Lecture Notes in Computer Science 3152

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

Matt Franklin (Ed.)

Advances in Cryptology – CRYPTO 2004

24th Annual International Cryptology Conference
Santa Barbara, California, USA, August 15-19, 2004
Proceedings

Springer

Volume Editor

Matt Franklin
University of California, Department of Computer Science
One Shields Avenue, Davis, CA 95616, USA
E-mail: franklin@cs.ucdavis.edu

Library of Congress Control Number: Applied for

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

ISSN 0302-9743
ISBN 3-540-22668-0 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

© International Association for Cryptologic Research
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN: 11302322 06/3142 5 4 3 2 1 0

Preface

Crypto 2004, the 24th Annual Crypto Conference, was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of California at Santa Barbara.

The program committee accepted 33 papers for presentation at the conference. These were selected from a total of 211 submissions. Each paper received at least three independent reviews. The selection process included a Web-based discussion phase, and a one-day program committee meeting at New York University.

These proceedings include updated versions of the 33 accepted papers. The authors had a few weeks to revise them, aided by comments from the reviewers. However, the revisions were not subjected to any editorial review.

The conference program included two invited lectures. Victor Shoup's invited talk was a survey on chosen ciphertext security in public-key encryption. Susan Landau's invited talk was entitled "Security, Liberty, and Electronic Communications". Her extended abstract is included in these proceedings.

We continued the tradition of a Rump Session, chaired by Stuart Haber. Those presentations (always short, often serious) are not included here.

I would like to thank everyone who contributed to the success of this conference. First and foremost, the global cryptographic community submitted their scientific work for our consideration. The members of the Program Committee worked hard throughout, and did an excellent job. Many external reviewers contributed their time and expertise to aid our decision-making. James Hughes, the General Chair, was supportive in a number of ways. Dan Boneh and Victor Shoup gave valuable advice. Yevgeniy Dodis hosted the PC meeting at NYU.

It would have been hard to manage this task without the Web-based submission server (developed by Chanathip Namprempre, under the guidance of Mihir Bellare) and review server (developed by Wim Moreau and Joris Claessens, under the guidance of Bart Preneel). Terri Knight kept these servers running smoothly, and helped with the preparation of these proceedings.

June 2004 Matt Franklin

CRYPTO 2004

August 15–19, 2004, Santa Barbara, California, USA

Sponsored by the
International Association for Cryptologic Research (IACR)

in cooperation with
IEEE Computer Society Technical Committee on Security and Privacy,
Computer Science Department, University of California, Santa Barbara

General Chair
James Hughes, StorageTek

Program Chair
Matt Franklin, U.C. Davis, USA

Program Committee

Bill Aiello ..... AT&T Labs, USA
Jee Hea An ..... SoftMax, USA
Eli Biham ..... Technion, Israel
John Black ..... University of Colorado at Boulder, USA
Anne Canteaut ..... INRIA, France
Ronald Cramer ..... University of Aarhus, Denmark
Yevgeniy Dodis ..... New York University, USA
Yuval Ishai ..... Technion, Israel
Lars Knudsen ..... Technical University of Denmark, Denmark
Hugo Krawczyk ..... Technion/IBM, Israel/USA
Pil Joong Lee ..... POSTECH/KT, Korea
Phil MacKenzie ..... Bell Labs, USA
Tal Malkin ..... Columbia University, USA
Willi Meier ..... Fachhochschule Aargau, Switzerland
Daniele Micciancio ..... U.C. San Diego, USA
Ilya Mironov ..... Microsoft Research, USA
Tatsuaki Okamoto ..... NTT, Japan
Rafail Ostrovsky ..... U.C.L.A., USA
Torben Pedersen ..... Cryptomathic, Denmark
Benny Pinkas ..... HP Labs, USA
Bart Preneel ..... Katholieke Universiteit Leuven, Belgium
Alice Silverberg ..... Ohio State University, USA
Nigel Smart ..... Bristol University, UK
David Wagner ..... U.C. Berkeley, USA
Stefan Wolf ..... University of Montreal, Canada

