Shai Halevi
Tal Rabin (Eds.)

LNCS 3876

Theory of Cryptography

Third Theory of Cryptography Conference, TCC 2006
New York, NY, USA, March 2006
Proceedings

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

iacr

Springer

Shai Halevi   Tal Rabin (Eds.)

Theory of Cryptography

Third Theory of Cryptography Conference, TCC 2006
New York, NY, USA, March 4-7, 2006
Proceedings

Springer

Volume Editors

Shai Halevi
Tal Rabin
IBM T.J. Watson Research Center
19 Skyline Drive, Hawthorne, NY 10532, USA
E-mail: shaih@alum.mit.edu; talr@watson.ibm.com

Library of Congress Control Number: 2006921180

CR Subject Classification (1998): E.3, F.2.1-2, C.2.0, G, D.4.6, K.4.1, K.4.3, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-32731-2 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-32731-8 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11681878 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3876

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Preface

TCC 2006 was the third Theory of Cryptography Conference, which was held at Columbia University in Manhattan, New York, March 4-7, 2006. TCC 2006 was sponsored by the International Association for Cryptologic Research (IACR) and organized in cooperation with the Computer Science Department of Columbia University. The local arrangements chair was Tal Malkin.

The Program Committee, consisting of 13 members, received 91 submissions and selected for publication 31 of these submissions. The quality of the submissions was very high, and the selection process was a challenging one. The proceedings consist of the revised versions of these 31 papers. Revisions were not checked as to their contents, and the authors bear full responsibility for the contents of their papers. In addition to the 31 accepted papers, the program included two tutorials: A tutorial on "Black-Box Separation Results" by Omer Reingold and a tutorial on "Non-Black-Box Techniques" by Boaz Barak. The conference featured a rump session for informal short presentations of new results, chaired by Charlie Rackoff and boosted by Tequilas!

We are in debt to the many people who contributed to the success of TCC 2006, and we apologize for those whom we have forgotten to mention. First and foremost we thank the authors who submitted their papers to TCC 2006; a conference is only as good as the submissions that it receives. The Program Committee members made a concentrated effort during the short review period contributing their time, knowledge, expertise and taste, and for that we are extremely grateful. We also thank the large number of external reviewers who assisted the committee in the review process.

A heartfelt thanks goes to our local arrangements chair Tal Malkin and her assistant Sophie Majewski for facilitating the communication with Columbia University. Their hard work made the local arrangements an effortless process for us. We also thank Angelos D. Keromytis, Michael Locasto, and Angelos Stavrou for giving us a web server at Columbia University on which to host the TCC work and helping us manage it. We also want to thank IBM for their generous donation of our time and the financial support for students attending TCC.

This was the first year that TCC was sponsored by the IACR. Several people at the IACR helped us navigate this new terrain, in particular Andy Clark, Helena Handschuh and Kevin McCurley. We also benefited from advice from members of the TCC Steering Committee, including Mihir Bellare, Ivan Damgård, Oded Goldreich and Moni Naor. Additional help came from the organizers of last year's TCC: Shafi Goldwasser, Joe Kilian and Joanne Talbot-Hanley, and the people at Springer, in particular Alfred Hofmann, Ingrid Beyer and Anna Kramer.

And last but not least, thanks to our group members Ran Canetti, Rosario Gennaro, Hugo Krawczyk and Masa Abe for all their support (emotional and otherwise).

