2201-COL759
IIT Delhi — Lecture 6 — Venkata K

1 Last Lecture

In the last lecture, we first outlined the *hybrid technique* for proving security, then introduced pseudorandom generators, and finally saw a construction of an encryption scheme $\mathcal{E}_G$ (with key space much smaller than message space), using a pseudorandom generator G. Today, we will complete our discussion on the hybrid technique, and present a proof outline for showing that $\mathcal{E}_G$ is secure (assuming G is a secure PRG).

1.1 Questions/clarifications from last class

- *Suppose the security parameter is n. Then does that fix the input space of the pseudorandom generator to be $\{0,1\}^n$? Or, in the case of encryption schemes, does the key space need to be $\{0,1\}^n$?*

  No, this need not be the case. In the case of pseudorandom generators, if the security parameter is n, the input space can be $\{0,1\}^{p(n)}$ where $p(\cdot)$ is some fixed polynomial. Strictly speaking, for every n, we have a different function $G_n : \{0,1\}^{p(n)} \to \{0,1\}^{\ell(n)}$ where G_n is efficiently implementable, $p(\cdot)$ and $\ell(\cdot)$ are fixed polynomials s.t. $\ell(n) > p(n)$. For example, in the case of our sample assignment solution, we had set the input space to be $\{0,1\}^{2n}$ and output space $\{0,1\}^{3n}$.

2 The Hybrid Proof Technique

The hybrid proof technique is one of the key takeaways from this couse. We will see this technique via a toy problem. Before we see an example of this proof technique, let us step back and understand why we need this technique.

Qn: Why do we use the hybrid proof technique?

Ans: In most of our cryptographic constructions, we will use one/more building blocks, and 'compose' the building blocks for the final construction. For instance, in Question 04.02 from Lecture 04, we had an encryption scheme $\mathcal{E}'$ built using a base encryption scheme $\mathcal{E}$. How can we prove that the construction is secure, assuming the building blocks are secure? In other words, suppose there is an adversary that breaks our construction. We want to use this adversary to break one of the building blocks. The hybrid technique enables us to do this — translate the adversary against our construction to an adversary against one of the building blocks.

2.1 Question 04.02 from Lecture 04

> **Question 04.02.** Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme that satisfies Definition 04.02. Consider the following modified encryption scheme $(\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Dec}')$:
>
> - KeyGen' = Run KeyGen twice, and let k_1, k_2 be the two output keys. Output $k = (k_1, k_2)$ as the key.
> - $\mathsf{Enc}'(m, k = (k_1, k_2)) = (\mathsf{Enc}(m, k_1), \mathsf{Enc}(m, k_2))$
> - $\mathsf{Dec}'(\mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2), k = (k_1, k_2)) = \mathsf{Dec}(\mathsf{ct}_1, k_1)$
>
> Show that $\mathcal{E}'$ satisfies Definition 04.02, assuming $\mathcal{E}$ does.

Suppose there exists an adversary $\mathcal{A}$ that can break the security of $\mathcal{E}'$. We want to show an adversary that breaks the security of $\mathcal{E}$. *More generally, suppose we build a crypto primitive using many different building blocks, and suppose there is an adversary that breaks the security of the crypto primitive. Then we want to show an adversary that breaks one of the building blocks.*

2.1.1 Attempts from last class

Let us assume the adversary is a near-perfect adversary — it can distinguish between $\mathsf{Enc}'(m_0, (k_1, k_2))$ and $\mathsf{Enc}'(m_1, (k_1, k_2))$, and win the No-Query-Semantic-Security game with probability close to 1.

Attempt 1: Reduction algorithm receives a ciphertext from the challenger, and sends two copies of the ciphertext to $\mathcal{A}$. Note that this adversary is indeed receiving a 'valid ciphertext' — both components are either encryptions of m_0, or encryptions of m_1. However, this ciphertext is coming from a very different distribution, and as a result, our reduction algorithm is not guaranteed to win against $\mathcal{E}$, even though there exists an adversary that can win the security game against $\mathcal{E}'$ with probability close to 1.

Suppose there exists an adversary that is (somehow) able to decrypt the ciphertext. It outputs 0 or 1 accordingly (in the security game), except when both the ciphertext components are identical — in this case, the adversary simply outputs 0. As a result, this is a near-perfect adversary, but if the reduction algorithm uses this adversary, it will not win the security game against $\mathcal{E}$.

