Moni Naor (Ed.)

LNCS 2951

Theory of Cryptography

First Theory of Cryptography Conference, TCC 2004
Cambridge, MA, USA, February 2004
Proceedings

Springer

Moni Naor (Ed.)

Theory of Cryptography

First Theory of Cryptography Conference, TCC 2004
Cambridge, MA, USA, February 19-21, 2004
Proceedings

Springer

Moni Naor
Weizmann Institute of Science
Department of Computer Science and Applied Mathematics
Rehovot 76100, Israel
E-mail: moni.naor@weizmann.ac.il

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

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

ISSN 0302-9743
ISBN 3-540-21000-8 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10986196 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 2951

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Preface

This volume contains the papers selected for presentation at the 1st Theory of Cryptography Conference (TCC) which was held at the Massachusetts Institute of Technology during February 19–21, 2004. The theory of cryptography deals with the paradigms, approaches and techniques used to conceptualize, define and provide solutions to natural cryptographic problems. The Theory of Cryptography Conference is a new venue dedicated to the dissemination of results in the area. The aim of the conference is to provide a meeting place for researchers and be instrumental in shaping the identity of the theory of cryptography community. A more detailed statement of purpose ('manifesto') is available on the TCC Web site (http://www-cse.ucsd.edu/users/mihir/tcc/).
The TCC 2004 program committee consisted of:

Ran Canetti	IBM T.J. Watson Research Center, USA
Ronald Cramer	Århus University, Denmark
Cynthia Dwork	Microsoft Research, USA
Yuval Ishai	Technion, Israel
Joe Kilian	NEC Research Labs, USA
Phil Mackenzie	Bell Labs, Lucent, USA
Daniele Micciancio	UCSD, USA
Moni Naor (PC Chair)	Weizmann Institute, Israel
Birgit Pfitzmann	IBM Research, Zurich, Switzerland
Omer Reingold	AT&T Research and IAS, USA
Salil Vadhan	Harvard University and Radcliffe Institute, USA

The program committee chose 29 papers out of the 70 submitted to the conference. Two sets of authors decided to merge, so the volume contains 28 papers altogether. In addition, given recent developments in the field, the committee decided to have a panel discussion on *Cryptography and Formal Methods.*

Acknowledgments : First and foremost I wish to thank all the people who submitted papers to the conference. Without them, of course, there would have been no conference. The hard task of reading, commenting on and selecting the papers to be accepted to the conference fell on the program committee members. Given that this is the first conference of its kind the mission was even trickier than usual. I am indebted to the committee members' collective knowledge, wisdom and effort. The committee also used external reviewers to extend the expertise and ease the burden. The names of these reviewers are listed on the pages that follow. My deepest gratitude to them as well.

I thank Joe Kilian for handling (and writing!) the server for submissions and reviews, as well as Omer Reingold and Edna Wigderson for helping out when Joe was away.

I thank Shafi Goldwasser for chairing this conference and making all the necessary arrangements at MIT. Shafi in turn is tremendously grateful to Joanne Talbot who coordinated the conference facilities, hotels, Web page, budgets, and the conference chair relentlessly and without a single complaint. Thank you Joanne. I thank Mihir Bellare for chairing the Steering Committee of TCC and the members of the committee (see the list in the pages that follow) for helping out with many issues concerning the conference, including the proceedings and the TCC Web-site. Finally a big thanks is due to Oded Goldreich who initiated this endeavor and pushed hard for it.

Rehovot, Israel
December 2003

Moni Naor
Program Chair
TCC 2004

External Referees

Masayuki Abe
Luis von Ahn
Michael Backes
Boaz Barak
Amos Beimel
Mihir Bellare
Alexandra Boldyreva
Harry Buhrman
Christian Cachin
Jan Camenisch
Claude Crépeau
Anand Desai
Yan Zong Ding
Yevgeniy Dodis
Marc Fischlin
Juan Garay
Rosario Gennaro
Daniel Gottesman
Jens Groth
Shai Halevi
Danny Harnik
Alejandro Hevia
Thomas Jakobsen
Markus Jakobsson
Ari Juels
Jonathan Katz
Hugo Krawczyk
Eyal Kushilevitz
Yehuda Lindell
Anna Lysyanskaya
Tal Malkin
David Meyer
Ashwin Nayak
Gregory Neven
Jesper Buus Nielsen
Adriana Palacio
Erez Petrank
Benny Pinkas
Tal Rabin
Oded Regev
Amit Sahai
Jean-Pierre Seifert
Adam Smith
Martijn Stam
Yael Tauman Kalai
Michael Waidner
John Watrous
Douglas Wikström
Bogdan Warinschi
Stephanie Wehner
Ke Yang

