Review of the book

"Algebraic Cryptanalysis"

by Gregory V. Bard

Springer, 2009

ISBN: 978-0-387-88756-2

Rusydi Hasan Makarim
Institute of Applied Mathematics
Middle East Technical University, Ankara, Turkey

1 Summary of the review

This is the introductory book for any researcher who would like to start to work on the topic related to solving multivariate polynomial equation and its application in cryptanalysis. It is based on the author's doctoral dissertation entitled "Algorithms for the Solution of Linear and Polynomial Systems of Equations over Finite Fields, with Application of Cryptanalysis". In general, the structure of the book consists of the topic on converting a cipher into a multivariate polynomial systems, discussion of linear algebra over $\mathbb{GF}(2)$, and the methods to solve the polynomial systems.

2 Summary of the book

Chapter 1 (Introduction : How to Use this Book)

In chapter 1, the author briefly explained the content of three (3) main parts of the book. In the explanation of part one of the book, several reasons why the author chooses Keeloq is given. The description on the topic from chapter 2 to chapter 5 are shortly explained to give a brief picture for the readers. The author also recommended the readers to study the attack on Keeloq that were released after the publication date of the book.

In the last part of this chapter, the author gives suggestion for chapter ordering throughout the book. He stated that most of the readers of this book have to read it twice. The readers who already have previous background of the topic are not required to follow the chapter in sequential order. The recommendation from the author himself is to skim each part, probably skipping chapter 4 (Iterated Permutations) and chapter 8 (On the Exponent of Certain Matrix Operations), and start over again with more detail, because the mathematics part and the cryptography part of algebraic attack depend heavily on each other.

2.1 Part I (Cryptanalysis)

Chapter 2 (The Block Cipher Keeloq and Algebraic Attack)

Chapter 2 discusses the block cipher Keeloq, the conversion of it into a system of polynomial equation, and straightforward algebraic attack on Keeloq. The author started with the description of Keeloq, a block cipher based on nonlinear feedback shift register (NLFSR), used mostly for remote keyless entry systems such as car locks. The strategy of modelling the non-linear function and the mathematical way to describe the shift register are explained in section 3 and 4 of the chapter. In section 5 the algebraic equation of Keeloq is given, followed by the number of variables and equations obtained in section 6. In the next two sections, the author explained two initial strategy in algebraic attack : reducing the

degree of the equations from cubic to quadratic by substitution, and guess-and-determine methodology by fixing/guessing key bits in advance before solving the equations. The last section is a short description why straightforward attempt to perform algebraic cryptanalysis on Keeloq resulted in a failure with some results of the initial experimental attack.

Chapter 3 (The Fixed-Point Attack)

In this chapter a more efficient attack specifically against Keeloq is presented. The equation system of Keeloq is rewritten by exploiting the existence of fixed point in order to reduce the number of equations and unknowns. Brief description of notations used throughout the chapter is described shortly in the introductory part. The consequences of fixed points and its impact on algebraic attack are given in section 2, followed by the description of the method and an algorithm to search for the fixed points on Keeloq. In section 4, the bound for the searching algorithm is defined using the approach from the analytic combinatorics as well as experimental method. The result of the fixed point attack on Keeloq and its efficiency compared to brute-force is presented in section 5. Overall summary and conclusion of the whole chapter is described in section 6. There is also some additional notes on Keeloq given in section 7, and description of Wagner's attack in section 8.

Chapter 4 (Iterated Permutations)

Chapter 4 is the study of iterated permutations with the approach using analytic combinatorics and its applications to cryptography. Various background topics required are explained in section 2, together with examples. Section 3 contained the explanation of strong and weak cycle structure theorems. The corollaries obtained from the previous lemmas and theorems are mentioned in the next section. Section 5 showed several results with connections to some topics in number theory, and could be considered as additional notes. In the last section the author explained two types of new attack and presented the results.

Chapter 5 (Stream Ciphers)

The chapter on stream ciphers presented to the reader interesting type of stream ciphers and described how the ciphers are converted to system of equations. There are two stream ciphers discussed in chapter 5 : trivium, and QUAD. In the beginning of the chapter, the author briefly explained the concept of stream cipher and eSTREAM projects, followed by the technical description of trivium. In the next subsection, the cipher bivium was introduced as the simpler variants of trivium that resembles similar structures. The author also described the equations system for bivium and gave some observations regarding the features of the equations. The family of stream ciphers QUAD is explained in the next section with description of how the cipher works, proof of its security, and the Yang-Chen-Bernstein attack against QUAD together with its extension. The conclusion for QUAD is given in the last part of this chapter.