Attempt 2: In this attempt, the reduction algorithm receives a ciphertext from the challenger, and puts it in the first slot. For the second slot, it picks a uniformly random key $\tilde{k}$, a uniformly random bit $\tilde{b}$, and puts $\mathsf{Enc}(m_{\tilde{b}}, \tilde{k})$. The reduction algorithm receives a bit b' from the adversary, and depending on whether $b' = \tilde{b}$ or not, it sends something to the $\mathcal{E}$-challenger. Consider the following adversary: it is (somehow) able to decrypt the second component of the ciphertext, and uses this component only to determine its output. Note that this adversary wins the security game against $\mathcal{E}'$ with probability 1. However, the reduction algorithm will not be able to use this adversary (since the adversary is not even looking at the first component of the ciphertext).

2.1.2 The Two World Formulation

Last class, we discussed the 'two world' formulation of adversary's winning advantage. As discussed before, this is just another (equivalent) definition for No-Query-Semantic-Security. There are two worlds — world-0 and world-1. In both worlds, the adversary first sends two messages m_0, m_1. In world-0 (resp. world-1), the adversary receives an encryption of m_0 (resp. m_1). Finally, after receiving the challenge ciphertext, it sends a bit b'. We say that the encryption scheme is secure if the adversary's behaviour is similar in both worlds. In particular, the probability of the adversary outputting 0 is nearly same in both worlds.

Qn: In the two worlds, the adversary sends b'. What does this bit signify?

Ans: In the bit-guessing definition (Definition 04.02), the bit b' was the adversary's guess (the adversary was trying to guess whether the challenger encrypted m_0 or m_1). However, in the two-worlds formulation, I find it more convenient to avoid attaching any 'semantics' to the adversary's final output b'. Instead, it might be easier to just think of b' as the adversary's behaviour after seeing a ciphertext. From Claim 05.01, it follows that an adversary wins the bit-guessing game with probability $1/2 + \epsilon$ **if and only if** the adversary's probability of outputting 0 in the two worlds differ by 2ϵ.

Qn: Why do we only consider $\Pr\left[\mathcal{A} \text{ outputs } 0\right]$ in both the worlds?

Ans: Since $\Pr\left[\mathcal{A} \text{ outputs } 1\right] = 1 - \Pr\left[\mathcal{A} \text{ outputs } 0\right]$, if the probabilities of output being 0 are close in both the worlds, the probabilities of output being 1 will also be close in the two worlds.

Depending on which formulation is more convenient, we will either use the bit-guessing based definition, or the two-worlds definition. Let us use the two-worlds formulation for proving security of $\mathcal{E}'$.

Since $\mathcal{A}$ breaks $\mathcal{E}'$, there exists a non-negligible function ϵ such that $p_0 - p_1 = \epsilon$,[1] where p_0 (resp. p_1) is the probability of $\mathcal{A}$ outputting 0 in *world 0* (resp. *world 1*). Recall, we also defined a *hybrid world*, and p_{hyb} is the probability of $\mathcal{A}$ outputting 0 in the hybrid world.

[1] An astute reader would observe that I've not considered the absolute value of $p_0 - p_1$ here. This is just to keep the analysis slightly simpler. If indeed our adversary was such that $p_0 < p_1$ and $|p_0 - p_1|$ is non-negligible, then one can show that the resulting reduction algorithm would have winning probability p s.t. $|p - 1/2|$ is non-negligible.

World 0:

1. $\mathcal{A}$ sends m_0, m_1.
2. Chall. chooses k_1, k_2, sends $\Big(\mathsf{Enc}(m_0, k_1), \mathsf{Enc}(m_0, k_1)\Big)$.
3. $\mathcal{A}$ outputs b'.

$$\Pr\Big[\mathcal{A} \text{ outputs } 0\Big] = p_0$$

Hybrid World:

1. $\mathcal{A}$ sends m_0, m_1.
2. Chall. chooses k_1, k_2, sends $\Big(\mathsf{Enc}(m_0, k_1),\ \underline{\mathsf{Enc}(m_1, k_1)}\Big)$.
3. $\mathcal{A}$ outputs b'.

