CS 6222 Graduate Cryptography September 25, 2025

Lecture 10: Hardness Amplification for OWFs

Lecturer: Jack Doerner *Scribe: Andrew Parkinson*

1 Topics Covered

- Review of Definitions
- Weak OWFs Imply Strong OWFs

2 Review of Definitions

Definition 1 (Strong One-Way Function)**.** *A function $f : \{0,1\}^* \to \{0,1\}^*$ is a strong OWF if*

1. *f is PPT*
2. *For all NUPPT $\mathcal{A}$, $\exists$ a negligable function ε, s.t. $\forall\ n \in \mathbb{N}$*

$$\Pr[f(x') = f(x) : x \leftarrow \{0,1\}^n, x' \leftarrow \mathcal{A}(1^n, f(x))] < \varepsilon(n)$$

Definition 2 (μ-Weak OWF)**.** *A function $f : \{0,1\}^* \to \{0,1\}^*$ is a weak OWF if*

1. *f is a PPT*
2. *$\exists$ a polynomial μ s.t. $\forall$ NUPPT $\mathcal{A}$, $\exists n_0 \in \mathbb{N}$ s.t. $\forall n > n_0$*

$$\Pr[f(x') = f(x) : x \leftarrow \{0,1\}^n, x' \leftarrow \mathcal{A}(1^n, f(x))] < 1 - \frac{1}{\mu(n)}$$

Note that the above definitions do not insist that $x' = x$. Multiple preimages of $f(x)$ might exist if f is not one-to-one, and the adversary wins the games if it finds any such pre-image.

3 Weak OWFs Imply Strong OWFs

Theorem 1 (OWF Hardness Amplification Theorem)**.** *For every weak OWF $f : \{0,1\}^n \to \{0,1\}^*$, $\exists$ some polynomial m s.t. if we define a function $f' : \{0,1\}^{n \cdot m(n)} \to \{0,1\}^*$ s.t.*

$$f' : (x_1, ..., x_{m(n)}) \mapsto (f(x_1), ..., f(x_{m(n)})$$

then f' is a strong OWF. If f is μ-weak for some polynomial μ, then it is sufficient to set $m(n) = 2n \cdot \mu(n)$.

We will give an intuitive overview before proving the above theorem formally. We need to construct a reduction $\mathcal{R}$ that inverts f w.p. $\geq 1 - \frac{1}{\mu(n)}$. given some $\mathcal{A}'$ that inverts f' with non-negligable probability. $\mathcal{R}$ receives a single OWF image y from the weak-OWF game, and must construct an instance $\vec{y}$ of the strong OWF game for f', and then uses $\mathcal{A}'$ to invert $\vec{y}$.

Notice that in the strong OWF game for f', the probability that any fixed location in $\vec{y}$ will contain a biprime[1] is noticeable but not overwhelming. This implies that it's possible for $\mathcal{A}'$ to invert $\vec{y}$ with noticeable probability while also *never* factoring biprimes that appear in any fixed location in $\vec{y}$, and consequently our reduction $\mathcal{R}$ cannot embed y in any fixed location.

Instead, $\mathcal{R}$ will sample a random position i, and embed y there (being careful to preserve the distribution of values at that position). At all other positions, we will sample random values a distribution to match those sampled in the strong OWF game for f'.

Proof of Theorem 1. We will prove the contrapositive statement. Suppose that there exists some adversary $\mathcal{A}'$ that violates the strong OWF property of f'. We will construct a reduction that uses $\mathcal{A}'$ to violate the μ-weak OWF property of f.

