

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

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

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

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

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

Table of Contents

Invited Talk

The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition	1
<i>Bart Preneel</i>	

Public-Key Cryptography

Errors Matter: Breaking RSA-Based PIN Encryption with Thirty Ciphertext Validity Queries	15
<i>Nigel P. Smart</i>	
Efficient CRT-RSA Decryption for Small Encryption Exponents	26
<i>Subhamoy Maitra and Santanu Sarkar</i>	
Resetable Public-Key Encryption: How to Encrypt on a Virtual Machine	41
<i>Scott Yilek</i>	
Plaintext-Awareness of Hybrid Encryption	57
<i>Shaoquan Jiang and Huaxiong Wang</i>	
Speed Records for NTRU	73
<i>Jens Hermans, Frederik Vercauteren, and Bart Preneel</i>	
High-Speed Parallel Software Implementation of the η_T Pairing	89
<i>Diego F. Aranha, Julio López, and Darrel Hankerson</i>	
Refinement of Miller's Algorithm Over Edwards Curves	106
<i>Lei Xu and Dongdai Lin</i>	
Probabilistic Public Key Encryption with Equality Test	119
<i>Guomin Yang, Chik How Tan, Qiong Huang, and Duncan S. Wong</i>	
Efficient CCA-Secure PKE from Identity-Based Techniques	132
<i>Junzuo Lai, Robert H. Deng, Shengli Liu, and Weidong Kou</i>	
Anonymity from Asymmetry: New Constructions for Anonymous HIBE	148
<i>Léo Ducas</i>	
Making the Diffie-Hellman Protocol Identity-Based	165
<i>Dario Fiore and Rosario Gennaro</i>	

On Extended Sanitizable Signature Schemes	179
<i>Sébastien Canard and Amandine Jambert</i>	

Side-Channel Attacks

Unrolling Cryptographic Circuits: A Simple Countermeasure Against Side-Channel Attacks	195
<i>Shivam Bhasin, Sylvain Guilley, Laurent Sauvage, and Jean-Luc Danger</i>	
Fault Attacks Against EMV Signatures	208
<i>Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi</i>	
Revisiting Higher-Order DPA Attacks: Multivariate Mutual Information Analysis	221
<i>Benedikt Gierlichs, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede</i>	
Differential Cache-Collision Timing Attacks on AES with Applications to Embedded CPUs	235
<i>Andrey Bogdanov, Thomas Eisenbarth, Christof Paar, and Malte Wienecke</i>	

Cryptographic Protocols

Usable Optimistic Fair Exchange	252
<i>Alptekin Küpçü and Anna Lysyanskaya</i>	
Hash Function Combiners in TLS and SSL	268
<i>Marc Fischlin, Anja Lehmann, and Daniel Wagner</i>	
Improving Efficiency of an ‘On the Fly’ Identification Scheme by Perfecting Zero-Knowledgeness	284
<i>Bagus Santoso, Kazuo Ohta, Kazuo Sakiyama, and Goichiro Hanaoka</i>	

Cryptanalysis

Linear Cryptanalysis of Reduced-Round PRESENT	302
<i>Joo Yeon Cho</i>	
Dependent Linear Approximations: The Algorithm of Biryukov and Others Revisited	318
<i>Miia Hermelin and Kaisa Nyberg</i>	
Practical Key Recovery Attack against Secret-IV Edon- <i>R</i>	334
<i>Gaëtan Leurent</i>	

Rebound Attacks on the Reduced Grøstl Hash Function	350
<i>Florian Mendel, Christian Rechberger, Martin Schl��ffer, and S��ren S. Thomsen</i>	

Symmetric Cryptography

The Sum of CBC MACs Is a Secure PRF	366
<i>Kan Yasuda</i>	
On Fast Verification of Hash Chains	382
<i>Dae Hyun Yum, Jin Seok Kim, Pil Joong Lee, and Sung Je Hong</i>	
Author Index	397