Advisory Members

Dan Boneh (Crypto 2003 Program Chair) ..... Stanford University, USA
Victor Shoup (Crypto 2005 Program Chair) ..... New York University, USA

External Reviewers

Masayuki Abe
Siddhartha Annapuredy
Frederik Armknecht
Daniel Augot
Boaz Barak
Elad Barkan
Amos Beimel
Mihir Bellare
Daniel Bleichenbacher
Dan Boneh
Carl Bosley
Ernie Brickell
Ran Canetti
Jung Hee Cheon
Don Coppersmith
Jean-Sébastien Coron
Nicolas Courtois
Christophe De Cannière
Anand Desai
Simon-Pierre Desrosiers
Irit Dinur
Mario di Raimondo
Orr Dunkelman
Glenn Durfee
Iwan Duursma
Stefan Dziembowski
Andreas Enge
Nelly Fazio
Serge Fehr
Marc Fischlin
Matthias Fitzi
Caroline Fontaine
Michael J. Freedman
Atsushi Fujioka
Eiichiro Fujisaki
Martin Gagne
Steven Galbraith
Juan Garay
Pierrick Gaudry
Rosario Gennaro
Craig Gentry
Shafi Goldwasser
Jovan Golic
Rob Granger
Jens Groth
Stuart Haber
Shai Halevi
Helena Handschuh
Danny Harnik
Johan Hastråd
Alejandro Hevia
Jim Hughes
Yong Ho Hwang
Oleg Izmerly
Markus Jakobsson
Stanislaw Jarecki
Rob Johnson
Yael Tauman Kalai
Jonathan Katz
Dan Kenigsberg
Dmitriy Kharchenko
Aggelos Kiayias
Eike Kiltz
Kihyun Kim
Ted Krovetz
Klaus Kursawe
Eyal Kushilevitz
Joseph Lano
In-Sok Lee
Arjen Lenstra
Yehuda Lindell
Hoi-Kwong Lo
Pierre Loidreau
Anna Lysyanskaya
John Malone-Lee
Dominic Mayers
Marine Minier
Bodo Moeller
Håvard Molland
David Molnar
Tal Mor
Sara Miner More
François Morain
Waka Nagao
Phong Nguyen
Antonio Nicolosi
Jesper Nielsen
Miyako Ohkubo
Kazuo Ohta
Roberto Oliveira
Seong-Hun Paeng
Dan Page
Dong Jin Park
Jae Hwan Park
Joonhah Park
Matthew Parker
Rafael Pass
Kenny Paterson
Erez Petrank
David Pointcheval
Prashant Puniya
Tal Rabin
Haavard Raddum
Zulfikar Ramzan
Oded Regev
Omer Reingold
Renato Renner
Leonid Reyzin
Vincent Rijmen
Phillip Rogaway
Pankaj Rohatgi
Adi Rosen
Karl Rubin
Alex Russell

Amit Sahai
Gorm Salomonsen
Louis Salvail
Tomas Sander
Hovav Shacham
Ronen Shaltiel
Jonghoon Shin
Victor Shoup
Thomas Shrimpton
Berit Skjernaa
Adam Smith
Jerome A. Solinas
Jessica Staddon
Martijn Stam
Jacques Stern
Douglas Stinson
Koutarou Suzuki
Keisuke Tanaka
Edlyn Teske
Christian Tobias
Yuuki Tokunaga
Vinod Vaikuntanathan
Brigitte Vallee
R. Venkatesan
Frederik Vercauteren
Felipe Voloch
Luis von Ahn
Jason Waddle
Shabsi Walfish
Andreas Winter
Christopher Wolf
Juerg Wullschleger
Go Yamamoto
Yeon Hyeong Yang
Sung Ho Yoo
Young Tae Youn
Dae Hyun Yum
Moti Yung

Table of Contents

Linear Cryptanalysis

On Multiple Linear Approximations 1
Alex Biryukov, Christophe De Cannière, and Michaël Quisquater

Feistel Schemes and Bi-linear Cryptanalysis 23
Nicolas T. Courtois

Group Signatures

Short Group Signatures 41
Dan Boneh, Xavier Boyen, and Hovav Shacham

Signature Schemes and Anonymous Credentials from Bilinear Maps 56
Jan Camenisch and Anna Lysyanskaya

