One Way Functions

Amit Suthar 05CS3016
Amar Patel 05CS3017

Computer Science and Engineering Department
Indian Institute of Kharagpur, Kharagpur
West Bengal, 721302
India

Contents

Chapter 1

Introduction

1.1 One Way Function

A one-way function is a mathematical function that is significantly easier to compute in one direction (the forward direction) than in the opposite direction (the inverse direction).It might be possible, for example, to compute the function in the forward direction in seconds but to compute its inverse could take months or years, if at all possible.

Informally, a function f is a one-way function if

1. The description of f is publicly known and does not require any secret information for its operation.
2. Given x, it is easy to compute $f(x)$.
3. Given y, in the range of f, it is hard to find an x such that $f(x) = y$. More precisely, any efficient algorithm solving a P-problem succeeds in inverting f with negligible probability.

The existence of one-way functions is an open conjecture. In fact, their existence would imply $P = NP$, resolving the foremost unsolved question of computer science. This is easy to show by showing the contrapositive: if $P = NP$, then $FP = FNP$, and so any function that can be computed in polynomial time can be inverted in polynomial time, since there is a simple FNP algorithm that inverts it by nondeterministically enumerating all possible inputs. However, it is not known whether $P = NP$ implies the existence of one-way functions, mainly because of the worst-case hardness vs. average-case hardness distinction.

For example, it is conjectured, but not proved, that the following are one-way functions:

1. Factoring problem: $f(p,q) = pq$, for randomly chosen primes p,q.
2. Discrete logarithm problem: $f(p,g,x) =< p,g,g^x(modp) >$for g a generator of Z_p^* for some prime p.
3. Discrete root extraction problem: $f(p,q,e,y) =< pq,e,y^e(modpq) >$, for y in $Z_(pq)^*$, e in $Z\_(pq)$ and relatively prime to $(p-1)(q-1)$, and p,q primes. This is the function commonly known as RSA encryption.
4. Subset sum problem: $f(a,b) =< sum\_(i=1)^(n)a\_ib\_i, b >, fora\_iin0,1$, and n-bit integers b_i.
5. Quadratic residue problem.

The existence of a one-way function implies the existence of many other useful cryptographic primitives, including:

* Pseudorandom number generators;
* Pseudorandom function families;
* Bit commitment schemes;
* Private-key encryption schemes secure against adaptive chosen-ciphertext attack;
* Message authentication codes;
* Digital signature schemes (secure against adaptive chosen-message attack.

A trapdoor one-way function is a one-way function for which the inverse direction is easy given a certain piece of information (the trapdoor), but difficult otherwise.

Chapter 2

Types of One Way Functions

There are two types of one way functions namely weak one way functions and strong one way functions

2.1 Strong One Way Function

A Strong One-Way function is a function which is easy to compute and 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.

Definition 1. *A function* $f : \{0,1\}^* \to \{0,1\}^*$ *is called strongly one way if two condition hold*

1. *easy to compute: There exists a polynomial-time algrithm, A, so that on input x algorithm A outputs f(x) (i.e f(x)=A(x)).*
2. *hard to invert: For every probabilistic polynomial-time algorithm* $A^{'}$*,every polynomial p() , and all sufficently large n's*

$$Pr(A^{'}(f(x)) \in f^{-1}f(x)) < \frac{1}{p(n)}$$

2.2 Weak One Way Function

A Weak One-Way function is a function which is easy to compute and slightly hard to invert for random inputs or easy to invert on some non-negligible fraction of the inputs.

Definition 2. *A function $f : \{0,1\}^n \to \{0,1\}^n$ is called weak one-way, if*

f is a polynomial-time computable function
there exists a polynomial $p(.)$, for every probabilistic polynomial-time algorithm A, and all sufficiently large $n^{'}s$
$Pr(A^{'}(f(x)) \in f^{-1}f(x)) < 1 - \frac{1}{p(n)}$
where x is chosen uniformly in $0, 1^n$ and the probability is also over the internal coin flaps of A flops

Example Integer Factoring

Consider $f(x, y) = x.y$

Easy to compute
Is it **one-way**?
No: if $f(x, y)$ is even can set inverse as $(f(x, y)/2, 2)$
If factoring a number into prime factors is hard
Specially given $N = P.Q$, the product of two random large (n-bit) primes, it is hard to factor
Then somewhat hard - **there are a non-negligible fraction of such numbers** $1//n^2$ from the density of primes.
Hence a **weak** one-way function.

