INF 247, spring 2018

Igor Semaev

December 6, 2017

The course is on basic cryptanalytic techniques for symmetric ciphers. The course mostly follows the lecture notes to be distributed before it starts. Prerequisites include basic algebra and probability theory, though necessary notions and results will be explained. Also it is good to have attended INF240 taught at the Department of Informatics, University of Bergen or any other introductory course in cryptography.

1 Cryptanalysis of historical ciphers.

1. General definition of a cryptographic system. Symmetric-key and public-key encryption, classes of cryptanalytic attacks.
2. Substitution cipher, cryptanalysis, unicity distance of a simple substitution cipher.
3. Homophonic cipher, cryptanalysis.
4. Simple Vigenère cipher, cryptanalysis, Kasiski test. Auto-correlation method.
5. Index of coincidence.
6. Transposition cipher, cryptanalysis.
7. Running-key cipher.
8. Hagelin cipher, idea of the cryptanalysis.
9. G-Schreiber, known plain-text attack.

2 Stream ciphers.

1. Cryptanalysis at depth.
2. Synchronous and self-synchronizing stream ciphers.
3. Linear feedback shift registers, characteristic polynomial and minimal polynomial of a matrix. Period of an irreducible polynomial.

4. Checking irreducibility of a polynomial modulo 2.
5. Constructing primitive polynomials modulo 2.
6. Linear complexity of binary sequences, linear complexity of the XOR of two sequences, linear complexity of element-wise product of two sequences.
7. Linear complexity profile of a sequence, properties.
8. Berlekamp-Massey algorithm. Complexity of the algorithm.
9. Boolean functions, algebraic normal form(ANF). Algorithm for computing the ANF. Complexity of the algorithm.
10. Time-memory trade off for a filter generator.
11. Solving nonlinear algebraic equation via linearization and extended linearization, algebraic attacks for stream ciphers.
12. Constructing annihilators for Boolean functions. Annihilator attack.
13. Berlekamp-Massey attack, complexity.
14. Algorithm for computing Walsh-Hadamard coefficients. Finding the best affine approximation for Boolean functions.
15. Affine approximation attack, complexity.
16. Bernoulli trials, de Moivre-Laplace Theorem. Chernoff bounds. Probability of missing the solution in affine approximation attack.
17. Boolean bent-functions, criterion and examples.
18. Fast correlation attack, complexity. Formula for computing new correlation probabilities.
19. Combining LFSRs, minimal period of the output. Linear complexity.
20. Correlation attack against a combiner, complexity. Probability of errors, necessary amount of the key-stream.
21. Correlation immune Boolean functions. Bound on their algebraic degree.
22. Piling-up lemma. The best affine approximation for the XOR of Boolean functions in independent variables.
23. Nonlinear Feedback Shift Registers. Generating de Bruijn sequences. Constructing full period NFSR.
24. Alternating step generator. Shrinking generator. Summation generator.
25. 2-adic expansion of rational numbers. Feedback with Carry Shift Registers.

26. Lattices of dimension 2. Gauss-Lagrange algorithm. Reconstruction of a rational number from its partial 2-adic expansion.

27. Modern stream ciphers: RC4, Trivium, Grain.

3 Block ciphers.

1. Modern block ciphers, round function and key schedule. Feistel ciphers and Substitution Permutation Networks.

2. Meet in the Middle attack. Time and memory complexity.

3. Linear approximations of S-boxes. Computing the most biased linear approximations with Walsh-Hadamard transform.

4. Linear Cryptanalysis for round block ciphers. Necessary amount of plaintext/cipher-text blocks.

5. Linear Cryptanalysis of DES.

4 Comments

The attendance to the lectures and group sessions is mandatory, up to four classes my be missed for reasons that include personal and professional commitments and personal/family emergencies. Any student who exceeds the four class limit may not be admitted to the exam. Weekly exercises will be distributed separately upon some necessary theory is studied. There should be three mandatory exercises, the deadline of handing them in is absolute. The students can get up to 30% of the final grade with mandatory exercises: up to 10% for each, the rest 70% comes from the written exam.