of two negligible functions. The proof of general case is left as an exercise.

Lemma 2 *If $f(\cdot)$ and $g(\cdot)$ are two negligible functions, then their sum $f(\cdot)+g(\cdot)$ is also negligible.*

Proof. Let $h(\cdot) = f(\cdot) + g(\cdot)$. We need to show that $\forall c \in \mathbb{N}, \exists n_0 \; s.t. \; \forall n \geq n_0, h(n) \leq \frac{1}{n^c}$.
Fix some $c \in \mathbb{N}$. Since $f(\cdot)$ and $g(\cdot)$ are negligible, $\exists n_f, n_g$ s.t.

- $\forall n \geq n_f, f(n) \leq \frac{1}{n^{c+1}}$,
- $\forall n \geq n_g, g(n) \leq \frac{1}{n^{c+1}}$.

Let $n_o = max(n_f, n_g, 2)$. Then, $\forall n \geq n_0$ we have:

$$\begin{aligned} h(n) &= f(n) + g(n) \\ &\leq \frac{2}{n^{c+1}} \\ &\leq \frac{n}{n^{c+1}} \\ &\leq \frac{1}{n^c}. \end{aligned}$$

■

1.2 Back to One-Way Functions

Now that we have formally defined negligible functions, we are ready to update our definition of strong one-way functions.

Definition 4 (Strong One-Way Functions: Attempt 2) *A function $f : \{0,1\}^n \to \{0,1\}^m$ is a strong one-way function if:*

1. **Easy to compute:** *$\exists$ a PPT algorithm C that computes $f(x)$ on all inputs $x \in \{0,1\}^n$.*
2. **Hard to invert:** *For every non-uniform PPT adversary A, there exists negligible function $\mu(.)$ such that:*

$$Pr\left[x \xleftarrow{\$} \{0,1\}^n, y \leftarrow f(x) : f\left(A\left(y\right)\right) = y\right] \leq \mu(n)$$

Is this a good definition? Consider a function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ where $m = \log n$. Note that a PPT adversary runs in time polynomial in its input length. Then, as per the above definition where the only input to the adversary is an output y of length $m = \log n$, a PPT adversary A runs in time $poly(m)$. This means A does not even have sufficient time to write down any x in the input domain of f since $|x| = 2^m$. Indeed, clearly invertible functions such as $f(x) = |x|$ are secure w.r.t. this definition!

To fix this issue, we give an additional input 1^n to the adversary to as allow her to run in time polynomial in the input length of the function. We are now ready to finish our definition of strong one-way functions.

Definition 5 (Strong One-Way Functions) *A function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ is a strong one-way function if:*

1. **Easy to compute:** *$\exists$ a PPT algorithm C that computes $f(x)$ on all inputs $x \in \{0,1\}^n$.*
2. **Hard to invert:** *For every non-uniform PPT adversary A, there exists negligible function $\mu(.)$ such that:*
$$Pr\left[x \overset{\$}{\leftarrow} \{0,1\}^n, y \leftarrow f(x) : f\left(A\left(1^n, y\right)\right) = y\right] \leq \mu(n)$$

In the opposite direction, (informally speaking) we say that an adversary "breaks" a one-way function f if it successfully inverts with probability $\frac{1}{p(n)}$ for some polynomial $p(\cdot)$.

1.3 Existence of One-Way Functions

We do not know if one-way functions exist unconditionally. Note that their existence would imply that P $\neq$ NP! However, their exist several candidates for one-way functions.

Let us consider the following function f_{mult}:

$$f_{mult}(x,y) = x \cdot y$$

Is this a (strong) one-way function? Note that if x and y are chosen independently at random, then with probability $\frac{3}{4}$, the output $x \cdot y$ will be even. In this case, one can simply output $(2, \frac{x \cdot y}{2})$ as a valid inversion in polynomial time. Therefore, f_{mult} is not a strong one-way function.

It turns out, however, that based on hardness of factoring assumption, we can prove that f_{mult} is a *weak* one-way function.

Let us first state the hardness of factoring assumption. We will use the following notation:

$$\Pi_n = \{p \mid p < 2^n \text{ and } p \text{ is a prime}\}$$

Assumption 1 (Hardness of Factoring) *For every PPT adversary A, there exists a negligible function $\mu(\cdot)$ s.t.*
$$Pr\left[p \leftarrow \Pi_n, q \leftarrow \Pi_n, N \leftarrow p \cdot q : A\left(N\right) \in \{p,q\}\right] \leq \mu(n)$$

We now state the definition of a weak one-way function.

Definition 6 (Weak One-Way Functions) *A function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ is a weak one-way function if:*

1. **Easy to compute:** *$\exists$ a PPT algorithm C that computes $f(x)$ on all inputs $x \in \{0,1\}^n$.*

2. **Slightly Hard to invert:** *There exists polynomial $q : \mathbb{N} \to \mathbb{N}$ s.t. for every non-uniform PPT adversary A:*

$$Pr\left[x \overset{\$}{\leftarrow} \{0,1\}^n, y \leftarrow f(x) : f\left(A\left(1^n, y\right)\right) = y\right] \leq 1 - \frac{1}{q(n)}$$

In a weak one-way function, the probability of inversion is only bounded away from 1 by some non-negligible amount.

Theorem 3 (f_{mult} is a Weak One-Way Function) *Assuming hardness of factoring, f_{mult} is a weak one way function.*

Proof. To be done in the next lecture.

2 Hardness Amplification: From Weak to Strong One-Way Functions

The security guarantee of a weak one-way function is really weak. As such, as is, it does not suffice for many cryptographic tasks. As it turns out, however, it is, in fact, possible to generically transform *any* weak one-way function into a strong one-way function.

Theorem 4 *For any weak one way function f, there exists a strong one way function g.*

More concretely, we can prove the following theorem by Yao:

Theorem 5 (Hardness Amplification) *Let $f : \{0,1\}^n \leftarrow \{0,1\}^\ell$ be a weak one way function. There exists a polynomial $m = m(n)$ such that $g : \{0,1\}^{m \cdot n} \leftarrow \{0,1\}^{\ell \cdot n}$ is a strong one-way function, where g is defined as follows:*

$$g\left(x_1, \ldots, x_m\right) = f\left(x_1\right), \ldots, f\left(x_n\right)$$