Foundations of Cryptography

Bar-Ilan University
Course number: 89-856

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 and a final exam. In addition, there will be reading assignments on important material that we will not have time to cover in class.

Course Syllabus

1. (a) **Introduction and background:** a rigorous approach to cryptography, the focus of the foundations of cryptography, background on the computational model
   (b) **One-way functions I:** definitions and variants, weak versus strong one-way functions (theorem statement without a proof)
2. **One-way functions II:** continued
3. **Hard-core predicates:** definition, proof of existence (the Goldreich-Levin hardcore bit).
4. **Pseudorandomness I:** definition, construction of pseudorandom generators
5. **Pseudorandomness II:** extending pseudorandom generators, pseudorandom functions

6. **Zero knowledge I:** definitions, the simulation paradigm, graph isomorphism
7. **Zero knowledge II:** constructions for all $\mathcal{NP}$
8. **Non-interactive zero knowledge**
9. **Encryption schemes I:** definitions – indistinguishability, semantic security and their equivalence, security under multiple encryptions.
10. **Encryption schemes II:** constructions of secure private-key and public-key encryption schemes; definitions of security for more powerful adversaries
11. **Digital signatures I:** definitions, constructions
12. **Digital signatures II:** constructions, constructions of hash functions
13. **Secure multiparty computation:** motivation, definitions, semi-honest oblivious transfer, the GMW construction

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.