CSL 759 – Cryptography and Network Security	Jan 21, 2013

Lecture 7: General Hardcore Bit of OWF

Instructor: Shweta Agrawal *Scribe: V.Rajeev*

1 Recap : OWF and hardcore bit

One Way Function: $h : \{0,1\}^k \to 0,1$ is a hardcore bit for a OWF 'f' if
1) h(x) is easy to compute given x
2) h(x) is hard to compute given f(x)
i.e. for any polynomial time algorithm A : $Pr(A(f(x) \to h(x))) \leq \frac{1}{2}+(negligible function)$

Hardcore bit:
given f(x), if MSB(x) can be computed, then entire of $f^{-1}(f(x))$ can be computed.

2 General hardcore bit of a OWF

Definition 1 *For a random parity :if* $x\epsilon 0,1^k and r\epsilon 0,1^k$ *, then* $hx,r = \sum r_i x_i mod 2$

Given OWF $f : \{0,1\}^k \to \{0,1\}^k$,
Define $g_f = 0,1^{2k} \to 0,1^{2k}$ such that: $g_f(x,r) = f(x), r$
(g_f - appendeded function such that inverting $g'_f \equiv inverting' f'$)

3 Goldreich - Levin Theorem

Theorem 1 *If 'f' is a OWF, then h(x,r) is a hardcore bit for* g_f *or more formally for all PPTA,* $P_{x,r}(A(f(x),r) \to h(x,r)) < 1/2 + (negligible function)$

Proof. Contra-positive Method
Assume A_{GL} such that $P_{x,r}(A(f(x),r) \to h(x,r)) \geq 1/2+(negligible function)$ will build an A_{OWF} that inverts f
Easy Case: Suppose A_{GL} is such that it always computers the hardcore bit. Set r = unit vector & directly recover x each time.
Medium Case: Suppose A_{GL} such that $Pr(A_{GL} succeeds) \geq 3/4 + \varepsilon$, where ε is a non-negligible function
Proof Idea: r needs to be random
(1)Observe that for every$'r', < x, r >$ and $< x, r \oplus e_i >$together recover x_i. Call A_{GL} on $< x, r >$ & $< x, r \oplus e_i >$
Note: Since we can't test when the algo A_{GL} is correct, we run it many times and take majority.
(2) If both answers are same, x_i is obtained.

Proposition 1 ***Claim:*** *there exits a set "GOOD"* $\Subset 0, 1^k$ *such that* $|GOOD| \geq 2^n.\varepsilon/2$ *and for all* $x \epsilon GOOD$*:* $Pr(A_{GL} wins) \geq 3/4 + (\varepsilon)/2$

Proof: *Define* $succ(x) = Pr(A(f(x), r) =< x, r >)$.

$$GOOD \text{ is the set of } x \text{ such that: } succ(x) \geq \tfrac{3}{4} + (\varepsilon)/2$$

$$Pr_{x,r}(A_{GL} wins) = Pr(A_{GL} wins | x \in GOOD) x Pr(x \in GOOD) + Pr(A_{GL} wins | x \notin GOOD) x Pr(x \notin GOOD)$$
$$\leq Pr(x \in GOOD) + Pr(A_{GL} wins | x \notin GOOD)$$

$$Pr(x \epsilon GOOD) \geq (3/4 + \varepsilon) - (3/4 + (\varepsilon)/2)$$
$$= (\varepsilon)/2 \equiv non - negligible$$
$$|GOOD| \geq (\varepsilon)/2.x^k$$

Observe: For any 'i' and x ϵ GOOD

$$Pr(A_{GL}(f(x, r)) \neq < x, r >) \leq 1/4 - (\varepsilon)/2$$
$$Pr(A_{GL}(f(x, r \oplus e_i)) \neq < x, r \oplus e_i >) \leq 1/4 - (\varepsilon)/2$$
$$Pr(A_{GL} \text{fails on atleast on of them}) \leq 1/2 - \varepsilon$$
$$Pr(A_{GL} \text{succeeds on both of them}) > 1/2 + \varepsilon$$

Statement 1: If $x \epsilon GOOD$, and suppose A_{OWF} inverts f with $Pr \geq 1/2$then, objective attained.

$$Pr(A_{OWF} \text{succeeds in inverting f}) \geq Pr(A_{OWF} succeeds | GOOD).Pr(GOOD)$$
$$\geq 1/2x(\varepsilon)/2 = (\varepsilon)/4.....eq^n(2)$$

Need: A'_{OWF} to invert f' with $Pr \geq 1/2$ for x ϵ GOOD
A'_{OWF}: for i=1 to k do
I) for j=1 to 't'
1) Pick $r_j \leftarrow 0, 1^k$
2) Run $A_{GL}(f(x), r_j) as well as A_{GL}(f(x), r_j \oplus e_i)$
3) Compute x_{ij} as XOR of answer.
II) Compute $x_i = majority(x_{ij})$

Proposition 2 ***Claim:*** *if t = log 2k, then Pr(*x_i *computes correctly)* $\geq 1 - 1/2k$

Lemma 2 *Chernoff: if* $z_1, z_2 .... z_t$ *are independant & identically distributed and* $E(z_i) = 1/2, z = \sum_{i=1-t} z_i$*, where* z_i *is indicator that* x_i *is correct then,* $Pr(z < t/2) \leq 2^t$

Justifying the Claim: *if t = log2k, Pr(Majority is wrong)* $\leq$ *1/2k*
thus, there exists i, such that x_i *computed with* A_{GL} *is wrong with Pr < k.1/2k*
So, Pr(A_{GL} *is correct for all i)* $\geq \frac{1}{2}$

From Statement 1 and $eq^n 2$, since A'_{OWF} inverts f with $Pr \geq 1/2$ for GOOD x and set GOOD is large enough. ■