EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)

Lecture 5 — January 19, 2018

Instructor: Saravanan Vijayakumaran *Scribe: Saravanan Vijayakumaran*

1 Lecture Plan

- Proof that perfect adversarial indistinguishability is equivalent to perfect secrecy

2 Perfect adversarial indistinguishability

Lemma. *Encryption scheme* $\Pi = (\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ *is perfectly secret if and only if it is perfectly indistinguishable.*

Proof.

- (**Forward direction**, $A \implies B$) Assume that Π is perfectly secret and that the adversary is deterministic. Prove that Π is perfectly indistinguishable. Prove it assuming the adversary is probabilistic.
- (**Reverse direction**, $B \implies A$) Proving $B \implies A$ is equivalent to proving $A^c \implies B^c$. Assume that Π is not perfectly secret. Prove that Π is not perfectly indistinguishable.

□

3 References and Additional Reading

- Sections 2.3 from Katz/Lindell