Lecture Notes in Computer Science 1751

Public Key Cryptography

Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, Melbourne, Victoria, Australia, January 18-20, 2000, Proceedings

Bearbeitet von
Hideki Imai, Yuliang Zheng

ISBN 978 3 540 66967 8
Format (B x L): 15,5 x 23,5 cm
Gewicht: 1540 g

Weitere Fachgebiete > EDV, Informatik > Datenbanken, Informationssicherheit, Geschäftsoftware > Zeichen- und Zahlendarstellungen

Zu Inhaltsverzeichnis

schnell und portofrei erhältlich bei

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

The PKC2000 conference was held at the Melbourne Exhibition Centre, Victoria, Australia, January 18-20, 2000. It was the third conference in the international workshop series dedicated to practice and theory in public key cryptography.

The program committee of the conference received 70 full submissions from around the world, of which 31 were selected for presentation. All submissions were reviewed by experts in the relevant areas.

The program committee consisted of 19 experts in cryptography and data security drawn from the international research community, these being Chin-Chen Chang (National Chung Cheng University, Taiwan), Claude Cr´epeau (McGill University, Canada), Ed Dawson (Queensland University of Technology, Australia), Yvo Desmedt (Florida State University, USA), Hideki Imai (Co-chair, University of Tokyo, Japan), Markus Jakobsson (Bell Labs, USA), Kwangjo Kim (Information and Communications University, Korea), Arjen Lenstra (Citibank, USA), Tsutomu Matsumoto (Yokohama National University, Japan), David Naccache (Gemplus, France), Eiji Okamoto (University of Wisconsin-Milwaukee, USA), Tatsuaki Okamoto (NTT Labs, Japan), Josef Pieprzyk (University of Wollongong, Australia), Jean-Jacques Quisquater (Université Catholique de Louvain, Belgium), Nigel Smart (HP Labs Bristol, UK), Vijay Varadharajan (University of Western Sydney, Australia), Serge Vaudenay (Ecole Polytechnique Fédérale de Lausanne, Switzerland), Moti Yung (CertCo, USA), and Yuliang Zheng (Co-chair, Monash University, Australia). Members of the committee spent numerous hours in reviewing the submissions and providing advice and comments on the selection of papers.


We would like to take this opportunity to thank all the program committee members and external experts for their invaluable help in producing such a high quality program. We are especially indebted to Chin-Chen Chang who made sure all the submissions assigned to him were properly reviewed in spite of the devastating earthquake and its countless aftershocks that rocked Taiwan in late September 1999.
The conference would not have been successful without the financial support from both Imai Laboratory (imailab-www.iis.u-tokyo.ac.jp) of the Institute of Industrial Science, University of Tokyo, and LINKS – Laboratory for Information and Network Security (www.pscit.monash.edu.au/links/) of the Faculty of Information Technology, Monash University. Our appreciation also goes to members of LINKS, including Jerald Chong, Chandana Gamage, Lionnel Heng, Khaled Khan, Jussi Leiwo, Patrik Mihaiescu, and E-Yang Tang for their skillful and professional assistance in organizing this conference. Chandana Gamage deserves special thanks for helping out during the entire refereeing and editing process.

Last, but not least, we would like to thank all the authors who submitted their papers to the conference (including those whose submissions were not successful), as well as the conference participants from around the world, for their support which made this conference possible.

January 2000

Hideki Imai

Yuliang Zheng
PKC2000

2000 International Workshop on Practice and Theory in Public Key Cryptography
Melbourne Exhibition Centre, Australia
January 18-20, 2000

Sponsored by

Imai Laboratory of the Institute of Industrial Science,
University of Tokyo, Japan (imailab-www.iis.u-tokyo.ac.jp)
and
LINKS – Laboratory for Information and Network Security
of Monash University, Australia (www.pscit.monash.edu.au/links/)

Program Committee

Hideki Imai, Co-chair (University of Tokyo, Japan)
Yuliang Zheng, Co-chair (Monash University, Australia)
Chin-Chen Chang (National Chung Cheng University, Taiwan)
Claude Crepeau (McGill University, Canada)
Ed Dawson (Queensland University of Technology, Australia)
Yvo Desmedt (Florida State University, USA)
Markus Jakobsson (Bell Labs, USA)
Kwangjo Kim (Information and Communications University, Korea)
Arjen Lenstra (Citibank, USA)
Tsutomu Matsumoto (Yokohama National University, Japan)
David Naccache (Gemplus, France)
Eiji Okamoto (University of Wisconsin-Milwaukee, USA)
Tatsuaki Okamoto (NTT Labs, Japan)
Josef Pieprzyk (University of Wollongong, Australia)
Jean-Jacques Quisquater (Université Catholique de Louvain, Belgium)
Nigel Smart (HP Labs Bristol, UK)
Vijay Varadharajan (University of Western Sydney, Australia)
Serge Vaudenay (EPFL, Switzerland)
Moti Yung (CertCo, USA)