

# Preface

Crypto 2001, the 21st Annual Crypto conference, was sponsored by the International 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The conference received 156 submissions, of which the program committee selected 34 for presentation; one was later withdrawn. These proceedings contain the revised versions of the 33 submissions that were presented at the conference. These revisions have not been checked for correctness, and the authors bear full responsibility for the contents of their papers.

The conference program included two invited lectures. Mark Sherwin spoke on, “Quantum information processing in semiconductors: an experimentalist’s view.” Daniel Weitzner spoke on, “Privacy, Authentication & Identity: A recent history of cryptographic struggles for freedom.” The conference program also included its perennial “rump session,” chaired by Stuart Haber, featuring short, informal talks on late-breaking research news.

As I try to account for the hours of my life that flew off to oblivion, I realize that most of my time was spent cajoling talented innocents into spending even more time on my behalf. I have accumulated more debts than I can ever hope to repay. As mere statements of thanks are certainly insufficient, consider the rest of this preface my version of Chapter 11.

I would like to first thank the many researchers from all over the world who submitted their work to this conference. Without them, Crypto is just a pile of shrimp and chocolate covered strawberries.

I thank David Balenson, the general chair, for shielding me from innumerable logistical headaches, and showing great generosity in supporting my efforts.

Selecting from so many submissions is a daunting task. My deepest thanks go to the members of the program committee, for their knowledge, wisdom, and near-masochistic work ethic. We in turn have relied heavily on the expertise of the many outside reviewers who assisted us in our deliberations. My thanks to all those listed on the following pages, and my thanks and apologies to any I have missed.

I thank Rebecca Wright for hosting the program committee meeting in New York City, AT&T for providing the space, and Sandy Barbu for helping out with the local arrangements. Thanks also go to Ran Canetti, my favorite native culinary guide, wherever I go, for organizing the post-deliberations dinner.

I thank the people who, by their past and continuing work, have greatly streamlined the submission and review process. All but one of the submissions were handled using Chanathip Namprempre’s web-based submission software. Reviews were administered using software written by Wim Moreau and Joris Claessens, developed under the guidance of Bart Preneel. These software packages have made the process idiot proof, and nearly theorist-proof. My thanks also go to Sam Rebelsky for writing the email-based predecessor of the submission

software. He and the other members of the SIGACT Electronic Publications Board have for many years made program committee chairs' lives much more bearable.

I am grateful to Mihir Bellare, last year's program chair, and Kevin McCurley and Josh Benaloh, my main contacts with the IACR board, for patiently trying to teach me my job.

Even if I can't really account for what I, personally, was doing, the hours did go somewhere. I thank my boss, Peter Yianilos, for being so supportive of my efforts, and so absurdly forgiving of the time it has taken away from my work. Last, and more importantly, I'd like to thank my family, Dina, Gersh, and Pearl, for their support, understanding, and love.

June 2001

Joe Kilian

# CRYPTO 2001

August 19–23, 2001, 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

David Balenson, NAI Labs, Network Associates, Inc., USA

## Program Chair

Joe Kilian, Yianilos Labs, USA

## Program Committee

Bill Aiello . . . . . AT&T Research, USA  
Don Beaver . . . . . CertCo, USA  
Josh Benaloh . . . . . Microsoft Research, USA  
Antoon Bosselaers . . . . . Katholieke Universiteit Leuven, Belgium  
Jan Camenisch . . . . . IBM Zurich, Switzerland  
Ran Canetti . . . . . IBM T. J. Watson, USA  
Claude Crépeau . . . . . McGill University, Canada  
Alfredo De Santis . . . . . Università di Salerno, Italy  
Marc Girault . . . . . France Telecom, France  
Stuart Haber . . . . . InterTrust STAR Lab, USA  
Tatsuaki Okamoto . . . . . NTT Labs, Japan  
Jacques Patarin . . . . . BULL, France  
Erez Petrank . . . . . Technion, Israel  
Omer Reingold . . . . . AT&T Research, USA  
Kazue Sako . . . . . NEC C&C Media Research Lab, Japan  
Tomas Sander . . . . . InterTrust STAR Lab, USA  
Doug Stinson . . . . . University of Waterloo, Canada  
Yacov Yacobi . . . . . Microsoft Research, USA

## Advisory Members

Mihir Bellare (Crypto 2000 program chair) . . . . . UCSD, USA  
Moti Yung (Crypto 2002 program chair) . . . . . CertCo, USA

## External Reviewers

Masayuki Abe	Stanislaw Jarecki	David Pointcheval
Mehdi-Laurent Akkar	Thomas Johansson	Bart Preneel
Seigo Arita	Jakob Jonsson	Jean-Jacques Quisquater
Mihir Bellare	Marc Joye	Tal Rabin
Juergen Bierbrauer	Ari Juels	Raj Rajagopalan
Eli Biham	Charanjit Jutla	Vincent Rijmen
Daniel Bleichenbacher	Jonathan Katz	Matt Robshaw
Carlo Blundo	Darko Kirovski	Phillip Rogaway
Dan Boneh	Andrew Klapper	Pankaj Rohatgi
Eric Brier	Francis Klay	Alon Rosen
Daniel Brown	Tetsutaro Kobayashi	Amit Sahai
Christian Cachin	Hugo Krawczyk	Taiichi Saitoh
Anne Canteaut	Eyal Kushilevitz	Louis Salvail
William Chambers	Kristin Lauter	Plash Sarkar
Joris Claessens	Arjen Lenstra	Claus Schnorr
Henry Cohn	Yehuda Lindell	Peter Shor
Don Coppersmith	Anna Lysyanskaya	Victor Shoup
Jean-Sébastien Coron	David M'Raihi	Alice Silverberg
Ronald Cramer	Spyros Magliveras	Dan Simon
Paolo D'Arco	Dahlia Malkhi	Dawn Song
Annalisa De Bonis	Tal Malkin	Markus Stadler
Patrick Dehornoy	Barbara Masucci	Jacques Stern
Giovanni Di Crescenzo	Minoru Matsui	Koutarou Suzuki
Markus Dichtl	Ueli Maurer	Paul Syverson
Marc Fischlin	Rita Mayer-Sommer	Jacques Traoré
Roger Fischlin	Alfred Menezes	Luca Trevisan
Gerhard Frey	Niodrag Mihaljevic	Shigenori Uchiyama
Eiichiro Fujisaki	Kazuhiko Minematsu	Serge Vaudenay
Jun Furukawa	Jean-François Misarsky	Ramarathnam Venkatesan
Clemente Galdi	Peter Montgomery	Frederik Vercauteren
Rosario Gennaro	Guglielmo Morgari	Eric Verheul
Oded Goldreich	Shiho Moriai	Ivan Visconti
Dieter Gollmann	David Naccache	David Wagner
Roberto Gorrieri	Moni Naor	Michael Waidner
Louis Goubin	Satoshi Obana	Yongge Wang
Gaëtan Haché	Rafail Ostrovsky	Ruizhong Wei
Shai Halevi	Christof Paar	Gideon Yuval
Helena Handschuh	Béatrice Peirani	
Nick Howgrave-Graham	Pino Persiano	
Yuval Ishai	Benny Pinkas	



<http://www.springer.com/978-3-540-42456-7>

Advances in Cryptology - CRYPTO 2001  
21st Annual International Cryptology Conference, Santa  
Barbara, California, USA, August 19-23, 2001,  
Proceedings  
Kilian, J. (Ed.)  
2001, XII, 604 p., Softcover  
ISBN: 978-3-540-42456-7