Lecture Notes in Computer Science 2442

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

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Moti Yung (Ed.)

Advances in Cryptology – CRYPTO 2002

22nd Annual International Cryptology Conference
Santa Barbara, California, USA, August 18-22, 2002
Proceedings

Springer

Volume Editor

Moti Yung
Columbia University
Department of Computer Science, 450 Computer Science Building
1214 Amsterdam Ave., New York, N.Y. 10027, USA
E-mail: moti@cs.columbia.edu

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Advances in cryptology : proceedings / CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18 - 22, 2002. Moti Yung (ed.). [IACR]. - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2442)
ISBN 3-540-44050-X

CR Subject Classification (1998): E.3, G.2.1, F.2.1-2, D.4.6, K.6.5, C.2, J.1

ISSN 0302-9743
ISBN 3-540-44050-X Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN 10871005 06/3142 5 4 3 2 1 0

Preface

Crypto 2002, the 22nd Annual Crypto Conference, was sponsored by IACR, the International Association for Cryptologic Research, 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. It is published as Vol. 2442 of the Lecture Notes in Computer Science (LNCS) of Springer Verlag. Note that 2002, 22 and 2442 are all palindromes... (Don't nod!)

The conference received 175 submissions, of which 40 were accepted; two submissions were merged into a single paper, yielding the total of 39 papers accepted for presentation in the technical program of the conference. In this proceedings volume you will find the revised versions of the 39 papers that were presented at the conference. The submissions represent the current state of work in the cryptographic community worldwide, covering all areas of cryptologic research. In fact, many high-quality works (that surely will be published elsewhere) could not be accepted. This is due to the competitive nature of the conference and the challenging task of selecting a program. I wish to thank the authors of all submitted papers. Indeed, it is the authors of all papers who have made this conference possible, regardless of whether or not their papers were accepted.

The conference program was also immensely benefited by two plenary talks. The first invited talk was by Andrew Chi-Chih Yao, who spoke on "New Directions in Quantum Cryptographic Protocols." In the second talk, David Chaum gave the 2002 IACR Distinguished Lecture, entitled "Privacy Technology: A Survey of Security without Identification."

My deepest thanks go to the program committee members. Serving on a program committee seems, at times, like a thankless job. When a paper is accepted certain people may believe it is due to the paper's intrinsic quality, whereas when a paper is rejected it is attributed to the misjudgment of committee members. The demanding nature of the task of careful evaluation and selection is, at times, easily forgotten. In reality, the reviewing process for this conference was a huge challenge that demanded from committee members top-level scientific capabilities, combined with a lot of time-consuming hard work. Each paper was reviewed by at least three members, and some papers (including those submitted by committee members) were reviewed by as many as six reviewers. The process followed the review directives of IACR. We reached our decisions via electronic discussions and in a meeting of the program committee; this was a tough job, the successful completion of which should be credited to each and every committee member. We were assisted by the program committee's advisory members, as well as by an army of external reviewers whose expertise and help is highly appreciated. Their names are given in a separate list. (I apologize for any possible omission.)

The conference was run by Rebecca Wright, who served as the general chair. I thank her for all her work, and in particular for her continuous assistance to the program committee and the program chair. Some of the committee members as well as other members of the community served as session chairs during the conference, and I thank them for their help in running the program. The conference program also included the traditional Rump Session, chaired by Stuart Haber, featuring short informal talks on recently completed research and work in progress.

The committee task was an international effort (as befits the IACR, where the "I" stands for "International"). We had members from all over the world, a chair in the USA, a program committee meeting in The Netherlands and a web server in Belgium. We utilized Internet technology as much as we could. This was possible due to efforts by a number of individuals. I thank Berry Schoenmakers for making all the necessary local arrangements for the Program Committee meeting in Amsterdam (just before Eurocrypt 2002). I thank Bart Preneel, and his great team at K.U. Leuven, Thomas Herlea and Wim Moreau, who administered the submission and web-review software. Their support has been instrumental. I thank my Ph.D. student Aggelos Kiayias, who served as a technical assistant to the chairs and helped me with the various technical and technological aspects of running the committee and preparing the conference proceedings. Further thanks are due to Bart Preneel, Wim Moreau and Joris Claessens for authoring the web-review software that was used in the refereeing process, and to Chanathip Namprempre, Sam Rebelsky and SIGACT's Electronic Publishing Board, for authoring the software for the electronic submissions. Thanks are also due to the publisher, Springer-Verlag.

To summarize, I benefited greatly from the pleasant and effective working relationships that I enjoyed with the many individuals I had to collaborate with in order to make the program possible, and it was a real learning experience. Indeed, the making of a program for a conference such as Crypto 2002 is an effort that requires a lot of work from a lot of individuals. Fortunately, the IACR and the cryptographic community at large form the active, strong, vibrant, and relevant community that supports our successful conferences. Long live Crypto!

