COMS 4261: Introduction to Cryptography	Oct. 10, 2014

Hybrid Arguments

Instructor: *Tal Malkin* Scribe: *Yuan Kang*

1 General Method

Suppose you have two oracles, or input distributions, $\mathcal{O}_0, \mathcal{O}_1$, and you want to prove that they're indistinguishable, *i.e.* for every probabilistic, polynomial-time (PPT) distinguisher, $\mathcal{D}$, the following must hold:

$$|\Pr[\mathcal{D}^{\mathcal{O}_1} = 1] - \Pr[\mathcal{D}^{\mathcal{O}_0} = 1]| \quad = \quad negl.$$

(Note that we are treating $\mathcal{O}_0, \mathcal{O}_1$ as oracles. But treating them as inputs just requires a change in notation to $\mathcal{D}(\mathcal{O}_0), \mathcal{D}(\mathcal{O}_1)$).

What do you do if you don't have any single assumption or theorem from which you can reduce?

The hybrid argument lets you take multiple steps, using the triangle inequality:

1. Define a polynomial set of hybrids. In other words, let $q(n)$ be a polynomial function of the security parameter, and you have hybrid oracles or input distributions, $\mathcal{H}_i$, for all $i \in \{0, 1, 2, \ldots, q(n)\}$, where $\mathcal{H}_0 = \mathcal{O}_0$, and $\mathcal{H}_{q(n)} = \mathcal{O}_1$. You want to choose hybrids $\mathcal{H}_i$ for $i \in \{1, 2, \ldots, q(n) - 1\}$ to be indistinguishable, intermediate steps between $\mathcal{O}_0$ and $\mathcal{O}_1$.

2. State that, according to the triangle inequality, as illustrated in Figure 1, the following is true:

$$|\Pr[\mathcal{D}^{\mathcal{O}_1} = 1] - \Pr[\mathcal{D}^{\mathcal{O}_0} = 1]| \quad \leq \quad \sum_{i=1}^{q(n)} |\Pr[\mathcal{D}^{\mathcal{H}_i}] - \Pr[\mathcal{D}^{\mathcal{H}_{i-1}}]|$$

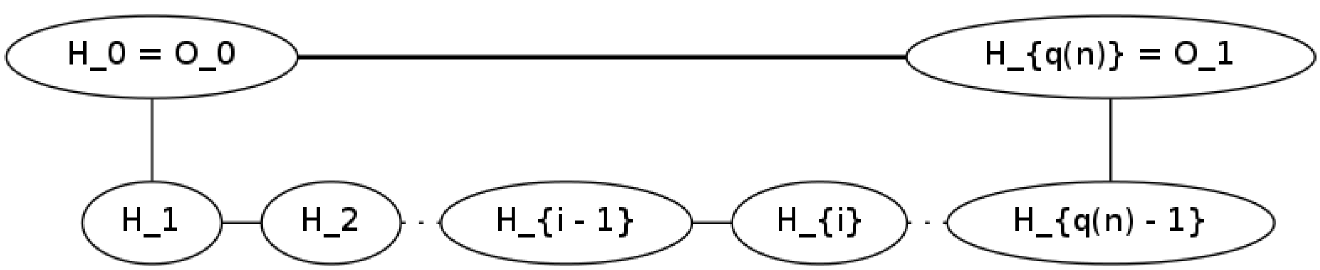

Figure 1: The triangle inequality applied to the general hybrid argument.

It therefore suffices to show that every $\mathcal{H}_{i-1}$ and $\mathcal{H}_i$ are indistinguishable.

3. For each $i \in \{1, 2, \ldots, q(n)\}$, prove, using reduction or a probabilistic argument, that $\mathcal{H}_{i-1}$ and $\mathcal{H}_i$ are indistinguishable, *i.e.* , that for every PPT distinguisher, $\mathcal{D}$:

   $$|\Pr[\mathcal{D}^{\mathcal{H}_i}] - \Pr[\mathcal{D}^{\mathcal{H}_{i-1}}]| \quad = \quad negl.$$

   Sometimes there are a few steps that you have to prove manually one-by-one; sometimes you can use the same argument for several steps.

