Foundations of Cryptography

Debdeep Mukhopadhyay
IIT Kharagpur

Syllabus

- Introduction to Cryptography: Basics of Symmetric Key Cryptography, Basics of Assymetric Key Cryptography, Hardness of Functions
- Notions of Semantic Security (SS) and Message Indistinguishability (MI): Proof of Equivalence of SS and MI, Hard Core Predicate, Trap-door permutation, Goldwasser-Micali Encryption
- Goldreich-Levin Theorem: Relation between Hardcore Predicates and Trap-door permutations

Syllabus

- Formal Notions of Attacks: Attacks under Message Indistinguishability:
  - Chosen Plaintext Attack(IND-CPA),
  - Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2),
  - Attacks under Message Non-malleability: NM-CPA and NM-CCA2,
  - Inter-relations among the attack model

Syllabus

- Random Oracles: Provable Security and asymmetric cryptography, hash functions
- One-way functions: Weak and Strong one way functions
- Pseudo-random Generators (PRG):
  - Blum-Micali-Yao Construction,
  - Construction of more powerful PRG,
  - Relation between One-way functions and PRG, Pseudo-random Functions (PRF)

Syllabus

- Building a Pseudorandom Permutation:
  - The Luby Rackoff Construction:
    - Formal Definition,
  - Application of the Luby Rackoff Construction to the construction of Block Ciphers,
    - The DES in the light of Luby Rackoff Construction

Syllabus

- Left or Right Security (LOR)
- Message Authentication Codes (MACs): Formal Definition of Weak and Strong MACs, Using a PRF as a MAC, Variable length MAC
- Public Key Signature Schemes: Formal Definitions, Signing and Verification, Formal Proofs of Security of Full Domain Hashing
- Assumptions for Public Key Signature Schemes: One way functions Imply Secure One-time Signatures
- Shamir's Secret Sharing Scheme
- Formally Analyzing Cryptographic Protocols
- Zero Knowledge Proofs and Protocols

Books

- **Text Books:**
  - Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, CRC Press.
  - Hans Delfs, Helmut Knebl, "Introduction to Cryptography, Principles and Applications", Springer Verlag.
  - Wenbo Mao, "Modern Cryptography, Theory and Practice", Pearson Education (Low Priced Edition)
  - Shaffi Goldwasser and Mihir Bellare, Lecture Notes on Cryptography, Available in **http://citeseerx.ist.psu.edu**
- **Reference Books:**
  - O. Goldreich, Foundations of Cryptography, CRC Press (Low Priced Edition Available), Part 1 and Part 2

Evaluation

- To be decided as the class progresses
  - Scribe (in groups)
  - Term paper (in groups)
  - Mid term and End Term Examinations
- Website:

  http://cse.iitkgp.ac.in/~debdeep/courses_iitkgp/FCrypto/index.htm

Great Expectations

- This is not an Introductory course.
- We should discuss and interact in the class and also beyond it.
- Please prepare regularly.
  - reading and writing is extremely important for the course.
  - This course is largely not about solving problems, but rather to understand the rigor of proving methods in the field of cryptography (not easy, as the goals are very hard to capture formally).
  - This course is expected to help us in future discourses of more deeper topics in theoretical cryptography (and may be other fields) and hence called foundations.