Topics in Cryptology: EE793

Virendra Sule
Department of EE
IIT Bombay
vrs@ee.iitb.ac.in

December 2021

Content

(List of the topics/sub-topics to be covered in the lectures/practicals/assignments):

1. Classical ciphers and their modern versions. Cryptanalysis of classical ciphers. Case studies: Vigenere, Diana algorithms, Rotor cipher.

2. Shannon's theorem and perfect secrecy. Computational security. Trapdoor one way functions for encryption, message authentication, public key encryption schemes, key exchange and signatures. Various applications to problems in practical world. Semantic security.

3. Pseudorandom sequences. Generation, Linear Complexity.

4. Structures in Block and Stream ciphers, Hash functions. Design of ciphers for practical use. Using modern ciphers securely.

5. Theory of Boolean systems of equations and solutions: Boolean elimination theory, Implicant based parallel all solution solver, orthogonal systems. Satisfiability and algorithms for CNF-SAT.

6. Theory of dynamical systems over finite fields (DSFF) and its applications in Cryptanalysis, Biological Networks.

7. Cryptanalysis of block and stream ciphers by Boolean approach. Symbolic Boolean computation in SAGE.

8. Realization of schemes for end to end encryption, authenticated encryption, encryption dependent on error correction, simultaneous coding and encryption, variation of ciphers.

9. Post Quantum Cryptographic schemes. Multivariate polynomial public key schemes. McEleiece scheme. Almost perfectly secure symmetric schemes.

Texts and References

1. Waade Trappe and L.C. Washington: Introduction to Cryptography and Coding Theory. Pearson. 2006.

2. Chen Lidong, Gunag Gong: Communication System Security. Chapman & Hall CRC, 2012.

3. Serge Vaudeney: Classical Introduction to Cryptography. Springer 2005.

4. Lars Knudson, Mathew Robshaw: Block cipher companion. Springer, 2011.

5. Stamp M. and Low R.M. Applied Cryptanalysis. Wiley Interscience 2007.

6. Papers from Internet sources on measures of pseudorandomness.

7. Papers and book chapters on Boolean systems, theory and computation. (A parallel all solution solver for Boolean satisfiability. Arxiv.org/1611.09590v3).

8. Selected Papers on Biological applications of Boolean systems.