Advances In Cryptology Crypto 2003 23rd Annual International Cryptology Conference Santa Barbara California Usa August 17 21 2003 Proceedings Lecture Notes In Computer Science

This volume consists of contributions by speakers at a Conference on Algebra and its Applications that took place in Athens, Ohio, in March of 2005. It provides a snapshot of the diversity of themes and applications that interest algebraists today. The papers in this volume include some of the latest results in the theory of modules, noncommutative rings, representation theory, matrix theory, linear algebra over noncommutative rings, cryptography, error-correcting codes over finite rings, and projective-geometry codes, as well as expository articles that will provide algebraists and other mathematicians, including graduate students, with an accessible introduction to areas outside their own expertise. The book will serve both the specialist looking for the latest result and the novice seeking an accessible reference for some of the ideas and results presented here.

This book constitutes the thoroughly refereed post-proceedings of the 6th International Conference on Information Security and Cryptology, ICISC 2003, held in Seoul, Korea, in November 2003. The 32 revised full papers presented together with an invited paper were

carefully selected from 163 submissions during two rounds of reviewing and improvement. The papers are organized in topical sections on digital signatures, primitives, fast implementations, computer security and mobile security, voting and auction protocols, watermarking, authentication and threshold protocols, and block ciphers and stream ciphers.

This book constitutes the thoroughly refereed postproceedings of the 10th Annual International Workshop on Selected Areas in Cryptography, SAC 2003, held in Ottawa, Canada, in August 2003. The 25 revised full papers presented were carefully selected from 85 submissions during two rounds of reviewing and improvement. The papers are organized in topical sections on elliptic and hyperelliptic curves, side channel attacks, security protocols and applications, cryptanalysis, cryptographic primitives, stream ciphers, and efficient implementations.

Crypto 2004, the 24th Annual Crypto Conference, was sponsored by the Int- national Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara. The program committee accepted 33 papers for presentation at the conf- ence. These were selected from a total of 211 submissions. Each paper received at least three independent reviews. The selection process included a Web-based discussion phase, and a one-day program committee meeting at New York U- versity. These proceedings include updated versions of the 33 accepted papers. The authors had a

few weeks to revise them, aided by comments from the reviewers. However, the revisions were not subjected to any editorial review. Theconferenceprogramincludedtwoi nvitedlectures.VictorShoup'sinvited talk was a survey on chosen ciphertext security in public-key encryption. Susan Landau's invited talk was entitled "Security, Liberty, and Electronic Commu- cations". Her extended abstract is included in these proceedings. We continued the tradition of a Rump Session, chaired by Stuart Haber. Those presentations (always short, often serious) are not included here.

As an intermediate model between conventional PKC and ID-PKC, CL-PKC can avoid the heavy overhead of certificate management in traditional PKC as well as the key escrow problem in ID-PKC altogether. Since the introduction of CL-PKC, many concrete constructions, security models, and applications have been proposed during the last decade. Differing from the other books on the market, this one provides rigorous treatment of CL-PKC. Definitions, precise assumptions, and rigorous proofs of security are provided in a manner that makes them easy to understand.

This book constitutes the thoroughly refereed post-proceedings of the 12th International Workshop on Security Protocols, April 2004. The book presents 21 revised full papers presented together with edited transcriptions of some of the discussions following the presentations. Among the topics addressed are authentication, anonymity, verification of cryptographic protocols, mobile ad-hoc network security, denial of service, SPKI, access control, timing attacks, API

security, biometrics for security, and others.
These are the proceedings of Crypto 2005, the 25th Annual International Cryptology Conference. The conference was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Science Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara. The conference was held in Santa Barbara, California, August 14–18, 2005.
SAC 2004 was the eleventh in a series of annual workshops on Selected Areas in Cryptography. This was the second time that the workshop was hosted by the University of Waterloo, Ontario, with previous workshops being held at Queen'sUniversityinKingston(1994,1996,1998and1999),CarletonUniversity in Ottawa (1995, 1997 and 2003), the Fields Institute in Toronto (2001) and Memorial University of Newfoundland in St. John's (2002). The primary intent of the workshop was to provide a relaxed atmosphere in which researchers in cryptography could present and discuss new work on selected areas of current interest. This year's themes for SAC were: – Design and analysis of symmetric key cryptosystems. – Primitives for symmetric key cryptography, including block and stream - phers, hash functions, and MAC algorithms. – E?cient implementation of cryptographic systems in public and symmetric key cryptography. – Cryptographic solutions for mobile (web) services. A record of 117 papers were submitted for consideration by the program committee. After an extensive review process, 25 papers were

