Multivariate Public Key Cryptosystems

Advances in Information Security

Sushil Jajodia
Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

UNDERSTANDING INTRUSION DETECTION THROUGH VISUALIZATION by Stefan Axelsson; ISBN-10: 0-387-27634-3
QUALITY OF PROTECTION: Security Measurements and Metrics by Dieter Gollmann, Fabio Massacci and Artsiom Yautsiukhin; ISBN-10: 0-387-29016-8
COMPUTER VIRUSES AND MALWARE by John Aycock; ISBN-10: 0-387-30236-0
HOP INTEGRITY IN THE INTERNET by Chin-Tser Huang and Mohamed G. Gouda; ISBN-10: 0-387-22426-3
CRYPTOGRAPHICS: Exploiting Graphics Cards For Security by Debra Cook and Angelos Keromytis; ISBN: 0-387-34189-7
PRIVACY PRESERVING DATA MINING by Jaideep Vaidya, Chris Clifton and Michael Zhu; ISBN-10: 0-387- 25886-8
BIOMETRIC USER AUTHENTICATION FOR IT SECURITY: From Fundamentals to Handwriting by Claus Vielhauer; ISBN-10: 0-387-26194-X
IMPACTS AND RISK ASSESSMENT OF TECHNOLOGY FOR INTERNET SECURITY:Enabled Information Small-Medium Enterprises (TEISMES) by Charles A. Shoniregun; ISBN-10: 0-387-24343-7
SECURITY IN E-LEARNING by Edgar R. Weippl; ISBN: 0-387-24341-0
IMAGE AND VIDEO ENCRYPTION: From Digital Rights Management to Secured Personal Communication by Andreas Uhl and Andreas Pommer; ISBN: 0-387-23402-0
INTRUSION DETECTION AND CORRELATION: Challenges and Solutions by Christopher Kruegel, Fredrik Valeur and Giovanni Vigna; ISBN: 0-387-23398-9
THE AUSTIN PROTOCOL COMPILER by Tommy M. McGuire and Mohamed G. Gouda; ISBN: 0-387-23227-3

Additional information about this series can be obtained from
http://www.springer.com

Multivariate Public Key Cryptosystems

by

Jintai Ding
Jason E. Gower
Dieter S. Schmidt
University of Cincinnati
USA

Springer

Jintai Ding
University of Cincinnati
Dept. Mathematical Sciences
P.O.Box 210025
Cincinnati OH 45221-0025
ding@math.uc.edu

Jason E. Gower
University of Cincinnati
Dept. Mathematical Sciences
P.O.Box 210025
Cincinnati OH 45221-0025
gowerj@math.uc.edu

Dieter S. Schmidt
Dept. of ECECS
P.O.Box 210030
Cincinnati, Ohio 45021-0030
dieter.schmidt@uc.edu

Library of Congress Control Number:

Multivariate Public Key Cryptosystems
by Jintai Ding, Jason E. Gower and Dieter S. Schmidt

ISBN-10: 0-387-32229-9
ISBN-13: 978-0-387-32229-2
e-ISBN-10: 0-387-36946-5
e-ISBN-13: 978-0-387-36946-4

Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

springer.com

This book is dedicated to our families,

in particular,

Romeliza Villegas-Ding

Contents

List of Figures

List of Tables

Introduction

In the last ten years, multivariate public key cryptosystems, or MPKCs for short, have increasingly been seen by some as a possible alternative to the public key cryptosystem RSA, which is widely in use today. The security of RSA depends on the difficulty of factoring large integers on a conventional computer. Shor's polynomial-time integer factorization algorithm for a quantum computer means that eventually such alternatives will be necessary, provided that we can build a quantum computer with enough quantum bits.

A result from complexity theory states that solving a set of randomly chosen nonlinear polynomial equations over a finite field is NP-hard. So far quantum computers have not yet been shown to be able to solve a set of multivariate polynomial equations efficiently, and the consensus is that quantum computers are unlikely to provide an advantage for this type of problem. Moreover, MPKC schemes are in general much more computationally efficient than number theoretic-based schemes. This has led to many new cryptographic schemes and constructions such as the Matsumoto-Imai cryptosystem (C^* or MI), the Hidden Field Equations cryptosystem (HFE), the Oil-Vinegar signature scheme, the Tamed Transformation Method cryptosystem (TTM), and cryptosystems derived from internal perturbation. Some of these schemes seem to be very suitable for use in the ubiquitous computing devices with limited computing capacity, such as smart cards, wireless sensor networks, and active RFID tags. Indeed, Flash, also known as Sflash^{v2}, a multivariate signature scheme, was recently accepted as a security standard for use in low-cost smart cards by the New European Schemes for Signatures, Integrity and Encryption (NESSIE): IST-1999-12324.

