Mathematics Monograph Series **31**

# Mathematical Foundations of Public Key Crytography

Xiaoyun Wang Guangwu Xu
Mingqiang Wang Xianmeng Meng

(公钥密码学的数学基础)

SCIENCE PRESS
Beijing

CRC Press
Taylor & Francis Group

Mathematics Monograph Series 31

# Mathematical Foundations of Public Key Cryptography

(公钥密码学的数学基础)

Xiaoyun Wang Guangwu Xu
Mingqiang Wang Xianmeng Meng

SCIENCE PRESS
Beijing

CRC Press
Taylor & Francis Group
Boca Raton London New York

Responsible Editor: Yuzhuo Chen

Published by Science Press
16 Donghuangchenggen North Street
Beijing 100717, P. R. China

Printed in Beijing

ISBN 978-7-03-047430-8 (Beijing)
ISBN 978-1-4987-0223-2 (New York)

# Editorial Board

# Preface to Mathematics Monograph Series

Science Press asked me to write a preface for their series of books called "Mathematics Monograph Series". They told me that the Press had published nearly 30 mathematical monographs in this series since 2006. This reminded me that, also in 2006, I received an email message from the Editor in Chief of "Sugaku Tushin" ("Mathematical Communications", the membership magazine of the Mathematical Society of Japan). The Editor in Chief told me that they were planning to have a special section on "Recent development in Chinese mathematical community", and invited me to write an article for the special section. As a result, I published in their magazine an article called "Some Aspects of Mathematical Community in China". Among other things, in the article I demonstrated that, with the favorable environment, the Chinese mathematical community had made great progress since the late 1970s (when China started to implement "Reform and Opening-up Policy"): A large number of publications (including articles and monographs) have been written by Chinese mathematicians, there have been always Chinese mathematicians presenting their speeches at various international academic conferences or workshops, many Chinese mathematicians have served as editors of international academic journals, or as members in various academic organizations. All these reveal that the Chinese mathematical community which has been growing rapidly has exerted more and more influence in the world.

Indeed, the series of mathematical monographs published by Science Press reflects partly more and more influence of Chinese mathematical community in the world. Chinese people are good at mathematics. In the past, Science Press published many high level mathematical monographs and textbooks. Among them some were written in Chinese and some were written in English. Some monographs which appeared originally in Chinese have been purchased by international publishers who then re-published them abroad in English, and this has gained influence in corresponding areas of the international mathematical community.

In recent years most Chinese mathematicians have mastered good English. In accordance with this situation, Science Press has decided to publish "Mathematics Monograph Series" — a series in which high level mathematical monographs and textbooks are written directly in English. The goal of this series is to provide further good service for Chinese mathematicians and to enhance further the influence of the mathematics study in China in the international mathematical community.

I would like to conclude this short preface with the following wish which I expressed also at the end of the afore mentioned article "Some Aspects of Mathematical Community in China":

The Chinese mathematical community will continuously make its effort to work hard, and to strengthen its international exchanges and collaborations, so as to make more contributions to the study and development of mathematics in the world.

Zhi-Ming Ma
March 15, 2015

# Foreword

As a cornerstone of information security, cryptography is a subject with an ancient history, but it also is an emerging discipline that is widely and effectively used in many areas of modern society. One of the two fundamental issues of cryptography is to securely encrypt information so that a third party will not get the content from its encrypted form. The other one, in contrast, is how to break the encryption and get the information from its encrypted form. There are many methods that can be used in cryptography to protect information and break codes. Mathematics has always been an important tool in cryptography. With the invention of public key cryptosystem, mathematics has been playing an indisputably important role in cryptography, so cryptography has also become a special subject of mathematics.

Professor Xiaoyun Wang has always attached great importance to training students in information security and building its core curricular structure. "Number Theory and Algebraic Structures" is a core course for cryptography, and she started to write lecture notes for the course as early as 2003. These lectures were successfully taught at both Shandong University and Tsinghua University, China. In collaboration with Guangwu Xu, Minqiang Wang, and Xianmeng Meng, Professor Wang revised and extended these lecture notes and published them in this book. Since the content of this book has been described in detail by the authors in the preface, I am not going to go over that again here. However, I do want to point out that this book has a distinctive feature; namely, it closely integrates basic number theory and algebra into cryptographic algorithms and complexity theory in a well-organized manner throughout this book. This is of great importance for training students in cryptography to have a unique way of thinking. My feeling is that the "formalization," which has been a quite effective way of thinking in mathematics, is hard to work directly in cryptography as it seems that the "formalization" thinking does not lead one to the essence of cryptographic problems. This is a key problem that needs special attention for mathematicians who decide to shift their research to cryptography. Therefore, this book will definitely play a very positive role in improving the quality of core courses in information security curriculum.