accepted for p- sentation at the workshop (two of these papers were merged). Unfortunately, many good papers could not be accommodated this year. These proceedings contain the revised versions of the 24 accepted papers. The revised versions were not subsequently checked for correctness. Also, we were very fortunate to have two invited speakers at SAC 2004. • Eli Biham arranged for some breaking news in his talk on “New Results on SHA-0 and SHA-1.” This talk was designated as the Sta?ord Tavares L- ture.

The three volume-set, LNCS 10991, LNCS 10992, and LNCS 10993, constitutes the refereed proceedings of the 38th Annual International Cryptology Conference, CRYPTO 2018, held in Santa Barbara, CA, USA, in August 2018. The 79 revised full papers presented were carefully reviewed and selected from 351 submissions. The papers are organized in the following topical sections: secure messaging; implementations and physical attacks prevention; authenticated and format-preserving encryption; cryptoanalysis; searchable encryption and differential privacy; secret sharing; encryption; symmetric cryptography; proofs of work and proofs of stake; proof tools; key exchange; symmetric cryptoanalysis; hashes and random oracles; trapdoor functions; round optimal MPC; foundations; lattices; lattice-based ZK; efficient MPC; quantum cryptography; MPC; garbling; information-theoretic MPC; oblivious transfer; non-

malleable codes; zero knowledge; and obfuscation.
This book constitutes the refereed proceedings of the 6th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2003, held in Miami, Florida, USA in January 2003. The 26 revised full papers presented were carefully reviewed and selected from 105 submissions. The papers are organized in topical sections on Diffie-Hellman based schemes, threshold cryptography, reduction proofs, broadcast and tracing, digital signatures, specialized multiparty cryptography, cryptanalysis, elliptic curves: implementation attacks, implementation and hardware issues, new public key schemes, and elliptic curves: general issues.
This book constitutes the refereed proceedings of the 7th International Conference on Information and Communications Security, ICICS 2005, held in Beijing, China in December 2005. The 40 revised full papers presented were carefully reviewed and selected from 235 submissions. The papers are organized in topical sections on fair exchange, digital signatures, cryptographic protocols, cryptanalysis, network security, applied cryptography, key management, access control, applications, watermarking, and system security.
This book constitutes the refereed proceedings of the 26th Annual International Cryptology Conference, CRYPTO 2006, held in Santa Barbara, California, USA in August 2006. The 34 revised full

papers presented together with 2 invited lectures were carefully reviewed and selected from 250 submissions. The papers address all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as well as advanced applications.

This book constitutes the refereed proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography, PKC 2005, held in Les Diablerets, Switzerland in January 2005. The 28 revised full papers presented were carefully reviewed and selected from 126 submissions. The papers are organized in topical sections on cryptanalysis, key establishment, optimization, building blocks, RSA cryptography, multivariate asymmetric cryptography, signature schemes, and identity-based cryptography.

This book constitutes the refereed proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2004, held in Interlaken, Switzerland in May 2004. The 36 revised full papers presented were carefully reviewed and selected from 206 submissions. The papers are organized in topical sections on private computation, signatures, inconditional security, distributed cryptography, foundations, identity based encryption, elliptic curves, public-key cryptography, multiparty computation, cryptanalysis, new applications,

algorithms and implementation, and anonymity. Here are the refereed proceedings of the 9th International Conference on Theory and Practice in Public-Key Cryptography, PKC 2006, held in New York City in April 2006. The 34 revised full papers presented are organized in topical sections on cryptanalysis and protocol weaknesses, distributed crypto-computing, encryption methods, cryptographic hash and applications, number theory algorithms, pairing-based cryptography, cryptosystems design and analysis, signature and identification, authentication and key establishment, multi-party computation, and PKI techniques.

