LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor Endre Süli, Mathematical Institute, University of Oxford,
Woodstock Road, Oxford OX2 6GG, United Kingdom

The titles below are available from booksellers, or from Cambridge University Press at
www.cambridge.org/mathematics

359 Moduli spaces and vector bundles, L. BRAMBILA-PAZ, S.B. BRADLOW, O. GARCÍA-PRADA & S. RAMANAN (eds)
360 Zariski geometries, B. ZILBER
361 Words: Notes on verbal width in groups, D. SEGAL
362 Differential tensor algebras and their module categories, R. BAUTISTA, L. SALMERÓN & R. ZUAZUA
363 Foundations of computational mathematics, Hong Kong 2008, F. CUCKER, A. PINKUS & M.J. TODD (eds)
364 Partial differential equations and fluid mechanics, J.C. ROBINSON & J.L. RODRIGO (eds)
365 Surveys in combinatorics 2009, S. HUCZYNSKA, J.D. MITCHELL & C.M. RONEY-DOUGAL (eds)
366 Highly oscillatory problems, B. ENGQUIST, A. FOKAS, E. HAIRER & A. ISERLES (eds)
367 Random matrices: High dimensional phenomena, G. BLOWER
368 Geometry of Riemann surfaces, F.P. GARDINER, G. GONZÁLEZ-DIEZ & C. KOUROUNIOTIS (eds)
369 Epidemics and rumours in complex networks, M. DRAIEF & L. MASSOULIÉ
370 Theory of *p*-adic distributions, S. ALBEVERIO, A.YU. KHRENNIKOV & V.M. SHELKOVICH
371 Conformal fractals, F. PRZYTYCKI & M. URBAŃSKI
372 Moonshine: The first quarter century and beyond, J. LEPOWSKY, J. MCKAY & M.P. TUITE (eds)
373 Smoothness, regularity and complete intersection, J. MAJADAS & A. G. RODICIO
374 Geometric analysis of hyperbolic differential equations: An introduction, S. ALINHAC
375 Triangulated categories, T. HOLM, P. JØRGENSEN & R. ROUQUIER (eds)
376 Permutation patterns, S. LINTON, N. RUŠKUC & V. VATTER (eds)
377 An introduction to Galois cohomology and its applications, G. BERHUY
378 Probability and mathematical genetics, N. H. BINGHAM & C. M. GOLDIE (eds)
379 Finite and algorithmic model theory, J. ESPARZA, C. MICHAUX & C. STEINHORN (eds)
380 Real and complex singularities, M. MANOEL, M.C. ROMERO FUSTER & C.T.C WALL (eds)
381 Symmetries and integrability of difference equations, D. LEVI, P. OLVER, Z. THOMOVA & P. WINTERNITZ (eds)
382 Forcing with random variables and proof complexity, J. KRAJÍČEK
383 Motivic integration and its interactions with model theory and non-Archimedean geometry I, R. CLUCKERS, J. NICAISE & J. SEBAG (eds)
384 Motivic integration and its interactions with model theory and non-Archimedean geometry II, R. CLUCKERS, J. NICAISE & J. SEBAG (eds)
385 Entropy of hidden Markov processes and connections to dynamical systems, B. MARCUS, K. PETERSEN & T. WEISSMAN (eds)
386 Independence-friendly logic, A.L. MANN, G. SANDU & M. SEVENSTER
387 Groups St Andrews 2009 in Bath I, C.M. CAMPBELL *et al* (eds)
388 Groups St Andrews 2009 in Bath II, C.M. CAMPBELL *et al* (eds)
389 Random fields on the sphere, D. MARINUCCI & G. PECCATI
390 Localization in periodic potentials, D.E. PELINOVSKY
391 Fusion systems in algebra and topology, M. ASCHBACHER, R. KESSAR & B. OLIVER
392 Surveys in combinatorics 2011, R. CHAPMAN (ed)
393 Non-abelian fundamental groups and Iwasawa theory, J. COATES *et al* (eds)
394 Variational problems in differential geometry, R. BIELAWSKI, K. HOUSTON & M. SPEIGHT (eds)
395 How groups grow, A. MANN
396 Arithmetic differential operators over the *p*-adic integers, C.C. RALPH & S.R. SIMANCA
397 Hyperbolic geometry and applications in quantum chaos and cosmology, J. BOLTE & F. STEINER (eds)
398 Mathematical models in contact mechanics, M. SOFONEA & A. MATEI
399 Circuit double cover of graphs, C.-Q. ZHANG
400 Dense sphere packings: a blueprint for formal proofs, T. HALES
401 A double Hall algebra approach to affine quantum Schur–Weyl theory, B. DENG, J. DU & Q. FU
402 Mathematical aspects of fluid mechanics, J.C. ROBINSON, J.L. RODRIGO & W. SADOWSKI (eds)
403 Foundations of computational mathematics, Budapest 2011, F. CUCKER, T. KRICK, A. PINKUS & A. SZANTO (eds)
404 Operator methods for boundary value problems, S. HASSI, H.S.V. DE SNOO & F.H. SZAFRANIEC (eds)
405 Torsors, étale homotopy and applications to rational points, A.N. SKOROBOGATOV (ed)
406 Appalachian set theory, J. CUMMINGS & E. SCHIMMERLING (eds)
407 The maximal subgroups of the low-dimensional finite classical groups, J.N. BRAY, D.F. HOLT & C.M. RONEY-DOUGAL
408 Complexity science: the Warwick master's course, R. BALL, V. KOLOKOLTSOV & R.S. MACKAY (eds)
409 Surveys in combinatorics 2013, S.R. BLACKBURN, S. GERKE & M. WILDON (eds)
410 Representation theory and harmonic analysis of wreath products of finite groups, T. CECCHERINI-SILBERSTEIN, F. SCARABOTTI & F. TOLLI

411 Moduli spaces, L. BRAMBILA-PAZ, O. GARCÍA-PRADA, P. NEWSTEAD & R.P. THOMAS (eds)
412 Automorphisms and equivalence relations in topological dynamics, D.B. ELLIS & R. ELLIS
413 Optimal transportation, Y. OLLIVIER, H. PAJOT & C. VILLANI (eds)
414 Automorphic forms and Galois representations I, F. DIAMOND, P.L. KASSAEI & M. KIM (eds)
415 Automorphic forms and Galois representations II, F. DIAMOND, P.L. KASSAEI & M. KIM (eds)
416 Reversibility in dynamics and group theory, A.G. O'FARRELL & I. SHORT
417 Recent advances in algebraic geometry, C.D. HACON, M. MUSTAŢĂ & M. POPA (eds)
418 The Bloch–Kato conjecture for the Riemann zeta function, J. COATES, A. RAGHURAM, A. SAIKIA & R. SUJATHA (eds)
419 The Cauchy problem for non-Lipschitz semi-linear parabolic partial differential equations, J.C. MEYER & D.J. NEEDHAM
420 Arithmetic and geometry, L. DIEULEFAIT *et al* (eds)
421 O-minimality and Diophantine geometry, G.O. JONES & A.J. WILKIE (eds)
422 Groups St Andrews 2013, C.M. CAMPBELL *et al* (eds)
423 Inequalities for graph eigenvalues, Z. STANIĆ
424 Surveys in combinatorics 2015, A. CZUMAJ *et al* (eds)
425 Geometry, topology and dynamics in negative curvature, C.S. ARAVINDA, F.T. FARRELL & J.-F. LAFONT (eds)
426 Lectures on the theory of water waves, T. BRIDGES, M. GROVES & D. NICHOLLS (eds)
427 Recent advances in Hodge theory, M. KERR & G. PEARLSTEIN (eds)
428 Geometry in a Fréchet context, C.T.J. DODSON, G. GALANIS & E. VASSILIOU
429 Sheaves and functions modulo p, L. TAELMAN
430 Recent progress in the theory of the Euler and Navier–Stokes equations, J.C. ROBINSON, J.L.RODRIGO, W. SADOWSKI & A. VIDAL-LÓPEZ (eds)
431 Harmonic and subharmonic function theory on the real hyperbolic ball, M. STOLL
432 Topics in graph automorphisms and reconstruction (2nd Edition), J. LAURI & R. SCAPELLATO
433 Regular and irregular holonomic D-modules, M. KASHIWARA & P. SCHAPIRA
434 Analytic semigroups and semilinear initial boundary value problems (2nd Edition), K. TAIRA
435 Graded rings and graded Grothendieck groups, R. HAZRAT
436 Groups, graphs and random walks, T. CECCHERINI-SILBERSTEIN, M. SALVATORI & E. SAVA-HUSS (eds)
437 Dynamics and analytic number theory, D. BADZIAHIN, A. GORODNIK & N. PEYERIMHOFF (eds)
438 Random walks and heat kernels on graphs, M.T. BARLOW
439 Evolution equations, K. AMMARI & S. GERBI (eds)
440 Surveys in combinatorics 2017, A. CLAESSON *et al* (eds)
441 Polynomials and the mod 2 Steenrod algebra I, G. WALKER & R.M.W. WOOD
442 Polynomials and the mod 2 Steenrod algebra II, G. WALKER & R.M.W. WOOD
443 Asymptotic analysis in general relativity, T. DAUDÉ, D. HÄFNER & J.-P. NICOLAS (eds)
444 Geometric and cohomological group theory, P.H. KROPHOLLER, I.J. LEARY, C. MARTÍNEZ-PÉREZ & B.E.A. NUCINKIS (eds)
445 Introduction to hidden semi-Markov models, J. VAN DER HOEK & R.J. ELLIOTT
446 Advances in two-dimensional homotopy and combinatorial group theory, W. METZLER & S. ROSEBROCK (eds)
