Lecture 19: An Introduction to Simulation Argument

Recall

- Suppose we use a one-time pad encryption scheme to encrypt two n-bit messages (m, m') and send the ciphertexts
- Suppose the messages are (m, m')
- Eve's view is the joint distribution of ciphertexts is $(m + \mathsf{sk}, m' + \mathsf{sk})$, where $\mathsf{sk} \xleftarrow{\$} \{0,1\}^n$
- We had claimed earlier that Eve learns $(m - m')$
- Today we will learn to prove that: Eve *only* learns $(m - m')$

Intuition

- Suppose we want to claim that an adversary $\mathcal{A}$ learns only x in a cryptographic protocol
- Then we construct a randomized algorithm called *simulator* Sim that takes x as input and its output distribution is identical to $\mathcal{A}$'s view

What does it achieve: Suppose the adversary $\mathcal{A}$ employs a "knowledge extractor" E given its view V to extract some information. We can run the same "knowledge extractor" on the outputs of Sim(x) and obtain the same information.

This effectively proves that: Any knowledge obtainable from adversary's view can be obtained from x itself (by considering E running on the output of Sim(x))

Proving "Only $(m - m')$ is learned"

- Code of $\mathsf{Sim}(x)$, where $x = (m - m')$
  - Sample $r \xleftarrow{\$} \{0,1\}^n$
  - Output $(r, r - x)$

Prove: Output distribution is identical to Eve's view

Simulation-based Security

Let $\mathbb{V}_{\mathcal{A}}$ be the random variable for adversary's view and we want to claim that it can be simulated by only the knowledge of x:

- Perfect Security: $\mathsf{Sim}(x) \equiv \mathbb{V}_{\mathcal{A}}$ (Simulated view is identical to the adversarial view)
- Statistical Security: $\mathsf{Sim}(x) \approx_{\varepsilon} \mathbb{V}_{\mathcal{A}}$ (Simulated view is ε-close to the adversarial view)
- Computational Security: $\mathsf{Sim}(x) \approx_{\varepsilon}^{(c)} \mathbb{V}_{\mathcal{A}}$ and Sim is an efficient algorithm (Simulated view is computationally indistinguishable from the adversarial view)

Think

- Simulation-based security definitions of primitives like private-key encryption, public-key encryption, pseudorandomness