This book constitutes the refereed proceedings of the 5th International Conference on Cryptology in India, INDOCRYPT 2004, held in Chennai, India in December 2004. The 30 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 181 submissions. The papers are organized in topical sections on cryptographic protocols, applications, stream ciphers, cryptographic Boolean functions, foundations, block ciphers, public key encryption, efficient representations, public key cryptanalysis, modes of operation, signatures, and traitor tracing and visual cryptography.

The discrete logarithm problem based on elliptic and hyperelliptic curves has gained a lot of popularity as a cryptographic primitive. The main reason is that no

subexponential algorithm for computing discrete logarithms on small genus curves is currently available, except in very special cases. Therefore curve-based cryptosystems require much smaller key sizes than RSA to attain the same security level. This makes them particularly attractive for implementations on memory-restricted devices like smart cards and in high-security applications. The Handbook of Elliptic and Hyperelliptic Curve Cryptography introduces the theory and algorithms involved in curve-based cryptography. After a very detailed exposition of the mathematical background, it provides ready-to-implement algorithms for the group operations and computation of pairings. It explores methods for point counting and constructing curves with the complex multiplication method and provides the algorithms in an explicit manner. It also surveys generic methods to compute discrete logarithms and details index calculus methods for hyperelliptic curves. For some special curves the discrete logarithm problem can be transferred to an easier one; the consequences are explained and suggestions for good choices are given. The authors present applications to protocols for discrete-logarithm-based systems (including bilinear structures) and explain the use of elliptic and hyperelliptic curves in factorization and primality proving. Two chapters explore their design and efficient implementations in smart cards. Practical and theoretical aspects of side-channel attacks and countermeasures and a chapter devoted to (pseudo-)random number generation round off the exposition. The broad coverage of all- important areas makes this book a complete handbook of elliptic and hyperelliptic curve cryptography and an invaluable reference to anyone interested in this exciting field.

Advances in Cryptology -- CRYPTO 200323rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, ProceedingsSpringer

Science & Business Media

In today's world, data must be sent around the world cheaply and securely, and that requires origin authentication, integrity protection, and confidentiality – the recipient of a message should be able to ascertain who sent the message, be sure that the message has not been changed en route, and be sure that the data arrives without having been read by anyone else. The second editor invented signcryption, an area of cryptography that studies systems that simultaneously provide origin authentication, integrity protection and confidentiality for data. Signcryption schemes combine the features of digital signature schemes with those of public-key encryption schemes and aim to provide security guarantees in a way that is provably correct and significantly less computationally expensive than the "encrypt-then-sign" method most commonly adopted in public-key cryptography. This is the first comprehensive book on signcryption, and brings together leading authors from the field of cryptography in a discussion of the different methods for building efficient and secure signcryption schemes, and the ways in which these schemes can be used in practical systems. Chapters deal with the theory of signcryption, methods for constructing practical signcryption schemes, and the advantages of using such schemes in practical situations. The book will be of benefit to cryptography researchers, graduate students and practitioners.

This book constitutes the refereed proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2004, held at Jeju Island, Korea in December 2004. The 35 revised full papers presented were carefully reviewed and selected from 208 submissions. The papers are organized in topical sections on block ciphers, public key encryption, number theory and applications, secure computation, hash functions,

key management, identification, XL algorithms, digital signatures, public key cryptanalysis, symmetric key cryptanalysis, and cryptographic protocols.

This book constitutes the refereed proceedings of the 28th Annual International Cryptology Conference, CRYPTO 2008, held in Santa Barbara, CA, USA in August 2008. The 32 revised full papers presented were carefully reviewed and selected from 184 submissions. Addressing all current foundational, theoretical and research aspects of cryptology, cryptography, and cryptanalysis as well as advanced applications, the papers are organized in topical sections on random oracles, applications, public-key crypto, hash functions, cryptanalysis, multiparty computation, privacy, zero knowledge, and oblivious transfer.

This book constitutes the thoroughly refereed post-proceedings of the International Workshop on Coding and Cryptography, WCC 2005, held in Bergen, Norway, in March 2005. The 33 revised full papers were carefully reviewed and selected during two rounds of review. The papers address all aspects of coding theory, cryptography and related areas, theoretical or applied.