June 2002 Moti Yung

CRYPTO 2002

August 18–22, 2002, Santa Barbara, California, USA

Sponsored by the
International Association for Cryptologic Research (IACR)

In cooperation with
IEEE Computer Society Technical Committee on Security and Privacy,
Computer Science Department, University of California, Santa Barbara

General Chair
Rebecca N. Wright, Stevens Institute of Technology, NJ, USA

Program Chair
Moti Yung, Columbia University, NY, USA

Program Committee

Tom Berson	Anagram Laboratories, USA
Don Coppersmith	IBM Research, USA
Giovanni Di Crescenzo	Telcordia, USA
Hans Dobbertin	University of Bochum, Germany
Matt Franklin	UC Davis, USA
Juan Garay	Bell Labs, USA
Stuart Haber	Surety, Inc., USA
Johan Håstad	Royal Institute of Technology, Sweden
Kwangjo Kim	ICU, Korea
Alfred Menezes	University of Waterloo, Canada
David Naccache	Gemplus, France
Tatsuaki Okamoto	NTT Labs, Japan
Rafail Ostrovsky	Telcordia, USA
Erez Petrank	Technion, Israel
Bart Preneel	K.U. Leuven, Belgium
Ron Rivest	Massachusetts Institute of Technology, USA
Rei Safavi-Naini	University of Wollongong, Australia
Dan Simon	Microsoft Research, USA
Nigel Smart	University of Bristol, UK
Markus Stadler	Crypto AG, Switzerland
Eric Verheul	PricewaterhouseCoopers, The Netherlands
Yiqun Lisa Yin	NTT MCL, USA

Advisory Members

Joe Kilian (Crypto 2001, Program Chair)	NEC, USA
Dan Boneh (Crypto 2003, Program Chair)	Stanford University, USA

External Reviewers

Yonathan Aumann
Dirk Balfanz
Mihir Bellare
Josh Benaloh
Alex Biryukov
John Black
Simon Blackburn
Dan Boneh
Antoon Bosselaers
Thomas Breuel
Eric Brier
Dan Brown
Joe Buhler
Christian Cachin
Jan Camenisch
Ran Canetti
Christophe De Cannière
Sungtaek Chee
Lily Chen
Jung Hee Cheon
Christophe Clavier
Scott Contini
Jean-Sébastien Coron
Ronald Cramer
Anand Desai
Glenn Durfee
Andreas Enge
Lars Engebretsen
Uri Feige
Marc Fischlin
Yair Frankel
Atsushi Fujioka
Eiichiro Fujisaki
Steven Galbraith
Clemente Galdi
Rosario Gennaro
Craig Gentry
Virgil Gligor
Mikael Goldmann
Jovan Golić
Guang Gong
Daniel Gottesman
Louis Goubin
Louis Granboulan
Rich Graveman
Shai Halevi
Helena Handschuh
Darrel Hankerson
Gustav Hast
Jon Herzog
Florian Hess
Martin Hirt
Susan Hohenberger
Jonas Holmerin
Yuval Ishai
Markus Jakobsson
Stanislaw Jarecki
Thomas Johansson
Antoine Joux
Marc Joye
Charanjit Jutla
Jonathan Katz
Aggelos Kiayias
Joe Kilian
Seung Joo Kim
Lars Knudsen
Neil Koblitz
Hugo Krawczyk
Hartono Kurnio
Eyal Kushilevitz
Tanja Lange
Alan Lauder
Arjen Lenstra
Matt Lepinski
Yehuda Lindell
Moses Liskov
Anna Lysyanskaya
Phil MacKenzie
Tal Malkin
John Malone-Lee
Renato Menicocci
Daniele Micciancio
Miodrag Mihaljevic
Tal Mor
Shiho Moriai
Christophe Mourtel
Yi Mu
Jen Mulligan

Mats Näslund
Kenny Nguyen
Svetla Nikova
Kazuo Ohta
Pascal Paillier
Rafael Pass
Christopher Peikert
Benny Pinkas
Michaël Quisquater
Tal Rabin
Raj Rajagopalan
Anna Redz
Omer Reingold
Vincent Rijmen
Phil Rogaway
Tomas Sander
Werner Schindler
Jasper Scholten
Stefaan Seys
Alice Silverberg
Diana Smetters
Adam Smith
David Soldera
Jessica Staddon
Martijn Stam
Koutarou Suzuki
Edlyn Teske
Prasad Tetali
Dong To
Yuki Tokunaga
Marten Trolin
Yiannis Tsiounis
Christophe Tymen
Ugo Vaccaro
Serge Vaudenay
Frederik Vercauteren
Huaxiong Wang
Yejing Wang
John Watrous
Steve Weis
Michael Wiener
Peter Winkler
Douglas Wikstrom
Duncan Wong
Hao-Chi Wong
Yoav Yerushalmi
Xian-Mo Zhang
Yuliang Zheng

Table of Contents

Block Ciphers

Multi-user Oriented Cryptosystems

Foundations and Methodology

Security of Practical Protocols

Secure Multiparty Computation

Public-Key Encryption

Information Theory and Secret Sharing

Cipher Design and Analysis

Elliptic Curves and Abelian Varieties

Password-Based Authentication

Distributed Cryptosystems

Pseudorandomness and Applications

Variations on Signatures and Authentication

Stream Ciphers and Boolean Functions

Commitment Schemes

Signature Schemes