Professor Xiaoyun Wang studied with my brother, Professor Chengdong Pang, a strong advocate in applying mathematics to science and technology. He participated in the preliminary research of seepage theory, thin shell theory, spline theory and application, directional blasting, and so on. Around 1990, he spearheaded the effort to establish a cryptography research group and train graduate students at Shandong University, China. Professor Xiaoyun Wang was the most accomplished researcher in this rather successful group. In the field of cryptanalysis, she has proposed and developed a theory and technique for collision attack of hash functions, successfully breaking some major popular cryptographic hash functions, such as MD5 designed by the Turing award recipient Rivest and SHA-1 designed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) of the United States. These hash functions were the core components of commonly used digital signatures and digital certificates. Professor Wang's research has surprised the cryptography community, prompting the NIST to initiate a 5-year project for the new standard hash function SHA-3 in 2007. She has also made great contributions in analyzing message authentication codes and designing cryptographic algorithms. She led the design of hash algorithm SM3, which has been adopted as the national commercial hash algorithm.

Although I am not an expert in cryptography, I am delighted to write the Foreword to Xiaoyun Wang's book, as I feel it is my responsibility and obligation to do so. I hope that she will continue to passionately dedicate herself to research and teaching without being distracted by fame and gain.

Chengbiao Pan

# Preface

Ever since Diffie and Hellman proposed the idea of public key cryptography, cryptographers have designed many topical public key algorithms. The security of all of these algorithms is based on some classical hard problems in mathematics, for examples, the integer factorization problem, the discrete logarithm problem, the knapsack problem, and the shortest vector problem in a lattice. The study of fast algorithms to solve these hard mathematical problems lies at the heart of the cryptanalysis of public key algorithms. In order for students in information security to successfully and effectively grasp the basic theory of modern cryptography and have a deeper understanding of the interdisciplinary nature of cryptography and mathematics, we wrote *Mathematical Foundations of Public Key Cryptography* as a textbook to help students lay a solid foundation in mathematics for their future study. The theoretical knowledge involved in this book includes the fundamentals of mathematics necessary for modern cryptography, especially public key cryptography. Therefore, this book serves as a textbook for undergraduate students in information security and also as a reference book for professionals in cryptography.

The lecture notes "Number Theory and Algebraic Structures," which the authors started to write when the information security program at Shandong University, China was founded in 2003, contain the basic mathematical knowledge needed for modern cryptography, especially public key cryptography. Rather than simply combining number theory and modern algebra, this book features the interdisciplinary characteristics of cryptography and reveals the integrations of mathematical theories and cryptographic applications. This book has three distinguishing features: First, the basic content of number theory and algebra covers the important mathematical concepts necessary for cryptography. For instance, we have introduced some fundamental concepts and methods in elementary number theory, such as the division algorithm, Euler's theorem, the Chinese remainder theorem, and primitive roots; we have also described some widely used mathematical theories and methods for cryptography, such as finding greatest common divisors using the division algorithm, the operation of computing modulo inverse, discrete logarithms, and integer factorization. Second, we emphasize the close integration of theory and practice while paying attention to the practical side. We provide a sufficient number of practical exercises when we discuss important algorithms so that students will understand the applications of theory in practical situations. The third feature is the incorporation of the complexity theory of algorithms throughout this book by introducing the basic number theoretic and algebraic algorithms and their complexities, so that readers would have some preliminary understanding of the applications of mathematical theories in cryptographic algorithms.

This book consists of 11 chapters. Basic theory and tools of elementary number theory, such as congruences, primitive roots, residue classes, and continued fractions, are covered in Chapters 1 through 6. Knowledge of primitive roots is the theoretical background required for the Diffie–Hellman public key algorithms, while continued fractions have important applications in the analysis of RSA public key algorithms as well as in integer factorization. The basic concepts of abstract algebra are introduced in Chapters 7 through 9, where three basic algebraic structures of groups, rings, and fields and their properties are explained. The Chinese remainder theorem, which has significant applications in the big integer multiplications and efficient implementation of cryptographic algorithms, is also covered in detail. Chapter 10 is about the basic theory of complexity and several related mathematical algorithms, including primality testing, the discrete logarithm problem, and the integer factorization problem. Chapter 11 presents the basics of lattice theory and the lattice basis reduction algorithm—the LLL algorithm and its application in the cryptanalysis of the RSA algorithm.

The early version of this book was used many times as lecture notes for information security majors at Shandong University. Based on the feedback, the authors revised and updated the lecture notes, which were eventually developed into the current version of this book. In Chapters 1 to 6, we mainly referenced *Elementary Number Theory* by Professors Chengdong Pan and Chengbiao Pan [1]. In Chapters 7 to 9, we referenced three independently authored textbooks on modern algebra, by Professors Pinsan Wu [2], Herui Zhang [3], and Shaoxue Liu [4] respectively.

Although we have strived to do our best with this book, it is inevitable that this book might still contain places of imperfections, so any suggestions or feedback will be greatly appreciated.

Xiaoyun Wang  
Guangwu Xu  
Mingqiang Wang  
Xianmeng Meng

# Contents