COM S 6830 – Cryptography	Sept 8, 2009

Lecture 4: More On One-Way Functions

Instructor: Rafael Pass — *Scribe: Matthew Paff*

1 Review:

1.1 Intuition:

A One-Way Function is a function that is easy to compute, but hard to invert. We've defined three kinds (worst-case, weak, and strong). They differ on how they define "hard":

Worst-Case: Always hard to invert, no matter what the key is

Weak: Hard to invert with good probability

Strong: Can only invert with negligable probability

1.2 Rigorous Definitions:

Definition 1. *A function* $\varepsilon : N \to \mathbb{R}$ *is* negligable *if* $\forall\ c,\ \exists\ n_0$ *st* $\forall\ n > n_0,\ \varepsilon(n) < 1/n^c$.

Note that μ is not negligable if $\exists$ a polynomial p st for infinitely many n, $\mu(n) \geq \frac{1}{p(n)}$.

Definition 2. *f is a* strong OWF *if:*

1. *f is easy to compute: $\exists$ a PPT C st $\forall\ x,\ C(x) = f(x)$*
2. *f is hard to invert: $\forall$ nuPPT A, $\exists$ a negligable function ε st $\forall\ n \in N$:*

$$\Pr\left[x \leftarrow \{0,1\}^n : A(1^n, f(x)) \in f^{-1}(f(x))\right] \leq \varepsilon(n)$$

Definition 3. *f is a* weak OWF *if:*

1. *f is easy to compute: $\exists$ a PPT C st $\forall\ x,\ C(x) = f(x)$*
2. *f is hard to invert: $\exists$ a polynomial q st $\forall$ nuPPT A, $\forall\ n \in N$:*

$$\Pr\left[x \leftarrow \{0,1\}^n : A(1^n, f(x)) \in f^{-1}(f(x))\right] \leq 1 - \frac{1}{q(n)}$$

The 1^n are input to A to allow A to compute in time polynomial in n. If that were not there, then A would have to compute in time polynomial in $\log(f(x))$, which could be considerably smaller than n. If $f(x) \in O(n)$, then for A to even return its answer, it would have to use exponential time in the size of its input (since $n = 2^{\log n}$).

2 Hardness Amplification:

The rest of the lecture will focus on the following theorem:

Theorem 1. *The existence of a weak OWF* $\iff$ *the existence of a strong OWF.*

The $\Leftarrow$ direction is trivial, so we just need to prove the $\Rightarrow$ direction. The proof of that direction follows immediately from the following theorem:

Theorem 2. *Let* $f : \{0,1\}^* \to \{0,1\}^*$ *be a weak OWF. Let* $f'(x_1, \ldots, x_m) = y_1, \ldots, y_m$ *where* $y_i = f(x_i)$*. Then* $\exists\ m$ *(polynomial in* n*) st* f' *is a strong OWF.*

Proof. Let f be a weak OWF, and $q(n)$ as in the definition of a weak OWF for f. First, we need to determine what m should be. We need m sufficiently large st $\left(1 - \frac{1}{q(n)}\right)^m$ is negligable. $m = 2nq(n)$ does the trick:

$$\left(1 - \frac{1}{q(n)}\right)^{2nq(n)} = \left(\left(1 - \frac{1}{q(n)}\right)^{q(n)}\right)^{2n} < e^{-2n} < 2^{-n}$$

Let f' be as defined above with $m = 2nq(n)$. Assume f' is not strong, which implies $\exists$ nuPPT A and polynomial p' st for infinitely many n':

$$\Pr\left[x \leftarrow \{0,1\}^{n'} : A \text{ inverts } f'\right] \geq \frac{1}{p'(n')}$$

By definition of f', this means that:

$$\Pr\left[x_i \leftarrow \{0,1\}^n : A(f'(x_1, \ldots, x_m)) \in f'^{-1}(f'(x_1, \ldots, x_m))\right] \geq \frac{1}{p'(mn)}$$

For convenience of notation, let $p(n) = p'(mn)$. Then we have:

$$\Pr\left[x_i \leftarrow \{0,1\}^n : A(f'(x_1, \ldots, x_m)) \in f'^{-1}(f'(x_1, \ldots, x_m))\right] \geq \frac{1}{p(n)}$$

Now we need to construct a machine B to invert f using machine A. Let y be the input to B. Since A is only guaranteed to work with some probability on *random* input, we must make sure the input we give to A is random. Define a machine C on input y as follows:

> $i \leftarrow \{1, \ldots, m\}$
>
> $x_j \leftarrow \{0,1\}^n$ and $y_j = f(x_j)\ \forall\ j \neq i$
>
> $y_i = y$
>
> $z_1, \ldots, z_m \leftarrow A(y_1, \ldots, y_m)$
>
> If $f(z_i) = y$, output z_i. Otherwise, output $\perp$.