2.2 Part II (Linear Systems Mod 2)

Chapter 6 (Some Basic Facts about Linear Algebra over $\mathbb{GF}(2)$)

In chapter 6, the author presented some facts about linear algebra over finite field with characteristics two. Useful sources that supported the topic on the chapter are mentioned in the first section. In the next section, the author described the term he used (boolean matrix and $\mathbb{GF}(2)$ matrix) to distinguish between matrix filled with elements from commutative semiring and the one with element from $\mathbb{GF}(2)$. In the same section the author also explained that the implementation of the operation may use the integers. In section 3, several well-known facts about the specific properties of vector spaces over $\mathbb{GF}(2)$ are mentioned in detail, particularly compared to $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{C}$. The discussion on recovering null space from the reduced row echelon form of a matrix is given in section 4. The last section described the number of solutions to a linear system that can be obtained.

Chapter 7 (The Complexity of $\mathbb{GF}(2)$-Matrix Operations)

The new model to estimate the complexity of matrix operation over $\mathbb{GF}(2)$ using matrix-memory operations instead of field operations is discussed in this chapter. It started with the model to count the cost

of the operations in section 1. Short description of notational convention used throughout the chapter is given in the second section. In section three and four, the comparison of pros and cons of methods to solve systems of equations defined by a square matrix is described, followed by the explanation of two type of data structures, array with swaps and permutation matrices, used to store the matrix efficiently. Using the model proposed, in section 5 the author gave example of the analysis of classical matrix operations (multiplication, addition, gaussian elimination, back-solving triangulated linear system). Section 6 contains the description of Strassen's matrix multiplication algorithm and clarification on Strassen's matrix inversion formula. The last section of this chapter is a description why the Strassen's algorithm is not suitable for inversion over $\mathbb{GF}(2)$.

Chapter 8 (On the Exponent of Certain Matrix Operations)

In the beginning of chapter 8, the author mentioned some of the complexities of different matrix multiplication algorithms. The theorems that prove the equivalent complexity of matrix multiplication, inversion, LUP factorization, and squaring, are given in section 2. The last section has the description of several background information on determinant and matrix inverses, the proof for Baur-Strassen-Morgenstern theorem, and its consequences on the determinant and the inverses.

Chapter 9 (The Method of Four Russians)

Chapter 9 contains an extensive treatment on the new algorithm used for matrix multiplication and inversion, known as "the method of four russians". The discussion on the origins of the algorithm and the previous work is given in the first section. The author presented the fast way to enumerate all the vector elements of a subspace in section 2. The detailed discussion on the matrix multiplication using the method of four russian is given in section 3, followed by the inversion algorithm in section 4. The complexity analysis and the experimental result on the algorithm are presented in section 5 and 6, respectively. Section 7 has the results of another experimental testing of the library that the author developed (M4RI). The integration of method of four russian and Strassen's multiplication algorithm is provided in section 8. The last section contains short discussion on the execution of the algorithm for finite field with elements greater than 2.

Chapter 10 (The Quadratic Sieve)

The topic on chapter 10 is not related directly to the topic on algebraic cryptanalysis. It discusses the quadratic sieve, one of the modern integer factorization algorithm that required linear algebra in one of its subroutine. In the first section the author started with motivation why factoring is important, and described the RSA algorithm in brief. Explanation on trial division algorithm, several additional ideas and sieve of eratosthenes algorithm are presented in section 2. The preliminary topics and theoretical foundations are given in section 3, continued with the naive sieving method in section 4. The author then introduced the notion of Gödel vectors in section 5. In section 6 and 7, the linear sieve algorithm and the example are explained. Generating smooth square integers and a new strategy are discussed in section 8. The chapter is ended with some suggestion for further reading and historical notes.

2.3 Part III (Polynomial Systems and Satisfiability)

Chapter 11 (Strategies for Polynomial Systems)

This chapter discussed the most important aspect in algebraic attack. It gave the reason and the importance of solving polynomial systems of equations over finite fields in the first section. In section 2 the explanation of corollaries and theorem that leads to the universal mapping theorem is given, followed by several important aspects of polynomial over $\mathbb{GF}(2)$ in section 3. Reducing the degree of the polynomials, which is a fundamental step to improve the efficiency of algebraic attack, is extensively explained in section 4. The discussion on complexity of MP-type problems and its associated complexity classes are shown in section 5, while in section 6 the author explained about the metrics that is used to measure the difficulties of solving MQ problem. The final section of this chapter gave an overview of the significance of guessing variables in improving the efficiency of algebraic attak.