The Seventh International Conference on Information and Communications - curity,ICICS2005,washeldinBeijing,China,10-13December2005. TheICICS conference series is an established forum for exchanging new research ideas and development results in the areas of information security and applied crypt- raphy. The ?rst event began here in Beijing in 1997. Since then the conference series has been interleaving its venues in China and the rest of the world: ICICS 1997 in Beijing, China; ICICS 1999 in Sydney, Australia; ICICS 2001 in Xi'an, China; ICICS 2002 in Singapore; ICICS 2003 in Hohhot City, China; and ICICS 2004 in Malaga, Spain. The conference proceedings of the past events have - ways been published by Springer in the Lecture Notes in Computer

Science series, with volume numbers, respectively: LNCS 1334,LNCS 1726,LNCS 2229, LNCS 2513, LNCS 2836, and LNCS 3269. ICICS 2005 was sponsored by the Chinese Academy of Sciences (CAS); the Beijing Natural Science Foundation of China under Grant No. 4052016; the National Natural Science Foundation of China under Grants No. 60083007 and No. 60573042;the NationalGrandFundamentalResearch973ProgramofChina under Grant No. G1999035802, and Hewlett-Packard Laboratories, China. The conference was organized and hosted by the Engineering Research Center for Information Security Technology of the Chinese Academy of Sciences (ERCIST, CAS) in co-operation with the International Communications and Information Security Association (ICISA). The aim of the ICICS conference series has been to o?er the attendees the opportunity to discuss the latest developments in theoretical and practical - pects of information and communications security.

Conference on Cryptologic Research, CRYPTO 2020, which was held during August 17–21, 2020. Crypto has traditionally been held at UCSB every year, but due to the COVID-19 pandemic it will be an online event in 2020. The 85 papers presented in the proceedings were carefully reviewed and selected from a total of 371 submissions. They were organized in topical sections as follows: Part I: Security Models; Symmetric and Real World Cryptography; Hardware Security and Leakage Resilience; Outsourced encryption; Constructions. Part II: Public Key Cryptanalysis; Lattice Algorithms and Cryptanalysis; Lattice-based and Post Quantum Cryptography; Multi-Party Computation. Part III: Multi-Party Computation; Secret Sharing; Cryptanalysis; Delay functions; Zero Knowledge.

This book constitutes the refereed proceedings of the

International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2003, held in Warsaw, Poland in May 2003. The 37 revised full papers presented together with two invited papers were carefully reviewed and selected from 156 submissions. The papers are organized in topical sections on cryptanalysis, secure multi-party communication, zero-knowledge protocols, foundations and complexity-theoretic security, public key encryption, new primitives, elliptic curve cryptography, digital signatures, information-theoretic cryptography, and group signatures.

This book constitutes the refereed proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2005, held in Chennai, India in December 2005. The 37 revised full papers presented were carefully reviewed and selected from 237 submissions. The papers are organized in topical sections on algebra and number theory, multiparty computation, zero knowledge and secret sharing, information and quantum theory, privacy and anonymity, cryptanalytic techniques, stream cipher cryptanalysis, block ciphers and hash functions, bilinear maps, key agreement, provable security, and digital signatures.

THE LEGACY... First introduced in 1995, Cryptography: Theory and Practice garnered enormous praise and popularity, and soon became the standard textbook for cryptography courses around the world. The second edition was equally embraced, and enjoys status as a perennial bestseller. Now in its third edition, this authoritative text continues to provide a solid foundation

for future breakthroughs in cryptography. WHY A THIRD EDITION? The art and science of cryptography has been evolving for thousands of years. Now, with unprecedented amounts of information circling the globe, we must be prepared to face new threats and employ new encryption schemes on an ongoing basis. This edition updates relevant chapters with the latest advances and includes seven additional chapters covering: Pseudorandom bit generation in cryptography Entity authentication, including schemes built from primitives and special purpose "zero-knowledge" schemes Key establishment including key distribution and protocols for key agreement, both with a greater emphasis on security models and proofs Public key infrastructure, including identity-based cryptography Secret sharing schemes Multicast security, including broadcast encryption and copyright protection THE RESULT... Providing mathematical background in a "just-in-time" fashion, informal descriptions of cryptosystems along with more precise pseudocode, and a host of numerical examples and exercises, Cryptography: Theory and Practice, Third Edition offers comprehensive, in-depth treatment of the methods and protocols that are vital to safeguarding the mind-boggling amount of information circulating around the world.