TCC Steering Committee

Mihir Bellare (Chair)	UCSD, USA
Ivan Damgård	Århus University, Denmark
Oded Goldreich	Weizmann Institute, Israel and Radcliffe Institute, USA
Shafi Goldwasser	MIT, USA and Weizmann Institute, Israel
Johan Håstad	Royal Institute of Technology, Sweden
Russell Impagliazzo	UCSD, USA
Ueli Maurer	ETH, Switzerland
Silvio Micali	MIT, USA
Moni Naor	Weizmann Institute, Israel
Tatsuaki Okamoto	NTT, Japan

Sponsoring Institutions

We acknowledge financial support from the following institutions:
CoreStreet Ltd.
IBM Corporation

Lecture Notes in Computer Science

For information about Vols. 1–2830

please contact your bookseller or Springer-Verlag

Vol. 2964: T. Okamoto (Eds.), Topics in Cryptology – CT-RSA 2004. Proceedings, 2004. XI, 387 pages. 2004.

Vol. 2957: P. Langendoerfer, M. Liu, I. Matta, V. Tsaoussidis (Eds.), Wired/Wireless Internet Communications. Proceedings, 2004. XI, 307 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. Proceedings, 2004. XI, 523 pages. 2004.

Vol. 2946: R. Focardi, R. Gorrieri (Eds.), Foundations of Security Analysis and Design II. VII, 267 pages. 2004.

Vol. 2930: F. Winkler, Automated Deduction in Geometry. VII, 231 pages. 2004. (Subseries LNAI).

Vol. 2923: V. Lifschitz, I. Niemelä (Eds.), Logic Programming and Nonmonotonic Reasoning. IX, 365 pages. 2004. (Subseries LNAI).

Vol. 2916: C. Palamidessi (Eds.), Logic Programming. Proceedings, 2003. XII, 520 pages. 2003.

Vol. 2914: P.K. Pandya, J. Radhakrishnan (Eds.), FST TCS 2003: Foundations of Software Technology and Theoretical Computer Science. Proceedings, 2003. XIII, 446 pages. 2003.

Vol. 2913: T.M. Pinkston, V.K. Prasanna (Eds.), High Performance Computing - HiPC 2003. Proceedings, 2003. XX, 512 pages. 2003. (Subseries LNAI).

Vol. 2911: T.M.T. Sembok, H.B. Zaman, H. Chen, S.R. Urs, S.H. Myaeng (Eds.), Digital Libraries: Technology and Management of Indigenous Knowledge for Global Access. Proceedings, 2003. XX, 703 pages. 2003.

Vol. 2910: M.E. Orlowska, S. Weerawarana, M.M.P. Papazoglou, J. Yang (Eds.), Service-Oriented Computing - ICSOC 2003. Proceedings, 2003. XIV, 576 pages. 2003.

Vol. 2908: K. Chae, M. Yung (Eds.), Information Security Applications. XII, 506 pages. 2004.

Vol. 2906: T. Ibaraki, N. Katoh, H. Ono (Eds.), Algorithms and Computation. Proceedings, 2003. XVII, 748 pages. 2003.

Vol. 2905: A. Sanfeliu, J. Ruiz-Shulcloper (Eds.), Progress in Pattern Recognition, Speech and Image Analysis. XVII, 693 pages. 2003.

Vol. 2904: T. Johansson, S. Maitra (Eds.), Progress in Cryptology - INDOCRYPT 2003. Proceedings, 2003. XI, 431 pages. 2003.

Vol. 2903: T.D. Gedeon, L.C.C. Fung (Eds.), AI 2003: Advances in Artificial Intelligence. Proceedings, 2003. XVI, 1075 pages. 2003. (Subseries LNAI).