$$\Pr\Big[\mathcal{A} \text{ outputs } 0\Big] = p_{\text{hyb}}$$

World 1:

1. $\mathcal{A}$ sends m_0, m_1.
2. Chall. chooses k_1, k_2, sends $\Big(\underline{\mathsf{Enc}(m_1, k_1)},\ \underline{\mathsf{Enc}(m_1, k_1)}\Big)$.
3. $\mathcal{A}$ outputs b'.

$$\Pr\Big[\mathcal{A} \text{ outputs } 0\Big] = p_0$$

Qn: What does the hybrid world signify? And what about the bit b' that the adversary sends at the end?

Ans: Before we ask about the significance of the hybrid world, let us understand what the two worlds (world-0 and world-1) signify. The two worlds are just part of the definition to capture the intuition that the behaviour of adversary does not change depending on whether it got an encryption of m_0 or m_1. Sometimes, it may be hard to directly prove that the two worlds are indistinguishable, since there could be many changing components across the two worlds. Therefore, to 'bridge' the gap, we introduce a few hybrid worlds. As we go from one hybrid world to the next, there is only one change, and this will allow us to argue that the consecutive hybrid worlds are indistinguishable. Once we do that, we can conclude that the two worlds are also indistinguishable. Also, if we don't attach any semantics to b' in world-0/world-1 (and instead think of it as a summary of the adversary's view after seeing the ciphertext), then there's no need to attach any meaning to b' in the hybrid world.

Since $p_0 - p_1 = \epsilon$, either $p_0 - p_{\text{hyb}} \geq \epsilon/2$, or $p_{\text{hyb}} - p_1 \geq \epsilon/2$ (by triangle inequality). Therefore, either $p_0 - p_{\text{hyb}}$ is non-negligible, or $p_{\text{hyb}} - p_1$ is non-negligible. In each of these cases, we have an adversary that can break the security of $\mathcal{E}$ (which we prove below). At the end of this section, we will present a unified reduction that breaks security of $\mathcal{E}$ with non-negligible advantage. To build intuition, let us consider these two cases separately in the following claims.

Claim 06.01. Suppose there exists a prob. poly. time adversary $\mathcal{A}$ and a non-negligible function ϵ s.t. $p_0 - p_{\text{hyb}} = \eta$, where p_0 (resp. p_{hyb}) is the probability of $\mathcal{A}$ outputting 0 in world 0 (resp. hybrid world). Then there exists a prob. poly. time algorithm $\mathcal{B}$ that wins the No-Query-Semantic-Security against $\mathcal{E}$ with probability η.

Proof. The reduction algorithm $\mathcal{B}$ interacts with the adversary $\mathcal{A}$, and the challenger for $\mathcal{E}$. It receives two messages m_0, m_1, which it forwards to the challenger. The challenger sends a ciphertext ct^*. The reduction algorithm then chooses a uniformly random key $k_1 \leftarrow \mathcal{K}$, computes $\mathsf{ct}_1 = \mathsf{Enc}(m_0, k_1)$, sets $\mathsf{ct}_2 = \mathsf{ct}^*$, and sends $(\mathsf{ct}_1, \mathsf{ct}_2)$ to $\mathcal{A}$. The adversary sends bit b', which the reduction algorithm forwards to the challenger.

Let us now analyse $\mathcal{B}'s$ success probability.

$$\begin{aligned}
&\Pr\Big[\mathcal{B} \text{ wins the } \textsf{No-Query-Semantic-Security} \text{ game w.r.t } \mathcal{E}\Big]\\
=&\Pr\Big[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 0\Big] \cdot \Pr\Big[\text{Challenger chose } b = 0\Big]\\
&+ \Pr\Big[\mathcal{B} \text{ outputs } 1 \mid \text{Challenger chose } b = 1\Big] \cdot \Pr\Big[\text{Challenger chose } b = 1\Big]\\
=&\Pr\Big[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 0\Big] \cdot \frac{1}{2} + \Big(1/2 - \Pr\Big[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 1\Big] \cdot \frac{1}{2}\Big)
\end{aligned}$$

Note that $\mathcal{B}$ simply forwards the output of $\mathcal{A}$, and if the challenger chose $b = 0$ (resp. $b = 1$), then it corresponds to world 0 (resp. hybrid world). Hence, $\Pr\Big[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 0\Big] = 0_0$, and $\Pr\left[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 1\right] = p_{\text{hyb}}$. Hence, the winning probability of $\mathcal{B}$ against the $\mathcal{E}$-challenger is $1/2 + (p_0 - p_{\text{hyb}}) = 1/2 + \eta$.