This book constitutes the refereed proceedings of the Cryptographers' Track at the RSA Conference 2003, CT-RSA 2003, held in San Francisco, CA, USA, in April 2003. The 26 revised full papers presented together with abstracts of 2 invited talks were carefully reviewed and selected from 97 submissions. The papers are organized

in topical sections on key self-protection, message authentication, digital signatures, pairing based cryptography, multivariate and lattice problems, cryptographic architectures, new RSA-based cryptosystems, chosen-ciphertext security, broadcast encryption and PRF sharing, authentication structures, elliptic curves and pairings, threshold cryptography, and implementation issues.

This book constitutes the refereed proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2003, held in Taipei, Taiwan in November/December 2003.The 32 revised full papers presented together with one invited paper were carefully reviewed and selected from 188 submissions. The papers are organized in topical sections on public key cryptography, number theory, efficient implementations, key management and protocols, hash functions, group signatures, block cyphers, broadcast and multicast, foundations and complexity theory, and digital signatures.

This book constitutes the refereed proceedings of the 11th International Workshop on Fast Software Encryption, FSE 2004, held in Delhi, India in February 2004. The 28 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 75 submissions. The papers are organized in topical sections on algebraic attacks, stream cipher cryptanalysis, Boolean functions, stream cipher design, design and analysis of block ciphers, cryptographic primitives-theory, modes of operation, and analysis of MACs and hash functions.

This book constitutes the refereed proceedings of the 23rd Annual International Cryptology Conference, CRYPTO 2003, held in Santa Barbara, California in August 2003. The 34 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 166 submissions. The papers are organized in topical sections on public key cryptanalysis, alternate adversary models, protocols, symmetric key cryptanalysis, universal composability, zero knowledge, algebraic geometry, public key constructions, new problems, symmetric key constructions, and new models.

This book constitutes the refereed proceedings of the 4th Theory of Cryptography Conference, TCC 2007, held in Amsterdam, The Netherlands in February 2007. The 31 revised full papers cover encryption, universally composable security, arguments and zero knowledge, notions of security, obfuscation, secret sharing and multiparty computation, signatures and watermarking, private approximation and black-box reductions, and key establishment.

This book constitutes the refereed proceedings of the 7th International Conference on Cryptology in India, INDOCRYPT 2006, held in Kolkata, India in December 2006. The 29 revised full papers and 2 invited papers cover such topics as symmetric cryptography, provable security, fast implementation of public key cryptography, id-based cryptography, as well as embedded systems and side channel attacks.

The two-volume set LNCS 4051 and LNCS 4052 constitutes the refereed proceedings of the 33rd International Colloquium on Automata, Languages and Programming, ICALP 2006, held in Venice, Italy, July 2006. In all, these volumes present more 100 papers and lectures. Volume II (4052) presents 2 invited papers and 2 additional conference tracks with 24 papers each, focusing on algorithms, automata, complexity and games as well as on security and cryptography foundation.

PKC2004wasthe7thInternationalWorkshoponPracticeandTheoryinPublic Key Cryptography and was sponsored by IACR, the International Association for Cryptologic Research (www. iacr. org). This year the workshop was organized 2 in cooperation with the Institute for Infocomm Research (I R), Singapore. There were 106 paper submissions from 19 countries to PKC 2004. That is the highest submission number in PKC history. Due to the large number of submissionsandthehighqualityofthe submittedpapers,notallthepapersthat contained new ideas were accepted. Of the 106 submissions, 32 were selected for the proceedings. Each paper was sent to at least 3 members of the Program Committee for comments. The revised versions of the accepted papers were not checked for correctness of their scienti?c aspects and the authors bear the full responsibility for the contents of their papers. Some authors will write ?nal versions of