Vol. 2902: F.M. Pires, S.P. Abreu (Eds.), Progress in Artificial Intelligence. Proceedings, 2003. XV, 504 pages. 2003. (Subseries LNAI).

Vol. 2901: F. Bry, N. Henze, J. Ma luszyński (Eds.), Principles and Practice of Semantic Web Reasoning. Proceedings, 2003. X, 209 pages. 2003.

Vol. 2900: M. Bidoit, P.D. Mosses (Eds.), Casl User Manual. XIII, 240 pages. 2004.

Vol. 2899: G. Ventre, R. Canonico (Eds.), Interactive Multimedia on Next Generation Networks. Proceedings, 2003. XIV, 420 pages. 2003.

Vol. 2898: K.G. Paterson (Eds.), Cryptography and Coding. Proceedings, 2003. IX, 385 pages. 2003.

Vol. 2897: O. Balet, G. Subsol, P. Torguet (Eds.), Virtual Storytelling. Proceedings, 2003. XI, 240 pages. 2003.

Vol. 2896: V.A. Saraswat (Eds.), Advances in Computing Science – ASIAN 2003. Proceedings, 2003. VIII, 305 pages. 2003.

Vol. 2895: A. Ohori (Eds.), Programming Languages and Systems. Proceedings, 2003. XIII, 427 pages. 2003.

Vol. 2894: C.S. Laih (Eds.), Advances in Cryptology - ASIACRYPT 2003. Proceedings, 2003. XIII, 543 pages. 2003.

Vol. 2893: J.-B. Stefani, I. Demeure, D. Hagimont (Eds.), Distributed Applications and Interoperable Systems. Proceedings, 2003. XIII, 311 pages. 2003.

Vol. 2892: F. Dau, The Logic System of Concept Graphs with Negation. XI, 213 pages. 2003. (Subseries LNAI).

Vol. 2891: J. Lee, M. Barley (Eds.), Intelligent Agents and Multi-Agent Systems. Proceedings, 2003. X, 215 pages. 2003. (Subseries LNAI).

Vol. 2890: M. Broy, A.V. Zamulin (Eds.), Perspectives of System Informatics. XV, 572 pages. 2003.

Vol. 2889: R. Meersman, Z. Tari (Eds.), On The Move to Meaningful Internet Systems 2003: OTM 2003 Workshops. Proceedings, 2003. XIX, 1071 pages. 2003.

Vol. 2888: R. Meersman, Z. Tari, D.C. Schmidt (Eds.), On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE. Proceedings, 2003. XXI, 1546 pages. 2003.

Vol. 2887: T. Johansson (Eds.), Fast Software Encryption. IX, 397 pages. 2003.

Vol. 2886: I. Nyström, G. Sanniti di Baja, S. Svensson (Eds.), Discrete Geometry for Computer Imagery. Proceedings, 2003. XII, 556 pages. 2003.

Vol. 2885: J.S. Dong, J. Woodcock (Eds.), Formal Methods and Software Engineering. Proceedings, 2003. XI, 683 pages. 2003.

Vol. 2884: E. Najm, U. Nestmann, P. Stevens (Eds.), Formal Methods for Open Object-Based Distributed Systems. Proceedings, 2003. X, 293 pages. 2003.

Vol. 2883: J. Schaeffer, M. Müller, Y. Björnsson (Eds.), Computers and Games. XI, 431 pages. 2003.

Vol. 2882: D. Veit, Matchmaking in Electronic Markets. XV, 180 pages. 2003. (Subseries LNAI).

Vol. 2881: E. Horlait, T. Magedanz, R.H. Glitho (Eds.), Mobile Agents for Telecommunication Applications. Proceedings, 2003. IX, 297 pages. 2003.

Vol. 2880: H.L. Bodlaender (Eds.), Graph-Theoretic Concepts in Computer Science. XI, 386 pages. 2003.

Vol. 2879: R.E. Ellis, T.M. Peters (Eds.), Medical Image Computing and Computer-Assisted Intervention - MICCAI 2003. Proceedings, 2003. XXXIV, 1003 pages. 2003.