□

Claim 06.02. Suppose there exists a prob. poly. time adversary $\mathcal{A}$ and a non-negligible function ϵ s.t. $p_{\text{hyb}} - p_1 = \eta$, where p_1 (resp. p_{hyb}) is the probability of $\mathcal{A}$ outputting 0 in world 1 (resp. hybrid world). Then there exists a prob. poly. time algorithm $\mathcal{B}$ that wins the No-Query-Semantic-Security against $\mathcal{E}$ with probability η.

The proof of this is very similar to the proof of Claim 06.01.

Proof. The reduction algorithm $\mathcal{B}$ interacts with the adversary $\mathcal{A}$, and the challenger for $\mathcal{E}$. It receives two messages m_0, m_1, which it forwards to the challenger. The challenger sends a ciphertext ct^*. The reduction algorithm then chooses a uniformly random key $k_2 \leftarrow \mathcal{K}$, computes $\mathsf{ct}_2 = \mathsf{Enc}(m_1, k_2)$, sets $\mathsf{ct}_1 = \mathsf{ct}^*$, and sends $(\mathsf{ct}_1, \mathsf{ct}_2)$ to $\mathcal{A}$. The adversary sends bit b', which the reduction algorithm forwards to the challenger.

Let us now analyse $\mathcal{B}'s$ success probability.

$$\begin{aligned}
&\Pr\left[\mathcal{B} \text{ wins the } \textsf{No-Query-Semantic-Security} \text{ game w.r.t } \mathcal{E}\right] \\
=&\Pr\left[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 0\right] \cdot \Pr\left[\text{Challenger chose } b = 0\right] \\
&+ \Pr\left[\mathcal{B} \text{ outputs } 1 \mid \text{Challenger chose } b = 1\right] \cdot \Pr\left[\text{Challenger chose } b = 1\right] \\
=&\Pr\left[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 0\right] \cdot \frac{1}{2} + \left(1/2 - \Pr\left[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 1\right] \cdot \frac{1}{2}\right)
\end{aligned}$$

Note that $\mathcal{B}$ simply forwards the output of $\mathcal{A}$, and if the challenger chose $b = 0$ (resp. $b = 1$), then it corresponds to hybrid world (resp. world-1). Hence, $\Pr\left[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 0\right] = p_{\text{hyb}}$, and $\Pr\left[\mathcal{B} \text{ outputs } 0 \mid \text{Challenger chose } b = 1\right] = p_1$. Hence, the winning probability of $\mathcal{B}$ against the $\mathcal{E}$-challenger is $1/2 + (p_{\text{hyb}} - p_1)/2 = 1/2 + \eta$.

□

Putting things together: Suppose there exists an adversary that can break security of $\mathcal{E}'$. Then, we know that $p_0 - p_1 = \epsilon$, for some non-negligible function ϵ. The reduction algorithm guesses with probability 1/2 whether $p_0 - p_{\text{hyb}}$ is large, or whether $p_{\text{hyb}} - p_1$ is large. Accordingly, it either follows the reduction in Claim 06.01, or it follows the reduction in Claim 06.02. You should check that the overall winning probability of $\mathcal{B}$ is $1/2 \cdot$ (winning prob. from Claim 06.01) + $1/2 \cdot$ (winning prob. from Claim 06.02), and this adds up to $1/2 + (p_0 - p_1)/2$.

Qn: In class, we discussed that it is possible for $\mathcal{B}$ to estimate p_0, p_1 and p_{hyb}, and use this estimate to determine whether to use Claim 06.01 or Claim 06.02. How is such estimation possible?

