CS276: Cryptography August 27, 2015

One-Way Functions

Instructor: Alessandro Chiesa *Scribe: Brian Gluzman*

1 Introduction

In this lecture, we will discuss the definition and construction of one-way functions. In addition, we will define negligible functions and noticeable functions. We will also discuss/define (uniform and non-uniform) probabalistic polynomial time algorithms. We finish with the definitions of weak one-way functions and what it means for a function to generate hard problems for an NP relation.

1.1 Motivating One-Way Functions

We begin by finding a working definition for a function that we could use for cryptographic purposes. Our intution tells us the the following must be satisfied by this function:

1. The function must be easy to compute
2. The function must be hard to invert

From these two requirements, we can now motivate the following definition of a one-way function (probabilistic polynomial time and negligible/noticeable functions will all be defined later in this document):

Definition 1 *A* **one-way function** *is a family of functions:*

$$F = \{f_k\}_{k\in\mathbb{N}} \qquad f_k : \{0,1\}^{\mathcal{N}(k)} \to \{0,1\}^{\mathcal{M}(k)}$$

(where $\mathcal{N}, \mathcal{M}$ are both polynomial in k) such that:

(i) $\exists M$ such that $\forall k \in \mathbb{N}, \forall x \in \{0,1\}^{\mathcal{N}(k)}, M(1^k, x) = f_k(x)$ where M runs in polynomial time

(ii) For all **probabalistic polynomial time** machines $A(1^k, y)$ for some $k \in \mathbb{N}$ and $y \in \mathcal{M}(k)$, we define*:*

$$\delta_A(k) = \Pr\left[\hat{x} \in f^{-1}(y) \mid x \leftarrow \{0,1\}^{\mathcal{N}(k)}, y \leftarrow f_k(x), \hat{x} \leftarrow A(1^k, y)\right]$$

where $x \leftarrow \{0,1\}^{\mathcal{N}(k)}$ means that x was sampled uniformly at random from the set $\{0,1\}^{\mathcal{N}(k)}$. Then we must have that*:*

$$\delta_A(k) \text{ is } \textbf{negligible} \text{ in } k$$

The natural number k is called the "security parameter".

Remark 2 *One may wonder why in part (i) of the definition above that we chose $f_k(x) = M(1^k, x)$ instead of $f_k(x) = M(k, x)$ for some machine M. The issue with selecting the latter definition is that we disallow possibily adversaries that can easily invert f_k computationally, but do not have sufficient time to print out the result.*
Take, for example, $f(x) = y$ where y means "the binary representation of the length of x". *It only takes $\log_2 |x|$ bits to represent y, but printing a corresponding x when given y would take at least $|x|$ steps (i.e. $O(2^{|y|})$ steps). Thus, for any adversarial machine, it is impossible to invert f_k if we we choose $f_k(x) = M(k, x)$ given that we want the inversion to run in polynomial time in k. However, it is clear that (ignoring printing) there is a polynomial time algorithm that inverts f_k, so we make the modifications noted above as not to limit the power of our adversary.*

We have left out the definitions of **probabalistic polynomial time** and **negligible** in the above. We now go back and define these terms to make the above definition more precise.

1.2 Probabalistic Polynomial Time

Definition 3 *The class* **uniform probabalistic polynomial time** *is given by the set of languages that are recognized by a turing machine A with the property:*

$$\exists c, n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0 \text{ the runtime of } A(z) \text{ for all } z \text{ of size } n \text{ is at most } |z|^c$$

Definition 4 *The class* **non-uniform probabalistic polynomial time** *is given by the set of languages recognized by a turing machine from a family of turing machines:*

$$A = \{A_1, A_2, ...\}$$

with the property:

$$\exists d \text{ such that } |A_k| \leq k^d$$

$$\exists c \text{ such that the running time of } A_{|z|}(z) \text{ is at most } |z|^c$$

1.3 Negligible and Noticeable Functions

We can now go on to define both **negligible** (and the contrary notion, **noticeable**) functions.

Definition 5 *A function $\mu : \mathbb{N} \to [0, 1]$ is* **negligible** *if:*

$$\frac{1}{\mu} \text{ grows faster than every polynomial}$$

$$\text{(i.e. } \forall c \in \mathbb{N}, \exists k_0 \text{ such that } \forall k \geq k_0, \mu(k) < k^{-c} \text{)}$$

Definition 6 *A function $\mu : \mathbb{N} \to [0, 1]$ is* **noticable** *if:*

$$\frac{1}{\mu} \text{ grows slower than some polynomial}$$

$$\text{(i.e. } \exists c \in \mathbb{N}, \exists k_0 \text{ such that } \forall k \geq k_0, \mu(k) > k^{-c} \text{)}$$

Remark 7 *A function being non-negligible does* **not** *mean that it is noticeable! Similarly, a function being non-noticeable does* **not** *mean that it is negligible! There are functions that* **are neither negligible nor noticeable***!*
For example, 2^{-k} *may be negligible and not noticeable and* k^{-1} *may be noticeable and not negligible, but the function:*

$$f(k) = \begin{cases} 2^{-k} & k \text{ even} \\ k^{-1} & k \text{ odd} \end{cases}$$

is neither.

Remark 8 *Suppose that* μ, μ' *are negligible. Then* $\mu + \mu'$ *is negligible.*
(Prove this for yourself - remember that $2k^{-(c+1)} < k^{-c}$*).*

Remark 9 *Suppose that* μ *is noticeable and* μ' *is negligible. Then* $\mu - \mu'$ *is noticeable.*
(Prove this for yourself)

1.4 Candidates for One-Way Functions

Do we know that one-way functions exists? **No!**
If we did, then we know that $P \neq NP$.

What about some candidates for one-way functions?
Related to the hardness of the subset-sum problem:

$$f(x_1, x_2, ..., x_n, I) = (x_1, x_2, ..., x_n, \oplus_{i \in I} x_i)$$

where $x_i \in \{0, 1\}$ and $I \subseteq [n]$.
Related to the hardness of factoring:

$$f((x, y)) = x \cdot y$$

where (x, y) is the concatination of the numbers x and y.

1.5 Weak One-Way Functions

Let's look at a weaker notion of one-way functions.

Definition 10 *A function f is a* $\alpha-$ **weak one-way function** *if:*

$$\delta_A(k) - \alpha(k) \text{ is negligible in } k$$

where $\delta_A(k)$ *is identical to the one defined in Definition 1.*

We will see next time that the existence of a $(1 - k^{-c})$-weak one-way functions imply strong one-way functions.

1.6 Generating Hard Problems

How can we relate NP problems to one-way functions? We recall the definition of an NP relation.

Definition 11 *$R \in NP$ if there exists a polynomial time machine M such that:*

(i) $(x, w) \in R \leftrightarrow M(x, w) = 1$

(ii) *$\exists c$ such that $M(z)$ that runs in $|z|^c$*

Definition 12 *We say that G* **generates hard problems for** *R if*

$$\Pr\left[(x, w') \in R \mid (x, w) \leftarrow G(1^k), w' \leftarrow A(1^k, x)\right] \text{ is negligible in } k$$