Vol. 2878: R.E. Ellis, T.M. Peters (Eds.), Medical Image Computing and Computer-Assisted Intervention - MICCAI 2003. Proceedings, 2003. XXXIII, 819 pages. 2003.

Vol. 2877: T. Böhme, G. Heyer, H. Unger (Eds.), Innovative Internet Community Systems. VIII, 263 pages. 2003.

Vol. 2876: M. Schroeder, G. Wagner (Eds.), Rules and Rule Markup Languages for the Semantic Web. Proceedings, 2003. VII, 173 pages. 2003.

Vol. 2875: E. Aarts, R. Collier, E.v. Loenen, B.d. Ruyter (Eds.), Ambient Intelligence. Proceedings, 2003. XI, 432 pages. 2003.

Vol. 2874: C. Priami (Eds.), Global Computing. XIX, 255 pages. 2003.

Vol. 2871: N. Zhong, Z.W. Raś, S. Tsumoto, E. Suzuki (Eds.), Foundations of Intelligent Systems. Proceedings, 2003. XV, 697 pages. 2003. (Subseries LNAI).

Vol. 2870: D. Fensel, K.P. Sycara, J. Mylopoulos (Eds.), The Semantic Web - ISWC 2003. Proceedings, 2003. XV, 931 pages. 2003.

Vol. 2869: A. Yazici, C. Şener (Eds.), Computer and Information Sciences - ISCIS 2003. Proceedings, 2003. XIX, 1110 pages. 2003.

Vol. 2868: P. Perner, R. Brause, H.-G. Holzhütter (Eds.), Medical Data Analysis. Proceedings, 2003. VIII, 127 pages. 2003.

Vol. 2866: J. Akiyama, M. Kano (Eds.), Discrete and Computational Geometry. VIII, 285 pages. 2003.

Vol. 2865: S. Pierre, M. Barbeau, E. Kranakis (Eds.), Ad-Hoc, Mobile, and Wireless Networks. Proceedings, 2003. X, 293 pages. 2003.

Vol. 2864: A.K. Dey, A. Schmidt, J.F. McCarthy (Eds.), UbiComp 2003: Ubiquitous Computing. Proceedings, 2003. XVII, 368 pages. 2003.

Vol. 2863: P. Stevens, J. Whittle, G. Booch (Eds.), "UML" 2003 - The Unified Modeling Language. Proceedings, 2003. XIV, 415 pages. 2003.

Vol. 2860: D. Geist, E. Tronci (Eds.), Correct Hardware Design and Verification Methods. Proceedings, 2003. XII, 426 pages. 2003.

Vol. 2859: B. Apolloni, M. Marinaro, R. Tagliaferri (Eds.), Neural Nets. X, 376 pages. 2003.

Vol. 2857: M.A. Nascimento, E.S. de Moura, A.L. Oliveira (Eds.), String Processing and Information Retrieval. Proceedings, 2003. XI, 379 pages. 2003.

Vol. 2856: M. Smirnov (Eds.), Quality of Future Internet Services. IX, 293 pages. 2003.

Vol. 2855: R. Alur, I. Lee (Eds.), Embedded Software. Proceedings, 2003. X, 373 pages. 2003.

Vol. 2854: J. Hoffmann, Utilizing Problem Structure in Planing. XIII, 251 pages. 2003. (Subseries LNAI).

Vol. 2853: M. Jeckle, L.-J. Zhang (Eds.), Web Services - ICWS-Europe 2003. VIII, 227 pages. 2003.

Vol. 2852: F.S. de Boer, M.M. Bonsangue, S. Graf, W.-P. de Roever (Eds.), Formal Methods for Components and Objects. VIII, 509 pages. 2003.

Vol. 2851: C. Boyd, W. Mao (Eds.), Information Security. Proceedings, 2003. XI, 453 pages. 2003.

Vol. 2849: N. García, L. Salgado, J.M. Martínez (Eds.), Visual Content Processing and Representation. Proceedings, 2003. XII, 352 pages. 2003.

Vol. 2848: F.E. Fich (Eds.), Distributed Computing. Proceedings, 2003. X, 367 pages. 2003.

Vol. 2847: R.d. Lemos, T.S. Weber, J.B. Camargo Jr. (Eds.), Dependable Computing. Proceedings, 2003. XIV, 371 pages. 2003.

