Review of the book

"Algebraic Cryptanalysis" by Gregory V. Bard Springer, 2009

ISBN: 978-0-387-88756-2

Wael Said Abdel mageed Mohamed
Cryptography and Computeralgebra, Informatik, TU-Darmstadt, Germany

1 Book Overview

This book introduces the predominant topics in multivariate-base cryptanalysis. It can be described to be a complementary text book in the field of algebraic attack as a result of the author's experience and knowledge. For a person who did not know much about algebraic cryptanalysis, this book is a good starting point.

The basic core of this book is the author's dissertation, under the title "Algorithms for the Solution of Linear and Polynomial Systems of Equations over Finite Fields, with Application of Cryptanalysis". As stated by the book title, this book is about how to represent a cipher as a system of multivariate equations. Then by solving these equations, one can break the cipher by obtaining the key used with the cipher.

The author's purposes in writing this book are:

- The difficulty of entering the field of algebraic cryptanalysis that the author faced when he started his research.
- The non-existence of text books in the algebraic cryptanalysis.
- The lack of explanations of several algorithms that are related to algebraic cryptanalysis.

2 Book Summary

The book consists of 15 chapters followed by 5 appendices. These 15 chapters are structured into an introduction chapter followed by 3 successive parts. Part I named "Cryptanalysis" as stated by the author covers the conversion of the cipher into a system of polynomial equations, what is known to be the first step in the algebraic cryptanalysis. It consista of 4 chapters "The Block Cipher Keeloq and Algebraic attacks", "The Fixed Point Attack", "Iterated Permutations", and "Stream Ciphers". Part II, "Linear Systems Mod 2", focuses on the importance of linear algebra. This is motivated by the fact that linear algebra is used in many algorithms like XL, ElimLin, F4, and F5. It contains the following 5 chapters: "Some Basic Facts about Linear Algebra over $GF(2)$", "The Complexity of $GF(2)$-Matrix Operations", "On The Exponent of Certain Matrix Operations", "The Method of Four Russians", and "The Quadratic Sieve". Part III, "Polynomial Systems and Satisfiability", discusses how to solve a polynomial systems which is the very heart of the book, as stated by the author. It also has five chapters named "Strategies for Polynomial Systems", "Algorithms for Solving Polynomial Systems", "Converting MQ to CNF-SAT", "How do SAT-Solvers Operate?", and "Applying SAT-Solvers to Extension Fields of Low Degree".

In chapter 1 “Introduction: How to Use this Book”, the author provides an introduction to the contents of the book with a summary description of each chapter. He also gives the reasons for choosing the block cipher Keeloq as a case study for generating a system of polynomial equations. Suggested chapter ordering and a brief note of numbering theorem, lemmas, facts, and definitions are presented at the end of the chapter.

Chapter 2 “The Block Cipher Keeloq and Algebraic attacks”, describes how to convert the block cipher Keeloq into a system of polynomial equations. The author first explains what is meant by algebraic cryptanalysis before a constraint satisfaction problem model for polynomial equations is explained. The Keeloq specification is described followed by a demonstration of how to model the non-linear function. The system of polynomial equations for Keeloq is given. The number of variables and number of equations is counted and dropping the degree of equations to quadratic is described. At the end of the chapter a failure of the direct construction of the equations is concluded because the experimental results on 128 rounds are slower than brute-force.

Chapter 3 “The Fixed-Point Attack”, explains a more efficient attack called Fixed-Point that generates the polynomial equations indirectly. The definition and how to find fixed-point is presented. The author gives two ways to search for such fixed-points. A comparison with brute force attacks concludes that the fixed-points attack is $2^{14.04}$ times faster. Finally, the author states a list of papers for other attacks on Keeloq that are published after the author’s attack.

Chapter 4 “Iterated Permutations”, describes the analysis of iterated permutations through analytic combinatorics. The author gives some background material about combinatorial classes, the ordinary and exponential generating functions of a sequence, the operations on these functions, and some practical examples on both types. The strong and weak cycle structure theorems are stated followed by some corollaries. At the end of the chapter the author highlights a new attack to any cipher that has iterated a large composite number of times.

Chapter 5 “Stream Ciphers”, presents an overview for some stream ciphers that can be represented by polynomial equations. These ciphers are Trivium, Bivium, and QUAD. The author gives some background material about what stream ciphers and the eSTREAM project are. A description for Trivium, Bivium, and how to generate an equivalent polynomial system for them is given. A list of papers related to these two ciphers is enumerated. Some highlights for QUAD cipher are given, its proof of security is outlined, and an attack for QUAD by Yang *et al.* is presented.

Chapter 6 “Some Basic Facts about Linear Algebra over $GF(2)$”, focuses on a few features of $GF(2)$ vector spaces and matrices over $GF(2)$ that are related to cryptanalysis. The author reviews the difference between Boolean matrices and $GF(2)$-matrices. How to find the null space from an RREF, Reduced Row Echlon Form, and how to find the number of solutions to a linear system over finite fields is discussed.

In chapter 7 “The Complexity of GF(2)-matrix Operations”, the author presents a new model for measuring the complexity of $GF(2)$-matrix operations. An analysis of some classical techniques with this new model is discussed.

Chapter 8 “On the Exponent of Certain Matrix Operations”, states some theorems with proofs and complexity for different matrix operations. These operations include matrix inversion, matrix multiplication, LU-factorization, and finding determinants.

Chapter 9 “The Method of Four Russians”, demonstrates two algorithms called Method of Four Russians for Multiplication (M4RM) and Method of Four Russians for Inversion (M4RI). Experimental results by SAGE, a free mathematics software system, staff are tabulated. A pairing for M4RI with Strassen’s algorithm is highlighted.

