

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

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Alfred Menezes (Ed.)

Topics in Cryptology – CT-RSA 2005

The Cryptographers' Track at the RSA Conference 2005
San Francisco, CA, USA, February 14-18, 2005
Proceedings

Volume Editor

Alfred Menezes
University of Waterloo
Department of Combinatorics and Optimization
Waterloo, Ontario, N2L 3G1, Canada
E-mail: ajmenez@uwaterloo.ca

Library of Congress Control Number: 2004117506

CR Subject Classification (1998): E.3, G.2.1, D.4.6, K.6.5, K.4.4, F.2.1-2, C.2, J.1

ISSN 0302-9743

ISBN 3-540-24399-2 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 is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11377726 06/3142 5 4 3 2 1 0

Preface

The RSA Conference is attended by over 10,000 security professionals each year. The Cryptographers' Track (CT-RSA), one of several parallel tracks at the conference, provides an excellent opportunity for cryptographers to showcase their research to a wide audience. CT-RSA 2005 was the fifth year of the Cryptographers' Track.

The selection process for the CT-RSA program is the same as for other cryptography research conferences. This year, the program committee selected 23 papers from 74 submissions (two of which were later withdrawn) that covered all aspects of cryptography. The program also included two invited talks by Cynthia Dwork and Moti Yung. These proceedings contain the revised versions of the selected papers. The revisions were not checked, and so the authors (and not the committee) bear full responsibility for the contents of their papers.

I am very grateful to the program committee for their very conscientious efforts to review each paper fairly and thoroughly. The initial review stage was followed by a tremendous amount of discussion which contributed to our high confidence in our judgements. Thanks also to the many external reviewers whose names are listed in the following pages. My apologies to those whose names were inadvertently omitted from this list.

Thanks to Eddie Ng for maintaining the submission server and the Web review system. The submission software was written by Chanathip Namprempre, and the Web review software by Wim Moreau and Joris Claessens. Thanks to Alfred Hofmann and his colleagues at Springer for the timely production of these proceedings. Finally, it is my pleasure to acknowledge Ari Juels and Mike Szydlo of RSA Laboratories for their assistance and cooperation during the past seven months.

October 2004

Alfred Menezes

RSA Cryptographers' Track 2005

February 14–18, 2005, San Francisco, CA, USA

The RSA Conference 2005 was organized by RSA Security Inc. and its partner organizations around the world. The Cryptographers' Track was organized by RSA Laboratories.

Program Chair

Alfred Menezes, University of Waterloo, Canada

Program Committee

Masayuki Abe	NTT Laboratories, Japan
Paulo Barreto	Scopus Tecnologia, Brazil
Alex Biryukov	K.U.Leuven, Belgium
John-Sebastien Coron	Gemplus, France
Steven Galbraith	Royal Holloway, University of London, UK
Amir Herzberg	Bar-Ilan University, Israel
Yuval Ishai	Technion, Israel
Stanislaw Jarecki	UC Irvine, USA
Lars Knudsen	Technical University of Denmark
Kaoru Kurosawa	Ibaraki University, Japan
Tanja Lange	Ruhr-Universität, Bochum, Germany
Helger Lipmaa	Helsinki University of Technology, Finland
Philip MacKenzie	DoCoMo, USA
Tal Malkin	Columbia University, USA
Wenbo Mao	HP Laboratories, UK
Ilya Mironov	Microsoft Research, USA
Josef Pieprzyk	Macquarie University, Australia
Palash Sarkar	Indian Statistical Institute, India
Jessica Staddon	Palo Alto Research Center, USA
Rene Struik	Certicom, Canada
Michael Szydlo	RSA Laboratories, USA
Tsuyoshi Takagi	TU Darmstadt, Germany

Steering Committee

Marc Joye	Gemplus, France
Tatsuaki Okamoto	NTT, Japan
Bart Preneel	K.U.Leuven, Belgium
Ron Rivest	MIT, USA
Moti Yung	Columbia University, USA

