Review of the book

"Gröbner Bases, Coding, and Cryptography" by Massimiliano Sala, Teo Mora, Ludovic Perret, Shojiro Sakata, and Carlo Traverso (Editors) Springer, 2009

ISBN: 978-3-540-93806-7

Stanislav Bulygin
Center for Advanced Security Research Darmstadt (CASED)

1 What the book is about

As the title of the book suggests the book as about applications of Gröbner bases to coding theory and cryptography. The book came as a result if the D1 workshop of the Special Semester on Gröbner Bases that took place in Spring of 2006 at RISC (Research Institute for Symbolic Computation), Austria.

The content of the book is divided into two parts: "Invited Papers", meaning overview chapters on select topics, and "Notes", meaning small notes that reflect some presentations at the D1 workshop of the Semester or related material. The core of the book is the "Invited papers" part. It, as well as "Notes", can be further divided into three parts: Gröbner bases, coding theory, and cryptography. In this review I will concentrate more on the cryptography part due to obvious reasons.

There are two chapters on Gröbner bases by Teo Mora, well-known expert in the field. The chapters give very general and quite deep introduction to the theory of Gröbner bases. Of special importance is the second chapter, which addresses techniques for zero-dimensional ideals that are relevant for applications in the book. Then a very considerable piece devoted to coding theory follows: eleven chapters. They cover a very wide range of topics, starting from a general introduction to codes and decoding, Gröbner-based techniques for decoding cyclic and algebraic-geometric codes, and ending with such "exotic" topics as codes over rings and Gröbner methods for those.

There are four chapters devoted to cryptography and cryptanalysis. Here I would like to be more detailed. First, there is a chapter about cryptanalysis of multivariate schemes by Oliver Billet and Jintai Ding. The chapter outlines different methods that are used for cryptanalyzing multivariate schemes. Starting with the initial scheme of Matsumoto and Imai the authors show an elegant method for breaking this scheme by finding bilinear relations between plaintext and ciphertext. This cryptanalysis led to creation of (unbalanced) Oil and Vinegar schemes and their variations. Some methods for attacking these schemes are described. Techniques that aim at preventing direct attacks, like removing and adding equations to a public key system are considered next. As opposed to direct attacks that basically try to solve the underlying hard multivariate system, structural attacks address inner structure of a public key. Here the problem of isomorphism of polynomials plays a crucial role, which is explained in the chapter. The chapter possesses an extensive reference list for the topic.

The second chapter by French/Italian team of F. Levy-dit-Vehel, M.G. Marinari, L. Perret, and

C. Traverso is devoted to the so-called Polly Cracker cryptosystems. In this chapter the topic is overviewed probably for the first in this broadness. A general definition of Barkee et al. as well as more specific of Koblitz and Fellows are given. Whereas Gröbner bases play a cryptanalytic role in multivariate schemes, they play a constructive role here: secret keys are certain Gröbner bases. Immediate, but quite interesting attacks on the Barkee scheme are outlined, which rely on linear algebra. It is shown that an attacker does not have to compute a secret Gröbner basis, because a plaintext simply "shines through" the corresponding ciphertext. Further in the chapter it is shown how to obtain Polly Cracker schemes (terminology of Fellows and Koblitz) from several NP-complete graph problems. An approach based on the hard 3-SAT problem is also considered. More sophisticated attacks break also these schemes. Again as was the case with the linear algebra attacks, monomials of the plaintext polynomial can be deduced from the ciphertext polynomial. It is shown that even further ideas, like Polly Two (using two different polynomial rings in the definition) and non-commutative Polly-Cracker have the same problem: it is just hard to disguise the plaintext good enough! Nevertheless, some new developments also mentioned that could possibly escape existent problems.

In the next chapter by Carlos Cid and Ralf-Philipp Weinmann the reader will get an overview of the algebraic cryptanalysis of block ciphers. After a brief introduction to block cipher cryptanalysis, methods of algebraic attacks are described. Namely, how to obtain different representations of block ciphers as algebraic systems of equations. As proving grounds for these ideas one is introduced next to experimental small ciphers that give an opportunity to test algebraic attacks. In particular, small scale AES, ciphers Flurry and Curry, inventions of the authors, are considered together with experimental results of Gröbner-based attacks. More advanced ideas are mentioned next, like meet-in-the-middle, combination with differential cryptanalysis, SAT-solving.

The last chapter in the crypto-series is by Frederik Armknecht and Gwenolé Ars and is devoted to algebraic attacks on stream ciphers. Due to their structure, stream ciphers appear to be much more susceptible to algebraic attacks, than blocks ciphers. The chapter starts with a brief introduction to stream ciphers, namely the notion of an (m, l)-combiner is introduced. Further it is shown how algebraic techniques, and in particular Gröbner bases, can help in obtaining and solving systems of equations for attacking stream ciphers. The notion of algebraic immunity, the lowest degree of an algebraic dependence relation between inputs and outputs, is defined and analyzed.

Finishing this section, I would like to mention also two short notes devoted to algebraic immunity and estimating pseudo-randomness of Boolean functions. In these short notes it is shown how Gröbner techniques may help in computing these quantities.

2 What is the book like

Now let me comment on the style of the book. It must be said that the Gröbner theory introduction is very thorough and is made for quite a general setting. This level of generality and detail makes it a hard-to-read material for those who are not very familiar with abstract algebra notions. So for those who just need a basic introduction some other source could be more appropriate. On the contrary, advanced algebra students will find the chapters very interesting and useful. It is a good exercise to go through the material, carefully reproducing all the "obvious" results there. The coding part is also very detailed and technical. It is a good field for algebraists that want to do some applications of the theory. In contrast to other coding-material, the introductory chapter by D. Augot, E. Betti, and E. Orsini is quite elementary and suitable for a novice reader. On the contrary from the most of the coding part, the crypto part is not very heavy and is quit easy to read. Extent to which material is detailed here is lower.

This will make the reader go for numerous references listed there. The authors of the crypto part made it really an overview, rather than self-contained theory-tools-examples kit of the coding theory. The reader is to decide, which solution is better. It must be stressed that many things that appear in this book appear really for the first time. It is the best book for getting an overview of applications of Gröbner bases in the fields of coding theory and cryptography.

3 Recommendation

As has already been mentioned, the Gröbner as well as coding parts are quite involved. Therefore, I would recommend them for advanced math/algebra students interested in Gröbner bases and their applications. The crypto part is quite readable, so is well suitable also for computer science/engineering students that have some background in algebra. For more elementary introduction to Gröbner bases for these students I would recommend the book of D. Cox, J. Little and D. O'Shea "Ideals, Varieties, and Algorithms". Below are some suggestions for further reading (very subjective choice, I guess):

- G.V. Bard, "Algebraic Cryptanalysis", Springer, 2009.
- S. Bulygin and R. Pellikaan, "Decoding and finding the minimum distance with Gröbner bases: history and new insights". To appear as a chapter in *"Selected Topics in Information and Coding Theory"*, World Scientific, 2009.
- C. Cid, S. Murphy, and R.J.B. Robshaw, "Algebraic aspects of the Advanced Encryption Standard", Springer, 2007.
- J. Ding, J.E. Gower, D. Schmidt, "Multivariate Public Key Cryptosystems", Springer, 2006.

The reviewer is a post-doctoral researcher at the CASED.