Lecture Notes in Computer Science 5985

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Josef Pieprzyk (Ed.)

Topics in Cryptology – CT-RSA 2010

The Cryptographers' Track at the RSA Conference 2010
San Francisco, CA, USA, March 1-5, 2010
Proceedings

Springer

Volume Editor

Josef Pieprzyk
Macquarie University
Department of Computing
Sydney, NSW 2109, Australia
E-mail: josef@science.mq.edu.au

Library of Congress Control Number: Applied for

CR Subject Classification (1998): E.3, D.4.6, K.6.5, C.2, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-642-11924-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-11924-8 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180 5 4 3 2 1 0

Preface

The RSA Conference is an annual event that attracts hundreds of vendors and thousands of participants from industry and academia. Since 2001, the conference has included an academic Cryptographers' Track (CT-RSA). This year was the 10th anniversary of CT-RSA. Since its conception, the CT-RSA conference has become a major avenue for publishing high-quality research papers. The RSA conference was held in San Francisco, California, during March 1–5, 2010.

This year we received 94 submissions. Each paper got assigned to three referees. Papers submitted by the members of the Program Committee got assigned to five referees. In the first stage of the review process, the submitted papers were read and evaluated by the Program Committee members and then in the second stage, the papers were scrutinized during an extensive discussion. Finally, the Program Committee chose 25 papers to be included in the conference program. The authors of the accepted papers had two weeks for revision and preparation of final versions. The revised papers were not subject to editorial review and the authors bear full responsibility for their contents. The submission and review process was supported by the iChair conference submission server. We thank Matthiew Finiasz and Thomas Baignères for letting us use iChair. The conference proceedings were published by Springer in this volume of *Lecture Notes in Computer Science*.

The Program Committee invited two distinguished researchers to deliver their keynote talks. The first speaker was Bart Preneel from Katholieke Universiteit Leuven, Belgium. His talk was entitled "The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition." The second speaker was Craig Gentry from IBM Research, USA who gave a talk on "Computing on Encrypted Data."

There are many people who contributed to the success of the 10th edition of CT-RSA. First we would like to thank the authors of all papers (both accepted and rejected) for submitting their papers to the conference. A special thanks to the members of the Program Committee and the external referees who gave their time, expertise and enthusiasm in order to ensure that each paper received a thorough and fair review. We are thankful to Vijayakrishnan Pasupathinathan for taking care of the iChair server. I thank the CT-RSA Steering Committee for giving me an opportunity to serve as the Program Chair. Last but not least, I would like to thank the RSA conference team, especially Bree LaBollita, for their help.

March 2010 Josef Pieprzyk

CT-RSA 2010

The 10th Cryptographers' Track at the RSA Conference

The Mascone Center, San Francisco, California, USA
March 1–5, 2010

Program Chair

Josef Pieprzyk	Macquarie University, Australia

Program Committee

Joonsang Baek	Institute for Infocomm Research, Singapore
Josh Benaloh	Microsoft Research, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Colin Boyd	QUT, Australia
Xavier Boyen	Stanford University, USA
Alex Dent	RHUL, UK
Christophe Doche	Macquarie University, Australia
Orr Dunkelman	Weizmann Institute, Israel, ENS, France
Serge Fehr	CWI, The Netherlands
Marc Fischlin	Darmstadt University of Technology, Germany
Goichiro Hanaoka	AIST, Japan
Stanisław Jarecki	UC, Irvine, USA
Jonathan Katz	University of Maryland, USA
Aggelos Kiayias	University of Connecticut, USA
Kwangjo Kim	KAIST, Korea
Mirosław Kutyłowski	Wroclaw University of Technology, Poland
Helger Lipmaa	Cybernetica AS, Estonia
Stefan Lucks	University of Weimar, Germany
Tal Malkin	Columbia University, USA
Ilya Mironov	Microsoft Research, USA
David Naccache	ENS, France
Giuseppe Persiano	University of Salerno, Italy
Vincent Rijmen	K.U. Leuven, Belgium, TU Graz, Austria
Matt Robshaw	France Telecom, France
Kazue Sako	NEC, Japan
Berry Schoenmakers	Eindhoven University, The Netherlands
Ron Steinfeld	Macquarie University, Australia
Huaxiong Wang	NTU, Singapore

Steering Committee

Masayuki Abe	NTT, Japan
Marc Fischlin	Darmstadt University of Technology, Germany
Tal Malkin	Columbia University, USA
Ron Rivest	MIT, USA
Moti Yung	Google Inc. and Columbia University, USA

External Reviewers

Abdalla, Michel
Alford, Amy
Avanzi, Roberto
Blömer, Johannes
Brzuska, Christina
Choi, Seung Geol
Chow, Sherman
Chu, Cheng-Kang
Crampton, Jason
Dachman-Soled, Dana
Dagdelen, Özgür
D'Arco, Paolo
Etrog, Jonathan
Farashahi, Reza Rezaeian
Farshim, Pooya
Fleischmann, Ewan
Forler, Christian
Furukawa, Jun
Galdi, Clemente
Gallais, Jean-Francois
Gierlichs, Benedikt
Gogolewski, Marcin
Golicz, Mateusz
Gonzalez, Juan
Gorantla, Choudary
Gordon, Dov
Gorski, Michael
Groschädl, Johann
Guo, Jian
Hinek, Jason
Isshiki, Toshiyuki
Izu, Tetsuya
Jiang, Shaoquan
Kiltz, Eike
Kizhvatov, Ilya
Klonowski, Marek
Konidala, Divyan M.
Koshiba, Takeshi
Krzywiecki, Łukasz
Kubiak, Przemysław
Lehmann, Anja
Liu, Joseph K.
Liu, Xiaomin
Marcello, Sandra
Marchwicki, Karol
Matsuda, Takahiro
Masucci, Barbara
Müller, Volker
Nikolić, Ivica
Nogami, Yasuyuki
Olsen, Josh
Onete, Maria Cristina
Pehlivanoglu, Serdar
Poschmann, Axel
Qiu, Ying
Raykova, Mariana
Sakai, Yasuyuki
Schmitd, Jörn-Marc
Schröder, Dominique
Seurin, Yannick
Shao, Jun
Shin, Sungmok
Standaert, Francois-Xavier
Stehlé, Damien
Stevens, Marc
Strumiński, Tomasz
Sugita, Makoto
Szymański, Piotr
Tadaki, Kohtaro
Takagi, Tsuyoshi
Tartary, Christophe
Teranishi, Isamu
Tillich, Stefan
Vercauteren, Frederik
Wan, Andrew
Wee, Hoeteck
Wu, Hongjun
Wu, Mu-En
Yang, Guomin
Yen, Sung-Ming
Yoneyama, Kazuki
Yoo, Myunghan
Zagórski, Filip
Zhou, Hong-Sheng

Table of Contents

Invited Talk

Public-Key Cryptography

Side-Channel Attacks

Cryptographic Protocols

Cryptanalysis

Symmetric Cryptography