COM S 6830 – Cryptography Sep 3, 2009

Lecture 3: One-Way Functions

Instructor: Rafael Pass *Scribe: Srivatsan Ravi*

1 Review

We saw that no encryption scheme can be perfectly secure if the keys it uses are shorter than the messages.

Theorem 1 *(Shannon) If E={M,K,Gen,Enc,Dec} is perfectly secure, then* $|K| \geqslant |M|$

Theorem 2 *Let E={M,K,Gen,Enc,Dec} be a public key encryption scheme with M={0,1}^{k} and K={0,1}$^{k-1}$. Then, E is not more than 1/2-statistically secret.*

This vulnerability can be used by Eve to carry out an attack with high probability in exponential time by computing a decryption $\forall$k ϵ K. Hence the need for an adversary model where the computation time is a bounded resource.

2 Non-uniform probabilistic polynomial time turing machines

A randomized Turing machine A runs in time T(n) if $\forall$ x ϵ L, A(x) halts within T(|x|) steps. It is said to run in POLY time if $\exists$ c, T(n) = n^c.

Definition 1 *Non-uniform PPT machine A is a sequence of probabilistic turing machines* $\{A_1 ... A_n\}$ *for which there exists a polynomial 'd' s.t* $|A_i| < d(i)$ *and the running time of* A_i *is* $\leqslant d(i)$ *on inputs of length i*

The intuition is to define a Turing machine model that can work on all inputs i.e an algorithm is allowed to have a different description for different input sizes as oppposed to the uniform model where the description is constant for all input sizes.
This is the model over which the definition of One way functions or OWF's will be formalized.

3 One way functions

3.1 Worst case OWF's

The basic notion of a OWF is that it is easy to compute, but hard to invert. Informally, it must be easy to compute c given m and c. But it must 'hard' to recover m and k given c, e.g., MUL defined as $f : Z \times Z \rightarrow Z$ where $f(x, y) = xy$

The existence of one-way functions is an important tool in modern cryptography.

Definition 2 *There is no NU-PPT algorithm A s.t* $\forall$ *x, Pr[A(f(x)* ϵ $f^{-1}(f(x))]$*=1.*

However, in-order to allow the adversary to work in poly-time in input, we introduce another parameter to the adversary algorithm so that the adversary can work in time polynomial in —x— even if f(x) is much shorter.
We will also need to relax the definition of this OWF because we need a one way function where for a randomly chosen x, the probability that we are able to invert the function is very small. This is introduced through the concept of a negligible function.

3.2 Strong OWF's

Definition 3 *Negligible function:* $\varepsilon(k)$ *is negligible if for every c, there exists some* k_o *s.t* $\varepsilon(k) \leqslant 1/k^c$ $\forall k_o < k$.

Intuitively, a negligible function is asymtotically smaller than the inverse of any fixed polynomial.

Definition 4 *Strong One way function:*
A function f : $\{0,1\}^\star \rightarrow \{0,1\}$ *is strongly one-way if for every NU-PPT algorithm A, there exists a negligible function* $\varepsilon(k)$ *s.t* $\forall k$ *, we have*

$$Pr[x \leftarrow \{0,1\}^k, y = f(x), A(1^k, y) = z; f(z) = y] \leqslant \varepsilon(k)$$

Note the extra parameter(1^k;binary length of x) introduced as input to the adversary algorithm to ensure the adversary can work in poly-time in —x—.
Now consider the example of MUL: f(x,y)=x.y. This is easy to compute. But, if at least one of x,y is even, the product will be even as well and a trivial attack is possible on the one-way function. However, if x,y ϵ PRIMES, then MUL will be hard to invert.
Hence the need for a weaker version of hardness which relaxes condition on inverting the function.
At this point, it is important to understand the difference between an asymptotic definition and a concrete notion of security.

Note 1 Concrete security: A function f is (t,s,ε) one-way if $\forall$ A with a running time t(n) and description length s(n), the inversion will succeed with Pr $\leqslant \varepsilon(n)$.

3.3 Weak OWF's

Definition 5 *Weak One way function:*
A function f : $\{0,1\}^\star \rightarrow \{0,1\}$ *is weak one-way if for every NU-PPT algorithm A, there exists a polynomial function Q s.t for sufficiently large k, we have*
Pr[$x \leftarrow \{0,1\}^k$*,y = f(x), A(*1^k*,y)=z , f(z)=y]* $\leqslant 1 - 1/Q(k)$

This relaxation for hardness only requires that all efficient attempts at inverting the function fail with some non-neglibible probability whereas a strong one-way function must be hard to invert on all, but a negligible fraction of all inputs.
But it is easier to find weak one-way functions even though strong one-way functions are more desirable. But it is possible to demonstrate the existence of strong one-way functions from weak one-way functions and also contruct them.

3.4 Hardness amplification

Theorem 3 *The existence of a weak one-way function implies the existence of a strong one-way function.*

Let f be a weak one-way function. Now define the function,
$g(x_1.....x_n) = f(x_1)f(x_2)...f(x_n)$ where n=k*Q(k) where Q is the polynomial function in the definition of the weak one-way function and k=—x_i—
i.e g is the concatenation of n copies of the function f.
Then g is a strong one-way function.