Preface

The 2005 issue of the International Workshop on Practice and Theory in Public Key Cryptography (PKC 2005) was held in Les Diablerets, Switzerland during January 23–26, 2005. It followed a series of successful PKC workshops which started in 1998 in Pacifico Yokohama, Japan. Previous workshops were successively held in Kamakura (Japan), Melbourne (Australia), Cheju Island (South Korea), Paris (France), Miami (USA), and Singapore. Since 2003, PKC has been sponsored by the International Association for Cryptologic Research (IACR). As in previous years, PKC 2005 was one of the major meeting points of worldwide research experts in public-key cryptography. I had the honor to co-chair the workshop together with Jean Monnerat and to head the program committee. Inspired by the fact that the RSA cryptosystem was invented on ski lifts, we decided that the best place for PKC was at a ski resort. Jean Monnerat and I hope that this workshop in a relaxed atmosphere will lead us to 25 more years of research fun.

PKC 2005 collected 126 submissions on August 26, 2004. This is a record number. The program committee carried out a thorough review process. In total, 413 review reports were written by renowned experts, program committee members as well as external referees. Online discussions led to 313 additional discussion messages and 238 emails. The review process was run using email and the Webreview software by Wim Moreau and Joris Claessens. Every submitted paper received at least 3 review reports. We selected 28 papers for publication on October 28, 2004. Authors were then given a chance to revise their submission over the following two weeks. This proceedings includes all the revised papers. Due to time constraints the revised versions could not be reviewed again.

Double submissions, where authors send the same or almost the same paper to multiple conferences that explicitly prohibit such practices, is an increasing problem for the research community worldwide. I do regret that we had to reject 6 such submissions without consideration of their scientific merits. I would like to thank the program chairs of other events who collaborated in this effort, in particular Anne Canteaut, Joe Kilian, Choonsik Park, and Seongtaek Chee.

With the approval of the IACR Board of Directors, PKC 2005 delivered the *PKC Best Paper Award* for the first time. The purpose of the award is to formally acknowledge authors of outstanding papers and to recognize excellence in the cryptographic research fields. Committee members were invited to nominate papers for this award. A poll then yielded a clear majority. This year, we were pleased to deliver the PKC Best Paper Award to Yevgeniy Dodis and Aleksandr Yampolskiy for their brilliant paper "A Verifiable Random Function with Short Proofs and Keys." This paper concluded the workshop.

I would like to thank Jean Monnerat who accepted the responsibility to co-chair the PKC 2005 workshop. I would like to thank the PKC steering committee for their support and trust. The program committee and external reviewers

worked extremely hard under a tight schedule. I heartily thank them for this volunteer work. Acknowledgments also go to the authors of submitted papers and the speakers who made the real meat of PKC 2005. I am grateful to Antoine Junod and Julien Brouchier for their support with the Webreview software. I also thank my assistants Pascal Junod, Thomas Baignères, Yi Lu, Gildas Avoine, and Matthieu Finiasz for their help in the PKC 2005 organization. Special thanks to Martine Corval who orchestrated the PKC 2005 logistics. We appreciate the kind help of Christian Cachin in the advertising and registration process. We also owe our gratitude to Kevin McCurley for spending a substantial amount of his valuable time to set up the online registration website. We thank our generous sponsors Gemplus and personally David Naccache, and HP Labs and personally Wenbo Mao, for supporting PKC 2005. We also thank EPFL and IACR for sponsoring this event. It was a very pleasant experience. Crypto is fun!