Ans: I had mentioned that it is fine to assume that p_0, p_1, p_{hyb} are known in advance. This was primarily to simplify our discussion in class (knowing these quantities allows you to know which Claim to use). However, as outlined above, knowing p_0, p_1, p_{hyb} is not necessary. As far as estimating these quantities is concerned, this can be done if you have black-box access to the adversary where you can reset the adversary to its starting state. In case this comment does not make much sense, please feel free to ignore it, and either use the combined reduction algorithm described above, or simply assume that p_0, p_1, p_{hyb} are known.

Summary of the hybrid technique This proof technique is one of the key ideas that we'll see in this course, and one that'll show up quite often. Therefore, please spend some time understanding it (and ask questions on Piazza if something is not clear). The first two steps are fairly 'mechanical':

1. Take the contrapositive. The statement to prove is as follows: *If there exists an adversary that breaks our construction ($\mathcal{E}'$ in this case), then there exists an adversary that breaks one of the building blocks ($\mathcal{E}$ in this case).*
2. Use the 'two worlds' formulation: suppose there exists an adversary that breaks our construction. Then its probability p_0 of outputting 0 in 'world-0' must be significantly different from its probability p_1 of outputting 0 in 'world-1'.
3. Define one (or more) hybrid worlds. You should think of this as a 'thought experiment'. In each hybrid world, the adversary has some probability of outputting 0. Show that if this probability is significantly different from the probability in the previous hybrid, then that implies an attack on one of the building blocks.

The part that involves 'creativity' in security proofs is defining the hybrid worlds. In our case, it was fairly simple. However, as we will proceed with the course, we will encounter more complex proofs via this technique.

Here are a couple of questions to think about:

- Consider the encryption scheme given below (Question 06.01). Use the hybrid technique to prove security here.

Question 06.01. Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme that satisfies Definition 04.02. Consider the following nested encryption scheme $(\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Dec}')$:

- KeyGen' = Run KeyGen twice, and let k_1, k_2 be the two output keys. Output $k = (k_1, k_2)$ as the key.
- $\mathsf{Enc}'(m, k = (k_1, k_2)) = \mathsf{Enc}\Big(\mathsf{Enc}(m, k_1), k_2\Big)$
- $\mathsf{Dec}'(\mathsf{ct}, k = (k_1, k_2)) = \mathsf{Dec}\Big(\mathsf{Dec}(\mathsf{ct}, k_2), k_1\Big)$

Show that $\mathcal{E}'$ satisfies Definition 04.02, assuming $\mathcal{E}$ does.

- Prove security of the following encryption scheme via the hybrid technique (Question 06.02). [2]

Question 06.02. Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme that satisfies Definition 04.02. Consider the following nested encryption scheme $(\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Dec}')$:

- KeyGen' = Run KeyGen thrice, and let k_1, k_2, k_3 be the three output keys. Output $k = (k_1, k_2, k_3)$ as the key.
- $\mathsf{Enc}'(m, k = (k_1, k_2, k_3)) = \mathsf{Enc}\Big(\mathsf{Enc}(m, k_1), \mathsf{Enc}(m, k_2), \mathsf{Enc}(m, k_3)\Big)$.
- $\mathsf{Dec}'(\mathsf{ct}, k = (k_1, k_2, k_3)) = \mathsf{Dec}(\mathsf{ct}_1, k_1)$

Show that $\mathcal{E}'$ satisfies Definition 04.02, assuming $\mathcal{E}$ does.

- When does the hybrid technique not work? For instance, consider the problem given below (Question 06.03). Why does the hybrid technique not work here?

Qn: If someone did not know the hybrid proof technique, what might have been their chain of thought?

Ans: I don't have a good answer to this (excellent) question. I can think of some proof strategies for this particular toy problem, but for more general cases (which we will encounter soon), I can't think of anything that doesn't involve some sort of hybrid worlds.

[2] Thanks to one of the students for this problem suggestion

Question 06.03. Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ be an encryption scheme that satisfies Definition 04.02. Consider the following modified encryption scheme $(\mathsf{KeyGen}', \mathsf{Enc}', \mathsf{Dec}')$:

- $\mathsf{KeyGen}' = \mathsf{KeyGen}$
- $\mathsf{Enc}'(m, k) = \Big(\mathsf{Enc}(m, k), \mathsf{Enc}(m, k \oplus 00\ldots01)\Big)$

  In words: the first component of the ciphertext is an encryption of m using key k. The second component is an encryption of m using key k' which is same as k, except that the last bit of k is flipped.
- $\mathsf{Dec}'(\mathsf{ct} = (\mathsf{ct}_1, \mathsf{ct}_2), k) = \mathsf{Dec}(\mathsf{ct}_1, k)$

Can we show that $\mathcal{E}'$ satisfies Definition 04.02, assuming $\mathcal{E}$ does?

