

Topics in Cryptology - CT-RSA 2002

The Cryptographer's Track at the RSA Conference 2002, San Jose, CA, USA, February 18-22, 2002,
Proceedings

Bearbeitet von
Bart Preneel

1. Auflage 2002. Taschenbuch. X, 318 S. Paperback
ISBN 978 3 540 43224 1
Format (B x L): 15,5 x 23,5 cm
Gewicht: 1020 g

Weitere Fachgebiete > EDV, Informatik > Datenbanken, Informationssicherheit,
Geschäftssoftware > Informations- und Kodierungstheorie

Zu Inhaltsverzeichnis

schnell und portofrei erhältlich bei

The logo for beck-shop.de features the text 'beck-shop.de' in a bold, red, sans-serif font. Above the 'i' in 'shop' are three red dots of increasing size. Below the main text, 'DIE FACHBUCHHANDLUNG' is written in a smaller, red, all-caps, sans-serif font.

beck-shop.de
DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beck-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Preface

This volume continues the tradition established in 2001 of publishing the contributions presented at the Cryptographers' Track (CT-RSA) of the yearly RSA Security Conference in Springer-Verlag's Lecture Notes in Computer Science series.

With 14 parallel tracks and many thousands of participants, the RSA Security Conference is the largest e-security and cryptography conference. In this setting, the Cryptographers' Track presents the latest scientific developments.

The program committee considered 49 papers and selected 20 for presentation. One paper was withdrawn by the authors. The program also included two invited talks by Ron Rivest ("Micropayments Revisited" – joint work with Silvio Micali) and by Victor Shoup ("The Bumpy Road from Cryptographic Theory to Practice").

Each paper was reviewed by at least three program committee members; papers written by program committee members received six reviews. The authors of accepted papers made a substantial effort to take into account the comments in the version submitted to these proceedings. In a limited number of cases, these revisions were checked by members of the program committee.

I would like to thank the 20 members of the program committee who helped to maintain the rigorous scientific standards to which the Cryptographers' Track aims to adhere. They wrote thoughtful reviews and contributed to long discussions; more than 400 Kbyte of comments were accumulated. Many of them attended the program committee meeting, while they could have been enjoying the sunny beaches of Santa Barbara.

I gratefully acknowledge the help of a large number of colleagues who reviewed submissions in their area of expertise: Masayuki Abe, N. Asokan, Tonnes Brekne, Emmanuel Bresson, Eric Brier, Jan Camenisch, Christian Collberg, Don Coppersmith, Jean-Sébastien Coron, Serge Fehr, Marc Fischlin, Matthias Fitzi, Pierre-Alain Fouque, Anwar Hasan, Clemens Holenstein, Kamal Jain, Marc Joye, Darko Kirovski, Lars Knudsen, Neal Kobnitz, Anna Lysyanskaya, Lennart Meier, David M'Raihi, Phong Nguyen, Pascal Paillier, Adrian Perrig, David Pointcheval, Tal Rabin, Tomas Sander, Berk Sunar, Michael Szydlo, Christophe Tymen, Frederik Vercauteren, Colin Walter, Andre Weimerskirch, and Susanne Wetzels. I apologize for any inadvertent omissions.

Electronic submissions were made possible by a collection of PHP scripts originally written by Chanathip Namprempe and some perl scripts written by Sam Rebelsky and SIGACT's Electronic Publishing Board. For the review procedure, web-based software was used which I designed for Eurocrypt 2000; the code was written by Wim Moreau and Joris Claessens.

I would like to thank Wim Moreau for helping with the electronic processing of the submissions and final versions, Ari Juels and Burt Kaliski for interfacing

with the RSA Security Conference, and Alfred Hofmann and his colleagues at Springer-Verlag for the timely production of this volume.

Finally, I wish to thank all the authors who submitted papers and the authors of accepted papers for the smooth cooperation which enabled us to process these proceedings as a single **LaTeX** document.

We hope that in the coming years the Cryptographers' Track will continue to be a forum for dialogue between researchers and practitioners in information security.

November 2001

Bart Preneel

RSA Cryptographers' Track 2002

February 18–22, 2002, San Jose, California

The RSA Conference 2002 was organized by RSA Security Inc. and its partner organizations around the world. The Cryptographers' Track was organized by RSA Laboratories (<http://www.rsasecurity.com>).

Program Chair

Bart Preneel, Katholieke Universiteit Leuven, Belgium

Program Committee

Dan Boneh	Stanford University, USA
Yvo Desmedt	Florida State University, USA
Dieter Gollmann	Microsoft Research, USA
Stuart Haber	Intertrust, USA
Shai Halevi	IBM Research, USA
Helena Handschuh	Gemplus, France
Martin Hirt	ETH, Switzerland
Markus Jakobsson	RSA Laboratories, USA
Ari Juels	RSA Laboratories, USA
Pil Jong Lee	Postech, Korea
Alfred Menezes	University of Waterloo, Canada
Kaisa Nyberg	Nokia, Finland
Tatsuaki Okamoto	NTT Labs, Japan
Christof Paar	Worcester Polytechnique Institute, USA
Jean-Jacques Quisquater	Univ. Cath. de Louvain, Belgium
Jacques Stern	Ecole Normale Supérieure, France
Michael Wiener	Canada
Yacov Yacobi	Microsoft Research, USA
Moti Yung	Certco, USA
Yuliang Zheng	Monash University, Australia