their papers for publication in refereed journals. I am very grateful to the members of the Program Committee for their hard work in the di?cult task of selecting fewer than 1 in 3 of the submitted papers, as well as the following external referees who helped the Program Committee: Nuttapong Attrapadung,RobertoMariaAvanzi,GildasAvoine,JoonsangBaek, Qingjun Cai, Jae Choon Cha, Chien-Ning Chen, Liqun Chen, Xiaofeng Chen, Koji Chida, Nicolas T. Courtois, Yang Cui, Jean-Franco ¸ is Dhem, Louis Goubin, Louis Granboulan, Rob Granger, Jens Groth, Yumiko Hanaoka, Darrel Hank- son,Chao-ChihHsu,TetsutaroKobayashi,YuichiKomano,HidenoriKuwakado, TanjaLange,PeterLeadbitter,ByoungcheonLee,Chun-KoLee,HenryC. J. Lee, JohnMaloneLee,YongLi,Benoˆ ?tLibert,Hsi-ChungLin,YiLu,JeanMonnerat, Anderson C. A. Nascimento, C.

TO CRYPTOGRAPHY EXERCISE BOOK Thomas Baignkres EPFL, Switzerland Pascal Junod EPFL, Switzerland Yi Lu EPFL, Switzerland Jean Monnerat EPFL, Switzerland Serge Vaudenay EPFL, Switzerland Springer - Thomas Baignbres Pascal Junod EPFL - I&C - LASEC Lausanne, Switzerland Lausanne, Switzerland Yi Lu Jean Monnerat EPFL - I&C - LASEC EPFL-I&C-LASEC Lausanne, Switzerland Lausanne, Switzerland Serge Vaudenay Lausanne, Switzerland Library of Congress Cataloging-in-Publication Data A C.I.P. Catalogue

record for this book is available from the Library of Congress. A CLASSICAL INTRODUCTION TO CRYPTOGRAPHY EXERCISE BOOK by Thomas Baignkres, Palcal Junod, Yi Lu, Jean Monnerat and Serge Vaudenay ISBN- 10: 0-387-27934-2 e-ISBN-10: 0-387-28835-X ISBN- 13: 978-0-387-27934-3 e-ISBN- 13: 978-0-387-28835-2 Printed on acid-free paper. O 2006 Springer Science+Business Media, Inc. All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, Inc., 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now know or hereafter developed is forbidden. The use in this publication of trade names, trademarks, service marks and similar terms, even if the are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights. Printed in the United States of America.

This book constitutes the refereed proceedings of the First International Conference on Cryptology hosted in Malaysia, held in Kuala Lumpur, Malaysia in September 2005, in conjunction with the e-Secure Malaysia 2005 convention. The 19 revised full

papers presented together with 3 invited papers were carefully reviewed and selected from a total of 90 submissions. The papers are organized in topical sections on stream ciphers analysis, cryptography based on combinatorics, cryptographic protocols, implementation issues, unconventional cryptography, block cipher cryptanalysis, and homomorphic encryption.

This book constitutes the thoroughly refereed post-proceedings of the First International Conference on Cryptology in Vietnam, VIETCRYPT 2006, held in Hanoi, Vietnam, September 2006. The 25 papers cover signatures and lightweight cryptography, pairing-based cryptography, algorithmic number theory, ring signatures and group signatures, hash functions, cryptanalysis, key agreement and threshold cryptography, as well as public-key encryption.

This book constitutes the refereed proceedings of the 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2006. 33 revised full papers are presented together with 2 invited talks. The papers are organized in topical sections on cryptanalysis, cryptography meets humans, stream ciphers, hash functions, oblivious transfer, numbers and lattices, foundations, block ciphers, cryptography without random oracles, multiparty computation, and cryptography for groups.

The Cryptographers' Track (CT-RSA) is a research conference within the RSA conference, the largest, regularly staged computer security event. CT-RSA 2004 was the fourth year of the Cryptographers' Track, and it is now an established venue for presenting practical research results related to cryptography and data security. The conference received 77 submissions, and the program committee sel- ted 28 of these for presentation. The program committee worked very hard to evaluate the papers with respect to quality, originality, and relevance to cryp- graphy. Each paper was reviewed by at least three program committee members. Extended abstracts of the revised versions of these papers are in these proc- dings. The program also included two invited lectures by Dan Boneh and Silvio Micali. I am extremely grateful to the program committee members for their en- mous investment of time and e?ort in the di?cult and delicate process of review and selection. Many of them attended the program committee meeting during the Crypto 2003 conference at the University of California, Santa Barbara.