December 2005

Shai Halevi and Tal Rabin
TCC 2006 Program Co-chairs

External Reviewers

Michel Abdalla
Masayuki Abe
Jesús F. Almansa
Benny Applebaum
Boaz Barak
Mihir Bellare
Alexandra Boldyreva
Dan Boneh
Xavier Boyen
Jan Camenisch
Ran Canetti
Melissa Chase
Richard Cleve
Ivan Damgård
Anupam Datta
Ante Derek
Yevgeniy Dodis
Cynthia Dwork
Ariel Elbaz
Marc Fischlin
Matthias Fitzi
Ariel Gabizon
Rosario Gennaro
Craig Gentry
Kristian Gjøsteen
Mikael Goldmann
Venkat Guruswami
Danny Harnik
Alejandro Hevia
Nick Howgrave-Graham
Yuval Ishai
Oleg Izmerly
Stanisław Jarecki
Yael Tauman Kalai
Joe Kilian
Eike Kiltz
Tadayoshi Kohno
Chiu-Yuen Koo
Hugo Krawczyk
Gunnar Kreitz
Homin Lee
Arjen Lenstra
Anna Lysyanskaya
Phillip MacKenzie
Stephen Miller
Sara Miner
Anton Mityagin
Tal Mor
Ruggero Morselli
Steven Myers
Gregory Neven
Damian Niwiński
Shien Jin Ong
Saurabh Panjwani
Thomas Brochmann Pedersen
Krzysztof Pietrzak
Benny Pinkas
Bartosz Przydatek
Oded Regev
Omer Reingold
Leonid Reyzin
Tom Ristenpart
Ron Rivest
Louis Salvail
Hovav Shacham
Tom Shrimpton
Alice Silverberg
Jessica Staddon
Tamir Tassa
Mårten Trolin
Wim van Dam
Salil Vadhan
Vinod Vaikuntanathan
Emanuele Viola
Andrew Wan
Bogdan Warinschi
Hoeteck Wee
Douglas Wikström

TCC 2006

The Third Theory of Cryptography Conference

Columbia University, New York, NY, USA
March 4-7, 2006

Sponsored by the *International Association for Cryptologic Research*

Organized in cooperation with the *Computer Science Department, Columbia University*

General and Program Co-chairs

Shai Halevi and Tal Rabin, IBM T.J. Watson Research Center

Program Committee

Stefan Dziembowski	Warsaw University
Johan Håstad	Royal Institute of Technology
Jonathan Katz	University of Maryland, College Park
Eyal Kushilevitz	Technion Israel Institute of Technology
Yehuda Lindell	Bar-Ilan University
Tal Malkin	Columbia University
Daniele Micciancio	University of California, San Diego
John C. Mitchell	Stanford University
Chanathip Namprempre	Thammasat University
Jesper Buus Nielsen	University of Århus
Manoj Prabhakaran	University of Illinois, Urbana-Champaign
Adam Smith	Weizmann Institute of Science
Luca Trevisan	University of California, Berkeley

TCC Steering Committee

Mihir Bellare	University of California, San Diego
Ivan Damgård	University of Århus
Oded Goldreich	Weizmann Institute of Science
Shafi Goldwasser	MIT
Johan Håstad	Royal Institute of Technology
Russell Impagliazzo	University of California, San Diego
Ueli Maurer	ETH Zurich
Silvio Micali	MIT
Moni Naor	Weizmann Institute of Science
Tatsuaki Okamoto	NTT Labs

Lecture Notes in Computer Science

For information about Vols. 1–3787

please contact your bookseller or Springer

Vol. 3889: J. Rosca, D. Erdogmus, J.C. Príncipe, S. Haykin (Eds.), Independent Component Analysis and Blind Signal Separation. XXI, 980 pages. 2006.

Vol. 3884: B. Durand, W. Thomas (Eds.), STACS 2006. XIV, 714 pages. 2006.

Vol. 3881: S. Gibet, N. Courty, J.-F. Kamp (Eds.), Gesture in Human-Computer Interaction and Simulation. XIII, 344 pages. 2006. (Sublibrary LNAI).

Vol. 3879: T. Erlebach, G. Persinao (Eds.), Approximation and Online Algorithms. X, 349 pages. 2006.

Vol. 3878: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVII, 589 pages. 2006.

Vol. 3877: M. Detyniecki, J.M. Jose, A. Nürnberger, C. J. '. van Rijsbergen (Eds.), Adaptive Multimedia Retrieval: User, Context, and Feedback. XI, 279 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3874: R. Missaoui, J. Schmid (Eds.), Formal Concept Analysis. X, 309 pages. 2006. (Sublibrary LNAI).

Vol. 3873: L. Maicher, J. Park (Eds.), Charting the Topic Maps Research and Applications Landscape. VIII, 281 pages. 2006. (Sublibrary LNAI).

Vol. 3872: H. Bunke, A. L. Spitz (Eds.), Document Analysis Systems VII. XIII, 630 pages. 2006.

Vol. 3870: S. Spaccapietra, P. Atzeni, W.W. Chu, T. Catarci, K.P. Sycara (Eds.), Journal on Data Semantics V. XIII, 237 pages. 2006.