Vol. 2846: J. Zhou, M. Yung, Y. Han (Eds.), Applied Cryptography and Network Security. Proceedings, 2003. XI, 436 pages. 2003.

Vol. 2845: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. VIII, 243 pages. 2004.

Vol. 2844: J.A. Jorge, N. Jardim Nunes, J. Falcão e Cunha (Eds.), Interactive Systems. Design, Specification, and Verification. XIII, 429 pages. 2003.

Vol. 2843: G. Grieser, Y. Tanaka, A. Yamamoto (Eds.), Discovery Science. Proceedings, 2003. XII, 504 pages. 2003. (Subseries LNAI).

Vol. 2842: R. Gavaldá, K.P. Jantke, E. Takimoto (Eds.), Algorithmic Learning Theory. Proceedings, 2003. XI, 313 pages. 2003. (Subseries LNAI).

Vol. 2841: C. Blundo, C. Laneve (Eds.), Theoretical Computer Science. Proceedings, 2003. XI, 397 pages. 2003.

Vol. 2840: J. Dongarra, D. Laforenza, S. Orlando (Eds.), Recent Advances in Parallel Virtual Machine and Message Passing Interface. Proceedings, 2003. XVIII, 693 pages. 2003.

Vol. 2839: A. Marshall, N. Agoulmine (Eds.), Management of Multimedia Networks and Services. Proceedings, 2003. XIV, 532 pages. 2003.

Vol. 2838: N. Lavrač, D. Gamberger, L. Todorovski, H. Blockeel (Eds.), Knowledge Discovery in Databases: PKDD 2003. Proceedings, 2003. XVI, 508 pages. 2003. (Subseries LNAI).

Vol. 2837: N. Lavrač, D. Gamberger, L. Todorovski, H. Blockeel (Eds.), Machine Learning: ECML 2003. Proceedings, 2003. XVI, 504 pages. 2003. (Subseries LNAI).

Vol. 2836: S. Qing, D. Gollmann, J. Zhou (Eds.), Information and Communications Security. Proceedings, 2003. XI, 416 pages. 2003.

Vol. 2835: T. Horváth, A. Yamamoto (Eds.), Inductive Logic Programming. Proceedings, 2003. X, 401 pages. 2003. (Subseries LNAI).

Vol. 2834: X. Zhou, M. Xu, S. Jähnichen, J. Cao (Eds.), Advanced Parallel Processing Technologies. Proceedings, 2003. XIV, 679 pages. 2003.

Vol. 2833: F. Rossi (Eds.), Principles and Practice of Constraint Programming – CP 2003. Proceedings, 2003. XIX, 1005 pages. 2003.

Vol. 2832: G.D. Battista, U. Zwick (Eds.), Algorithms - ESA 2003. Proceedings, 2003. XIV, 790 pages. 2003.

Table of Contents

Notions of Reducibility between Cryptographic Primitives*

Omer Reingold[1]**, Luca Trevisan[2]***, and Salil Vadhan[3]†

[1] AT&T Labs - Research. Room A201, 180 Park Avenue, Bldg. 103
Florham Park, NJ, 07932. omer@research.att.com
[2] Computer Science Division, U.C. Berkeley, 615 Soda Hall
Berkeley, CA 94720. luca@cs.berkeley.edu
[3] Division of Engineering & Applied Sciences, Harvard University,
33 Oxford Street
Cambridge, MA 02138. salil@eecs.harvard.edu

Abstract. Starting with the seminal paper of Impagliazzo and Rudich [17], there has been a large body of work showing that various cryptographic primitives cannot be reduced to each other via "black-box" reductions. The common interpretation of these results is that there are inherent limitations in using a primitive as a black box, and that these impossibility results can be overcome only by explicitly using the *code of the primitive* in the *construction*.

In this paper we revisit these negative results, give a more careful taxonomy of the ways in which "black-box reductions" can be formalized, strengthen some previous results (in particular giving unconditional impossibility results for reductions that were previously only shown to imply $P \neq NP$), and offer a new interpretation of them: in many cases, there is no limitation in using a primitive as a black box, but there is a limitation in treating *adversaries* as such. In particular, these negative results may be overcome by using the *code of the adversary* in the *analysis*.