Foundations

Complete Classification of Bilinear Hard-Core Functions 73
Thomas Holenstein, Ueli Maurer, and Johan Sjödin

Finding Collisions on a Public Road,
or Do Secure Hash Functions Need Secret Coins? 92
Chun-Yuan Hsiao and Leonid Reyzin

Security of Random Feistel Schemes with 5 or More Rounds 106
Jacques Patarin

Efficient Representations

Signed Binary Representations Revisited 123
Katsuyuki Okeya, Katja Schmidt-Samoa, Christian Spahn,
and Tsuyoshi Takagi

Compressed Pairings 140
Michael Scott and Paulo S.L.M. Barreto

Asymptotically Optimal Communication for Torus-Based Cryptography . . 157
Marten van Dijk and David Woodruff

How to Compress Rabin Ciphertexts and Signatures (and More) 179
Craig Gentry

Public Key Cryptanalysis

On the Bounded Sum-of-Digits Discrete Logarithm Problem in Finite Fields 201
Qi Cheng

Computing the RSA Secret Key Is Deterministic Polynomial Time Equivalent to Factoring 213
Alexander May

Zero-Knowledge

Multi-trapdoor Commitments and Their Applications to Proofs of Knowledge Secure Under Concurrent Man-in-the-Middle Attacks 220
Rosario Gennaro

Constant-Round Resettable Zero Knowledge with Concurrent Soundness in the Bare Public-Key Model 237
Giovanni Di Crescenzo, Giuseppe Persiano, and Ivan Visconti

Zero-Knowledge Proofs and String Commitments Withstanding Quantum Attacks 254
Ivan Damgård, Serge Fehr, and Louis Salvail

The Knowledge-of-Exponent Assumptions and 3-Round Zero-Knowledge Protocols 273
Mihir Bellare and Adriana Palacio

Hash Collisions

Near-Collisions of SHA-0 290
Eli Biham and Rafi Chen

Multicollisions in Iterated Hash Functions. Application to Cascaded Constructions 306
Antoine Joux

Secure Computation

Adaptively Secure Feldman VSS and Applications to Universally-Composable Threshold Cryptography 317
Masayuki Abe and Serge Fehr

Round-Optimal Secure Two-Party Computation 335
Jonathan Katz and Rafail Ostrovsky

Invited Talk

Security, Liberty, and Electronic Communications 355
Susan Landau

Stream Cipher Cryptanalysis

An Improved Correlation Attack Against Irregular Clocked and Filtered Keystream Generators 373
Håvard Molland and Tor Helleseth

Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers 390
Philip Hawkes and Gregory G. Rose

Faster Correlation Attack on Bluetooth Keystream Generator E0 407
Yi Lu and Serge Vaudenay

Public Key Encryption

A New Paradigm of Hybrid Encryption Scheme 426
Kaoru Kurosawa and Yvo Desmedt

Secure Identity Based Encryption Without Random Oracles 443
Dan Boneh and Xavier Boyen

Bounded Storage Model

Non-interactive Timestamping in the Bounded Storage Model 460
Tal Moran, Ronen Shaltiel, and Amnon Ta-Shma

Key Management

IPAKE: Isomorphisms for Password-Based Authenticated Key Exchange . . . 477
Dario Catalano, David Pointcheval, and Thomas Pornin

Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes 494
Yevgeniy Dodis, Rosario Gennaro, Johan Håstad, Hugo Krawczyk, and Tal Rabin

Efficient Tree-Based Revocation in Groups of Low-State Devices 511
Michael T. Goodrich, Jonathan Z. Sun, and Roberto Tamassia

Computationally Unbounded Adversaries

Privacy-Preserving Datamining on Vertically Partitioned Databases 528
Cynthia Dwork and Kobbi Nissim

Optimal Perfectly Secure Message Transmission 545
K. Srinathan, Arvind Narayanan, and C. Pandu Rangan

Pseudo-signatures, Broadcast, and Multi-party Computation from Correlated Randomness 562
Matthias Fitzi, Stefan Wolf, and Jürg Wullschleger

Author Index 579