‘This volume celebrates the research career of Arjen Lenstra. The volume covers the latest research in many areas of applied cryptography: from algorithms for factoring and discrete log, to fast implementations of computer algebra, to the selection of cryptographic key sizes. Each topic is masterfully covered by a top researcher in the respective area. The information covered in this volume will serve readers for many years to come, and is sure to inspire further research on these topics.’

– Dan Boneh, Stanford University

‘This book demonstrates the breathtaking diversity of Arjen Lenstra’s research over the last 40 years, and the deep influence his work has had on computational aspects of cryptography. Each chapter is written by a leading domain expert and provides an “in a nutshell” overview of a specific topic. The book is sure to become an important reference for experts and beginners alike.’

– Kenneth Paterson, ETH Zurich

‘With highly accessible surveys by leading cryptographers, this book hits all pins with a single strike: framing the important area of “computational cryptography” through its fascinating history, peeking into its (no less prominent) future, and celebrating the impactful research career of one of its principal architects, Arjen Lenstra.’

– Ronald Cramer, CWI Amsterdam and Leiden University
Computational Cryptography
Algorithmic Aspects of Cryptology

Edited by

JOPPE W. BOS
NXP Semiconductors, Belgium

MARTIJN STAM
Simula UiB, Norway
Contents

**List of Contributors**

page x

**Preface**

xi

1 **Introduction**  *Joppe W. Bos and Martijn Stam*  
1.1 Biographical Sketch  
1.2 Outline  

9

**Part I Cryptanalysis**

2 **Lattice Attacks on NTRU and LWE:**  *Martin R. Albrecht and Léo Ducas*  
2.1 Introduction  
2.2 Notation and Preliminaries  
2.3 Lattice Reduction: Theory  
2.4 Practical Behaviour on Random Lattices  
2.5 Behaviour on LWE Instances  
2.6 Behaviour on NTRU Instances  

34

3 **History of Integer Factorisation**  *Samuel S. Wagstaff, Jr*  
3.1 The Dark Ages: Before RSA  
3.2 The Enlightenment: RSA  
3.3 The Renaissance: Continued Fractions  
3.4 The Reformation: A Quadratic Sieve  
3.5 The Revolution: A Number Field Sieve  
3.6 An Exquisite Diversion: Elliptic Curves  
3.7 The Future: How Hard Can Factoring Be?  

67
4 Lattice-Based Integer Factorisation: An Introduction to Coppersmith’s Method
Alexander May

4.1 Introduction to Coppersmith’s Method
4.2 Useful Coppersmith-Type Theorems
4.3 Applications in the Univariate Case
4.4 Multivariate Applications: Small Secret Exponent RSA
4.5 Open Problems and Further Directions

5 Computing Discrete Logarithms
Robert Granger and Antoine Joux

5.1 Introduction
5.2 Elliptic Curves
5.3 Some Group Descriptions with Easier Discrete Logarithms
5.4 Discrete Logarithms for XTR and Algebraic Tori
5.5 Discrete Logarithms in Finite Fields of Fixed Characteristic
5.6 Conclusion

6 RSA, DH and DSA in the Wild
Nadia Heninger

6.1 Introduction
6.2 RSA
6.3 Diffie–Hellman
6.4 Elliptic-Curve Diffie–Hellman
6.5 (EC)DSA
6.6 Conclusion

7 A Survey of Chosen-Prefix Collision Attacks
Marc Stevens

7.1 Cryptographic Hash Functions
7.2 Chosen-Prefix Collisions
7.3 Chosen-Prefix Collision Abuse Scenarios
7.4 MD5 Collision Attacks

Part II Implementations

8 Efficient Modular Arithmetic
Joppe W. Bos, Thorsten Kleinjung and Dan Page

8.1 Montgomery Multiplication
8.2 Arithmetic for RSA
8.3 Arithmetic for ECC
8.4 Special Arithmetic
Contents

9 Arithmetic Software Libraries  Victor Shoup  251
9.1 Introduction  251
9.2 Long-Integer Arithmetic  254
9.3 Number-Theoretic Transforms  259
9.4 Arithmetic in \( \mathbb{Z}_p[X] \) for Multi-Precision \( p \)  270
9.5 Arithmetic in \( \mathbb{Z}_p[X] \) for Single-Precision \( p \)  282
9.6 Matrix Arithmetic over \( \mathbb{Z}_p \)  286
9.7 Polynomial and Matrix Arithmetic over Other Finite Rings  289
9.8 Polynomial and Matrix Arithmetic over \( \mathbb{Z} \)  289
9.9 The Future of NTL  291

10 XTR and Tori  Martijn Stam  293
10.1 The Birth of XTR  293
10.2 The Magic of XTR  297
10.3 The Conservative Use of Tori  304
10.4 Pairings with Elliptic Curves  308
10.5 Over the Edge: Cyclotomic Subgroups Recycled  311