1 Introduction

In most of the current body of work in the foundations of cryptography, cryptographic protocols are not shown to be unconditionally secure, but, rather, their security is reduced to the security of seemingly weaker or simpler primitives. We now know that, if one-way functions exist, then there exist private-key encryption and message authentication schemes, as well as (public-key) digital signatures

* Research supported in part by US-Israel BSF Grant 2002246.
** Part of this research was performed while visiting the IAS, Princeton, NJ.
*** Supported by NSF grant CCR-9984703, a Sloan Research Fellowship and an Okawa Foundation Grant.
† Supported by NSF Grant CCR-0205423 and a Sloan Research Fellowship. Parts of this research were performed while at the IAS in Princeton and the Radcliffe Institute for Advanced Study at Harvard University.

M. Naor (Ed.): TCC 2004, LNCS 2951, pp. 1–20, 2004.

and zero-knowledge proofs [14,12,24,21,13]. On the other hand, if one-way functions do not exist then most interesting cryptographic problems, including all of the above, have no solution [15,23].

Some cryptographic primitives, however, such as public-key encryption, key agreement, oblivious transfer, collision-resistant hash functions, and non-interactive zero knowledge, are not known to be equivalent to the existence of one-way functions. Furthermore, several of the known constructions based on one-way functions run in polynomial time but are extremely inefficient (e.g. the construction of pseudorandom generators from one-way functions [14], which is a component in several other constructions). Since these are some of the main gaps in our systematization of the foundations of cryptography, it is natural to ask whether additional primitives, such as public-key encryption, can be constructed from one-way functions, and whether known constructions can be made more efficient. One has to be careful in formalizing such questions. It is commonly believed that one-way functions exist and that public-key encryption is possible, which would mean that the existence of one-way functions *implies* the existence of public key encryption in a trivial logical sense. The question is whether *the techniques that we typically use to prove implications of one-way functions in cryptography* have some inherent limitation that prevents us from deriving the existence of public-key encryption from one-way functions.

Impagliazzo and Rudich [17] were the first to give a formal treatment of such issues. They observed that most implications in cryptography are proved using a reduction, where the starting primitive is treated as an oracle, or a "black box," and the analysis shows that if the primitive is secure in a black-box sense then the constructed primitive is also secure. Impagliazzo and Rudich consider various models of black-box reductions (where there are some additional constraints beyond the primitive being treated as a black box) and show that, in one such model, a black-box construction of key agreement based on one-way functions implies a proof that $P \neq NP$. They also show that in a more constrained model such a construction is unconditionally impossible. The formal framework of Impagliazzo and Rudich has subsequently been used to address other "implication" questions, such as one-way functions versus one-way permutations [26,19], one-way functions versus collision-resistant hash functions [27], and between key agreement, oblivious transfer, public-key encryption and trapdoor functions and permutations [9,10]. Variants of the framework have also been used to address the issue of the number of rounds in KA protocols [25], of the efficiency of constructions of universal one-way hash functions based on one-way permutations [20,8], of pseudorandom generators based on one-way permutations [8] and of public-key encryption based on trapdoor permutations [7].

The common interpretation of these results is that there are inherent limitations in using a primitive as a black box, and that these impossibility results can be overcome only by explicitly using the *code of the primitive* in the *construction.*

In this paper we revisit these negative results, give a more careful taxonomy of the ways in which "black-box reductions" can be formalized, strengthen some previous results (in particular giving unconditional impossibility results for re-

ductions that were previously only shown to imply $P \neq NP$), and offer a new interpretation of them: in many cases, there is no limitation in using a primitive as a black box, but there is a limitation in treating *adversaries* as such. In particular, these negative results may be overcome by using the *code of the adversary* in the *analysis*.

1.1 Impossibility Results for Reductions

The starting point of the work of Impagliazzo-Rudich is the observation that most known cryptographic constructions based on one-way functions treat the one-way function as a "black box." (Exceptions are discussed in Section 1.5.) Roughly speaking, a *black-box (BB) reduction* of a primitive Q to one-way functions (OWF) is a construction that uses oracle access to a function f, and guarantees that if f is one-way then the construction is secure. In particular:

- The construction does not use the code of the function f;
- The construction is well defined and efficient even if f is not efficiently computable (as long as it is given as an oracle);
- There is a proof of security that shows that an adversary breaking the protocol yields an adversary that inverts f.