Vol. 3869: S. Renals, S. Bengio (Eds.), Machine Learning for Multimodal Interaction. XIII, 490 pages. 2006.

Vol. 3868: K. Römer, H. Karl, F. Mattern (Eds.), Wireless Sensor Networks. XI, 342 pages. 2006.

Vol. 3863: M. Kohlhase (Ed.), Mathematical Knowledge Management. XI, 405 pages. 2006. (Sublibrary LNAI).

Vol. 3861: J. Dix, S.J. Hegner (Eds.), Foundations of Information and Knowledge Systems. X, 331 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3857: M.P.C. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. XI, 350 pages. 2006.

Vol. 3855: E. A. Emerson, K.S. Namjoshi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 443 pages. 2005.

Vol. 3853: A.J. Ijspeert, T. Masuzawa, S. Kusumoto (Eds.), Biologically Inspired Approaches to Advanced Information Technology. XIV, 388 pages. 2006.

Vol. 3852: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision - ACCV 2006, Part II. XXXI, 977 pages. 2005.

Vol. 3851: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision - ACCV 2006, Part I. XXXI, 973 pages. 2006.

Vol. 3850: R. Freund, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 371 pages. 2006.

Vol. 3849: I. Bloch, A. Petrosino, A.G.B. Tettamanzi (Eds.), Fuzzy Logic and Applications. XIV, 438 pages. 2006. (Sublibrary LNAI).

Vol. 3848: J.-F. Boulicaut, L. De Raedt, H. Mannila (Eds.), Constraint-Based Mining and Inductive Databases. X, 401 pages. 2006. (Sublibrary LNAI).

Vol. 3847: K.P. Jantke, A. Lunzer, N. Spyratos, Y. Tanaka (Eds.), Federation over the Web. X, 215 pages. 2006. (Sublibrary LNAI).

Vol. 3846: H. J. van den Herik, Y. Björnsson, N.S. Netanyahu (Eds.), Computers and Games. XIV, 333 pages. 2006.

Vol. 3845: J. Farré, I. Litovsky, S. Schmitz (Eds.), Implementation and Application of Automata. XIII, 360 pages. 2006.

Vol. 3844: J.-M. Bruel (Ed.), Satellite Events at the MoDELS 2005 Conference. XIII, 360 pages. 2006.

Vol. 3843: P. Healy, N.S. Nikolov (Eds.), Graph Drawing. XVII, 536 pages. 2006.

Vol. 3842: H.T. Shen, J. Li, M. Li, J. Ni, W. Wang (Eds.), Advanced Web and Network Technologies, and Applications. XXVII, 1057 pages. 2006.

Vol. 3841: X. Zhou, J. Li, H.T. Shen, M. Kitsuregawa, Y. Zhang (Eds.), Frontiers of WWW Research and Development - APWeb 2006. XXIV, 1223 pages. 2006.

Vol. 3840: M. Li, B. Boehm, L.J. Osterweil (Eds.), Unifying the Software Process Spectrum. XVI, 522 pages. 2006.

Vol. 3839: J.-C. Filliâtre, C. Paulin-Mohring, B. Werner (Eds.), Types for Proofs and Programs. VIII, 275 pages. 2006.

Vol. 3838: A. Middeldorp, V. van Oostrom, F. van Raamsdonk, R. de Vrijer (Eds.), Processes, Terms and Cycles: Steps on the Road to Infinity. XVIII, 639 pages. 2005.

Vol. 3837: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks. IX, 307 pages. 2005.

Vol. 3836: J.-M. Pierson (Ed.), Data Management in Grids. X, 143 pages. 2006.

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Sublibrary LNAI).

Vol. 3834: D.G. Feitelson, E. Frachtenberg, L. Rudolph, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. VIII, 283 pages. 2005.

Vol. 3833: K.-J. Li, C. Vangenot (Eds.), Web and Wireless Geographical Information Systems. XI, 309 pages. 2005.

Vol. 3832: D. Zhang, A.K. Jain (Eds.), Advances in Biometrics. XX, 796 pages. 2005.

Vol. 3831: J. Wiedermann, G. Tel, J. Pokorný, M. Bieliková, J. Štuller (Eds.), SOFSEM 2006: Theory and Practice of Computer Science. XV, 576 pages. 2006.

