Review of the book

"Multivariate Public Key Cryptosystems"

by Jintai Ding, Jason E. Gower and Dieter S. Schmidt

Springer, 2006

ISBN: 0-387-32229-9, 978-0-387-32229-2

Albrecht Petzoldt
Technische Universität Darmstadt, Germany

1 What the book is about

As the title says, this book is about Multivariate cryptography. Besides code-, lattice- and hash-based cryptosystems, Multivariate cryptography is one of the main fields of cryptosystems which are believed to be secure against attacks with quantum computers.
Multivariate cryptography deals with systems of nonlinear polynomial equations in several variables over a finite field which are difficult to invert. Encryption and signature verification consists in simple evaluation of the polynomials. Only with some knowledge about the internal structure of the systems it is possible to invert them and therefore to decrypt or sign messages.

2 What is this book about (summary)?

The book gives an overview of the field of multivariate cryptography.
In the first chapter the authors give an introduction into public key cryptography and multivariate cryptography. Furthermore, they present the three techniques to build multivariate cryptosystems: Bipolar Schemes, Mixed Systems and Isomorphism of Polynomials. The chapter ends with some general remarks concerning the security and efficiency of multivariate schemes and an overview of the first attempts to create such cryptosystems.

The next three chapters describe in detail the three most important types of practically used and historically important multivariate schemes.

Chapter 2 deals with multivariate schemes of the Matsumoto-Imai (MI) type, which include the oldest multivariate schemes. After describing the basic construction of the original C*-scheme by Matsumoto and Imai and a toy example of the scheme, the authors describe a variant of C* called Multiple branch MI and make some remarks concerning key size and efficiency of the scheme. The next two subsections deal with the cryptanalysis of C* including the Linearization attack of Patarin which he used to break the original system. Finally, the authors present some variants of C* which defend the original scheme against those attacks, including Sflash, which was chosen in 2003 by the European Commission as a standard for signatures on low cost devices.

In Chapter 3 the authors describe multivariate schemes of the Oil and Vinegar type, which are convenient for signatures. In the first Section one can find a detailed description of the scheme and a toy example. The next Section deals with the cryptanalysis of the original balanced Oil and Vinegar scheme and countermeasures against this attack. After that the authors describe the Rainbow signature scheme, which is based on Oil and Vinegar, but provides higher efficiency and security as well as a security analysis of this scheme. The chapter ends with a short comparison of Rainbow with other multivariate schemes.

The topic of Chapter 4 are HFE schemes (Hidden Field Equations), which are an extension of the MI schemes presented in Chapter 2. After the basic construction and a toy example of such a scheme the authors describe a possible attack against HFE. The last two sections of this chapter deal with variants of the basic HFE scheme, especially with HFEv and QUARTZ, and their cryptanalysis.

In Chapter 5 the authors describe a technique called Internal Perturbation, which can be applied on several multivariate schemes to increase their security. They present how Internal Perturbation can be applied to the MI Scheme of Chapter 2 and give a toy example for it. After that, they present attacks against the perturbed scheme and show a way how to prevent them. In the last section of this chapter it is shown how to apply Internal Perturbation to the HFE scheme of Chapter 4.

Chapter 6 deals with the so called triangular schemes, which play a major role when creating multivariate schemes with sparse keys. In the first section the authors discuss the Jacobian conjecture and the problem of tame transformations on which these schemes are based. The next five sections contain a description of TTM (Tame Transformation Method) and TTS (Tame Transformation Signature) schemes and attacks against them. The focus here lies on the cryptanalysis, and it is shown, that all the systems presented so far in this chapter are insecure. At the end of the chapter the authors mention the existence of TTS schemes which resist these attacks and therefore are thought to be secure. They also describe how triangular schemes could be further generalized.

In Chapter 7 the authors discuss the various possibilities to attack a multivariate scheme "directly", which means by solving the public equations. The first two sections give results from algebraic geometry and from the theory of Groebner bases and present Buchbergers algorithm. Section 3 describes Faugere's F_4 and F_5 algorithms and shows how these algorithms can be used to break the HFE scheme. Section 4 deals with the XL-algorithm and its variants, whereas Section 5 discusses connections between XL and Groebner Basis algorithms and gives complexity estimations for them. Finally, Section 6 describes the Zhuang-Zi-algorithm, which solves a system of polynomial equations by lifting it to an extension field.

The 8-th and last chapter has the title "Future Research". It contains general remarks and open questions about the construction of multivariate schemes, their security and possible applications, as well as some additional remarks about the mathematics underlying this field of cryptography.

In an appendix the authors present in short form the basic results from the theory of finite fields as far as needed during the book.
The book ends with a large number of references for further reading.

3 What is the book like (style)?

The authors of this book describe both schemes and attacks in great detail. They divide between short descriptions, how a given scheme works and the mathematical background behind it. The descriptions of cryptosystems are clear and well-structured in key-generation, encryption and decryption. The same can be said for the description of attacks: You can find both algorithms which tell you in short form what has to be done during the attack as well as passages which explain the underlying mathematics. Especially in these sections the structure of the book is very similar to other mathematical textbooks and consists mainly of definitions, lemmata and theorems. But, as already said, the essentials of a scheme or an attack are always summarized in a short block. So a reader, who is only interested in implementing a scheme, can easily find the information he needs.
Many toy examples (both for the schemes and for attacks) help the reader to understand the matters correctly. The MAGMA codes used to create them can be found on the webpage of the book.

4 Would you recommend this book?

I would recommend the book for people who want to get an overview over this new field of cryptography. For example, it should be useful as a textbook for masterstudents in the field of information security. It is also a good starting point for those, who are interested to begin their own research in Multivariate cryptography. In the book, they can learn about the most important families of multivariate schemes and the main attacks against them. Especially in the last chapter a number of open questions which encourage the reader to do his own research in this field can be found.
Of course, a book of 250 pages can not contain every detail of this area. For those, who are interested in further reading, there are a huge number of references (9 pages).
The only little drawback of this book is, that it was written four years ago, which is, in a fast developing area like Multivariate cryptography, a long time. Therefore some of the more recent developments, like differential attacks against Sflash or the liC-schemes, are not contained in this book. So, the authors should think of a new edition of this book.

The reviewer is a Ph.D. student at Technische Universität Darmstadt, Germany.