Lausanne, November 19, 2004 Serge Vaudenay

PKC Steering Committee (as of November 2004)

Yvo Desmedt	University College London, UK
Hideki Imai (Chair)	University of Tokyo, Japan
Kwangjo Kim	Information and Communications University, South Korea
David Naccache	Gemplus, France, and Royal Holloway, University of London, UK
Jacques Stern	Ecole Normale Supérieure, France
Moti Yung	Columbia University, USA
Yuliang Zheng (Secretary)	University of North Carolina at Charlotte, USA
Ronald Cramer	CWI and Leiden University, The Netherlands
Tatsuaki Okamoto	NTT Labs, Japan

Organizing Committee

General Co-chairs	Jean Monnerat
	Serge Vaudenay
Local Organization	Martine Corval
Assistants	Gildas Avoine
	Thomas Baignères
	Matthieu Finiasz
	Pascal Junod
	Yi Lu

Program Committee

Carlisle Adams	University of Ottawa, Canada
Feng Bao	Institute for Infocomm Research, Singapore
Yvo Desmedt	University College London, UK
Juan Garay	Bell Labs – Lucent Technologies, USA
Martin Hirt	ETH Zurich, Switzerland
Kwangjo Kim	Information and Communications University, South Korea
Kaoru Kurosawa	Ibaraki University, Japan
Anna Lysyanskaya	Brown University, USA
Wenbo Mao	HP Labs Bristol, UK
David Naccache	Gemplus, France and Royal Holloway, University of London, UK
Kaisa Nyberg	Nokia, Finland
Tatsuaki Okamoto	NTT Labs, Japan
Josef Pieprzyk	Macquarie University, Australia
David Pointcheval	CNRS-ENS, France
Reihaneh Safavi-Naini	University of Wollongong, Australia
Kazue Sako	NEC, Japan
Claus-Peter Schnorr	University of Frankfurt am Main, Germany
Berry Schoenmakers	Technische Universiteit Eindhoven, The Netherlands
Nigel Smart	University of Bristol, UK
Edlyn Teske	University of Waterloo, Canada
Serge Vaudenay	EPFL, Switzerland
Moti Yung	University of Columbia, USA
Yuliang Zheng	University of North Carolina at Charlotte, USA

External Reviewers

Masayuki Abe
Ben Adida
Gildas Avoine
Joonsang Baek
Thomas Baignères
Mihir Bellare
Daniel Bleichenbacher
Colin Boyd
Emmanuel Bresson
Eric Brier
Duncan Buell
Srdjan Capkun
Dario Catalano
Liqun Chen
Benoît Chevallier-Mames
Jean-Sébastien Coron
Ronald Cramer
Jean-François Dhem
Christophe Doche
Atsushi Fujioka
Eiichiro Fujisaki
Jun Furukawa
Steven Galbraith
Pierrick Gaudry
Louis Granboulan
Rob Granger
Jaime Gutierrez
Darrel Hankerson
Anwar Hasan
Alex Healy
Jason Hinek
Susan Hohenberger
Thomas Holenstein
Heng Swee Huay
Toshiyuki Isshiki
Kouichi Itoh
Michael Jacobson
Marc Joye
Pascal Junod
Charanjit Jutla
Jonathan Katz
Tetsutaro Kobayashi
Robert König
Byoungcheon Lee
Arjen Lenstra
Moses Liskov
Javier Lopez
Yi Lu
John Malone-Lee
Toshihiko Matsuo
Noel McCullagh
Anton Mityagin
Atsuko Miyaji
Jean Monnerat
Waka Nagao
Phong Q. Nguyễn
Satoshi Obana
Takeshi Okamoto
Katsuyuki Okeya
Dan Page
Pascal Paillier
Jacques Patarin
Kenneth Paterson
Chris Peikert
Krzysztof Pietrzak
Bartosz Przydatek
Tal Rabin
Peter Roelse
Hans-Georg Rueck
Ryuichi Sakai
Takakazu Satoh
Katja Schmidt-Samoa
Michael Scott
Hovav Shacham
Andrey Sidorenko
Johan Sjödin
Martijn Stam
Andreas Stein
Ron Steinfeld
Makoto Sugita
Willy Susilo
Koutarou Suzuki
Tsuyoshi Takagi
Keisuke Tanaka
Isamu Teranishi
Jacques Traoré
Shigenori Uchiyama
Frederik Vercauteren
Duong Quang Viet
Jorge L. Villar
Guilin Wang
Huaxiong Wang
Stephen Weis
Claire Whelan
Christopher Wolf
Go Yamamoto
Chung-Huang Yang
Danfeng Yao
Sung-Ming Yen
Huafei Zhu