Vol. 3829: P. Pettersson, W. Yi (Eds.), Formal Modeling and Analysis of Timed Systems. IX, 305 pages. 2005.

Vol. 3828: X. Deng, Y. Ye (Eds.), Internet and Network Economics. XVII, 1106 pages. 2005.

Vol. 3827: X. Deng, D.-Z. Du (Eds.), Algorithms and Computation. XX, 1190 pages. 2005.

Vol. 3826: B. Benatallah, F. Casati, P. Traverso (Eds.), Service-Oriented Computing - ICSOC 2005. XVIII, 597 pages. 2005.

Vol. 3824: L.T. Yang, M. Amamiya, Z. Liu, M. Guo, F.J. Rammig (Eds.), Embedded and Ubiquitous Computing – EUC 2005. XXIII, 1204 pages. 2005.

Vol. 3823: T. Enokido, L. Yan, B. Xiao, D. Kim, Y. Dai, L.T. Yang (Eds.), Embedded and Ubiquitous Computing – EUC 2005 Workshops. XXXII, 1317 pages. 2005.

Vol. 3822: D. Feng, D. Lin, M. Yung (Eds.), Information Security and Cryptology. XII, 420 pages. 2005.

Vol. 3821: R. Ramanujam, S. Sen (Eds.), FSTTCS 2005: Foundations of Software Technology and Theoretical Computer Science. XIV, 566 pages. 2005.

Vol. 3820: L.T. Yang, X.-s. Zhou, W. Zhao, Z. Wu, Y. Zhu, M. Lin (Eds.), Embedded Software and Systems. XXVIII, 779 pages. 2005.

Vol. 3819: P. Van Hentenryck (Ed.), Practical Aspects of Declarative Languages. X, 231 pages. 2005.

Vol. 3818: S. Grumbach, L. Sui, V. Vianu (Eds.), Advances in Computer Science – ASIAN 2005. XIII, 294 pages. 2005.

Vol. 3817: M. Faundez-Zanuy, L. Janer, A. Esposito, A. Satue-Villar, J. Roure, V. Espinosa-Duro (Eds.), Nonlinear Analyses and Algorithms for Speech Processing. XII, 380 pages. 2006. (Sublibrary LNAI).

Vol. 3816: G. Chakraborty (Ed.), Distributed Computing and Internet Technology. XXI, 606 pages. 2005.

Vol. 3815: E.A. Fox, E.J. Neuhold, P. Premsmit, V. Wuwongse (Eds.), Digital Libraries: Implementing Strategies and Sharing Experiences. XVII, 529 pages. 2005.

Vol. 3814: M. Maybury, O. Stock, W. Wahlster (Eds.), Intelligent Technologies for Interactive Entertainment. XV, 342 pages. 2005. (Sublibrary LNAI).

Vol. 3813: R. Molva, G. Tsudik, D. Westhoff (Eds.), Security and Privacy in Ad-hoc and Sensor Networks. VIII, 219 pages. 2005.

Vol. 3812: C. Bussler, A. Haller (Eds.), Business Process Management Workshops. XIII, 520 pages. 2006.

Vol. 3811: C. Bussler, M.-C. Shan (Eds.), Technologies for E-Services. VIII, 127 pages. 2006.

Vol. 3810: Y.G. Desmedt, H. Wang, Y. Mu, Y. Li (Eds.), Cryptology and Network Security. XI, 349 pages. 2005.

Vol. 3809: S. Zhang, R. Jarvis (Eds.), AI 2005: Advances in Artificial Intelligence. XXVII, 1344 pages. 2005. (Sublibrary LNAI).

Vol. 3808: C. Bento, A. Cardoso, G. Dias (Eds.), Progress in Artificial Intelligence. XVIII, 704 pages. 2005. (Sublibrary LNAI).

Vol. 3807: M. Dean, Y. Guo, W. Jun, R. Kaschek, S. Krishnaswamy, Z. Pan, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005 Workshops. XV, 275 pages. 2005.

Vol. 3806: A.H. H. Ngu, M. Kitsuregawa, E.J. Neuhold, J.-Y. Chung, Q.Z. Sheng (Eds.), Web Information Systems Engineering – WISE 2005. XXI, 771 pages. 2005.

