Topics in Applied Cryptography (89-658-01)

Yehuda Lindell
Bar-Ilan University

Abstract

This course is a continuation of the course Introduction to Cryptography (89-656), with a focus on topics that are of importance in practice, but are not covered in the introductory course due to lack of time. Material will be taken from *Introduction to Modern Cryptography* by Lindell-Katz, and from *A Graduate Course in Applied Cryptography* by Boneh-Shoup (the latter can be found at https://crypto.stanford.edu/~dabo/cryptobook/). The course consists of 12-13 lectures of two hours each.

Detailed Course Syllabus

1. **Topic 1 – Block cipher modes of operation and concrete security**
   (a) Tight security bounds for CTR mode (upper and lower bounds)
   (b) Tight security bounds for CBC mode (upper and lower bounds)
   (c) Why it's important; the Sweet32 attack, upper bounds on security for CTR and CBC modes
   (d) Constructing MACs from universal hash functions and PRFs
   (e) Defining authenticated encryption
   (f) GCM
      i. Give "easy" bound by first converting the block cipher to a PRF
      ii. Give stronger bound using the permutation method
   (g) Nonce-misuse resistance: attack on GCM, defining security, GCM-SIV
   (h) The search for better security – beyond birthday bounds; key-derivation method
2. **Topic 2 – public-key encryption**
   (a) Cramer-Shoup: CCA-security from DDH without random oracles (tentative; this is difficult)
   (b) Public-key encryption from LWE
   (c) The Paillier encryption scheme
3. **Topic 3 – Schnorr signatures**
   (a) Identification schemes
   (b) The Fiat-Shamir transform
   (c) Sigma protocols
   (d) The Schnorr Sigma protocol
4. **Topic 4 – Factoring and Discrete Log:** a brief overview of algorithms and their complexity

Prerequisites: Introduction to Cryptography (89-656)

Evaluation: Theoretical exercises and an exam