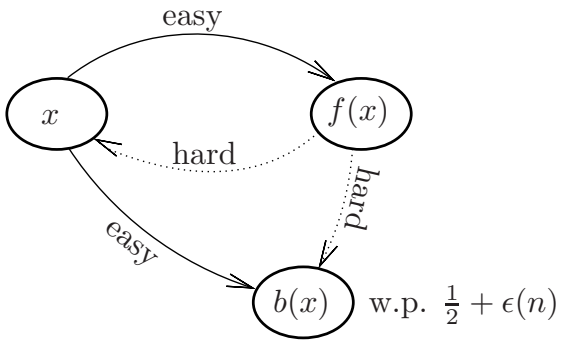
COM S 6830 – Cryptography September 15, 2011

Lecture 7: Hard-Core Bits from Any OWF

Instructor: Rafael Pass *Scribe: Remus Radu*

A one-way function is a function that is easy to compute, but hard to invert. Intuitively, if a function is hard to invert then there should be some bits in the input x that are hard to invert given $f(x)$. This is briefly summarized by the figure below.



Let $\langle x, r \rangle$ denote the inner product of x and r, that is $\langle x, r \rangle = \sum x_i r_i \mod 2$. The main purpose of this lecture is to prove the following theorem.

Theorem 1 *Let f be a OWF. Then $f'(x, r) = (f(x), r)$ where $|x| = |r|$ is a OWF and $b(x, r) = \langle x, r \rangle$ is a hardcore predicate for f'.*

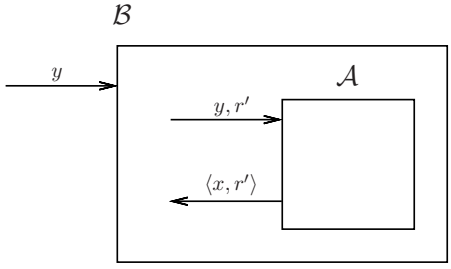
Idea of the proof. If there exists a n.u. PPT $\mathcal{A}$ that predicts $b(x, r)$ with probability $\geq \frac{1}{2} + neg$ then there exists a n.u. PPT $\mathcal{B}$ that inverts f with probability $> neg$.

Oversimplified case.

Assume $\mathcal{A}$ predicts b with probability 1. Let $e_i = 0 \ldots 010 \ldots 0$ be an n-bit string with 1 on the i^{th} position and zeros otherwise. Notice that $\langle x, e_i \rangle = x_i$. The following algorithm:

1. $\mathcal{B}(y)$: $\forall i$
2. $x_i = \mathcal{A}(y, e_i)$
3. OUTPUT x

on input $y = f(x)$ will invert y with probability 1.



Simplified case.

Assume $\mathcal{A}$ predicts b with probability $\geq \frac{3}{4} + \epsilon$. Consider the set S of "good" x

$$S = \left\{ x \;\middle|\; \Pr[\mathcal{A}(f(x), r) = b(x, r)] \geq \frac{3}{4} + \frac{\epsilon}{2} \right\},$$

where the probability is considered only over the choices of r.

Claim 1.1 $\Pr[x \in S] \geq \frac{\epsilon}{2}$.

Proof of Claim. Suppose by contradiction that the probability is less than $\frac{\epsilon}{2}$. We have

$$\begin{aligned} \Pr[\mathcal{A}(f(x), r) = b(x, r)] &\leq \Pr[x \in S] + (\Pr[x \notin S] \cdot \Pr[\mathcal{A}(f(x), r) = b(x, r) \mid x \notin S]) \\ &< \frac{\epsilon}{2} + \left(\left(1 - \frac{\epsilon}{2}\right) \cdot \left(\frac{3}{4} + \frac{\epsilon}{2}\right) \right) = \frac{3}{4} + \epsilon - \frac{3\epsilon + 2\epsilon^2}{8} < \frac{3}{4} + \epsilon \end{aligned}$$

which is a contradiction to our initial assumption. ■

Lemma 2 $\langle a, b \oplus c \rangle = \langle a, b \rangle \oplus \langle a, c \rangle$.

Proof. This follows directly from the definition of the inner product

$$\begin{aligned} \langle a, b \oplus c \rangle &= \sum a_i (b_i + c_i) \bmod 2 \\ &= \sum a_i b_i + \sum a_i c_i \bmod 2 = \langle a, b \rangle \oplus \langle a, c \rangle. \end{aligned}$$

■

The idea is to ask $\mathcal{A}$ to recover $\langle x, r \rangle$ and $\langle x, r \oplus e_i \rangle$ for random r, and then XOR the results. If $\mathcal{A}$ answers correct on both queries, then since $\langle x, r_i^j \oplus e_i \rangle \oplus \langle x, r_i^j \rangle = \langle x, e_i \rangle$, the i^{th} bit of x can be recovered.

