

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!

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

Mats Näslund
Kenny Nguyen
Svetla Nikova
Kazuo Ohta
Pascal Paillier
Rafael Pass
Christopher Peikert
Benny Pinkas
Michaël Qisquater
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