Lecture Notes in Computer Science 4965

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
University of Dortmund, Germany

Madhu Sudan
Massachusetts Institute of Technology, 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

Nigel Smart (Ed.)

Advances in Cryptology – EUROCRYPT 2008

27th Annual International Conference on the Theory and Applications of Cryptographic Techniques
Istanbul, Turkey, April 13-17, 2008
Proceedings

Springer

Volume Editor

Nigel Smart
University of Bristol
Department of Computer Science
Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK
E-mail: nigel@cs.bris.ac.uk

Library of Congress Control Number: 2008923745

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

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-78966-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-78966-6 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

springer.com

© International Association for Cryptologic Research 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12251506 06/3180 5 4 3 2 1 0

Preface

These are the proceedings of Eurocrypt 2008, the 27th Annual IACR Eurocrypt Conference. The conference was sponsored by the International Association for Cryptologic Research (*www.iacr.org*), this year in cooperation with Tubitak (*www.tubitak.gov.tr*).

The Eurocrypt 2008 Program Committee (PC) consisted of 28 members whose names are listed on the next page. There were 163 papers submitted to the conference and the PC chose 31 of them. Each paper was assigned to at least three PC members, who either handled it themselves or assigned it to an external referee. After the reviews were submitted, the committee deliberated both online for several weeks and finally in a face-to-face meeting held in Bristol. Papers were refereed anonymously, with PC papers having a minimum of five reviewers. All of our deliberations were aided by the *Web Submission and Review Software* written and maintained by Shai Halevi. In addition to notification of the decision of the committee, authors received reviews; the default for any report given to the committee was that it should be available to the authors as well.

The committee decided to give the Best Paper Award to Ben Smith for his paper "Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves." The conference program also included two invited lectures: one by Andy Clark entitled "From Gamekeeping to Poaching - Information Forensics and Associated Challenges," and the other by Clifford Cocks on "The Growth and Development of Public Key Cryptography."

I wish to thank all the people who made the conference possible. First and foremost the authors who submitted their papers. The hard task of reading, commenting, debating and finally selecting the papers for the conference fell on the PC members. Without the hard work of the committee members and their respective sub-reviewers the whole process would be so much harder to organize. I thank Shai Halevi for handling the submissions and reviews server, and for also organizing the phone conference for those people unable to attend the Bristol PC meeting in person. I am also grateful to members of the IACR board, and previous PC Chairs, who shared their invaluable advice with me and to A. Murat Apohan and the rest of the local Organizing Committee.

Finally, I would like to say that it has been a great honor to be PC Chair for Eurocrypt 2008 and I only hope the readers of the following papers obtain as much enjoyment as I did in selecting them.

February 2008 Nigel Smart

EuroCrypt 2008

Istanbul, Turkey, April 13–17

Sponsored by *International Association for Cryptologic Research*

Organized in cooperation with *Tubitak*

General Chair

A. Murat Apohan

Program Chair

Nigel Smart, University of Bristol

Program Committee

Sasha Boldyreva	Georgia Institute of Technology
Orr Dunkelman	K.U. Leuven
Serge Fehr	CWI
Eiichiro Fujisaki	NTT
Shai Halevi	IBM
Antoine Joux	DGA and Université de Versailles
Marc Joye	Thomson R&D
Jonathan Katz	University of Maryland
Lars R. Knudsen	DTU Mathematics
Yoshi Kohno	University of Washington
Arjen Lenstra	EPFL and Alcatel-Lucent Bell Laboratories
Stefan Lucks	B.-U. Weimar
Anna Lysyanskaya	Brown University
Wenbo Mao	EMC Research China
Alfred Menezes	Univeristy of Waterloo
Atsuko Miyaji	JAIST
David Naccache	ENS
Gregory Neven	K.U. Leuven
Phong Nguyen	CNRS and ENS
Kenny Paterson	Royal Holloway, University of London
Matt Robshaw	Orange Labs
Ahmad-Reza Sadeghi	Ruhr University Bochum
Rei Safavi-Naini	University of Calgary

Berry Schoenmakers	T.U. Eindhoven
Hovav Shacham	UC San Diego
Brent Waters	SRI
Stefan Wolf	ETH Zurich
Moti Yung	Google