11 History of Cryptographic Key Sizes  Nigel P. Smart and Emmanuel Thomé  314
11.1 Introduction  314
11.2 Attacking Symmetric Algorithms with Software and Hardware  315
11.3 Software Attacks on Factoring and Discrete Logarithms  318
11.4 Hardware for Factoring  323
11.5 Attacking Cryptosystems Based on Elliptic Curves  325
11.6 Post-Quantum Cryptography  329
11.7 Key-Size Recommendation  332

References  335
Index  383
Contributors

Martin R. Albrecht  Information Security Group, Royal Holloway, University of London, United Kingdom
Joppe W. Bos  NXP Semiconductors, Leuven, Belgium
Léo Ducas  Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
Robert Granger  University of Surrey, Guildford, United Kingdom
Nadia Heninger  University of California, San Diego, USA
Antoine Joux  CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
Thorsten Kleinjung  EPFL, Lausanne, Switzerland
Alexander May  RUB, Bochum, Germany
Dan Page  University of Bristol, Bristol, United Kingdom
Victor Shoup  New York University, New York, USA
Nigel P. Smart  imec-COSIC, KU Leuven, Leuven, Belgium
Martijn Stam  Simula UiB, Bergen, Norway
Marc Stevens  Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
Emmanuel Thomé  Université de Lorraine, CNRS, INRIA, Nancy, France
Samuel S. Wagstaff, Jr  Purdue University, West Lafayette, USA
Preface

This book is a tribute to the scientific research career of Professor Arjen K. Lenstra, on the occasion of his 65th birthday. Its main focus is on computational cryptography. This area, which he has helped to shape during the past four decades, is dedicated to the development of effective methods in algorithmic number theory that improve implementation of cryptosystems or that further their cryptanalysis. Here, cryptanalysis of cryptosystems entails both the assessment of their overall security and the evaluation of the hardness of any underlying computational assumptions. In the latter case, the area intersects non-trivially with high-performance scientific computing. The technical chapters in this book are inspired by his achievements in computational cryptography.

Arjen is best known for his seminal work on the algorithmic aspects of various factorisation problems. In the early 1980s, he started with efficient factorisation of polynomials with rational coefficients. This work led to the celebrated Lenstra–Lenstra–Lovász lattice reduction algorithm. Furthermore, he devised factorisation techniques for polynomials defined over other algebraic structures, such as finite fields or number fields. Towards the end of the decade, his focus shifted to integer factorisation methods, particularly development of the number field sieve, and its impact on the selection of strong cryptographic keys for widely deployed cryptographic standards. His honours include the RSA Award for Excellence in Mathematics in 2008 and his lifetime appointment as Fellow of the International Association for Cryptologic Research (IACR) in 2009.

In addition to his rich research career, Arjen is a great educator and he has provided lasting inspiration to many of his students. We both were lucky enough to have him as our PhD supervisor and we will come back to our respective experiences momentarily. This book is intended for students in security and cryptography as well as for security engineers and architects in
industry who want to develop a deeper understanding about the algorithms used in computational cryptography.

When I (Martijn) started my PhD studies at the TU Eindhoven, Arjen was not yet appointed as a part-time professor there, but as soon as he did, there was an immediate click. Although he wasn’t physically in Eindhoven that often, his availability and generosity with his time always struck me. We often met at conferences, where he would invariably join the front row, providing me with a running commentary, but also where he would introduce me to his wider academic network. One peculiarity when working with Arjen is his absolute aversion of footnotes, which he enthusiastically weeded out of early drafts of papers and also discouraged by expecting some friendly ‘compensation’ for each footnote remaining in my final PhD thesis. When he was appointed as a full professor at EPFL, a few years after my graduation, he asked me whether I wanted to join as a post-doctoral researcher. During those years he encouraged me to explore my own research agenda and helped me to mature as an independent academic.

After I (Joppe) obtained my master’s degree in Amsterdam, the required funding for a PhD position related to integer factorisation failed to materialise. When Arjen learned about this, he arranged for me to come over and eventually start my PhD study in Lausanne. There we had the coolest equipment to brag about at birthday parties: a cluster of PlayStation 3 game consoles. More seriously, with his broad academic network he ensured I could collaborate with the brightest minds in public-key cryptology. This led to a summer internship under the supervision of Peter Montgomery at Microsoft Research, where I eventually became a post-doctoral researcher which paved the way for me to join the Competence Center Crypto & Security at NXP Semiconductors. I learned a lot from Arjen’s direct but honest way of conducting research and to always ask critical questions when people skim over the sometimes complicated but necessary details.

It was a genuine pleasure for both of us (being PhD siblings) to honour Arjen’s scientific career. We would like to thank all the contributors who are leading researchers in the various fields for their participation and hope you (the reader) will enjoy reading this book and be as enthusiastic about the fascinating and interesting field of computational cryptography as we are.