Chapter 12 (Algorithms for Solving Polynomial Systems)

Chapter 12 discussed various algorithms, from mathematical to heuristic approach, for solving polynomial systems. A short note from philosophical point on complexity theory is given in the beginning of the chapter. A brief discussion of gröbner bases algorithms, which is an exact algorithm to solve the multivariate polynomial system, is written in section 2. Short note on linearization technique, a strategy to improve the efficiency of solving polynomial systems by reducing its degree,is explained in section 3 followed by eXtended Linearization (XL) algorithm in section 4. Description of ElimLin algorith, which was also developed by the author of XL, is given in section 5. Section 6 gives the comparison between eXtended Linearization (XL) algorithm with F4, recently introduced algorithm for solving multivariate polynomial system. Short decription of heuristic approach using SAT-Solvers is noted in section 7. The author presented, in section 8, a technique of fragmenting a system of polynomial equations into two or more set of equations by giving an algorithm to determine if a polynomial systems is separable together with the actual method of splitting the systems. The other three methods, Resultans, Raddum-Semaev, and Zhuang-Zhi, are described in section 9, 10, and 11 respectively. The last section contains an alternative approach of solving polynomial systems using homotopy methods.

Chapter 13 (Converting MQ to CNF-SAT)

In the previous chapter, the author said that SAT-Solvers can be used to solve polynomial equations over finite field since both problems belong to the same complexity class. The overall content of chapter 13 discusses the method on how to convert multivariate polynomial equations, especially in quadratic forms, into 3-conjunctive normal form (CNF). Summary of the content of the chapter is given in the beginning with short introductory topic in section 2. The notations and definitions throughout the chapter is described in section 3. The main content of the chapter, which is the explanation of the method to convert the multivariate quadratic polynomial systems over finite field to CNF-SAT, is discussed in section 4. The author, then, presented the experimental results of the conversion method in section 5. There are also brief discussion on the conversion of cubic system in section 6, followed by some reading suggestion and conclusion in section 7 and 8, respectively.

Chapter 14 (How do SAT-Solvers Operate?)

Chapter 14 gives an insight on what SAT problem is, and how the so-called SAT-Solvers works. It starts with the description of SAT problem and the conjunctive normal form (CNF). Explanation of Walk-SAT, as one of the leading method of SAT-solvers family, is described in section 2. The backtracking subroutine, one of the important step in Chaff SAT-solver family, is introduced in section 3 followed by the discussion of Chaff methods and its extensions in section 4. Several enhancement from the basic Chaff's algorithm is briefly described in section 5. In section 6, there is a non-technical notes about the economical motivation behind the development of SAT-solver algorithm. The author ended the chapter with some references for further study on the topic.

Chapter 15 (Applying SAT-Solvers to Extension Fields of Low Degree)

The very last chapter of the book discusses about applying SAT-Solvers to the extension field of $\mathbb{GF}(2)$ such as $\mathbb{GF}(4)$, $\mathbb{GF}(8)$, $\mathbb{GF}(16)$, etc. An introductory note is given in the first section of the chapter. In section 2, the author gives brief review of the topic on solving the $\mathbb{GF}(2)$ system using SAT-Solvers. Overview of the method to solve polynomial systems over extension field of $\mathbb{GF}(2)$ is described in section 3. Some necessary explanation of the polynomial systems over extension fields of $\mathbb{GF}(2)$ used in the chapter is given in section 4. A strategy to represent the finite field elements via matrices is discussed in section 5 using $\mathbb{GF}(2)$ as an example. In section 6, there are some remarks on using the algebraic normal forms in solving the polynomial system of equations using SAT-Solvers. The experimental results with various settings and parameters are presented in section 7, followed by discussion on computing the inverses and determinants by taking the example from $\mathbb{GF}(16)$ and its matrix representation. The author then concluded the entire chapter in section 9 also with some review on the topic of extension field in section 10. The last section contains the proof of the so-called "dead give-aways" matrix entry's.

3 Style of the book

It is quite difficult to find a book dedicated to one particular type of cryptanalytic attack. Algebraic cryptanalysis has a completely different approach compared to other cryptanalysis techniques, such as linear and differential attacks, that require statistical analysis. This book is able to fill the gap and describes the background required in order to understand the nature of how algebraic attack works. However, there are several suggestions that could improve the content and structure of the book such as

- The beginning part of the book should give extensive discussion about the mathematical background required (i.e. linear algebra, finite field, polynomials, etc) in order to help those readers with a lack of mathematical background.
- The application of algebraic attacks should cover various types of cryptosystems. The strategy of converting a cipher into multivariate polynomial systems over a finite field and the algebraic attack presented should be applied to other types of schemes as well, such as block ciphers that do not resemble the structure of stream ciphers, hash functions, multivariate public-key cryptosystems, etc.
- The part where the author introduce the SAT problem, in chapter 13, should be more descriptive and should provide more information on the SAT problem itself and necessary topics from complexity theory.

4 Recommendations

This book is highly recommended for graduate or final year undergraduate students intended to start research work on algebraic crytanalysis. It is an excellent starting point on algebraic cryptanalysis that covers most of the important topics required to study and apply algebraic attack on a modern cipher. However, the reader is advised to have previous background on linear algebra, finite field, and boolean satisfiability problem (SAT) before using this resource and entering the field of algebraic cryptanalysis.

The reviewer is a graduate student at Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey