

**Zeitschrift:** L'Enseignement Mathématique  
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique  
**Band:** 63 (2017)  
**Heft:** 3-4

**Buchbesprechung:** Bulletin bibliographique

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 27.04.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

## Bulletin bibliographique

### *Généralités*

Evelyne BARBIN, Dominique BÉNARD, Guillaume MOUSSARD, (Directeurs). — **Les mathématiques et le réel : expériences, instruments, investigations.** — Un vol. broché, 14×23, de IX, 246 p. — ISBN 978-2-7535-6531-9. — Prix : €20.00. — Presses universitaires de Rennes, Rennes, 2018.

Quels rôles joue l'expérience dans les investigations et dans les pratiques mathématiques ? Quel rapport au «réel», voire au sensible, se trouve ainsi construit ? Pour tenter de répondre à ces questions, cet ouvrage prend l'histoire des sciences comme terrain d'épreuves des problématiques mathématiques et enseignantes. Ce livre traite des instruments pour mesurer et pour tracer, des instruments et des machines pour calculer, des mathématiques entre réel et réalité. Il montre l'importance pour les enseignants d'une connaissance de l'histoire des sciences et de la lecture de textes anciens.

Andrew GELMAN, Deborah NOLAN. — **Teaching statistics: a bag of tricks.** — Second edition. — Un vol. relié, 16×24, de XVI, 404 p. — ISBN 978-0-19-878569-9. — Prix: £70.00. — Oxford University Press, Oxford, 2017.

Students in the sciences, economics, social sciences, and medicine take an introductory statistics course. And yet statistics can be notoriously difficult for instructors to teach and for students to learn. To help overcome these challenges, Gelman and Nolan have put together this fascinating and thought-provoking book. Based on years of teaching experience the book provides a wealth of demonstrations, activities, examples, and projects that involve active student participation.

Allan McROBIE. — **The seduction of curves: the lines of beauty that connect mathematics, art and nude.** — With photography by Helena Weightman. — Un vol. relié, 21×26, 159 p. — ISBN 9780691175331. — Prix: £27.95. — Princeton University Press, Princeton/Oxford, 2017.

Curves are seductive. These smooth, organic lines and surfaces—like those of the human body—appeal to us in an instinctive, visceral way that straight lines or the perfect shapes of classical geometry never could. In this large-format book, lavishly illustrated in color throughout, Allan McRobie takes the reader on an alluring exploration of the beautiful curves that shape our world—from our bodies to Salvador Dalí's paintings and the space-time fabric of the universe itself. The book focuses on seven curves—the fold, cusp, swallowtail, and butterfly, plus the hyperbolic, elliptical, and parabolic “umbilics”—and describes the surprising origins of their taxonomy in the catastrophe theory of mathematician René Thom. In an accessible discussion illustrated with many photographs of the human nude, McRobie introduces these curves and then describes their role in nature, science, engineering, architecture, art, and other areas. The reader learns how these curves play out in everything from the stability of oil rigs and the study of distant galaxies to rainbows, the patterns of light on pool floors, and even the shape of human genitals. The book also discusses the role of these curves in the work of such artists as David Hockney, Henry Moore, and Anish Kapoor, with particular attention given to the delicate sculptures of Naum Gabo and the final paintings of Dalí, who said that Thom's theory “bewitched all of my atoms.” A unique introduction to the language of beautiful curves, this book may change the way you see the world.

Allan McRobie is a Reader in the Engineering Department at the University of Cambridge, where he teaches stability theory and structural engineering. He previously worked as an engineer in Australia, designing bridges and towers.

## *Logique et fondements*

Neil TENNANT. — **Core logic**. — Un vol. relié, 17,5×25, de XVII, 357 p. — ISBN 978-0-19-877789-2. — Prix: £45.00. — Oxford University Press, Oxford, 2017.

Neil Tennant presents an original logical system with unusual philosophical, proof-theoretic, metalogical, computational, and revision-theoretic virtues. *Core logic*, which lies deep inside classical logic, best formalizes rigorous mathematical reasoning. It captures constructive relevant reasoning. And the classical extension of *Core logic* handles non-constructive reasoning. These core systems fix all the mistakes that make standard systems harbor counterintuitive irrelevancies. Conclusions reached by means of core proof are relevant to the premises used. These are the first systems that ensure both relevance and adequacy for the formalization of all mathematical and scientific reasoning. They are also the first systems to ensure that one can make deductive progress with potential logical strengthening by chaining proofs together: one will prove, if not the conclusion sought, then (even better!) the inconsistency of one's accumulated premises. So *Core logic* provides transitivity of deduction with potential epistemic gain. Because of its clarity about the true internal structure of proofs, *Core logic* affords advantages also for the automation of deduction and our appreciation of the paradoxes.

Jon WILLIAMSON. — **Lectures on inductive logic**. — Un vol. relié, 16×24, de XIII, 201 p. — ISBN 978-0-19-966647-8. — Prix: £55.00. — Oxford University Press, Oxford, 2017.

Inductive logic (also known as confirmation theory) seeks to determine the extent to which the premisses of an argument entail its conclusion. This book offers an introduction to the field of inductive logic and develops a new Bayesian inductive logic. Chapter 1 introduces perhaps the simplest and most natural account of inductive logic, classical inductive logic, which is attributable to Ludwig Wittgenstein. Classical inductive logic is seen to fail in a crucial way, so there is a need to develop more sophisticated inductive logics. Chapter 2 presents enough logic and probability theory for the reader to begin to study inductive logic, while Chapter 3 introduces the ways in which logic and probability can be combined in an inductive logic. Chapter 4 analyses the most influential approach to inductive logic, due to W.E. Johnson and Rudolf Carnap. Again, this logic is seen to be inadequate. Chapter 5 shows how an alternative approach to inductive logic follows naturally from the philosophical theory of objective Bayesian epistemology. This approach preserves the inferences that classical inductive logic gets right (Chapter 6). On the other hand, it also offers a way out of the problems that beset classical inductive logic (Chapter 7). Chapter 8 defends the approach by tackling several key criticisms that are often levelled at inductive logic. Chapter 9 presents a formal justification of the version of objective Bayesianism which underpins the approach. Chapter 10 explains what has been achieved and poses some open questions.

## *Théorie des ensembles*

Patrick DEHORNOY. — **La théorie des ensembles: introduction à une théorie de l'infini et des grands cardinaux**. — Tableau noir. — Un vol. relié, 16×24, de XX, 649 p. — ISBN 978-2-91-635240-4. — Prix: €59.00. — Calvage & Mounet, Paris, 2017.

NON, la théorie des ensembles, ce n'est pas dessiner des patates et des flèches ... c'est élaborer en une théorie mathématique notre exploration de l'infini, ni plus, ni moins. NON, la théorie des ensembles n'est pas le système fondationnel unique des mathématiques ... c'est un des systèmes possibles, tout comme par exemple la récente théorie homotopique des types. NON, l'entier 2 n'est pas l'ensemble  $\emptyset, \emptyset$ ... celui-ci n'est qu'une représentation de l'entier 2 par un ensemble. NON, la non-prouvabilité de l'hypothèse du continu à partir du système ZF n'indique pas que la question doit rester à jamais ouverte ... c'est juste le signe que les bases axiomatiques actuelles sont incomplètes: le système ZF a d'ores et déjà été amendé,

et le sera probablement à nouveau dans le futur. OUI, la théorie des ensembles est une magnifique théorie qui, peu à peu, apporte de la lumière dans le monde de l'infini, et OUI, même si les détails sont parfois arides et exigeants, il est possible de bien saisir les grandes étapes de son cheminement. C'est le sujet de ce livre.

## ***Théorie des nombres***

Markus SZYMON FRACZEK. — **Selberg zeta functions and transfer operators: an experimental approach to singular perturbations.** — Lecture notes in mathematics, vol. 2139. — Un vol. broché, 15,5×23,5, de XV, 352 p. — ISBN 978-3-319-51294-5. — Prix: SFr. 77.00. — Springer Nature, Cham, 2017.

This book presents a method for evaluating Selberg zeta functions via transfer operators for the full modular group and its congruence subgroups with characters. Studying zeros of Selberg zeta functions for character deformations allows us to access the discrete spectra and resonances of hyperbolic Laplacians under both singular and non-singular perturbations. Areas in which the theory has not yet been sufficiently developed, such as the spectral theory of transfer operators or the singular perturbation theory of hyperbolic Laplacians, will profit from the numerical experiments discussed in this book. Detailed descriptions of numerical approaches to the spectra and eigenfunctions of transfer operators and to computations of Selberg zeta functions will be of value to researchers active in analysis, while those researchers focusing more on numerical aspects will benefit from discussions of the analytic theory, in particular those concerning the transfer operator method and the spectral theory of hyperbolic spaces.

Paul POLLACK. — **A conversational introduction to algebraic number theory: arithmetic beyond  $Z$ .** — Student mathematical library, vol. 84. — Un vol. broché, 14×21,5, de IX, 316 p. — ISBN 978-1-4704-3653-7. — Prix: US\$52.00. — American Mathematical Society, Providence, 2017.

Gauss famously referred to mathematics as the “queen of the sciences” and to number theory as the “queen of mathematics”. This book is an introduction to algebraic number theory, meaning the study of arithmetic in finite extensions of the rational number field  $Q$ . Originating in the work of Gauss, the foundations of modern algebraic number theory are due to Dirichlet, Dedekind, Kronecker, Kummer, and others. This book lays out basic results, including the three “fundamental theorems”: unique factorization of ideals, finiteness of the class number, and Dirichlet’s unit theorem. While these theorems are by now quite classical, both the text and the exercises allude frequently to more recent developments. In addition to traversing the main highways, the book reveals some remarkable vistas by exploring scenic side roads. Several topics appear that are not present in the usual introductory texts. One example is the inclusion of an extensive discussion of the theory of elasticity, which provides a precise way of measuring the failure of unique factorization. The book is based on the author’s notes from a course delivered at the University of Georgia; pains have been taken to preserve the conversational style of the original lectures.

Thomas R. SHEMANSKE. — **Modern cryptography and elliptic curves: a beginner’s guide.** — Student mathematical library, vol. 83. — Un vol. broché, 14×21,5, de XII, 250 p. — ISBN 978-1-4704-3582-0. — Prix: US\$52.00. — American Mathematical Society, Providence, 2017.

This book offers the beginning undergraduate student some of the vista of modern mathematics by developing and presenting the tools needed to gain an understanding of the arithmetic of elliptic curves over finite fields and their applications to modern cryptography. This gradual introduction also makes a significant effort to teach students how to produce or discover a proof by presenting mathematics as an exploration, and at the same time, it provides the necessary mathematical underpinnings to investigate the practical and implementation side of elliptic curve cryptography (ECC). Elements of abstract algebra, number theory, and affine and projective geometry are introduced and developed, and their interplay is exploited. Algebra and geometry combine to characterize congruent numbers via rational points on the unit circle, and group law for the set of points on an elliptic curve arises from geometric intuition provided by Bezout’s theorem as well as the construction of projective space. The structure of the unit group of the integers modulo a prime explains RSA encryption, Pollard’s method of factorization, Diffie-Hellman key exchange, and ElGamal

encryption, while the group of points of an elliptic curve over a finite field motivates Lenstra’s elliptic curve factorization method and ECC. The only real prerequisite for this book is a course on one-variable calculus; other necessary mathematical topics are introduced on-the-fly. Numerous exercises further guide the exploration.

Martin W. WEISSMAN. — **An illustrated theory of numbers**. — Un vol. relié, 12×28,5, de XV, 223 p. — ISBN 978-1-4704-3493-9. — Prix: US\$69.00. — American Mathematical Society, Providence, 2017.

*An illustrated theory of numbers* gives a comprehensive introduction to number theory, with complete proofs, worked examples, and exercises. Its exposition reflects the most recent scholarship in mathematics and its history. Almost 500 sharp illustrations accompany elegant proofs, from prime decomposition through quadratic reciprocity. Geometric and dynamical arguments provide new insights, and allow for a rigorous approach with less algebraic manipulation. The final chapters contain an extended treatment of binary quadratic forms, using Conway’s topograph to solve quadratic Diophantine equations (e.g., Pell’s equation) and to study reduction and the finiteness of class numbers. Data visualizations introduce the reader to open questions and cutting-edge results in analytic number theory such as the Riemann hypothesis, boundedness of prime gaps, and the class number 1 problem. Accompanying each chapter, historical notes curate primary sources and secondary scholarship to trace the development of number theory within and outside the Western tradition. Requiring only high school algebra and geometry, this text is recommended for a first course in elementary number theory, and to all mathematicians seeking a fresh perspective on an ancient subject.

## *Géométrie algébrique*

Dennis GAITSGORY, Nick ROZENBLYUM. — **A study in derived algebraic geometry. Volume I: Correspondances and duality**. — Mathematical surveys and monographs, vol. 221. — Un vol. relié, 18×26, de XL, 533 p. — ISBN 978-1-4704-3569-1. — Prix: US\$124.00. — American Mathematical Society, Providence, 2017.

Derived algebraic geometry is a far-reaching generalization of algebraic geometry. It has found numerous applications in various parts of mathematics, most prominently in representation theory. This volume develops the theory of ind-coherent sheaves in the context of derived algebraic geometry. Ind-coherent sheaves are a “renormalization” of quasi-coherent sheaves and provide a natural setting for Grothendieck-Serre duality as well as geometric incarnations of numerous categories of interest in representation theory. This volume consists of three parts and an appendix. The first part is a survey of homotopical algebra in the setting of  $\infty$ -categories and the basics of derived algebraic geometry. The second part builds the theory of ind-coherent sheaves as a functor out of the category of correspondences and studies the relationship between ind-coherent and quasi-coherent sheaves. The third part sets up the general machinery of the  $(\infty, 2)$ -category of correspondences needed for the second part. The category of correspondences, via the theory developed in the third part, provides a general framework for Grothendieck’s six-functor formalism. The appendix provides the necessary background on  $(\infty, 2)$ -categories needed for the third part.

Dennis GAITSGORY, Nick ROZENBLYUM. — **A study in derived algebraic geometry. Volume II: Deformations, Lie theory and formal geometry**. — Mathematical surveys and monographs, vol. 221. — Un vol. relié, 18,5×26, de XXXV, 436 p. — ISBN 978-1-4704-3570-7. — Prix: US\$124.00. — American Mathematical Society, Providence, 2017.

Derived algebraic geometry is a far-reaching generalization of algebraic geometry. It has found numerous applications in other parts of mathematics, most prominently in representation theory. This volume develops deformation theory, Lie theory and the theory of algebroids in the context of derived algebraic geometry. To that end, it introduces the notion of inf-scheme, which is an infinitesimal deformation of a scheme and studies ind-coherent sheaves on such. As an application of the general theory, the six-functor formalism for D-modules in derived geometry is obtained. This volume consists of two parts. The first part introduces the notion of ind-scheme and extends the theory of ind-coherent sheaves to inf-schemes, obtaining the theory of D-modules as an application. The second part establishes the equivalence between formal Lie group(oids) and Lie algebr(oids) in the category of ind-coherent sheaves. This equivalence gives a vast generalization of

the equivalence between Lie algebras and formal moduli problems. This theory is applied to study natural filtrations in formal derived geometry generalizing the Hodge filtration.

Shane KELLY. — **Voevodsky motives and  $l$ dh-descent**. — Astérisque, vol. 391. — Un vol. broché,  $17,5 \times 24$ , 125 p. — ISBN 978-2-85629-861-9. — Prix: €24.00. — Société mathématique de France, Paris, 2017.

This work applies Gabber’s theorem on alterations to Voevodsky’s work on mixed motives. We extend many fundamental theorems to  $DM(k, Z[1/p])$  where  $p$  is the exponential characteristic of the perfect field  $k$ . Two applications are an isomorphism of Suslin that compares higher Chow groups and étale cohomology, and calculation of the motivic Steenrod algebra.

## *Algèbre linéaire et multilinéaire, théorie des matrices*

László ERDŐS, Horn-Tzer YAU. — **A dynamical approach to random matrix theory**. — Courant lecture notes in mathematics, vol. 28. — Un vol. broché,  $17,7 \times 25,5$ , de IX, 226 p. — ISBN 978-1-4704-3648-3. — Prix: US\$43.00. — Courant Institute of Mathematical Sciences/American Mathematical Society, New York/Providence, 2017.

This book is a concise and self-contained introduction of recent techniques to prove local spectral universality for large random matrices. Random matrix theory is a fast expanding research area, and this book mainly focuses on the methods that the authors participated in developing over the past few years. Many other interesting topics are not included, and neither are several new developments within the framework of these methods. The authors have chosen instead to present key concepts that they believe are the core of these methods and should be relevant for future applications. They keep technicalities to a minimum to make the book accessible to graduate students. With this in mind, they include in this book the basic notions and tools for high-dimensional analysis, such as large deviation, entropy, Dirichlet form, and the logarithmic Sobolev inequality. This manuscript has been developed and continuously improved over the last five years. The authors have taught this material in several regular graduate courses at Harvard, Munich, and Vienna, in addition to various summer schools and short courses.

David C. MELLO. — **Invitation to linear algebra**. — Textbooks in mathematics. — Un vol. relié,  $18,5 \times 26$ , de XIII, 394 p. — ISBN 978-1-4987-7956-2. — Prix: £65.60. — CRC Press, Boca Raton, 2017.

Unlike most books of this type, the book has been organized into “lessons” rather than chapters. This has been done to limit the size of the mathematical morsels that students must digest during each class, and to make it easier for instructors to budget class time. The book contains considerably more material than normally appears in a first course. For example, several advanced topics such as the Jordan canonical form and matrix power series have been included. This was done to make the book more flexible than most books presently available, and to allow instructors to choose enrichment material which may reflect their interests, and those of their students.

## *Anneaux et algèbres*

Igor BURBAN, Yuri DROZD. — **Maximal Cohen–Macaulay modules over non-isolated surface singularities and matrix problems**. — Memoirs of the American Mathematical Society, vol. 1178. — Un vol. broché,  $17,7 \times 25,5$ , de XIV, 114 p. — ISBN 978-1-4704-2537-1. — Prix: US\$75.00. — American Mathematical Society, Providence, 2017.

In this article the authors develop a new method to deal with maximal Cohen-Macaulay modules over non-isolated surface singularities. In particular, they give a negative answer on an old question of Schreyer about surface singularities with only countably many indecomposable maximal Cohen-Macaulay modules. Next, the authors prove that the degenerate cusp singularities have tame Cohen-Macaulay representation type. The authors’ approach is illustrated on the case of  $\mathbb{k}[[x, y, z]]/(xyz)$  as well as several other rings.

This study of maximal Cohen-Macaulay modules over non-isolated singularities leads to a new class of problems of linear algebra, which the authors call representations of decorated bunches of chains. They prove that these matrix problems have tame representation type and describe the underlying canonical forms.

Friedrich WEHRUNG. — **Refinement monoids, equidecomposability types, and boolean inverse semigroups.** — Lecture notes in mathematics, vol. 2188. — Un vol. broché, 15,5×23,5, de VII, 240 p. — ISBN 978-3-319-61598-1. — Prix: SFr. 49.50. — Springer Nature, Cham, 2017.

Adopting a new universal algebraic approach, this book explores and consolidates the link between Tarski's classical theory of equidecomposability types monoids, abstract measure theory (in the spirit of Hans Dobbertin's work on monoid-valued measures on boolean algebras) and the nonstable K-theory of rings. This is done via the study of a monoid invariant, defined on boolean inverse semigroups, called the type monoid. The new techniques contrast with the currently available topological approaches. Many positive results, but also many counterexamples, are provided.

## ***Théorie des groupes et généralisations***

Manjul BHARGAVA, Robert GURALNICK, Gerhard HISS, Klaus LUX, Pham Huu TIEP, (Editors). — **Finite simple groups: thirty years of the atlas and beyond : International Conference celebrating the Atlases and honoring John Conway, November 2-5 2015, Princeton University, Princeton, NJ.** — Contemporary mathematics, vol. 694. — Un vol. broché, 17,5×25,5, de IX, 229 p. — ISBN 978-1-4704-3678-0. — Prix: US\$111.00. — American Mathematical Society, Providence, 2017.

This volume contains the proceedings of the international conference *Finite Simple Groups: Thirty Years of the Atlas and Beyond Celebrating the Atlases and Honoring John Conway*, which was held from November 2–5, 2015, at Princeton University, Princeton, New Jersey. Classification of finite simple groups, one of the most monumental accomplishments of modern mathematics, was announced in 1983 with the proof completed in 2004. Since then, it has opened up a new and powerful strategy to approach and resolve many previously inaccessible problems in group theory, number theory, combinatorics, coding theory, algebraic geometry, and other areas of mathematics. This strategy crucially utilizes various information about finite simple groups, part of which is catalogued in “the atlas of finite groups” (John H. Conway et al.), and in “an atlas of Brauer characters” (Christoph Jansen et al.). It is impossible to overestimate the roles of the atlases and the related computer algebra systems in the everyday life of researchers in many areas of contemporary mathematics. The main objective of the conference was to discuss numerous applications of the atlases and to explore recent developments and future directions of research, with focus on the interaction between computation and theory and applications to number theory and algebraic geometry. The papers in this volume are based on talks given at the conference. They present a comprehensive survey on current research in all of these fields.

Vaughn CLIMENHAGA, Anatole KATOK. — **From groups to geometry and back.** — Student mathematical library, vol. 81. — Un vol. broché, 14×21,5, de XIX, 420 p. — ISBN 978-1-4704-3479-3. — Prix: US\$58.00. — American Mathematical Society, Providence, 2017.

Groups arise naturally as symmetries of geometric objects, and so groups can be used to understand geometry and topology. Conversely, one can study abstract groups by using geometric techniques and ultimately by treating groups themselves as geometric objects. This book explores these connections between group theory and geometry, introducing some of the main ideas of transformation groups, algebraic topology, and geometric group theory. The first half of the book introduces basic notions of group theory and studies symmetry groups in various geometries, including Euclidean, projective, and hyperbolic. The classification of Euclidean isometries leads to results on regular polyhedra and polytopes; the study of symmetry groups using matrices leads to Lie groups and Lie algebras. The second half of the book explores ideas from algebraic topology and geometric group theory. The fundamental group appears as yet another group associated to a geometric object and turns out to be a symmetry group using covering spaces and deck transformations. In the other direction, Cayley graphs, planar models, and fundamental domains appear as geometric objects associated to groups. The final chapter discusses groups themselves as geometric objects, including a gentle

introduction to Gromov’s theorem on polynomial growth and Grigorchuk’s example of intermediate growth. The book is accessible to undergraduate students (and anyone else) with a background in calculus, linear algebra, and basic real analysis, including topological notions of convergence and connectedness. This book is a result of the MASS course in algebra at Penn State University in the fall semester of 2009. This book is published in cooperation with Mathematics Advanced Study Semesters.

Luis RIBES. — **Profinite graphs and groups**. — *Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge. A series of modern surveys in mathematics*, vol. 66. — Un vol. relié, 16×24, de XV, 471 p. — ISBN 978-3-319-61041-2. — Prix: SFr. 96.50. — Springer Nature, Cham, 2017.

This book offers a detailed introduction to graph theoretic methods in profinite groups and applications to abstract groups. It is the first to provide a comprehensive treatment of the subject. The author begins by carefully developing relevant notions in topology, profinite groups and homology, including free products of profinite groups, cohomological methods in profinite groups, and fixed points of automorphisms of free pro- $p$  groups. The final part of the book is dedicated to applications of the profinite theory to abstract groups, with sections on finitely generated subgroups of free groups, separability conditions in free and amalgamated products, and algorithms in free groups and finite monoids. *Profinite graphs and groups* will appeal to students and researchers interested in profinite groups, geometric group theory, graphs and connections with the theory of formal languages. A complete reference on the subject, the book includes historical and bibliographical notes as well as a discussion of open questions and suggestions for further reading.

## *Groupes topologiques, groupes et algèbres de Lie*

Katarina BARRON, Elisabeth JURISICH, Antun MILAS, Kailash MISRA, (Editors). — **Lie algebras, vertex operator algebras, and related topics : Conference in honor of J. Lepowsky and R. Wilson on Lie algebras, vertex operator algebras, and related topics, August 14–18, 2015, University of Notre Dame, Notre Dame, IN**. — *Contemporary mathematics*, vol. 695. — Un vol. relié, 17,5×25,5, de VI, 274 p. — ISBN 978-14704-2666-8. — Prix: US\$110.00. — American Mathematical Society, Providence, 2017.

This volume contains the proceedings of the conference on Lie Algebras, Vertex Operator Algebras, and Related Topics, celebrating the 70th birthday of James Lepowsky and Robert Wilson, held from August 14–18, 2015, at the University of Notre Dame, Notre Dame, Indiana. Since their seminal work in the 1970s, Lepowsky and Wilson, their collaborators, their students, and those inspired by their work, have developed an amazing body of work intertwining the fields of Lie algebras, vertex algebras, number theory, theoretical physics, quantum groups, the representation theory of finite simple groups, and more. The papers presented here include recent results and descriptions of ongoing research initiatives representing the broad influence and deep connections brought about by the work of Lepowsky and Wilson and include a contribution by Yi-Zhi Huang summarizing some major open problems in these areas, in particular as they pertain to two-dimensional conformal field theory.

Matthew EMERTON. — **Locally analytic vectors in representations of locally  $p$ -adic analytic groups**. — *Memoirs of the American Mathematical Society*, vol. 1175. — Un vol. broché, 17,5×25,5, de IV, 158 p. — ISBN 978-0-8218-7562-9. — Prix: US\$75.00. — American Mathematical Society, Providence, 2017.

The goal of this memoir is to provide the foundations for the locally analytic representation theory that is required in three of the author’s other papers on this topic. In the course of writing those papers the author found it useful to adopt a particular point of view on locally analytic representation theory: namely, regarding a locally analytic representation as being the inductive limit of its subspaces of analytic vectors (of various “radii of analyticity”). The author uses the analysis of these subspaces as one of the basic tools in his study of such representations. Thus in this memoir he presents a development of locally analytic representation theory built around this point of view. The author has made a deliberate effort to keep the exposition reasonably self-contained and hopes that this will be of some benefit to the reader.

## *Fonctions d'une variable complexe*

Ara S. BASMAIAN, Yair N. MINSKY, Alan W. REID, (Editors). — **In the tradition of Ahlfors-Bers, VII : 6th Ahlfors-Bers Colloquium, October 23–26, 2014, Yale University, New Haven, CT.** — Contemporary mathematics, vol. 696. — Un vol. relié, 17,5×25,5, de IX, 250 p. — ISBN 978-1-4704-2651-4. — Prix: US\$110.00. — American Mathematical Society, Providence, 2017.

The Ahlfors-Bers Colloquia commemorate the mathematical legacy of Lars Ahlfors and Lipman Bers. The core of this legacy lies in the fields of geometric function theory, Teichmüller theory, hyperbolic geometry, and partial differential equations. Today we see the influence of Ahlfors and Bers on algebraic geometry, mathematical physics, dynamics, probability, geometric group theory, number theory and topology. Recent years have seen a flowering of this legacy with an increased interest in their work. This current volume contains articles on a wide variety of subjects that are central to this legacy. These include papers in Kleinian groups, classical Riemann surface theory, Teichmüller theory, mapping class groups, geometric group theory, and statistical mechanics.

Frederick W. GEHRING, Gaven J. MARTIN, Bruce P. PALKA. — **An introduction to the theory of higher-dimensional quasiconformal mappings.** — Mathematical surveys and monographs, vol. 216. — Un vol. relié, 18×26, de IX, 330 p. — ISBN 978-0-8218-4360-4. — Prix: US\$116.00. — American Mathematical Society, Providence, 2017.

This book offers a modern, up-to-date introduction to quasiconformal mappings from an explicitly geometric perspective, emphasizing both the extensive developments in mapping theory during the past few decades and the remarkable applications of geometric function theory to other fields, including dynamical systems, Kleinian groups, geometric topology, differential geometry, and geometric group theory. It is a careful and detailed introduction to the higher-dimensional theory of quasiconformal mappings from the geometric viewpoint, based primarily on the technique of the conformal modulus of a curve family. Notably, the final chapter describes the application of quasiconformal mapping theory to Mostow's celebrated rigidity theorem in its original context with all the necessary background. This book will be suitable as a textbook for graduate students and researchers interested in beginning to work on mapping theory problems or learning the basics of the geometric approach to quasiconformal mappings. Only a basic background in multidimensional real analysis is assumed.

## *Fonctions de plusieurs variables complexes*

Vincent GUEDJ, Ahmed ZERIAHI. — **Degenerate complex Monge–Ampère equations**. — Winner of the 2016 EMS Monograph award. — Tracts in mathematics, vol. 26. — Un vol. relié, 17,5×24,5, de XV, 472 p. — ISBN 978-3-03719-167-5. — Prix: €88.00. — European Mathematical Society, Zürich, 2017.

Complex Monge–Ampère equations have been one of the most powerful tools in Kähler geometry since Aubin and Yau's classical works, culminating in Yau's solution to the Calabi conjecture. A notable application is the construction of Kähler–Einstein metrics on some compact Kähler manifolds. In recent years degenerate complex Monge–Ampère equations have been intensively studied, requiring more advanced tools. The main goal of this book is to give a self-contained presentation of the recent developments of pluripotential theory on compact Kähler manifolds and its application to Kähler–Einstein metrics on mildly singular varieties. After reviewing basic properties of plurisubharmonic functions, Bedford–Taylor's local theory of complex Monge–Ampère measures is developed. In order to solve degenerate complex Monge–Ampère equations on compact Kähler manifolds, fine properties of quasi-plurisubharmonic functions are explored, classes of finite energies defined and various maximum principles established. After proving Yau's celebrated theorem as well as its recent generalizations, the results are then used to solve the (singular) Calabi conjecture and to construct (singular) Kähler–Einstein metrics on some varieties with mild singularities. The book is accessible to advanced students and researchers of complex analysis and differential geometry.

## *Fonctions spéciales*

Akihito EBISU. — **Special values of the hypergeometric series.** — Memoirs of the American Mathematical Society, vol. 1177. — Un vol. relié, 17,5×26,5, de V, 96 p. — ISBN 978-1-4704-2533-3. — Prix: US\$75.00. — American Mathematical Society, Providence, 2017.

In this paper, the author presents a new method for finding identities for hypergeometric series, such as the (Gauss) hypergeometric series, the generalized hypergeometric series and the Appell-Lauricella hypergeometric series. Furthermore, using this method, the author gets identities for the hypergeometric series  $F(a, b; c; x)$  and shows that values of  $F(a, b; c; x)$  at some points  $x$  can be expressed in terms of gamma functions, together with certain elementary functions. The author tabulates the values of  $F(a, b; c; x)$  that can be obtained with this method and finds that this set includes almost all previously known values and many previously unknown values.

## *Équations aux dérivées partielles*

Bernard DACOROGNA, Nicola FUSCO, Stefan MÜLLER, Vladimir SVERAK ; John BALL, Paolo MARCELLINI, (Editors). — **Vector-valued partial differential equations and applications, Cetraro, Italy 2013.** — Lecture notes in mathematics, vol. 2179 / CIME foundation subseries. — Un vol. broché, 15,5×23,5, de VII, 248 p. — ISBN 978-3-319-54513-4. — Prix: SFr. 104.50. — Springer Nature, Cham, 2017.

Collating different aspects of *Vector-valued partial differential equations and applications*, this volume is based on the 2013 CIME course with the same name which took place at Cetraro, Italy, under the scientific direction of John Ball and Paolo Marcellini. It contains the following contributions: *The pullback equation* (Bernard Dacorogna), *The stability of the isoperimetric inequality* (Nicola Fusco), *Mathematical problems in thin elastic sheets: scaling limits, packing, crumpling and singularities* (Stefan Müller), and *Aspects of PDEs related to fluid flows* (Vladimir Sverák). These lectures are addressed to graduate students and researchers in the field.

Nam Q. LE, Hiroyoshi MITAKE, Hung V. TRAN. — **Dynamical and geometric aspects of Hamilton-Jacobi and linearized Monge-Ampère equations : VIASM 2016.** — Lecture notes in mathematics, vol. 2183. — Un vol. broché, 15,5×23,5, de VII, 228 p. — ISBN 978-3-319-54207-2. — Prix: SFr. 30.50. — Springer Nature, Cham, 2017.

Consisting of two parts, the first part of this volume is an essentially self-contained exposition of the geometric aspects of local and global regularity theory for the Monge–Ampère and linearized Monge–Ampère equations. As an application, we solve the second boundary value problem of the prescribed affine mean curvature equation, which can be viewed as a coupling of the latter two equations. Of interest in its own right, the linearized Monge–Ampère equation also has deep connections and applications in analysis, fluid mechanics and geometry, including the semi-geostrophic equations in atmospheric flows, the affine maximal surface equation in affine geometry and the problem of finding Kahler metrics of constant scalar curvature in complex geometry. Among other topics, the second part provides a thorough exposition of the large time behavior and discounted approximation of Hamilton–Jacobi equations, which have received much attention in the last two decades, and a new approach to the subject, the nonlinear adjoint method, is introduced. The appendix offers a short introduction to the theory of viscosity solutions of first-order Hamilton–Jacobi equations.

## *Systèmes dynamiques et théorie ergodique*

Sergei Yu. PILYUGIN, Kazuhiro SAKAI. — **Shadowing and hyperbolicity.** — Lecture notes in mathematics, vol. 2193. — Un vol. broché, 15,5×23,5, de XIV, 216 p. — ISBN 978-3-319-65183-5. — Prix: SFr. 46.79. — Springer Nature, Cham, 2017.

Focusing on the theory of shadowing of approximate trajectories (pseudotrajectories) of dynamical systems, this book surveys recent progress in establishing relations between shadowing and such basic

notions from the classical theory of structural stability as hyperbolicity and transversality. Special attention is given to the study of “quantitative” shadowing properties, such as Lipschitz shadowing (it is shown that this property is equivalent to structural stability both for diffeomorphisms and smooth flows), and to the passage to robust shadowing (which is also equivalent to structural stability in the case of diffeomorphisms, while the situation becomes more complicated in the case of flows). Relations between the shadowing property of diffeomorphisms on their chain transitive sets and the hyperbolicity of such sets are also described. The book will allow young researchers in the field of dynamical systems to gain a better understanding of new ideas in the global qualitative theory. It will also be of interest to specialists in dynamical systems and their applications.

### *Analyse de Fourier, analyse harmonique abstraite*

Michael CWIKEL, Mario MILMAN, (Editors). — **Functional analysis, harmonic analysis, and image processing: a collection of papers in honor of Björn Jawerth.** — Contemporary mathematics, vol. 693. — Un vol. relié, 17,5×25,5, de VII, 411 p. — ISBN 978-1-4704-2836-5. — Prix: US\$110.00. — American Mathematical Society, Providence, 2017.

This volume is dedicated to the memory of Bjorn Jawerth. It contains original research contributions and surveys in several of the areas of mathematics to which Bjorn made important contributions. Those areas include harmonic analysis, image processing, and functional analysis, which are of course interrelated in many significant and productive ways. Among the contributors are some of the world’s leading experts in these areas. With its combination of research papers and surveys, this book may become an important reference and research tool. This book should be of interest to advanced graduate students and professional researchers in the areas of functional analysis, harmonic analysis, image processing, and approximation theory. It combines articles presenting new research with insightful surveys written by foremost experts.

### *Analyse fonctionnelle*

Guillaume AUBRUN, Stanislav J. SZAREK. — **Alice and Bob meet Banach: the interface of asymptotic geometric analysis and quantum information theory.** — Mathematical surveys and monographs, vol. 223. — Un vol. relié, 18,5×26, de XXI, 414 p. — ISBN 978-1-4704-3468-7. — Prix: SFr. 116.00. — American Mathematical Society, Providence, 2017.

The quest to build a quantum computer is arguably one of the major scientific and technological challenges of the twenty-first century, and quantum information theory (QIT) provides the mathematical framework for that quest. Over the last dozen or so years, it has become clear that quantum information theory is closely linked to geometric functional analysis (Banach space theory, operator spaces, high-dimensional probability), a field also known as asymptotic geometric analysis (AGA). In a nutshell, asymptotic geometric analysis investigates quantitative properties of convex sets, or other geometric structures, and their approximate symmetries as the dimension becomes large. This makes it especially relevant to quantum theory, where systems consisting of just a few particles naturally lead to models whose dimension is in the thousands, or even in the billions. *Alice and Bob meet Banach* is aimed at multiple audiences connected through their interest in the interface of QIT and AGA: at quantum information researchers who want to learn AGA or apply its tools; at mathematicians interested in learning QIT, especially the part that is relevant to functional analysis/convex geometry/random matrix theory and related areas; and at beginning researchers in either field. Moreover, this user-friendly book contains numerous tables and explicit estimates, with reasonable constants when possible, which make it a useful reference even for established mathematicians generally familiar with the subject.

Huaxin LIN. — **From the basic homotopy Lemma to the classification of  $C^*$ -algebras.** — CBMS regional conference series in mathematics, vol. 124. — Un vol. broché, 15,5×23,5, de XIX, 420 p. — ISBN 978-14704-3490-8. — Prix: US\$52.00. — American Mathematical Society, Providence, 2017.

This book examines some recent developments in the theory of  $C^*$ -algebras, which are algebras of operators on Hilbert spaces. An elementary introduction to the technical part of the theory is given via a basic homotopy lemma concerning a pair of almost commuting unitaries. The book presents an outline of the background as well as some recent results of the classification of simple amenable  $C^*$ -algebra, otherwise known as the Elliott program. This includes some stable uniqueness theorems and a revisiting of Bott maps via stable homotopy. Furthermore,  $KK$ -theory related rotation maps are introduced. The book is based on lecture notes from the CBMS lecture sequence at the University of Wyoming in the summer of 2015.

### *Calcul des variations et contrôle optimal*

Guy DAVID, Marcel FILOCHE, David JERISON, Svitlana MAYBORODA. — **A free boundary problem for the localization of eigenfunctions.** — Astérisque, vol. 392. — Un vol. broché,  $17,5 \times 24$ , de IX, 203 p. — ISBN 978-85629-863-3. — Prix: €32.00. — Société mathématique de France, Paris, 2017.

We study a variant of the Alt, Caffarelli, and Friedman free boundary problem, with many phases and a slightly different volume term, which we originally designed to guess the localization of eigenfunctions of a Schrödinger operator in a domain. We prove Lipschitz bounds for the functions and some nondegeneracy and regularity properties for the domains.

Daniela TONON, Maria SOLEDAD ARONNA, Dante KALISE, (Editors). — **Optimal control: novel directions and applications.** — Lecture notes in mathematics, vol. 2180. — Un vol. broché,  $15,5 \times 23,5$ , de XIV, 386 p. — ISBN 978-3-319-60770-2. — Prix: SFr. 77.00. — Springer Nature, Cham, 2017.

Focusing on applications to science and engineering, this book presents the results of the ITN-FP7 SADCO network's innovative research in optimization and control in the following interconnected topics: optimality conditions in optimal control, dynamic programming approaches to optimal feedback synthesis and reachability analysis, and computational developments in model predictive control. The novelty of the book resides in the fact that it has been developed by early career researchers, providing a good balance between clarity and scientific rigor. Each chapter features an introduction addressed to PhD students and some original contributions aimed at specialist researchers. Requiring only a graduate mathematical background, the book is self-contained. It will be of particular interest to graduate and advanced undergraduate students, industrial practitioners and to senior scientists wishing to update their knowledge.

### *Topologie des variétés, analyse globale et analyse des variétés*

H. HOFER, K. WYSOCKI, E. ZEHNDER. — **Applications of polyfold theory I: the polyfolds of Gromov–Witten theory.** — Memoirs of the American Mathematical Society, vol. 1179. — Un vol. relié,  $17,5 \times 26,5$ , de V, 218 p. — ISBN 978-1-4704-2203-5. — Prix: US\$75.00. — American Mathematical Society, Providence, 2017.

In this paper the authors start with the construction of the symplectic field theory (SFT). As a general theory of symplectic invariants, SFT has been outlined in Introduction to symplectic field theory (2000), by Y. Eliashberg, A. Givental and H. Hofer who have predicted its formal properties. The actual construction of SFT is a hard analytical problem which will be overcome by means of the polyfold theory due to the present authors. The current paper addresses a significant amount of the arising issues and the general theory will be completed in part II of this paper. To illustrate the polyfold theory the authors use the results of the present paper to describe an alternative construction of the Gromov–Witten invariants for general compact symplectic manifolds.

Françoise MICHEL, Claude WEBER. — **Higher-dimensional knots according to Michel Kervaire.** — EMS series of lectures in mathematics. — Un vol. broché,  $17 \times 24$ , de IX, 134 p. — ISBN 978-3-03719-180-4. — Prix: €32.00. — European Mathematical Society, Zürich, 2017.

Michel Kervaire wrote six papers which can be considered fundamental to the development of higher-dimensional knot theory. They are not only of historical interest but naturally introduce to some of the

essential techniques in this fascinating theory. This book is written to provide graduate students with the basic concepts necessary to read texts in higher-dimensional knot theory and its relations with singularities. The first chapters are devoted to a presentation of Pontrjagin's construction, surgery and the work of Kervaire and Milnor on homotopy spheres. We pursue with Kervaire's fundamental work on the group of a knot, knot modules and knot cobordism. We add developments due to Levine. Tools (like open books, handlebodies, plumbings, ...) often used but hard to find in original articles are presented in appendices. We conclude with a description of the Kervaire invariant and the consequences of the Hill-Hopkins-Ravenel results in knot theory.

## ***Probabilités et processus stochastiques***

SOURAV CHATTERJEE. — **Large deviations for random graphs : Ecole d'été de probabilités de Saint-Flour XLV - 2015.** — Lecture notes in mathematics, vol. 2139. — Un vol. broché, 15,5×23,5, de XI, 167 p. — ISBN 978-3-319-65815-5. — Prix: SFr. 85.00. — Springer Nature, Cham, 2017.

This book addresses the emerging body of literature on the study of rare events in random graphs and networks. For example, what does a random graph look like if by chance it has far more triangles than expected? Until recently, probability theory offered no tools to help answer such questions. Important advances have been made in the last few years, employing tools from the newly developed theory of graph limits. This work represents the first book-length treatment of this area, while also exploring the related area of exponential random graphs. All required results from analysis, combinatorics, graph theory and classical large deviations theory are developed from scratch, making the text self-contained and doing away with the need to look up external references. Further, the book is written in a format and style that are accessible for beginning graduate students in mathematics and statistics.

## ***Statistique***

RUSSEL CHENG. — **Non-standard parametric statistical inference.** — Un vol. relié, 16×24, de XII, 417 p. — ISBN 978-0-19-850504-4. — Prix: £80.00. — Oxford University Press, Oxford, 2017.

This book discusses the fitting of parametric statistical models to data samples. Emphasis is placed on: (i) how to recognize situations where the problem is non-standard when parameter estimates behave unusually, and (ii) the use of parametric bootstrap resampling methods in analyzing such problems. A frequentist likelihood-based viewpoint is adopted, for which there is a well-established and very practical theory. The standard situation is where certain widely applicable regularity conditions hold. However, there are many apparently innocuous situations where standard theory breaks down, sometimes spectacularly. Most of the departures from regularity are described geometrically, with only sufficient mathematical detail to clarify the non-standard nature of a problem and to allow formulation of practical solutions. The book is intended for anyone with a basic knowledge of statistical methods, as is typically covered in a university statistical inference course, wishing to understand or study how standard methodology might fail. Easy to understand statistical methods are presented which overcome these difficulties, and demonstrated by detailed examples drawn from real applications. Simple and practical model-building is an underlying theme. Parametric bootstrap resampling is used throughout for analyzing the properties of fitted models, illustrating its ease of implementation even in non-standard situations. Distributional properties are obtained numerically for estimators or statistics not previously considered in the literature because their theoretical distributional properties are too hard to obtain theoretically. Bootstrap results are presented mainly graphically in the book, providing an accessible demonstration of the sampling behaviour of estimators.

DAVID SALSBERG. — **Errors, blunders and lies: how to tell the difference.** — ASA-CRC series on statistical reasoning in science and society. — Un vol. relié, 14,5×22,5, de XII, 154 p. — ISBN 978-1-138-72698-7. — Prix: £61.60. — CRC Press/Taylor & Francis Group, Boca Raton, 2017.

We live in a world that is not quite “right.” The central tenet of statistical inquiry is that Observation = Truth + Error because even the most careful of scientific investigations have always been bedeviled by uncertainty. Our attempts to measure things are plagued with small errors. Our attempts to understand our world are blocked by blunders. And, unfortunately, in some cases, people have been known to lie. In this long-awaited follow-up to his well-regarded bestseller, *The lady tasting tea*, David Salsburg opens a door to the amazing widespread use of statistical methods by looking at historical examples of errors, blunders and lies from areas as diverse as archeology, law, economics, medicine, psychology, sociology, Biblical studies, history, and war-time espionage. In doing so, he shows how, upon closer statistical investigation, errors and blunders often lead to useful information. And how statistical methods have been used to uncover falsified data. Beginning with Edmund Halley’s examination of the *Transit of Venus* and ending with a discussion of how many tanks Rommel had during the Second World War, the author invites the reader to come along on this easily accessible and fascinating journey of how to identify the nature of errors, minimize the effects of blunders, and figure out who the liars are.

Walter SCHACHERMAYER. — **Asymptotic theory of transaction costs.** — Zürich lectures in advanced mathematics. — Un vol. broché, 17×24, de X, 150 p. — ISBN 978-3-03719-173-6. — Prix: €34.00. — European Mathematical Society, Zürich, 2017.

A classical topic in mathematical finance is the theory of portfolio optimization. Robert Merton’s work from the early seventies had enormous impact on academic research as well as on the paradigms guiding practitioners. One of the ramifications of this topic is the analysis of (small) proportional transaction costs, such as a Tobin tax. The lecture notes present some striking recent results of the asymptotic dependence of the relevant quantities when transaction costs tend to zero. An appealing feature of the consideration of transaction costs is that it allows for the first time to reconcile the no arbitrage paradigm with the use of non-semimartingale models, such as fractional Brownian motion. This leads to the culminating theorem of the present lectures which roughly reads as follows: for a fractional Brownian motion stock price model we always find a shadow price process for given transaction costs. This process is a semimartingale and can therefore be dealt with using the usual machinery of mathematical finance.

## ***Information, communication, circuits***

JØRN JUSTEN, TOM HØHOLDT. — **A course in error-correcting codes.** — Second edition. — EMS textbooks in mathematics. — Un vol. relié, 17×24, de X, 216 p. — ISBN 978-3-03719-179-8. — Prix: €39.50. — European Mathematical Society, Zürich, 2017.

This book, updated and enlarged for the second edition, is written as a text for a course aimed at 3rd or 4th year students. Only some familiarity with elementary linear algebra and probability is directly assumed, but some maturity is required. The students may specialize in discrete mathematics, computer science, or communication engineering. The book is also a suitable introduction to coding theory for researchers from related fields or for professionals who want to supplement their theoretical basis. The book gives the coding basics for working on projects in any of the above areas, but material specific to one of these fields has not been included. The chapters cover the codes and decoding methods that are currently of most interest in research, development, and application. They give a relatively brief presentation of the essential results, emphasizing the interrelations between different methods and proofs of all important results. A sequence of problems at the end of each chapter serves to review the results and give the student an appreciation of the concepts. In addition, some problems and suggestions for projects indicate direction for further work. The presentation encourages the use of programming tools for studying codes, implementing decoding methods, and simulating performance. Specific examples of programming exercises are provided on the book’s home page.

Keith M. MARTIN. — **Everyday cryptography: fundamental principles and applications.** — Second edition. — Un vol. relié, 16×24, de XXX, 674 p. — ISBN 978-0-19-878800-3. — Prix: £75.00. — Oxford University Press, Oxford, 2017.

Cryptography is a vital technology that underpins the security of information in computer networks. This book presents a comprehensive introduction to the role that cryptography plays in providing information security for technologies such as the Internet, mobile phones, payment cards, and wireless local area networks. Focusing on the fundamental principles that ground modern cryptography as they arise in modern applications, it avoids both an over-reliance on transient technologies and overwhelming theoretical research. The first part of the book provides essential background, identifying the core security services provided by cryptography. The next part introduces the main cryptographic mechanisms that deliver these security services such as encryption, hash functions, and digital signatures, discussing why they work and how to deploy them, without delving into any significant mathematical detail. In the third part, the important practical aspects of key management are introduced, which is essential for making cryptography work in real systems. The last part considers the application of cryptography. A range of application case studies is presented, alongside a discussion of the wider societal issues arising from use of cryptography to support contemporary cyber security.