4. Finally, by the previous two steps, we know that:

   $$\begin{aligned} |\Pr[\mathcal{D}^{\mathcal{O}_1} = 1] - \Pr[\mathcal{D}^{\mathcal{O}_0} = 1]| &\leq \sum_{i=1}^{q(n)} negl. \\ &= q(n) \times negl. \\ &\quad \text{Since } q(n) \text{ is a polynomial} \\ &= negl. \end{aligned}$$

This completes the proof

Example 1. *You want to show that, for a PRG G, $G'(s) = G(G(s))$ is also a PRG. In other words, you want to show that for every PPT distinguisher, $\mathcal{D}$:*

$$|\Pr_s[\mathcal{D}(G(G(s))) = 1] - \Pr_{r'}[\mathcal{D}(r') = 1]| \quad = \quad negl.$$

If you directly tried to prove by reduction from the PRG property of G, your distinguisher would be given some x, that is either $G(s)$ or some random r. Following the structure of the construction of G', you could try something like $G(x)$, and give it to the assumed distinguisher against G'. Now you have two cases:

- *$x = G(s)$: you would generate $G(G(s)) = G'(s)$. So far, so good.*
- *$x = r$: you would generate $G(r)$. But the assumed algorithm is supposed to distinguish between $G'(s)$ and some random r' – not some pseudorandom $G(r)$! Fortunately, we've just stumbled across a step in the hybrid proof, which we will show.*

Proof. We define a hybrid, $G(r)$, for some random r.

Therefore, by the triangle inequality, as shown in Figure 2, for every PPT distinguisher, $\mathcal{D}$:

$$\begin{aligned} |\Pr_s[\mathcal{D}(G(G(s))) = 1] - \Pr_{r'}[\mathcal{D}(r') = 1]| \quad &\leq \quad |\Pr_s[\mathcal{D}(G(G(s))) = 1] - \Pr_r[\mathcal{D}(G(r)) = 1]| \\ &\quad + |\Pr_r[\mathcal{D}(G(r)) = 1] - \Pr_{r'}[\mathcal{D}(r') = 1]| \end{aligned}$$

Next, we prove the indistinguishability between the hybrids:

1. $G(G(s))$ is indistinguishable from $G(r)$, for some random r.

   We do so by reduction from the PRG property of G. Assume that $G(G(s))$ is not indistinguishable from $G(r)$. Then we have a PPT distinguisher, $\mathcal{D}$, so that:

   $$|\Pr_s[\mathcal{D}(G(G(s))) = 1] - \Pr_r[\mathcal{D}(G(r)) = 1]| \quad > \quad nonnegl.$$

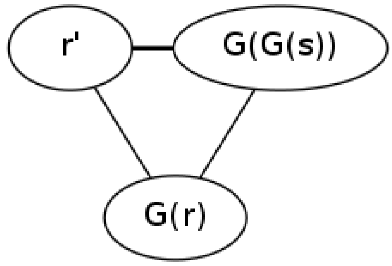

Figure 2: The triangle inequality applied to $G'(s) = G(G(s))$.

Then we define the following PPT distinguisher, $\mathcal{D}_0$, against G: Given input x, return $\mathcal{D}(G(x))$. Since we are playing the PRG game, we have two cases:

(a) $x = G(s)$: $\mathcal{D}_0(x)$ would generate $G(G(s)) = G'(s)$, and return $\mathcal{D}(G(G(s)))$.

(b) $x = r$: $\mathcal{D}_0(x)$ would generate $G(r)$, and return $\mathcal{D}(G(r))$.

So the advantage of $\mathcal{D}_0$ is:

$$\begin{aligned} |\Pr_s[\mathcal{D}_0(G(s)) = 1] - \Pr_r[\mathcal{D}_0(r) = 1]| &= |\Pr_s[\mathcal{D}(G(G(s))) = 1] - \Pr_r[\mathcal{D}(G(r)) = 1]| \\ &> \mathit{nonnegl.} \end{aligned}$$

This contradicts the PRG property of G, so $G(G(s))$ must be indistinguishable from $G(r)$, completing this mini reduction.

2. $G(r)$ is indistinguishable from a random r' by the PRG property.

By the previous steps, we know that:

$$|\Pr_s[\mathcal{D}(G(G(s))) = 1] - \Pr_{r'}[\mathcal{D}(r') = 1]| \quad \leq \quad \mathit{negl.} + \mathit{negl.} = \mathit{negl.}$$

Thus completing the proof. □

We could explicitly relate this proof to the parts of the general hybrid method:

- $q(n) = 2$
- $\mathcal{H}_0 = \mathcal{O}_0 = r'$, *although here they are treated as inputs.*
- $\mathcal{H}_1 = G(r)$
- $\mathcal{H}_2 = \mathcal{O}_1 = G(G(s))$