Vol. 3805: G. Subsol (Ed.), Virtual Storytelling. XII, 289 pages. 2005.

Vol. 3804: G. Bebis, R. Boyle, D. Koracin, B. Parvin (Eds.), Advances in Visual Computing. XX, 755 pages. 2005.

Vol. 3803: S. Jajodia, C. Mazumdar (Eds.), Information Systems Security. XI, 342 pages. 2005.

Vol. 3802: Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, Y.-C. Jiao (Eds.), Computational Intelligence and Security, Part II. XLII, 1166 pages. 2005. (Sublibrary LNAI).

Vol. 3801: Y. Hao, J. Liu, Y.-P. Wang, Y.-m. Cheung, H. Yin, L. Jiao, J. Ma, Y.-C. Jiao (Eds.), Computational Intelligence and Security, Part I. XLI, 1122 pages. 2005. (Sublibrary LNAI).

Vol. 3799: M. A. Rodríguez, I.F. Cruz, S. Levashkin, M.J. Egenhofer (Eds.), GeoSpatial Semantics. X, 259 pages. 2005.

Vol. 3798: A. Dearle, S. Eisenbach (Eds.), Component Deployment. X, 197 pages. 2005.

Vol. 3797: S. Maitra, C. E. V. Madhavan, R. Venkatesan (Eds.), Progress in Cryptology - INDOCRYPT 2005. XIV, 417 pages. 2005.

Vol. 3796: N.P. Smart (Ed.), Cryptography and Coding. XI, 461 pages. 2005.

Vol. 3795: H. Zhuge, G.C. Fox (Eds.), Grid and Cooperative Computing - GCC 2005. XXI, 1203 pages. 2005.

Vol. 3794: X. Jia, J. Wu, Y. He (Eds.), Mobile Ad-hoc and Sensor Networks. XX, 1136 pages. 2005.

Vol. 3793: T. Conte, N. Navarro, W.-m.W. Hwu, M. Valero, T. Ungerer (Eds.), High Performance Embedded Architectures and Compilers. XIII, 317 pages. 2005.

Vol. 3792: I. Richardson, P. Abrahamsson, R. Messnarz (Eds.), Software Process Improvement. VIII, 215 pages. 2005.

Vol. 3791: A. Adi, S. Stoutenburg, S. Tabet (Eds.), Rules and Rule Markup Languages for the Semantic Web. X, 225 pages. 2005.

Vol. 3790: G. Alonso (Ed.), Middleware 2005. XIII, 443 pages. 2005.

Vol. 3789: A. Gelbukh, Á. de Albornoz, H. Terashima-Marín (Eds.), MICAI 2005: Advances in Artificial Intelligence. XXVI, 1198 pages. 2005. (Sublibrary LNAI).

Vol. 3788: B. Roy (Ed.), Advances in Cryptology - ASIACRYPT 2005. XIV, 703 pages. 2005.

¥615.00元

Table of Contents

Zero-Knowledge

Primitives

Assumptions and Models

The Bounded-Retrieval Model

Privacy

Secret Sharing and Multi-party Computation (I)

Universally-Composible Security

One-Way Functions and Friends

Secret Sharing and Multi-party Computation (II)

Pseudo-Random Functions and Encryption

Concurrent Zero Knowledge Without Complexity Assumptions*

Daniele Micciancio[1,**], Shien Jin Ong[2,***], Amit Sahai[3,†], and Salil Vadhan[2,‡]

[1] University of California, San Diego, La Jolla CA 92093, USA
daniele@cs.ucsd.edu
[2] Harvard University, Cambridge MA 02138, USA
{shienjin, salil}@eecs.harvard.edu
[3] University of California, Los Angeles, Los Angeles CA 90095, USA
sahai@cs.ucla.edu

Abstract. We provide *unconditional* constructions of *concurrent* statistical zero-knowledge proofs for a variety of non-trivial problems (not known to have probabilistic polynomial-time algorithms). The problems include Graph Isomorphism, Graph Nonisomorphism, Quadratic Residuosity, Quadratic Nonresiduosity, a restricted version of Statistical Difference, and approximate versions of the (**coNP** forms of the) Shortest Vector Problem and Closest Vector Problem in lattices.