Then define B on input y as follows:

Run $C(y)$ up to $2nm^2p(n)$ times, outputing the first answer different than $\perp$.
If $C(y)$ outputs $\perp$ each time, output $\perp$ as well.

Now we need to show that B inverts f with probability greater than $1 - \frac{1}{q(n)}$, which will contradict the definition of f being a weak OWF, as desired.

For $x \in \{0,1\}^n$, define x to be *good* if:

$$\Pr\left[C(f(x)) \neq \perp\right] \geq \frac{1}{2m^2p(n)}$$

And *bad* if that does not hold.

Lemma 3. *If the number of good elements of* $\{0,1\}^n$ *is greater than or equal to* $2^n\left(1 - \frac{1}{2q(n)}\right)$, *then we get our contradiction.*

Proof. Let $x \in \{0,1\}^n$.

$$\begin{aligned}
\Pr\left[B(x) = \perp\right] &= \Pr\left[(B(x) = \perp) \cap (x \text{ is bad})\right] + \Pr\left[(B(x) = \perp) \cap (x \text{ is good})\right] \\
&\leq \Pr\left[x \text{ is bad}\right] + \Pr\left[B(x) = \perp \mid x \text{ is good}\right] \\
&\leq \frac{1}{2q(n)} + \left(1 - \frac{1}{2m^2p(n)}\right)^{n2m^2p(n)} \\
&< \frac{1}{2q(n)} + e^{-n} < \frac{1}{2q(n)} + 2^{-n} < \frac{1}{q(n)}
\end{aligned}$$

which implies:

$$\Pr\left[B \text{ succeeds on input } f(x)\right] > 1 - \frac{1}{q(n)}$$

This contradicts the definition of weak OWF, as desired.

Now we just need to show that the hypothesis of Lemma 3 holds. Assume for contradiction that the number of bad elements is greater than $\frac{2^n}{2q(n)}$. Consider:

$$\begin{aligned}
\Pr\left[A(f(x_1,\ldots,x_m)) \text{ succeeds}\right] = &\Pr\left[(A \text{ succeeds}) \cap (\exists\ i \text{ st } x_i \text{ is bad})\right] \\
&+ \Pr\left[(A \text{ succeeds}) \cap (\forall\ i,\ x_i \text{ is good})\right]
\end{aligned}$$

To get our contradiction, we need to show that this is less than $\frac{1}{p(n)}$. Consider each term separately:

$$\begin{aligned}
\Pr\left[(A \text{ succeeds}) \cap (\exists i \text{ st } x_i \text{ is bad})\right] &\leq \sum_{i=1}^{n} \Pr\left[(A \text{ succeeds}) \cap (x_i \text{ is bad})\right] \\
&\leq \sum_{i=1}^{n} \Pr\left[A \text{ succeeds} \mid x_i \text{ is bad}\right]
\end{aligned}$$

And by the definition of bad, $\forall\ i$:

$$\begin{aligned}
\Pr\left[A \text{ succeeds} \mid x_i \text{ is bad}\right] &\leq m \cdot \Pr\left[C(f(x_i)) \neq \perp \mid x_i \text{ is bad}\right] \\
&< m \cdot \frac{1}{2m^2 p(n)} = \frac{1}{2mp(n)}
\end{aligned}$$

Thus, the first term is bounded by:

$$\begin{aligned}
\Pr\left[(A \text{ succeeds}) \cap (\exists i \text{ st } x_i \text{ is bad})\right] &\leq \sum_{i=1}^{m} \Pr\left[A \text{ succeeds} \mid x_i \text{ is bad}\right] \\
&< m \cdot \frac{1}{2mp(n)} = \frac{1}{2p(n)}
\end{aligned}$$

Now let's consider the second term:

$$\begin{aligned}
\Pr\left[(A \text{ succeeds}) \cap (\forall\ i,\ x_i \text{ is good})\right] &\leq \Pr\left[\forall\ i,\ x_i \text{ is good}\right] \\
&\leq \left(1 - \frac{1}{2q(n)}\right)^{2q(n)n} \\
&< e^{-n} < 2^{-n}
\end{aligned}$$

Thus, we get:

$$\Pr\left[A(f(x_1, \ldots, x_m)) \text{ succeeds}\right] < \frac{1}{2p(n)} + 2^{-n} < \frac{1}{p(n)}$$

This contradicts the definition of p. Therefore, there are at least $2^n\left(1 - \frac{1}{2q(n)}\right)$ good elements. Hence, lemma 3 applies, and we still get a contradiction. Therefore, f' is a strong OWF, as desired. $\square$