Bard, Gregory V.

Algebraic cryptanalysis. (English) Zbl 1183.94019

New York, NY: Springer (ISBN 978-0-387-88756-2/hbk; 978-0-387-88757-9/ebook). xxxiii, 356 p. (2009).

The book contains 3 parts, each having 5 chapters, and 5 appendices which describe code-breaking by solving systems of equations. The author explains the mathematical background of the breaking method and exemplifies it on various ciphers. The algebraic cryptanalysis contains two steps: first the cipher is converted into a polynomial system of equations and then the system is solved, finding the secret key of the cipher from the obtained solution.

Part 1 deals only with the first step applied to the Keeloq cipher. Chapter 2 describes the Keeloq specifications and the steps for obtaining the polynomial system of equations using a non-linear function. In the next chapter the author presents an attack which is faster than the brute-force one. It is based on a function f iterated 8 times on the plaintext. Then, the cipher is rewritten as another function g executed on the output of f. In the end fixed points of f will be obtained which will be used to recover the secret key by solving the polynomial system. Chapter 4 describes a new attack based on iterated permutations. To count permutations of particular types the author uses analytic combinatorics. After describing the mathematical background of combinatorics, including examples, the author explains their application in cryptography. A detailed explanation on two attacks: distinguishing attack on 3-DES and a key recovery attack on AES-256 is given at the end of this chapter. Chapter 5 deals with examples on stream ciphers like Trivium, Bivium and QUAD. For each of these ciphers a detailed presentation is offered including the algorithm, and then is given a numerical example for an attack based on polynomial system of equations.

Part 2 of the book deals with solving the polynomial system of equations obtained in Part 1. Chapter 6 describes "Some Basic Facts about Linear Algebra over $GF(2)$". The purpose of this chapter is to emphasize the differences between matrices over $\mathbb{R}$ or $\mathbb{C}$ and matrices over $GF(2)$. In chapter 7 a new model for counting matrix-memory operations is proposed and also the circumstances in which this model works and the ones in which it fails are described. In chapter 8 the author describes matrix operations such as finding determinants, inversion, multiplication, QR-decomposition, LU-factorization etc. All these operations are described step by step on numerical examples. If the reader is not interested, the chapter can be skipped (as the author himself recommends). Chapter 9 presents the Method of Four Russians which deals with multiplication of boolean matrices and extension $GF(2)$-matrices. The author gives a good explanation of the algorithm and compares its running time with other popular algorithms. Chapter 10 describes two algorithms for factoring the product of two distinct prime integers: Linear Sieve and Quadratic Sieve. The chapter omits many variations, improvements and enhancements of the two algorithms developed over time. This chapter can, also, be skipped because it does not contain vital information for the rest of the book.

Part 3 contains a detailed presentation of the methods for solving the polynomial systems of equations. Chapter 11 discusses properties of polynomials over finite fields including properties of these systems. It also contains theorems which prove that any polynomial system can be written with degree 2. Some algorithms with a polynomial running time for doing this are presented. An important part of the chapter contains a discussion of the NP-Completeness for solving the polynomial systems of equations. Chapter 12 presents several algorithms for solving the systems. Some of these are the methods of Nicolas Courtois, the XL and ElimLin algorithms, the Buchberger algorithm etc. In the second half of the chapter an application of graph theory for simplifying the polynomial systems is presented. The author targets systems of polynomial equations where there are two sets which have only a few common variables. An algorithm for discovering these systems is presented. At the end is described Resultants with Raddum-Semaev method, Zhang-Zi algorithm and homotopy methods. The next three chapters (13,14,15) are dedicated to SAT-Solvers. The author presents how to approach polynomial systems over $GF(2)$ with SAT-Solvers and, in the end, he extends the examples up to $GF(64)$.

The first appendix describes block ciphers with very short plaintexts but normal-size keys. This is more a subjective discussion since the author presents his own opinion (not a sequence of provable theorems) about what is relevant and what is not, and what "faster than brute-force" means. The next appendix contains the equations used in chapter 15 for converting the multiplication over $GF(2^n)$ into $GF(2)$. The

third appendix offers other aplications of polynomials over finite field, in particular the connection to graph coloring. The fourth appendix deals with sparse matrix algorithms describing, also, the Created Catastrophes algorithm developed by Carl Pomerance. The last appendix contains quotes which inspired the author during his research.

The entire work is well structured having a good mathematical background. The book is recommended to graduate students who want to do their dissertation in any part of cryptanalysis. It is also useful to researchers in applied abstract algebra, cryptography or any other area of these domains.

Reviewer: Nicolae Constantinescu (Craiova)

MSC:

94A60	Cryptography
11T71	Algebraic coding theory; cryptography (number-theoretic aspects)
05E99	Algebraic combinatorics
15A30	Algebraic systems of matrices
08A99	Algebraic structures

Keywords:

algebraic cryptanalysis; applied abstract algebra; code breaking

Software:

ATLAS

Full Text: DOI