For some of the problems, such as Graph Isomorphism and Quadratic Residuosity, the proof systems have provers that can be implemented in polynomial time (given an **NP** witness) and have $\tilde{O}(\log n)$ rounds, which is known to be essentially optimal for black-box simulation.

To the best of our knowledge, these are the first constructions of concurrent zero-knowledge proofs in the plain, asynchronous model (i.e., without setup or timing assumptions) that do not require complexity assumptions (such as the existence of one-way functions).

1 Introduction

In the two decades since their introduction [2], zero-knowledge proofs have taken on a central role in the study of cryptographic protocols, both as a basic building block for more complex protocols and as a testbed for understanding important new issues such as composability (e.g., [3]) and concurrency (e.g., [4]). The "classic" constructions of zero-knowledge proofs came primarily in two flavors. First, there were direct constructions of zero-knowledge proofs for specific problems, such as QUADRATIC RESIDUOSITY [2] and GRAPH ISOMORPHISM [5]. Second, there were general constructions of zero-knowledge proofs for entire classes of

[*] A full version of this paper is available [1].

[**] Supported by NSF grant 0313241 and an Alfred P. Sloan Research Fellowship.

[***] Supported by ONR grant N00014-04-1-0478.

[†] Supported by NSF ITR and Cybertrust programs, an equipment grant from Intel, and an Alfred P. Sloan Foundation Fellowship.

[‡] Supported by NSF grants CNS-0430336 and CCR-0205423.

S. Halevi and T. Rabin (Eds.): TCC 2006, LNCS 3876, pp. 1–20, 2006.

problems, such as all of **NP** [5].[1] Both types of results have played an important role in the development of the field.

The general results of the second type show the wide applicability of zero knowledge, and are often crucial in establishing general feasibility results for other cryptographic problems, such as secure multiparty computation [8,5] and CCA-secure public-key encryption [9, 10, 11]. However, they typically are too inefficient to be used in practice. The specific results of the first type are often much more efficient, and are therefore used in (or inspire) the construction of other efficient cryptographic protocols, e.g., identification schemes [12] and again CCA-secure public-key encryption [13, 14, 15]. Moreover, the specific constructions typically do not require any unproven complexity assumptions (such as the existence of one-way functions), and yield a higher security guarantee (such as *statistical* zero-knowledge proofs).[2] The fact that the proof systems are unconditional is also of conceptual interest, because they illustrate the nontriviality of the notion of zero knowledge even to those who are unfamiliar with (or who do not believe in the existence of) one-way functions.[3]

Concurrent zero knowledge. In recent years, a substantial effort has been devoted to understanding the security of cryptographic protocols when many executions are occurring concurrently (with adversarial scheduling). As usual, zero-knowledge proofs led the way in this effort, with early investigations of concurrency for relaxations of zero knowledge dating back to Feige's thesis [22], and the recent interest being sparked by the work of Dwork, Naor, and Sahai [4], which first defined the notion of concurrent zero knowledge. Research on concurrent zero knowledge has been very fruitful, with a sequence of works leading to essentially tight upper and lower bounds on round complexity for black-box simulation [23, 24, 25, 26, 27, 28], and partly motivating the first non-black-box-simulation zero-knowledge proof [29]. However, these works are primarily of the *second* flavor mentioned in the first paragraph. That is, they are general feasibility results, giving protocols for all of **NP**. As a result, these protocols are fairly inefficient (in terms of computation and communication), rely on unproven complexity assumptions, and only yield computational zero knowledge (or, alternatively, computational soundness).

There have been a couple of works attempting to overcome these deficiencies. Di Crescenzo [30] gave unconditional constructions of concurrent zero-knowledge

[1] See the textbook [6] and survey [7] by Oded Goldreich for a thorough introduction to zero-knowledge proofs.

[2] Of course, this partition into two types of zero-knowledge protocols is not a precise one. For example, there are some efficient zero-knowledge proofs for specific problems that use complexity assumptions (e.g., [16] and there are some general results that are unconditional (e.g., [17, 18, 19]).