2.3 Hardness Amplication

Given: a function f that is guaranteed to be a **weak** one-way Let $p(n)$ be such that

$$Pr(A^{'}(f(x)) \in f^{-1}f(x)) < 1 - \frac{1}{p(n)}$$

Can we construct a function that is **Strong** one-way ?

2.4 An instance of a Hardness Amplication problem

Simple idea: repetition.

For some polynomial q(n) define

$g(x_1, x_2, ..., x_{q(n)}) = f(x_1), f(x_2), ..., f(x_{q(n)})$

To invert g need to succeed in inverting f in all $q(n)$ places

If q(n) = p2(n) seems unlikely $(1 - 1/p(n))^{p2(n)}$ is approximately equal to $e^{p(n)}$

To prove : Let $f : \{0,1\}^* \rightarrow \{0,1\}^*$ be a weak OWF. Then there exists a polynomial t(n), such that for input length m, the following function: $g(x_1, x_2, , ..., x_m) = f(x_1)f(x_2)...f(x_m)$ is a strong OWF.

Proof by contradiction: We assume that g is not strongly one-way

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

Goal: To construct $A^{'}$ that uses A to invert with probability $>$ 1- $\frac{1}{q(n)}$; that is violate the weak one-wayness.

$A^{'}$: repeat procedure I below 2nmp(n) times:

Procedure I

for $i \leftarrow 1$ to 4

Select uniformly and independently a sequence of strings $x_1, x_2, , , , x_m \in \{0,1\}^n$

Compute:

$(z_1, z_2, , , z_m) = A(f(x_1), , , f(x_i - 1), y, f(x_i + 1), , , f(x_m))$

If $f(z_i)$ = y ; halt and output y.

We define:

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

Bad = otherwise.

Claim: Pr[$x_i isGood$] $> 1 - \frac{1}{2q(n)}$

We first prove the claim by contradiction as follows.

2.5 Proof of Claim

$Pr[A(g(x_1, x_2, , ..., x_m))succeeds] = Pr[A(g(x_1, x_2, , ..., x_m)succeeds \wedge \exists Badx_i]$
$+ Pr[A(g(x_1, x_2, , ..., x_m))succeeds \wedge \forall i, x_i isGood]$
a) $Pr[A(g(x_1, x_2, , ..., x_m))succeeds \wedge \exists Badx_i]$
$\leq \sum_i Pr[A(g(x_1, x_2, , ..., x_m))succeeds \wedge Badx_i]$
$\leq \sum_i \sum_{x \in Bad} Pr[A(g(x_1, x_2, , ..., x_m))succeed \wedge x_i = x]$
= $\sum_i \sum_{x \in Bad} Pr[x_i = x]Pr[A(g(x_1, x_2, , ..., x_m)) \mid x_i = x]$
$\leq \sum_i Pr_{max}[A(g(x_1, x_2, , ..., x_m))$ succeed when x_i is Bad]
$\leq \sum_i Pr_{max}$[I succeed in inverting f(x_i) when x_i is Bad]
$\leq m\frac{1}{2mp(n)} = \frac{1}{2p(n)}$

b) $Pr[A(g(x_1, x_2, , ..., x_m))succeeds \wedge \forall i, x_i isGood]$
$\leq Pr[\forall i, x_i isGood]$
$\leq (1 - \frac{1}{2q(n)})^m$ [if we contradict the claim]
=$(1 - \frac{1}{2q(n)})^{2nq(n)}$ [putting m = 2nq(n)]
$\approx \frac{1}{e^n}$
$\therefore Pr[A(g(x_1, x_2, , ..., x_m))succeed] \leq \frac{1}{2p(n)} + \frac{1}{e^n}$

This contradicts the fact that A is successful against g.

$\therefore Pr[x_i isGood] \geq 1 - \frac{1}{2q(n)}$
and $Pr[x_i isBad] \leq \frac{1}{2q(n)}$

Finally,
Pr[$A^{'}$(f(x) fails]
=Pr[$A^{'}$(f(x) fails | x is Good]Pr[x is Good]+Pr[$A^{'}$(f(x) fails | x is Bad]Pr[x is Bad]
Pr[$A^{'}$(f(x) fails | x is Good]+Pr[x is Bad]
We know, Pr[x is Bad] $\leq \frac{1}{2q(n)}$
Pr[$A^{'}$(f(x)) fails | x is Good] $\approx \frac{1}{e^n}$
Pr[$A^{'}$(f(x) fails] $\leq \frac{1}{e^n} + \frac{1}{2p(n)} \approx \frac{1}{2q^n}$
Pr[$A^{'}$(f(x) succeeds] $\geq 1 - \frac{1}{2q^n}$

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