External Reviewers

Toru Akishita	David Hwang	Yasuhiro Ohtaki
Alexandr Andoni	Kouichi Itoh	Akira Otsuka
Roberto Avanzi	Tetsu Iwata	Pascal Paillier
Sara Bitan	Antoine Joux	Zulfikar Ramzan
Alexandra Boldyreva	Masanobu Katagi	Leo Reyzin
Reinier Bröker	Jonathan Katz	Matt Robshaw
Daniel Brown	Jeff King	Markku-Juhani Saarinen
Bertrand Byramjee	Lea Kissner	Taiichi Saito
Christophe De Canniere	Yuichi Komano	Akashi Satoh
Dario Catalano	Hugo Krawczyk	Kai Schramm
Liqun Chen	Caroline Kudla	Daniel Schepers
Joe Cho	Joseph Lano	Igor Shparlinski
Carlos Cid	Kerstin Lemke	Nigel Smart
Mathieu Ciet	John Linn	Angelos Stavrou
Scott Contini	Anna Lysyanskaya	Ron Steinfeld
Claus Diem	Dahlia Malkhi	Makoto Sugita
Yevgeniy Dodis	Daniele Micciancio	Matti Tommiska
Eiichiro Fujisaki	Anton Mityagin	Eran Tromer
Juan Garay	Atsuko Miyaji	Huaxiong Wang
Craig Gentry	David Molnar	Michael Wiener
Philippe Golle	Michael Mueller	Kai Wirt
Shai Halevi	Jorge Nakahara	Christopher Wolf
Darrel Hankerson	Wakaha Ogata	Shoko Yonezawa
Heng Swee Huay	Kazuo Ohata	Yunlei Zhao

Table of Contents

Invited Talks

Sub-linear Queries Statistical Databases: Privacy with Power	1
<i>Cynthia Dwork</i>	
Malicious Cryptography: Kleptographic Aspects	7
<i>Adam Young and Moti Yung</i>	

Cryptanalysis

Resistance of SNOW 2.0 Against Algebraic Attacks	19
<i>Olivier Billet and Henri Gilbert</i>	
A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes	29
<i>An Braeken, Christopher Wolf, and Bart Preneel</i>	
Hold Your Sessions: An Attack on Java Session-Id Generation	44
<i>Zvi Gutterman and Dahlia Malkhi</i>	
Update on SHA-1	58
<i>Vincent Rijmen and Elisabeth Oswald</i>	
A Fast Correlation Attack on the Shrinking Generator	72
<i>Bin Zhang, Hongjun Wu, Dengguo Feng, and Feng Bao</i>	

Public-Key Encryption

Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption	87
<i>Dan Boneh and Jonathan Katz</i>	
A Generic Conversion with Optimal Redundancy	104
<i>Yang Cui, Kazukuni Kobara, and Hideki Imai</i>	
Choosing Parameter Sets for NTRUEncrypt with NAEP and SVES-3	118
<i>Nick Howgrave-Graham, Joseph H. Silverman, and William Whyte</i>	

Signature Schemes

Foundations of Group Signatures: The Case of Dynamic Groups	136
<i>Mihir Bellare, Haixia Shi, and Chong Zhang</i>	
Time-Selective Convertible Undeniable Signatures	154
<i>Fabien Laguillaumie and Damien Vergnaud</i>	

Design Principles

On Tolerant Cryptographic Constructions	172
<i>Amir Herzberg</i>	

Password-Based Protocols

Simple Password-Based Encrypted Key Exchange Protocols	191
<i>Michel Abdalla and David Pointcheval</i>	

Hard Bits of the Discrete Log with Applications to Password Authentication	209
<i>Philip Mackenzie and Sarvar Patel</i>	

Proofs for Two-Server Password Authentication	227
<i>Michael Szydlo and Burton Kaliski</i>	

Design and Analysis of Password-Based Key Derivation Functions	245
<i>Frances F. Yao and Yiqun Lisa Yin</i>	

Pairings

A New Two-Party Identity-Based Authenticated Key Agreement	262
<i>Noel McCullagh and Paulo S.L.M. Barreto</i>	

Accumulators from Bilinear Pairings and Applications	275
<i>Lan Nguyen</i>	

Computing the Tate Pairing	293
<i>Michael Scott</i>	

Fast and Proven Secure Blind Identity-Based Signcryption from Pairings . .	305
<i>Tsz Hon Yuen and Victor K. Wei</i>	

Efficient and Secure Implementation

A Systematic Evaluation of Compact Hardware Implementations for the Rijndael S-Box	323
<i>Nele Mentens, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede</i>	

CryptoGraphics: Secret Key Cryptography Using Graphics Cards	334
<i>Debra L. Cook, John Ioannidis, Angelos D. Keromytis, and Jake Luck</i>	

Side-Channel Leakage of Masked CMOS Gates	351
<i>Stefan Mangard, Thomas Popp, and Berndt M. Gammel</i>	

New Minimal Weight Representations for Left-to-Right Window Methods .	366
<i>James A. Muir and Douglas R. Stinson</i>	

Author Index	385
------------------------	-----