CSL 759 – Cryptography and Network Security Jan 21, 2014

Lecture 7: Hardcore Bits

Instructor: Shweta Agrawal *Scribe: Ishaan Preet Singh*

1 Recall

Definition 1 *$h : \{0,1\}^* \rightarrow \{0,1\}$ is a hardcore bit for a One Way Function f if $h(x)$ is easy to compute given x and $h(x)$ is hard to compute given $f(x)$. Formally, $\forall PPT\ A$;*

$$Pr(A : f(x) \leftarrow h(x)) \leq \frac{1}{2} + negligible \tag{1}$$

2 General Hardcore Bit for a OWF

Definition 2 Random Parity : *If $x \in \{0,1\}^k$ and $r \in \{0,1\}^k$ then*

$$h(x,r) = \sum r_i x_i \mod 2 \tag{2}$$

Given a OWF $f : \{0,1\}^k \rightarrow \{0,1\}^k$ define a new function $g_f : \{0,1\}^k \rightarrow \{0,1\}^k$ such that

$$g_f(x,r) = f(x), r \tag{3}$$

Theorem 1 Goldreich Levin Theorem: *If f is a OWF, the $h(x,r)$ is a hardcore bit for f. Formally, $\forall PPT\ A$;*

$$Pr(A : (f(x),r) \leftarrow h(x,r)) \leq \frac{1}{2} + negligible \tag{4}$$

Proof. Assume we have a PPT algorithm that can predict the hardcore bit with high probability, A_{GL} that is,

$$Pr(A_{GL} : (f(x),r) \leftarrow h(x,r)) > \frac{1}{2} + negligible \tag{5}$$

We will now build an algorithm A_{OWF} that will be able to invert f. Initially, we observe that

1. For every r, $< x, r >$ and $< x, r \oplus e_i >$ can together recover x_i, the ith bit of x.
2. We can't test if the algorithm A_{GL} gave us the correct bit but can only give a probability of its correctness. Hence, we can run the algorithm many times and take a majority of the results to get a final answer with a higher probability.

We will not provide a complete proof but we will try and prove the theorem for a subset of our sample set for which we have an inverting function with better chances of success.

Claim 1 $\exists$ *a set* Good $\subseteq \{0,1\}^k$ *with* $|\text{Good}| \geq 2^k \frac{\epsilon}{2}$ *and* $x \; \epsilon$ *where* ϵ *is a non-negligible function and Good if for* x *we have* A_{GL} *such that*

$$Pr(A_{GL} : (f(x), r) \leftarrow h(x, r)) \geq \frac{3}{4} + \frac{\epsilon}{2} \tag{6}$$

Proof. We will now develop a lower bound for the cardinality of Good.
Define $succ(x)$ as $Pr(A_{GL} : (f(x), r) \leftarrow h(x, r))$ For $x \; \epsilon \; Good$, $succ(x) \geq \frac{3}{4} + \frac{\epsilon}{2}$ and let A_{GL} wins mean A_{GL} succeeds in predicting $h(x)$

$$\begin{aligned} Pr(A_{GL}wins) &= Pr(A_{GL}wins|x \in Good)Pr(x \in Good) \\ &\quad + Pr(A_{GL}wins|x \notin Good)Pr(x \notin Good) \\ &\leq Pr(x \in Good) + Pr(A_{GL}wins|x \notin Good) \end{aligned} \tag{7}$$

$$\Longrightarrow Pr(x \in Good) \geq Pr(A_{GL}wins) - Pr(A_{GL}wins|x \notin Good) \tag{8}$$

$$\Longrightarrow Pr(x \in Good) \geq \frac{3}{4} + \epsilon - (\frac{3}{4} + \frac{\epsilon}{2}) \tag{9}$$

$$\Longrightarrow Pr(x \in Good) \geq \frac{\epsilon}{2} \tag{10}$$

$$\Longrightarrow |Good| \geq \frac{\epsilon}{2} * 2^n \tag{11}$$

We observe that for any i and $x \in Good$ since we know the value $Pr(A_{GL}wins)$ we can calculate that

$$Pr(A_{GL} : (f(x), r) \neq \langle x, r \rangle) \leq \frac{1}{4} - \frac{\epsilon}{2} \tag{12}$$

$$Pr(A_{GL} : (f(x), r) \neq \langle x, r \oplus e_i \rangle) \leq \frac{1}{4} - \frac{\epsilon}{2} \tag{13}$$

Now, to predict the actual ith bit we need to XOR both these bits. The predicted value will be correct either if both are correct or if both are incorrect. Hence the only case in which the predicted bit is incorrect is when only one of them is incorrect.
Hence,

$$Pr(A_{GL}\text{fails on only one of the two}) \leq 2 * Pr(A_{GL}\text{fails on first}) = \frac{1}{2} - \epsilon \tag{14}$$

$$\Longrightarrow Pr(A_{GL}\text{succeeds to predict the bit}) \geq 1 - (\frac{1}{2} - \epsilon) = \frac{1}{2} + \epsilon \tag{15}$$

■

Now we have A_{GL} that can predict one bit of f with $Pr \geq \frac{1}{2} + non - negligble$ and will construct $A^{'}_{OWF}$ to invert the entire string of bits with a non-negligible probability.

Algorithm: A'_{OWF}

```
For $i = 1$ to $k$ do
    For $j = 1$ to $t$ do
        1. Pick $r_j$ at random
        2. Run $A_{GL}$ on $f(x, r_j)$ as well as on $f(x, r_j \oplus e_i)$
        3. Compute $x_{ij}$ as XOR of the two
    Compute $x_i = Majority(x_{ij})$
```

Claim 2 *If $t = \log(2k)$ then $Pr(x$ computed correctly$) \geq \frac{1}{2}$.*

Proof.

Definition 3 Chernoff Bounds: *If $Z_1, Z_2, \ldots Z_t$ are iid(independent and identically distributed) and $E(Z_i) = \frac{1}{2}, Z = \sum_{i=1}^{t}$ then*

$$Pr(Z < \frac{t}{2}) \leq 2^{-\Omega(t)} \tag{16}$$

Here, Z_i is an indicator variable that x_i is correct.
If $t = \log(2k)$

$$\begin{aligned}
& Pr(\text{Majority of bits is incorrect}) && \leq && \frac{1}{2k} && (17)\\
\implies & Pr(x_i \text{ is wrong}) && \leq && \frac{1}{2k} && (18)\\
\implies & Pr(\text{Bit string is incorrect}) && \leq && k * \frac{1}{2k} = \frac{1}{2} && (19)\\
\implies & Pr(\text{Bit string is correct}) && \geq && \frac{1}{2} && (20)
\end{aligned}$$

■

Now, we've proved that for $x \in Good$, A'_{OWF} inverts f with $Pr \geq \frac{1}{2}$ then

$$\begin{aligned}
& Pr(A'_{OWF} \text{ succeeds in inverting} f) \geq Pr(succ|x \in Good) * Pr(x \in Good) && (21)\\
\implies & Pr(A'_{OWF} \text{ succeeds in inverting} f) \geq \frac{1}{2} * \frac{\epsilon}{2} = \frac{\epsilon}{4} && (22)\\
& && (23)
\end{aligned}$$

Hence, we have inverted f with non-negligible probability. ■