There are various ways to formalize the third condition (which we make precise in Section 2. One possibility considered in [17], which we call *fully-BB*, is that there is an algorithm that converts every adversary that supposedly breaks the construction (according to the definition of security for Q) into a procedure that inverts f. This algorithm is efficient and it is given oracle access to the adversary and to f. In this setting, both the *construction* and the *analysis* are black box. Another way to look at it is that both the *primitive* and the *adversary* are treated as black boxes. Most reductions in the cryptography literature are fully-BB.

Impagliazzo and Rudich [17] prove that there can be no fully-BB reduction of key agreement (KA) to OWF. Since public-key encryption, trapdoor permutations and oblivious transfer all imply KA (by fully-BB reductions), it then follows that there are no fully-BB transformations of OWF into these other primitives as well. It is natural to ask whether the impossibility is due to the fact both the primitive and the adversaries are treated as oracles, or if it is enough that just the primitive is.

Impagliazzo and Rudich also consider a weaker form a BB reduction of KA to OWF, a form that we call *semi-BB* in this paper. In a semi-BB reduction, we have a BB construction of KA based on a function f given as an oracle. The analysis proves that for every *efficient* adversary with oracle to f that breaks the construction, there is an efficient adversary that inverts f if given oracle access to f. This seems to formalize the notion of a BB construction with an arbitrary analysis, but we argue that it does not. If f is a one-way function in the black-box sense,[1] then the construction has to be secure not only against

[1] Meaning that no efficient procedure with oracle access to f can invert f on a non-negligible fraction of inputs.

efficient adversaries, but also against adversaries that have oracle access to f. A proof technique that makes use of the code of the adversary is not BB in this sense.

Impagliazzo and Rudich prove that, if $P = NP$, there is no semi-BB reduction of KA to OWF. This means that, in order to come up with a proof that OWF implies KA, one must either avoid semi-BB reductions or find, along the way, a proof that $P \neq NP$. Impagliazzo and Rudich prove their result by establishing the stronger (and independently interesting) statement that if $P = NP$, then there is no secure KA in the random oracle model. (Note that a random oracle is one-way in the black-box sense even if P=NP.)

1.2 The Limitations of Semi-BB Reductions

In this paper we prove, unconditionally, that there is no semi-BB reduction of OWF to KA. We prove this unconditional result by embedding a PSPACE oracle into a small part of the random oracle used in the Impagliazzo–Rudich result, and use the fact that $P^{PSPACE} = NP^{PSPACE}$. This embedding technique is due to Simon [27].

Following the lead of Impagliazzo and Rudich, several other works explored the limitations of black-box reductions with examples being [25,27,20,8,9,10]. Most results ruled out fully-BB reductions unconditionally, and semi-BB reductions if P=NP. An exception is the work of Gertner et al [10], which involves a model that is slightly different from the one of [17], and which only rules out fully-BB reductions. The embedding technique allows us to prove that semi-BB reductions are unconditionally impossible in all case where semi-BB reductions were previously ruled out conditionally.

More generally, we show that, under mild conditions satisfied by most natural primitives, semi-BB reductions are equivalent to *relativizing reductions* (proofs that the implication holds relative to any oracle). Since the above works rule out relativizing reductions unconditionally, we obtain unconditional impossibility of semi-BB reductions.

1.3 The Power of Mildly-BB Reductions

Semi-BB reductions have typically been considered to be BB constructions with arbitrary proofs, and negative results about semi-BB reductions have typically been interpreted as limitations for constructions that do not use the code of the primitive. In this paper, we present a different perspective.

We first formalize the notion of a BB construction with an arbitrary proof, which we call a mildly-BB reduction. In a mildly-BB reduction of, say, KA to OWF, the construction refers to an oracle function, and it is secure whenever the oracle function is one-way in a black-box sense, but the *analysis* of the construction may be arbitrary. This means that for every oracle f and for every efficient adversary that breaks the KA protocol constructed from f, there is an efficient procedure that inverts f when given oracle access to f. The difference