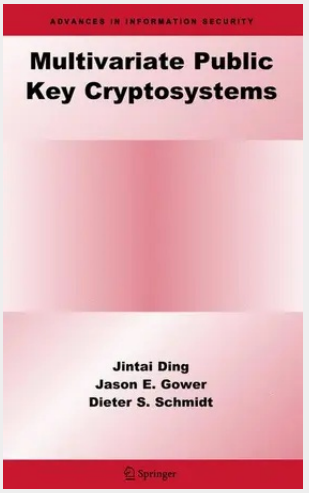
Ding / Gower / Schmidt

Multivariate Public Key Cryptosystems

Multivariate public key cryptosystems (MPKC) is a fast-developing area in cryptography. This book systematically presents the subject matter for a broad audience and is the first book to focus on this exciting new topic. Information security experts in industry can use the book as a guide for understanding what is needed to implement these cryptosystems for practical applications, and researchers in both computer science and mathematics will find it a good starting point for exploring this new field. It is also suitable as a textbook for advanced-level students.

Multivariate public key cryptosystems (MPKC) is a fast-developing new area in cryptography. In the past 10 years, MPKC schemes have increasingly been seen as a possible alternative to number theoretic-based cryptosystems such as RSA, as they are generally more efficient in terms of computational effort. As quantum computers are developed, MPKC will become a necessary alternative. Multivariate Public Key Cryptosystems systematically presents the subject matter for a broad audience. The first chapter is an introduction to the basic ideas and early development of both multivariate public key cryptography and signature schemes. The next five chapters deal with the main families of multivariate schemes, and the concept of perturbation, the means by which the security of various schemes can be improved without much cost in efficiency. Each family is introduced in terms of the origin of the mathematical idea behind its construction, followed by generalizations and related attacks specific to that family. Generic attacks that apply to any family, in particular methods for solving systems of multivariate polynomial equations over a finite field, are addressed in Chapter 7, followed by a discussion in Chapter 8 of the future of MPKCs. Information security experts in industry can use the book as a guide for understanding what is needed to implement these cryptosystems for practical applications, and researchers in both computer science and mathematics will find it a good starting point for exploring this new field. It is also suitable as a textbook for advanced-level students. Written more from a computational perspective, the authors provide the necessary mathematical theory behind MPKC; students with some previous exposure to abstract algebra will be well-prepared to read and understand the material.



146,50 €
136,92 € (zzgl. MwSt.)

Nicht mehr lieferbar

Artikelnummer: 9780387322292
Medium: Buch
ISBN: 978-0-387-32229-2
Verlag: SPRINGER NATURE
Erscheinungstermin: 31.08.2006
Sprache(n): Englisch
Auflage: 2006
Serie: Advances in Information Security
Produktform: Gebunden
Gewicht: 1270 g
Seiten: 260
Format (B x H): 160 x 241 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)