Consider the following algorithm:

1. $\mathcal{B}(y)$: $\forall i \in [n]$
2. Pick $r_i^j \leftarrow \{0,1\}^n$
3. $g_i^j = \mathcal{A}(y, r_i^j \oplus e_i) \oplus \mathcal{A}(y, r_i^j)$
4. REPEAT "poly" times
5. OUTPUT x, where
   $x_i = \text{majority}(g_i^1, g_i^2, \ldots)$

Note that

- with probability at most $\frac{1}{4} - \frac{\epsilon}{2}$, $\mathcal{A}(y, r \oplus e_i) \neq b(x, r \oplus e_i)$, and
- with probability at most $\frac{1}{4} - \frac{\epsilon}{2}$, $\mathcal{A}(y, r) \neq b(x, r)$.

By the union bound, it follows that both answers of $\mathcal{A}$ fail with probability at most $\frac{1}{2} - \epsilon$. This means that they are correct with probability at least $\frac{1}{2} + \epsilon$ and therefore each guess g_i^j is correct with probability $\frac{1}{2} + \epsilon$. By Chernoff's inequality we have that x_i (computed by $\mathcal{B}$) is correct except with probability $\simeq 2^{-n}$. Using the union bound we obtain that all x_i are correct except with negligible probability. Hence, for a non-negligible fraction of x's, $\mathcal{B}$ inverts f; a contradiction.

General case.

Assume $\mathcal{A}$ predicts b with probability $\frac{1}{2} + \epsilon$, where $\epsilon \geq \frac{1}{\text{poly}(n)}$ for infinitely many n. Consider, as before, the set

$$S = \left\{ x \;\middle|\; \Pr[\mathcal{A}(f(x), r) = b(x, r)] \geq \frac{1}{2} + \frac{\epsilon}{2} \right\},$$

where the probability is considered only over the choices of r.

Claim 2.1 $\Pr[x \in S] \geq \frac{\epsilon}{2}$.

Assume further that we have access to an oracle $\mathcal{C}$ that given x, gives us m samples

$$\begin{array}{ll} \langle x, r_1 \rangle, & r_1 \\ \langle x, r_2 \rangle, & r_2 \\ \quad \vdots & \\ \langle x, r_m \rangle, & r_m \end{array}$$

where r_i are (pairwise) independent random from $\{0,1\}^n$.

Consider the following algorithm:

1. $\mathcal{B}(y = f(x))$: $\forall i \in [n]$
2. $\mathcal{C}^x \to \langle b_1, r_1 \rangle, \langle b_2, r_2 \rangle, \ldots, \langle b_m, r_m \rangle$
3. $g_i^j = b_j \oplus \mathcal{A}(y, r_j \oplus e_i)$
4. REPEAT m times
5. OUTPUT x, where
$$x_i = \text{majority}(g_i^1, g_i^2, \ldots, g_i^m)$$

For $x \in S$, each guess g_i^j is correct with probability $\frac{1}{2} + \epsilon'$, where $\epsilon' = \frac{\epsilon}{2}$. We apply Chebyshev's inequality for pairwise independent random variables and obtain that each x_i is wrong with probability $\leq \frac{1 - 4\epsilon'^2}{4\epsilon'^2} \leq \frac{1}{m\epsilon'^2}$. If we apply the Chernoff bound directly, we would get probability $\leq 2^{-\epsilon'^2 m}$.

By the union bound, the probability that one of x_i is wrong is $\leq \frac{n}{m\epsilon'^2}$. Note that $\frac{n}{m\epsilon'^2} \leq \frac{1}{2}$ iff $m \geq \frac{2n}{\epsilon'^2}$. Therefore, if we could get $m \geq \frac{2n}{\epsilon'^2}$ pairwise independent samples $\langle x, r_i \rangle,\ r_i$, then the probability that we guess all bits is at least $\frac{1}{2}$ and we are done.

Describe oracle $\mathcal{C}$. Pick $\log(m)$ samples $s_1, s_2, \ldots, s_{\log(m)}$ and guess bits $b'_1, b'_2, \ldots, b'_{\log(m)}$. All guesses are correct with probability $\frac{1}{m}$.

Generate $r_1, r_2, \ldots, r_{m-1}$ as all possible sums (modulo 2) of subsets of $s_1, s_2, \ldots, s_{\log(m)}$, and $b_1, b_2, \ldots, b_{m-1}$ as the corresponding subsets of $b'_1, b'_2, \ldots, b'_{\log(m)}$. For this, let

$$\begin{aligned} r_I &= \oplus_{j \in I}\ s_j, \quad j \in I \text{ iff } i_j = 1 \\ b_I &= \oplus_{j \in I}\ b'_i. \end{aligned}$$

There are m pairwise independent samples (r_I, b_I). With probability $\frac{1}{m}$, all guesses for $b'_1, b'_2, \ldots, b'_{\log(m)}$ are correct, so $b_1, b_2, \ldots, b_{m-1}$ are also correct.

For a fraction of ϵ' of x', with probability $\frac{1}{m}$, we have that the algorithm $\mathcal{B}$ inverts f with probability $\frac{1}{2}$. Thus $\mathcal{B}$ inverts f with probability

$$\frac{\epsilon}{2} \cdot \frac{1}{m} \cdot \frac{1}{2} = \frac{\epsilon}{4m} \geq \frac{1}{\text{poly}(n)},$$

which contradicts the fact that f is one-way.