447 New directions in locally compact groups, P.-E. CAPRACE & N. MONOD (eds)
448 Synthetic differential topology, M.C. BUNGE, F. GAGO & A.M. SAN LUIS
449 Permutation groups and cartesian decompositions, C.E. PRAEGER & C. SCHNEIDER
450 Partial differential equations arising from physics and geometry, M. BEN AYED *et al* (eds)
451 Topological methods in group theory, N. BROADDUS, M. DAVIS, J.-F. LAFONT & I. ORTIZ (eds)
452 Partial differential equations in fluid mechanics, C.L. FEFFERMAN, J.C. ROBINSON & J.L. RODRIGO (eds)
453 Stochastic stability of differential equations in abstract spaces, K. LIU
454 Beyond hyperbolicity, M. HAGEN, R. WEBB & H. WILTON (eds)
455 Groups St Andrews 2017 in Birmingham, C.M. CAMPBELL *et al* (eds)
456 Surveys in combinatorics 2019, A. LO, R. MYCROFT, G. PERARNAU & A. TREGLOWN (eds)
457 Shimura varieties, T. HAINES & M. HARRIS (eds)
458 Integrable systems and algebraic geometry I, R. DONAGI & T. SHASKA (eds)
459 Integrable systems and algebraic geometry II, R. DONAGI & T. SHASKA (eds)
460 Wigner-type theorems for Hilbert Grassmannians, M. PANKOV
461 Analysis and geometry on graphs and manifolds, M. KELLER, D. LENZ & R.K. WOJCIECHOWSKI
462 Zeta and L-functions of varieties and motives, B. KAHN
463 Differential geometry in the large, O. DEARRICOTT *et al* (eds)
464 Lectures on orthogonal polynomials and special functions, H.S. COHL & M.E.H. ISMAIL (eds)
465 Constrained Willmore surfaces, Á.C. QUINTINO
466 Invariance of modules under automorphisms of their envelopes and covers, A.K. SRIVASTAVA, A. TUGANBAEV & P.A.GUIL ASENSIO
467 The genesis of the Langlands program, J. MUELLER & F. SHAHIDI
468 (Co)end calculus, F. LOREGIAN
469 Computational cryptography, J.W. BOS & M. STAM

'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

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi - 110025, India

103 Penang Road, #05-06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108795937
DOI: 10.1017/9781108854207

First published 2021

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging in Publication data
Names: Bos, Joppe W., editor. | Stam, Martijn, editor.
Title: Computational cryptography : algorithmic aspects of cryptology / edited by Joppe W. Bos, NXP Semiconductors, Belgium, Martijn Stam, Simula UiB, Norway.
Description: Cambridge, United Kingdom ; New York, NY, USA : Cambridge University Press, 2021. | Series: London mathematical society lecture note series | Includes bibliographical references and index.
Identifiers: LCCN 2021012303 (print) | LCCN 2021012304 (ebook) | ISBN 9781108795937 (paperback) | ISBN 9781108854207 (epub)
Subjects: LCSH: Cryptography. | BISAC: MATHEMATICS / Number Theory | MATHEMATICS / Number Theory
Classification: LCC QA268 .C693 2021 (print) | LCC QA268 (ebook) | DDC 005.8/24–dc23
LC record available at https://lccn.loc.gov/2021012303
LC ebook record available at https://lccn.loc.gov/2021012304

ISBN 978-1-108-79593-7 Paperback

Contents

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.