Let p' be a polynomial, let $p(n) = p'(n \cdot m(n)) = p'(2n^2 \cdot \mu(n))$, and let $\mathcal{A}'$ be a NUPPT adversary such that for infinitely many $n \in \mathbb{N}$ we have

$$\Pr[f'(\mathcal{A}'(1^{n \cdot m(n)}, \vec{y})) = \vec{y} : \vec{x} \leftarrow \{0,1\}^{n \cdot m(n)}, \vec{y} := f'(x)] > \frac{1}{p'(n \cdot m(n)} = \frac{1}{p(n)}.$$

We first specify a "base-case" reduction that can be called repeatedly:

Construction 1 $(\mathcal{R}_0(1^n, y))$**.**

1. $i \leftarrow [m(n)], y_i := y$
2. $\forall j \in [m(n)] \setminus \{i\}$, $x_j \leftarrow \{0,1\}^n, y_j := f(x_j)$
3. *let* $\vec{z} \leftarrow \mathcal{A}'(1^{n \cdot m(n)}, \vec{y})$
4. *Output* z_i *if* $f(z_i) = y$*; otherwise output* $\perp$

For some polynomial q we define a set of "good" inputs $G_n \subseteq \{0,1\}^n$ s.t.

$$G_n = \left\{ x \in \{0,1\}^n : \Pr[\mathcal{R}_0(1^n, f(x)) = \perp] < 1 - \frac{1}{q(n)} \right\} \tag{1}$$

And then we define the full reduction $\mathcal{R}(1^n, y)$ to call $n \cdot q(n)$ instances of $\mathcal{R}_0(1^n, y)$, and output the first non-$\perp$ result. If all $n \cdot q(n)$ instances of $\mathcal{R}_0$ output $\perp$, then $\mathcal{R}$ does too.

We will argue that there is a way to set q such that G_n is big enough that there is a non-negligible chance that a random input is in it, and the probability that $\mathcal{R}$ inverts the image of that input is also non-negligible.

We begin with a few inequalities that do not depend upon the value of q. Recall that $\mathcal{R}$ only outputs $\perp$ if all of its internal calls to $\mathcal{R}_0$ output $\perp$. Thus we have

$$\Pr[(\mathcal{R}(1^n, f(x)) = \perp \mid x \in G_n : x \leftarrow \{0,1\}^n] < \left(1 - \frac{1}{q(n)}\right)^{n \cdot q(n)} < e^{-n}$$

[1] A biprime is simply the product of two primes.

for infinitely many $n \in \mathbb{N}$, and we can use this to compute a general upper bound on the probability that $\mathcal{R}$ fails in the strong OWF game. For infinitely many $n \in \mathbb{N}$

$$\begin{aligned}\Pr[\mathcal{R}(1^n, f(x)) = \perp : x \leftarrow \{0,1\}^n] &= \Pr_x[\mathcal{R}(1^n, f(x)) = \perp \mid x \in G_n] \cdot \Pr_x[x \in G_n] \\ &\quad + \Pr_x[\mathcal{R}(1^n, f(x)) = \perp \mid x \notin G_n] \cdot \Pr_x[x \notin G_n] \\ &< e^{-n} + \Pr_x[x \notin G_n]\end{aligned}$$

The above equation is an upper bound on failure probability. The next claim follows easily:

Claim 1. *f is not a μ-weak OWF if $\exists n_0 \in \mathbb{N}$ s.t. $\forall n \geq n_0$*

$$e^{-n} + \Pr_x[x \notin G_n] \leq \frac{1}{\mu(n)}$$

Now we observe that for any polynomial μ, $\exists n_0 \in \mathbb{N}$ s.t. $\forall n \geq n_0$

$$e^{-n} + \Pr_x[x \notin G_n] \leq e^{-n} + \frac{1}{2\mu(n)} \leq \frac{1}{\mu(n)}$$

and thus we have:

Claim 2. *f is not a μ-weak OWF if*

$$|G_n| \geq 2^n \cdot \left(1 - \frac{1}{2\mu(n)}\right).$$

Finally, we are ready to specify a particular polynomial q.

Claim 3. *If $q(n) = 2m^2(n) \cdot p(n) = 8n^2 \cdot \mu^2(n) \cdot p'(2n^2 \cdot \mu(n))$, then $|G_n| \geq 2^n \cdot \left(1 - \frac{1}{2\mu(n)}\right)$, and f is not a μ-weak OWF.*