[3] It should be noted that the results of [20,21] show that the existence of a zero-knowledge proof for a problem outside **BPP** implies some weak form of one-way function. Still, appreciating something like the perfect zero-knowledge proof system for Graph Isomorphism [5] only requires believing that there is no *worst-case* polynomial-time algorithm for Graph Isomorphism, as opposed to appreciating notions of average-case complexity as needed for standard one-way functions.

proofs in various timing models. That is, his protocols assume that the honest parties have some synchronization and may employ delays in the protocol, and thus do not work in the standard, asynchronous model (and indeed he states such a strengthening as an open problem). Micciancio and Petrank [31] gave an efficient (in terms of computation and communication) transformation from honest-verifier zero-knowledge proofs to concurrent zero-knowledge proofs. However, their transformation relies on the Decisional Diffie–Hellman assumption, and yields only computational zero knowledge.

Our Results. We give the first unconditional constructions of concurrent zero-knowledge proofs in the standard, asynchronous model. Our proof systems are statistical zero knowledge and statistically sound (i.e. they are interactive proofs, not arguments [32]). Specifically, our constructions fall into two categories:

1. Efficient proof systems for certain problems in **NP**, including QUADRATIC RESIDUOSITY, GRAPH ISOMORPHISM and a restricted form of quadratic nonresiduosity for Blum integers, which we call BLUM QUADRATIC NONRESIDUOSITY. These proof systems all have prover strategies that can be implemented in polynomial time given an **NP** witness and have $\widetilde{O}(\log n)$ rounds, which is essentially optimal for black-box simulation [27].
2. Inefficient proof systems for other problems, some of which are not known to be in **NP**. These include QUADRATIC NONRESIDUOSITY, GRAPH NONISOMORPHISM, the approximate versions of the complements of the CLOSEST VECTOR PROBLEM and SHORTEST VECTOR PROBLEM in lattices, and a restricted version of STATISTICAL DIFFERENCE (the unrestricted version is complete for statistical zero knowledge [33]). These proof systems have a polynomial number of rounds, and do not have polynomial-time prover strategies. These deficiencies arise from the fact that our construction begins with a public-coin, honest-verifier zero-knowledge proof for the problem at hand, and the only such proofs known for the problems listed here have a polynomial number of rounds and an inefficient prover strategy.

Techniques. One of the main tools for constructing zero-knowledge proofs are commitment schemes, and indeed the only use of complexity assumptions in the construction of zero-knowledge proofs for all of **NP** [5] is to obtain a commitment scheme (used by the prover to commit to the **NP** witness, encoded as, e.g., a 3-coloring of a graph). Our results rely on a relaxed notion of commitment, called an *instance-dependent commitment scheme*,[4] which is implicit in [35] and formally defined in [36,34,19]. Roughly speaking, for a language L (or, more generally, a promise problem), a instance-dependent commitment scheme for L is a commitment protocol where the sender and receiver algorithms also depend on the instance x. The security requirements of the protocol are relaxed so that the hiding property is only required when $x \in L$, and the binding property is only required when $x \notin L$ (or vice-versa).

[4] Previous works [34,19] have referred to this as "problem-dependent" commitment scheme, but this new terminology of "instance-dependent" seems more accurate.

As observed in [36], many natural problems, such as Graph Isomorphism and Quadratic Residuosity, have simple, unconditional instance-dependent commitment schemes. This is useful because in many constructions of zero-knowledge proofs (such as that of [5]), the hiding property of the commitment scheme is only used to establish the zero-knowledge property and the binding property of the commitment scheme is only used to establish soundness. Since, by definition, the zero-knowledge property is only required when the input x is in the language, and the soundness condition is only required when x is not in the language, it suffices to use a instance-dependent commitment scheme. Specifically, if a language $L \in \mathbf{NP}$ (or even $L \in \mathbf{IP}$) has a instance-dependent commitment scheme, then L has a zero-knowledge proof [36] (see also [34,19]).

Existing constructions of *concurrent* zero-knowledge proofs [24,27,28] also rely on commitment schemes (and this is the only complexity assumption used). Thus it is natural to try to use instance-dependent commitments to construct them. However, these protocols use commitments not only from the prover to the verifier, but also from the verifier to the prover. Naturally, for the latter type of commitments, the roles of the hiding and binding property are reversed from the above — the hiding property is used to prove soundness and the binding property is used to prove (concurrent) zero knowledge. Thus, it seems that we need not only a instance-dependent commitment as above, but also one where the security properties are reversed (i.e. binding when $x \in L$, and hiding when $x \notin L$).

