Foundations of Cryptography

Bar-Ilan University
Course number: 89-653

Yehuda Lindell

February 24, 2019

Abstract

In this course, we will study the *theoretical foundations* of modern cryptography. The focus of the course is to understand what cryptographic problems can be solved, and under what assumptions. Most of the course will follow the presentation of the relevant material in [1] and [2]. The course obligations include exercises (composing 30% of the grade) and a final exam (composing 70% of the grade). Lecture notes on approximately half of the material appear at `http://u.cs.biu.ac.il/~lindell/89-856/main-89-856.pdf`.

Course Syllabus (tentative)

1. **Introduction and background:** a rigorous approach to cryptography, the focus of the foundations of cryptography, background on the computational model

2. **One-way functions:** definitions and variants, weak versus strong one-way functions

3. **Hard-core predicates:** definition, proof of existence (the Goldreich-Levin hardcore bit).

4. **Pseudorandomness:** definition, construction of pseudorandom generators, extending pseudorandom generators, pseudorandom functions and pseudorandom permutations

5. **Zero knowledge:** definitions, the simulation paradigm, graph isomorphism, perfect zero knowledge of DH tuples, zero knowledge for

all $\mathcal{NP}$, witness indistinguishability, constant-round zero-knowledge proofs (Goldreich Kahan), zero-knowledge proofs of knowledge

6. **Zero knowledge lower bounds:** impossibility of NIZK and the necessity of randomness, black-box lower bounds for public-coin zero knowledge

7. **Composition of zero knowledge:** sequential composition (counter-example without auxiliary input and proof with auxiliary input), counter example for parallel composition

8. **Non-interactive zero knowledge**

9. **Encryption schemes:** definitions – indistinguishability, semantic security and their equivalence, security under multiple encryptions, non-malleability, achieving CPA-NM (DDN), CCA1-security (Naor-Yung), CCA2-security

10. **Secure multiparty computation:** motivation, definitions, semi-honest oblivious transfer, the GMW semi-honest protocol, the GMW compiler

11. **The random-oracle methodology:** proofs of impossibility of instantiation

12. **Obfuscation:** proof of impossibility of black-box obfuscation, definition of indistinguishability obfuscation

Course webpage: Detailed information on the course, including lecture notes, can be found at
`http://www.cs.biu.ac.il/~lindell/89-856/main-89-856.html`.

References

[1] O. Goldreich. *Foundations of Cryptography: Volume 1 – Basic Tools.* Cambridge University Press, 2001.

[2] O. Goldreich. *Foundations of Cryptography: Volume 2 – Basic Applications.* Cambridge University Press, 2004.