Proof of Claim 3. We will prove that if

$$q(n) = 2m^2(n) \cdot p(n) \qquad \text{and} \qquad |G_n| < 2^n \cdot \left(1 - \frac{1}{2\mu(n)}\right)$$

then f' must be a strong OWF, contradicting our assumption that there exists some NUPPT $\mathcal{A}'$ that inverts f' with probability greater than $1/p(n)$ for some polynomial p. We will begin by giving a name to the event that $\mathcal{A}'$ that inverts f', and partitioning that event into two two sub-events that correspond to inverting f' on inputs that are or are not "good" ones, as defined by Equation 1. We have:

$$\begin{aligned}\Pr_{\vec{x}}[\underbrace{f'(\mathcal{A}'(1^{n \cdot m(n)}, \vec{y})) = \vec{y} : \vec{y} := f'(\vec{x})}_{\text{"}\mathcal{A}' \text{ Succeeds"}}] &= \Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds } \wedge \exists i \in [m(n)] \text{ s.t. } x_i \notin G_n] \\ &\quad + \Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds } \wedge \forall i \in [m(n)],\ x_i \in G_n]\end{aligned} \tag{2}$$

We will bound the two terms on the right hand side of the above equation using the next two claims.

Claim 3A. $\Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds } \wedge \exists i \text{ s.t } x_i \notin G_n] < 1/2p(n)$

Proof. We have

$$\begin{aligned}
&\Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds } \wedge \exists i \text{ s.t } x_i \notin G_n] \\
&\leq \sum_{j \in [m(n)]} \Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds } \wedge x_j \notin G_n] \\
&\leq \sum_{j \in [m(n)]} \Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds } \mid x_j \notin G_n] \\
&\leq \sum_{j \in [m(n)]} m(n) \cdot \Pr_{x}[\mathcal{R}_0(f(x) \neq \perp \mid x \notin G_n] \qquad (3) \\
&< \sum_{j \in [m(n)]} m(n) \cdot \frac{1}{q(n)} \qquad (4) \\
&= \frac{m^2(n)}{2m^2(n) \cdot p(n)} = \frac{1}{2p(n)}
\end{aligned}$$

where Equation 3 follows from the fact that $\mathcal{R}_0$ calls $\mathcal{A}'$ internally, and it has a $1/m(n)$ chance of guessing the correct value of j when constructing the instance $\vec{y}$ that it gives to $\mathcal{A}'$ as input, and where Equation 4 follows from Equation 1. □

Claim 3B. $\Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds } \wedge \forall i \in [m(n)], x_i \in G_n] < e^{-n}$

Proof. We have

$$\begin{aligned}
&\Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds } \wedge \forall i \in [m(n)], x_i \in G_n] \\
&\leq \Pr_{\vec{x}}[\forall i \in [m(n)], x_i \in G_n] \\
&< \left(1 - \frac{1}{2\mu(n)}\right)^{m(n)} \qquad (5) \\
&= \left(1 - \frac{1}{2\mu(n)}\right)^{2n \cdot \mu(n)} < e^{-n}
\end{aligned}$$

where Equation 5 follows from the assumption toward contradiction at the beginning of our proof of Claim 3 that

$$|G_n| < 2^n \cdot \left(1 - \frac{1}{2\mu(n)}\right)$$ □

Now we can plug Claims 3A and 3B into Equation 2, and we see that

$$\Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds}] < \frac{1}{2p(n)} + \frac{1}{e^n}.$$

It remains only to observe that since p is a polynomial, we have

$$\exists n_0 \in \mathbb{N} \text{ s.t. } \forall n \geq n_0 \Pr_{\vec{x}}[\mathcal{A}' \text{ Succeeds}] < \frac{1}{p(n)}$$

which contradicts our assumption (at the beginning of the proof of Claim 3) that $\mathcal{A}'$ inverts f' with probability greater than $1/p(n)$. Thus it must be the case that relative to the $\mathcal{A}'$, p, and q we have specified,

$$|G_n| \geq 2^n \cdot \left(1 - \frac{1}{2\mu(n)}\right)$$

and by Claim 2, it follows that f is not a μ-weak OWF. □

Note that the choice of q is free—the upper bound on $\mathcal{R}$'s failure probability depends upon it, but nothing in the construction f' does. Claim 3 shows simply that there exists a q such that G_n has the properties we need; it follows that if f' is not a strong OWF, then f is not a weak OWF. □