CSL 759 – Cryptography and Network Security	Jan 08, 2014

Lecture 3: Strong and Weak One Way Functions

Instructor: Shweta Agrawal *Scribe: Sudarshan Maurya*

1 Strong-One Way Function

Definition 1 *A function $f : \{0,1\}^* \to \{0,1\}^*$ is one-way function if it satisfies the following two conditions:*

1. *f can be computed in PPT.*
2. *For every PPT algoritm A,*
   $\exists$ negligible function ϵ such that $\forall$ n, $Pr[x \xleftarrow{Rand.} \{0,1\}^n, A(f(x)) \to z$ $s.t. f(z) = f(x)] \leq \epsilon(n)$

In simple words, Pr(A inverts f(x) for random x)≤negligible.

2 Weak-One Way Function

Definition 2 *A function $f : \{0,1\}^* \to \{0,1\}^*$ is one-way function if it satisfies the following two conditions:*

1. *f can be computed in PPT.*
2. *For every PPT algoritm A,*
   $\exists$ poly q: N $\to$ R such that $\forall n$,
   $Pr[x \xleftarrow{Rand.} \{0,1\}^n, A(f(x)) \to z$ s.t. f(z) = f(x)] $< 1 - \dfrac{1}{q(n)}$

Lemma 1 *Let f be a weak OWF then $\exists$ polynomial m s.t. for $\dfrac{1}{p}$ XXX length n, the following function*

$$g : \{0,1\}^{mn} \to \{0,1\}^m$$

Or, $g(x_1, x_2, x_3......x_m) = f(x_1).f(x_2)....f(x_m)$

3 Converting Weak OWF to Strong OWF

Definition 3 *Let q be polynominal in weak OWF, Define m=2nq. We want,*

$$(1-\frac{1}{q})^m \rightarrow negligible \ \& \ (1-\frac{1}{q})^{2nq} = (\frac{1}{e})^n$$

Proof. (By contradiction)
Basic Idea: Assume g is not a strong OWF and then derive that f is not weak OWF.

$Pr[x_1 \leftarrow \{0,1\}^n, A^{strong}(g(x_1,x_2,x_3......x_m)) \rightarrow inverse] \geq \frac{1}{p'(mn)} = \frac{1}{p'(m)}$[1]

$Pr([x_1 \leftarrow \{0,1\}^n, A^{strong} suceeds] \geq \frac{1}{p(n)}$

GOAL: Given $A^{strong}(y_1,y_2,....y_m) = z_1,z_2...z_m$ such that $f(z_i) = y_i$

We want to build some A^{weak} that inverts of $XXXX > 1-\frac{1}{q}$.

* We want to build $A^{weak}(f(x))$ which outputs $f^{-1}(f(x))$ and it already has $A^{str}(g(x_1,x_2,x_3......x_m))$

Algo A^{weak} **:**
(i). Run Algo I $2npm^2$ times
// Begin Algo I

1. Pick $i \epsilon [1,m]$ randomly and let $y_i = f(x)$
2. $\forall j \neq i$, pick $x_j \leftarrow \{0,1\}^n$& let $y_1 = f(x_j)$
3. Invoke $A^{str}(y_1,y_2,...ym)$
4. Test if output is correct

//End Algo I
(ii)Output first answer of I that is not XXXX
//End $Algo^{str}$

Now: Show that A^{weak} succeeds with probability $P > 1-\frac{1}{q}$

Relate Pr(A^{wk} succeeds) to Pr(Algo I success)

- $GOOD = \{x :$ Pr (Algo I succeeds in inverting $f(x)) \geq \frac{1}{2m^2p}\}$
- P_r (Algo I fails | x is good) $< 1-\frac{1}{2m^2p}$

[1]As m is dependant on n

- $P_r(A_{weak}$ fails | x is good $) < (1 - \frac{1}{2m^2p})^{2}m^2p \approx (\frac{1}{e})^n$
- For "GOOD" input, A^{weak} succeeds with high probability

Claim: There are at least $2^n(1 - \frac{1}{2q})$ good inputs.