Review of the book

"Algebraic Aspects of the Advanced Encryption Standard"

by Carlos Cid, Sean Murphy, and Matthew Robshaw

Springer, 2006

ISBN: 0-387-24363-1, 978-0-387-24363-4

Stanislav Bulygin
Center for Advanced Security Research Darmstadt (CASED)

2009-11-02

1 What the book is about

In their book the authors give an algebraic perspective of the Advanced Encryption Standard (AES). The cipher Rijndael won the AES competition in 2000 after three years of considerations. Unlike many block ciphers known at that time and proposed nowadays, AES-Rijndael has very explicit algebraic description. The rich algebraic structure of the cipher attracted cryptologists from the moment of appearance of Rijndael. The excellent book of Cid et. al. gives exactly an overview of properties of Rijndael from the algebraic point of view.

The book is structured as follows. It contains **seven chapters** and an appendix, among which the first three are introductory, the next three are the core of the book, and there is also a concluding chapter.

After giving a short introduction to the topic and historic remarks in **Chapter 1**, the authors move to giving the necessary algebraic background in **Chapter 2**. This chapter contains all the algebraic notions one needs for understanding the follow-up chapters. The chapter covers such fundamental topics as groups, rings, and fields; univariate, including the Lagrange Interpolation Formula, and multivariate, including the notion of the polynomial ordering, polynomial rings. Further, necessary notions from linear and matrix algebra are presented using linear and matrix parts of the AES description as examples. As is usual for cryptology, one is dealing with finite fields as an underlying object. So the topic of the finite fields is considered next: which finite fields exist out there and how one works with them efficiently. A quite significant part of the book is devoted to algebraic attacks on the AES, therefore the notion of a Gröbner basis is a central notion for that. The section "Varieties and Gröbner bases" gives a succinct overview of this important area.

After providing the reader with necessary tools, the book continues with the actual description of the AES in **Chapter 3**. While giving a description of the AES, the authors make sure that the algebraic essence of the cipher is seen and the underlying algebraic features are emphasized. In particular, the reader realizes the fact that the nonlinear S-Box transformation in the AES is essentially an inversion operation over the field $GF(2^8)$, unlike the usual way of defining an S-Box via a look-up table, so that underlying algebraic structure is usually not apparent. The chapter ends with an introduction to the small scale variants of the AES: a handy tool for algebraic attacks considered later on.

The next **Chapter 4** is devoted to the algebraic properties of the AES. In particular, linear

components of the AES are analyzed. One sees that the affine part of the AES S-Box can be moved to the diffusion part and together with linear maps defined there forms an *augmented linear diffusion*. It is shown that the linear map, which is the composition of the S-Box linear part, `ShiftRows`, and `MixColumns` (both latter are defined in the previous chapter), has an order 16 and, among other things, has a 16-dimensional invariant subspace. Further the chapter explores different algebraic representations of the AES. It is shown that one may embed state and key spaces of a cipher to other state and key spaces in order to get a representation different from the initial one. As an example the authors provide the Big Encryption Standard (BES). By embedding the AES to BES the authors solve the problem of using two different inner representations that exist in the AES: considering bytes as $GF(2)$-vectors of length 8 and as elements of the finite field $GF(2^8)$. The S-Box inversion operation is then efficiently implemented in BES, which has certain advantages for writing the corresponding algebraic system of equations over $GF(2^8)$, see below. After considering some more cipher representations, the reader is going to find out more about group structure of the AES. Since group properties of ciphers play an important role for their analysis, this question deserves careful attention. The main results of the section are the facts that the AES round function is an even permutation and that the group generated by the AES round functions is the alternating group $A_{2^{128}}$.
Chapter 5 "Equation Systems for the AES" together with the next Chapter 6 give an introduction to the algebraic cryptanalysis of the AES. Namely, **Chapter 5** shows how one can compose different algebraic systems of equations for the AES, which solution would reveal the secret key. The idea here is, having one (or few) plaintext/ciphertext pairs, to compose a system of equations over a finite field. Unknowns of such systems would be variables that reflect encryption process and key schedule. The chapter first shows how one can obtain such a system over $GF(2)$, by efficiently deriving equations for S-Boxes. Therewith one obtains a sparse quadratic system of equations over $GF(2)$. Using the BES, see above, one is able to write the quadratic system over $GF(2^8)$, which is even sparser than the former one: the non-linear component of the cipher is simply written as $xw = 1$ for an input byte x and an output byte w. Sizes of such systems are analyzed as well as some other related issues.
Chapter 6 focuses on the tools that are needed to solve the algebraic systems from the previous chapter. The overview of algorithms that compute Gröbner bases: Buchberger's algorithm and F4/F5, is given. Complexity issues as well as some experimental results using the small scale variants are considered here. Next the well-known in crypto community XL-method is considered: its description, properties, and problems. It is mentioned that actual performance of algorithms from the XL-family was somewhat overestimated in some previous studies. More exact complexity estimates are provided. The chapter ends with describing some dedicated methods for solving systems that arise in the algebraic cryptanalysis of the AES. In particular, the meet-in-the-middle approach is discussed, where instead of solving the whole system one tries to do computations for the first and the second half of the encryption process separately. Then one combines obtained pieces of information, the corresponding Gröbner bases, to obtain the desired solution.
The book is concluded in **Chapter 7** with some closing remarks and Appendix. **Appendix**, in particular, contains an algebraic system for one of the small scale variants to illustrate the idea from Chapter 5.

2 What is the book like

The book of Cid et. al. gives an excellent introduction and an overview of algebraic properties of the AES and contains results of the authors' own research. Although the book is not big, it contains precise and quite thorough description of the subject. Since the book is also suitable

for "advanced level students" as the authors state, it would not be unnecessary to have some exercises in the book.
The way the book is written is overall pleasant. The reader who is ok with mathematical language should have no problem reading it. The material is not overwhelmed with heavy mathematical results/proofs/notions. Section 1 and 5 of Chapter 4, though, require some more preparation and in principle can be dropped out during the first reading.
A reader will not find too much technical details in the book. Instead the book presents main ideas of algebraic structure of the AES. The long list of references provides further reading targets. Therewith one may go deeper into detail.

3 Recommendation

Considering that the book contains also necessary mathematical background overview, it is readable for engineers and cryptographers without a particular pre-knowledge of algebra. On the other hand, the book will be also interesting for mathematics and computer science students who may obtain a great insight to possible applications of modern algebraic notions, such as Gröbner bases. I would not recommend the book as a course text, but rather a supplementary reading material. An instructor could use certain pieces of the book for student seminars, either on applications of algebra or on cryptology. As such a supplementary reading material the book is appropriate for Master and Ph.D. students.
The book was published in 2006. Since then some new developments in the area of algebraic cryptanalysis appeared. Namely, solving equations in the Boolean ring, using SAT-solvers for cryptanalysis etc. As newly appeared further reading I may recommend:

- C. Cid, R.-P. Weinmann, "Block Ciphers: Cryptanalysis and Gröbner Bases," in *M. Sala et. al (Eds.) "Gröbner Bases, Coding, and Cryptography"*, Springer, pp. 307–327, 2009.

- G.V. Bard, "Algebraic Cryptanalysis", Springer, 2009.

The reviewer is a post-doc at the CASED, Darmstadt, Germany.