In general, multivariate public key cryptosystem is a public key cryptosystem in which the public key is a set of multivariate polynomials $f_1, \ldots, f_m$ in $k[x_1, \ldots, x_n]$, where k is a given finite field. If Alice wants to send the message $(x'_1, \dots, x'_n) \in k^n$ to Bob, she looks up Bob's public key, computes $y'_i = f_i(x'_1, \dots, x'_n)$ for $i = 1, \dots, m$, and sends the encrypted message $(y'_1, \dots, y'_m)$. Bob's secret key will be some information about the construction of the f_i without which it is computationally infeasible to solve the system $f_1(x_1, \dots, x_n) = y'_1, \dots, f_m(x_1, \dots, x_n) = y'_m$ for $x_1, \dots, x_n$.

Of course, Bob will need a secret key to recover Alice's message, and this indicates that the NP-hardness of the multivariate polynomial equation solving problem does not necessarily guarantee the security of practical schemes, though intuitively it does suggest that the more we can make the polynomial appear to be "random," the more secure the scheme is likely to be.

Research on MPKCs has undergone rapid development in the last decade, providing many interesting results in designing and attacking the MPKCs with examples as previously stated. In addition, the study of MPKCs has also resulted in new ideas in solving systems of multivariate polynomial equations over a finite field, a purely mathematical problem that lies in the area of algebraic geometry. This has also attracted a lot of attention. New work in this direction includes the linearization equations, the XL family of algorithms, the new Gröbner basis algorithms, and the Zhuang-Zi algorithm.

We believe that this area has developed to the point where a book is needed to systematically present the subject matter to a broad audience, including information security experts in industry, computer scientists and mathematicians. We hope that this book can be used in the following ways: by industry experts as a guide for understanding the basic mathematical structures needed to implement these cryptosystems for practical applications, as a starting point for researchers in both computer science and mathematics looking to explore this exciting new field, or as a textbook for a course in MPKC suitable for beginning graduate students in mathematics or computer science. Due to the above considerations, this book has been written more from the computational perspective, though we have tried to provide the necessary mathematical background.

It should be noted that there are usually several improvements on the schemes that we present, in particular in terms of the efficiency of the computation in both implementation and attacks. However, to keep the size of this book reasonable and to keep the book more focused, we have chosen not to cover some of these details. Instead, we have tried to present the essential ideas, methods, and examples so that a reader will not be distracted by technical details that can be found in the references provided. Nevertheless, for those readers interested in the practical side of the MPKCs, we highly recommend reading through the details in order to discover improvements. Improving the performance of a cryptosystem by even a small factor may not be significant from a mathematical perspective, but can be very important in practice.

This book is arranged not in historical order but rather in terms of the mathematical ideas behind each topic. We begin with an overview of the basic ideas and early development of both multivariate public key cryptography and signature schemes. We next present the main families of multivariate schemes: MI, Oil-Vinegar, HFE, and TTM. We also present 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 can be applied to any MPKC, in particular methods for solving systems of multivariate polynomial equations over a finite field, are then addressed, followed by a discussion of the future of MPKCs. The reader will find one supplementary appendix at the end of the book where we have collected results from finite field theory needed in the main text of the book.

This book grew out of a survey paper written by Jintai Ding and Dieter Schmidt, and from the lecture notes for a graduate course at the University of Cincinnati taught by Jintai Ding during the 2004–2005 and 2005–2006 academic years. Indeed, we have written this book to be used as a text for a year-long course in advanced topics in cryptography or applied algebra, or as a supplementary text for a first course in cryptography. Students with some previous exposure to abstract algebra (groups, rings, fields and ideals) will be more than well-prepared to read and understand the various topics. For those with a programming background, we plan to develop a website where we will make our related software available at

`http://math.uc.edu/~aac/MPKC/software.html`

for public use. This will provide interested readers a starting point to further develop their understanding and computational intuition by experimenting with the software. Those readers new to the field of MPKC will be best served by first reading the introductory chapter, after which the chapters are written so as to be essentially self-contained. Readers with previous exposure to MPKC may use the text to learn more about a given scheme and as a guide to related articles. Although it was our intention to include all related references, we apologize to those we have missed. Also, the amount of space devoted to a given topic is not necessarily related to how important we consider it. Rather it is likely due to space constraints or to maintain the consistency and convenience of the structure and flow of the book.

We plan to maintain a webpage at

`http://math.uc.edu/~aac/MPKC/errata.html`

where we will list corrections to the book. Readers are encouraged to submit their findings to that website or send them via e-mail to `aac@math.uc.edu`.

We would like to thank Robert Hess, Timothy Hodges, Gregory Hull, Crystal Updegrove, and John Wagner for attending the lectures and giving thoughtful feedback about the lectures and the early stages of the book. We would like to also thank Jiun-ming Chen, Lei Hu, Christopher Wolf, Bo-yin Yang for reading the book and providing us with their valuable comments. Many thanks go to the staff at Springer for their constant support and help, and to the Department of Mathematical Sciences at the University of Cincinnati for their support. Finally, we would like to thank our families for their constant support and encouragement.