3 $\mathcal{E}_G$ is a secure encryption scheme, assuming G is a secure PRG

Recall the encryption scheme $\mathcal{E}_G$ with key space $\mathcal{K} = \{0,1\}^n$, message and ciphertext space $\{0,1\}^\ell$. The construction uses a secure pseudorandom generator $G : \{0,1\}^n \to \{0,1\}^\ell$.

- $\mathsf{KeyGen}(1^n)$: chooses a uniformly random key $k \in \{0,1\}^n$
- $\mathsf{Enc}(m \in \mathcal{M}, k \in \mathcal{K}) = m \oplus G(k)$
- $\mathsf{Dec}(\mathsf{ct}, k) = \mathsf{ct} \oplus G(k)$

Claim 06.03. Suppose there exists a prob. poly. time adversary $\mathcal{A}$ and a non-negligible function ϵ such that $\mathcal{A}$ wins the No-Query-Semantic-Security game w.r.t $\mathcal{E}_G$ with probability $1/2 + \epsilon$. Then there exists a prob. poly. time adversry $\mathcal{B}$ that wins the PRG security game w.r.t. G with probability $1/2 + \epsilon_{\mathcal{B}}$, for some non-negligible function $\epsilon_{\mathcal{B}}$.

Proof. Again, we will work with the two worlds formulation, and we will define appropriate intermediate hybrid worlds. Let p_0 (resp. p_1) denote the probability of $\mathcal{A}$ outputting 0 in world 0 (resp. world 1).

World 0:

1. $\mathcal{A}$ sends m_0, m_1.
2. Chall. chooses $k \leftarrow \{0,1\}^n$, computes $r = G(k)$. It sends $m_0 \oplus r$.
3. $\mathcal{A}$ outputs b'.

$$\Pr\Big[\mathcal{A} \text{ outputs } 0\Big] = p_0$$

World 1:

1. $\mathcal{A}$ sends m_0, m_1.
2. Chall. chooses $k \leftarrow \{0,1\}^n$, computes $r = G(k)$. It sends $\underline{m_1 \oplus r}$.
3. $\mathcal{A}$ outputs b'.

$$\Pr\Big[\mathcal{A} \text{ outputs } 0\Big] = p_0$$

Next, we will define two hybrid worlds: hybrid-world-0, and hybrid-world-1. Hybrid-world-0 (resp. hybrid-world-1) is exactly identical to world-0 (resp. world-1), except that r is chosen uniformly at random (instead of being computed using key k).

Hybrid-World-0:

1. $\mathcal{A}$ sends m_0, m_1.
2. Chall. chooses $\underline{r \leftarrow \{0,1\}^\ell}$. It sends $m_0 \oplus r$.
3. $\mathcal{A}$ outputs b'.

$$\Pr\Big[\mathcal{A} \text{ outputs } 0\Big] = p_{\text{hyb},0}$$

Hybrid-World-1:

1. $\mathcal{A}$ sends m_0, m_1.
2. Chall. chooses $\underline{r \leftarrow \{0,1\}^\ell}$. It sends $m_1 \oplus r$.
3. $\mathcal{A}$ outputs b'.

$$\Pr\Big[\mathcal{A} \text{ outputs } 0\Big] = p_{\text{hyb},1}$$

First, note that $p_{\text{hyb},0} = p_{\text{hyb},1}$. This follows from the perfect secrecy of Shannon's One Time Pad. Since $p_0 - p_1 \geq \epsilon$, it follows that either $p_0 - p_{\text{hyb},0} \geq \epsilon/2$, or $p_1 - p_{\text{hyb},1} \geq \epsilon/2$. In both these cases, we have a reduction algorithm that breaks the PRG security with probability at least $1/2 + \epsilon/2$.

□

4 Additional Resources

Relevant sections from textbook [Boneh-Shoup]: Sections 3.2 discusses the security of $\mathcal{E}_G$.