Our first observation is that actually we only need to implement the commitment schemes from the verifier to the prover. This is because the concurrent zero-knowledge proof system of Prabhakaran, Rosen and Sahai [28] is constructed by a general compiler that converts *any* public-coin zero-knowledge proof into a concurrent zero-knowledge proof, and this compiler only uses commitments from the verifier to the prover. (Intuitively, the verifier commits to its messages in an initial "preamble" stage, which is designed so as to allow concurrent simulation.) Since all the problems we study are unconditionally known to have public-coin zero-knowledge proofs, we only need to implement the compiler. So we are left with the task finding instance-dependent commitments that are binding when $x \in L$ and hiding when $x \notin L$. Thus, for the rest of the paper, we use this as our definition of instance-dependent commitment.

This idea works directly for some problems, such as Graph Nonisomorphism and Quadratic Nonresiduosity. For these problems, we have instance-dependent commitments with the desired security properties, and thus we can directly use these commitments in the compiler of [28]. Unfortunately, for the complement problems, such as Graph Isomorphism and Quadratic Residuosity, we only know of instance-dependent commitments that are hiding when $x \in L$, and binding when $x \notin L$.

Thus, for some of our results, we utilize a more sophisticated variant of instance-dependent commitments, due to Bellare, Micali, and Ostrovsky [35]. Specifically, they construct something like a instance-dependent commitment scheme for the Graph Isomorphism problem, but both the hiding and binding properties are non-standard. For example, the binding property is as follows: they show that if $x \in L$ and the sender can open a commitment in two different ways, then it is possible for the sender to extract an **NP** witness for $x \in L$. Thus we call these *witness-binding commitments.* Intuitively, when we use such commitments, we prove concurrent zero knowledge by the following case analysis: either the verifier is bound to its commitments, in which case we can simulate our proof system as in [28], *or* the simulator can extract a witness, in which case it can be simulated by running the honest prover strategy. In reality, however, the analysis does not break into such a simple case analysis, because the verifier may break the commitment scheme in the middle of the protocol. Thus we require that, in such a case, an already-begun simulation can be "continued" once we are given an **NP** witness. Fortunately, the classic (stand-alone) proof systems for GRAPH ISOMORPHISM and QUADRATIC RESIDUOSITY turn out to have the needed "witness-completable simulation" property.

An additional contribution of our paper is to provide abstractions and generalizations of all of the above tools that allow them to be combined in a modular way, and may facilitate their use in other settings. First, we show how the "preamble" of the Prabhakaran–Rosen–Sahai concurrent zero-knowledge proof system [28] can be viewed as a way to transform any commitment scheme into one that is "concurrently extractable," in the sense that we are able to simulate the concurrent execution of many sessions between an adversarial sender and the honest receiver in a way that allows us to extract the commitments of the sender in every session. This may be useful in constructing other concurrently secure protocols (not just proof systems). Second, we provide general definitions of witness-binding commitment schemes as well as witness-completable zero-knowledge proofs as possessed by GRAPH ISOMORPHISM and QUADRATIC RESIDUOSITY and as discussed above.

Perspective. The recent works of Micciancio and Vadhan [34] and Vadhan [19] hypothesized that every problem that has a statistical (resp., computational) zero-knowledge proof has a instance-dependent commitment scheme.[5] There are several pieces of evidence pointing to this possibility:

1. A restricted form of a complete problem for statistical zero knowledge has a instance-dependent commitment scheme [34].
2. If instance-dependent commitments exist for all problems with statistical zero-knowledge proofs, then instance-dependent commitments exist for all of problems with (general, computational) zero-knowledge proofs [19].
3. Every problem that has (general, computational) zero-knowledge proofs also has inefficient instance-dependent commitments. These commitments are in-

[5] Actually, the works of [34] and [19] refer to instance-dependent commitments where the hiding property holds on YES instances and the binding property on NO instances, which is opposite of what we use. For statistical zero knowledge, this does not matter because the class of problems having statistical zero-knowledge proofs is closed under complement [17]. But for computational zero knowledge, it means that outline presented here might yield a concurrent zero-knowledge *argument* system rather than a proof system.