Chapter 10 “The Quadratic Sieve”, discusses two important algorithms: Linear Sieve and Quadratic Sieve that are used in integer factoring problem. Solving this problem is the basic part in the cryptanalysis of RSA, and serves as an example for using linear algebra for breaking a public-key cryptosystem.

In chapter 11 "Strategies for Polynomial Systems", a variety of different applications that depend on solving polynomial systems of equations over finite fields is considered. The author explains the concept of universal maps. Then he focuses on polynomials over $GF(2)$ and how to reduce their degree. Two algorithms for this reduction are suggested, simple degree dropper algorithm and greedy degree-dropper algorithm. The NP-completeness of the multivariate problem and measures of difficulty in MQ is discussed. At the end of this chapter, the author discusses the role of guessing a few variables before proceeding with solving.

In chapter 12 "Algorithms for Solving Polynomial Systems", the author reviews most of the methods of solving polynomial systems of equations that are used nowadays. These algorithms include Gröbner bases algorithms, Linearization, XL algorithm, ElimLin, Resultant, Raddum-Semaev method, and Zhuang-Zi algorithm. A snapshot for the comparison between XL and F4 is presented. An approach based on system fragmentation is explained. The author closes the chapter by introducing homotopy methods, a class of algorithms that the author thought might be a new research opportunity in cryptography.

Chapter 13 "Converting MQ to CNF-SAT", describes methods for efficiently converting $GF(2)$ systems of multivariate polynomial equations into a satisfiability problem in the conjunctive normal form. The author explains how SAT applies to algebraic cryptanalysis, defines some notations and terms and reviews previous work. Finally, the author notes possible applications to cubic systems.

Chapter 14 "How do SAT-Solvers Operate?", as the title of this chapter suggests, two main algorithms that are used by some SAT-solvers are explained. These are Chaff family and Walk-SAT family algorithms. A selection of papers for further reading is listed.

Chapter 15 "Applying SAT-Solvers to Extension Fields of Low Degree", discusses extension fields, their importance in algebraic cryptanalysis, and polynomial systems over extension fields of $GF(2)$. How to apply SAT-solvers and Gröbner basis to extension fields is explained. Some experimental results for comparing Magma, Singular and Mini-SAT are tabulated.

3 Book Style

The writing style of the author can be described by simplicity and clarity. The author chooses a book title "algebraic cryptanalysis" that covers a very predominant topic in the next 10 years. He gives a brief overview of the entire book by an introduction chapter. This chapter summarizes what is this book going to be about. Each chapter starts with a short notes about the purpose of it and most of these chapters ends with a list of references for further reading.

Generating polynomial equations from a cipher is a very important step in algebraic cryptanalysis, indeed it is the step one in algebraic cryptanalysis. The author's approach is to give an example of how to obtain polynomial equations from a block cipher using one concrete block cipher. In my opinion, it would be better to have more general explanation here, not just use Keeloq as a block cipher case study or Trivium and Bivium as stream cipher examples.

As an example for how to break a public-key system using algebraic cryptanalysis, the author introduces in chapter 10 "The Quadratic Sieve" as a martial for breaking RSA. This chapter is presented in the second part of the book, which covers linear algebra as an important tool in the solving process. The author did not tell us about Wiedemann as an important linear algebra step in integer factoring process. Moreover, what about multivariate-based public key systems and hash functions? There is no such examples to show that they are applicable to algebraic cryptanalysis.

In my opinion the contents of this book is not comprehensive enough, as the book title suggests, specially for a beginner to this field. It tends to be a big survey rather than a text book. I expected to see a more detailed and technical explanations under this book title. The book structure may be rearranged in four parts instead of three. for example, mathematical basis and backgrounds, converting ciphers into polynomial systems, how to solve, then other related topics. In the converting ciphers into polynomials section, it should cover stream ciphers, block ciphers, public-key cryptosystems, and hash functions. This should be done in general explanations followed by case studies. In "how to solve" part, it should contain the explanations for the existing algorithms that solve multivariate systems with a detailed example for each algorithm. Indeed the author did this already with some algorithms. Moreover at least F4 algorithm should also be discussed. In the fourth part "other related topic", SAT-solvers, graph coloring and other related applications to algebraic cryptanalysis could be discussed. Chapters 13-15 that are related to SAT-solvers are discussed in a very good structure.

Some sections may be combined with others instead of reference to each others. For example, section 2.8 on page 15 with section 11.7.1 on page 206, section 6.4 on page 85 with section 10.5.5 on page 174. In section 3.4.1 on page 21, In the proof of Theorem 1, there is an abbreviation "EGF" that is first used here without any reference to it which is in section 4.2.1 on page 30. Section 3.7.1 may be moved to Keeloq specification.

4 Recommendations

The book at hand gives a good starting point for a person who did not know much about algebraic cryptanalysis. It can be thought of as an appetizer at a new cryptographer's table. According to its simplicity and readability a researcher who wants to start a real algebraic attack can find a lot of references for precise and detailed information. As such a reference the book is suitable for Master or Ph.D. students.

In general words, this book is suited for the intended audience, which are as stated by the author and the book web-site:

- Motivated graduate students who wish to learn something about algebraic cryptanalysis.
- Graduate students who are about to begin a dissertation or master thesis in that topic.
- Advanced-level students in computer sciences and mathematics, as a secondary text or reference book for self-guided students.
- Practitioners working for intelligence agencies or security companies.
- Researchers in Applied Abstract Algebra or Algebraic Geometry who wish to find more applied topics.

The reviewer is a Ph.D. student at TU-Darmstadt, Germany.