External Reviewers

Michel Abdalla
Masayuki Abe
Omran Ahmadi
Elena Andreeva
Kazumaro Aoki
Frederik Armknecht
Giuseppe Ateniese
Nuttapong Attrapadung
Roberto Avanzi
Mira Belenkiy
Côme Berbain
Guido Blady
Andrey Bogdanov
Colin Boyd
Matt Campagna
Sébastien Canard
Ran Canetti
David Cash
Dario Catalano
Nishanth Chandran
Melissa Chase
Sanjit Chatterjee
Benoît Chevallier-Mames
Carlos Cid
Scott Contini
Jason Crampton
Ivan Damgård
Cécile Delerablée
Claus Diem
Yevgeniy Dodis
Dror Eiger
Jean-Charles Faugère
Marc Fischlin
Matthias Fitzi
Ewan Fleischmann
Pierre-Alain Fouque
Georg Fuchsbauer
Eiichiro Fujisaki
Jun Furukawa
Steven Galbraith
Nicolas Gama
Pierrick Gaudry
Praveen Gauravaram
Rosario Gennaro
Henri Gilbert
Vanessa Gratzer
Robbert de Haan
Goichiro Hanaoka
Darrel Hankerson
Guillaume Hanrot
Aram Harrow
Johan Håstad
Florian Hess
Jason Hinek
Martin Hirt
Dennis Hofheinz
Susan Hohenberger
Nick Howgrave-Graham
Yuval Ishai
Mitsugu Iwamoto
Stas Jarecki
Shaoquan Jiang
Ellen Jochemsz
Pascal Junod
Ulrich Kühn
Marcelo Kaihara
Alexandre Karlov
Mohamed Karroumi
Shahram Khazaei
Hiroaki Kikuchi
Eike Kiltz
Mehmet Kiraz
Takashi Kitagawa
Kazukuni Kobara

Hiroki Koga
Markulf Kohlweiss
Vlad Kolesnikov
Yuichi Komano
Matthias Krause
Hugo Krawczyk
Virendra Kumar
Alptekin Küpçü
Kaoru Kurosawa
Tanja Lange
Kristin Lauter
Stephane Lemieux
Gaetan Leurent
Eric Levieil
Jun Li
Benoît Libert
Hans Loehr
Bodo Möller
Phil MacKenzie
Subhomay Maitra
Mark Manulis
Sandra Marcello
Keith Martin
Ueli Maurer
Alexander May
Daniele Micciancio
Lorenz Minder
Toshiyuki Miyazawa
Sean Murphy
Toru Nakanishi
Jesper Buus Nielsen
Svetla Nikova
Ryo Nishimaki
Masayuki Numao
Wakaha Ogata
Koji Okada
Tatsuaki Okamoto
Elisabeth Oswald
Roger Oyono
Carles Padró
Dan Page
Pascal Paillier
Adriana Palacio
Omkant Pandey
Rafael Pass
Chris Peikert
Olivier Pereira
Ludovic Perret
Krzysztof Pietrzak
David Pointcheval
Marcin Poturalski
Manoj Prabhakaran
Tal Rabin
Vaibhav Rajan
Vibhor Rastogi
Dominik Raub
Eric Rescorla
Reza Reyhanitabar
Leonid Reyzin
Thomas Ristenpart
Louis Salvail
Jorge Villar Santos
Yu Sasaki
Nitesh Saxena
Rüdiger Schack
Werner Schindler
Yannick Seurin
Siamak Shahandashti
Emily Shen
Junji Shikata
Jamshid Shokrollahi
Thomas Shrimpton
Andrey Sidorenko
Adam Smith
Masakazu Soshi
Igor Spharlinski
Michal Sramka
Martijn Stam
Heiko Stamer
François-Xavier Standaert
Dirk Stegemann
Willy Susilo
Koutarou Suzuki
Keisuke Tanaka
Emin Tatli
Yael Tauman-Kalai
Stefano Tessaro
Soeren Steffen Thomsen
Tomas Toft
Frederik Vercauteren

Damien Vergnaud
José Villegas
Marcus Wagner
Bogdan Warinschi
Hoeteck Wee
Daniel Wichs
Andreas Winter
Christopher Wolf
David Woodruff
Jürg Wullschleger
Brecht Wyseur
Keita Xagawa
Go Yamamoto
Kan Yasuda
Kazuki Yoneyama
Rui Zhang
Yunlei Zhao
Sebastien Zimmer

Table of Contents

A Practical Attack on KeeLoq 1
Sebastiaan Indesteege, Nathan Keller, Orr Dunkelman, Eli Biham, and Bart Preneel

Key Recovery on Hidden Monomial Multivariate Schemes 19
Pierre-Alain Fouque, Gilles Macario-Rat, and Jacques Stern

Predicting Lattice Reduction 31
Nicolas Gama and Phong Q. Nguyen

Efficient Sequential Aggregate Signed Data 52
Gregory Neven

Proving Tight Security for Rabin–Williams Signatures 70
Daniel J. Bernstein

Threshold RSA for Dynamic and Ad-Hoc Groups 88
Rosario Gennaro, Shai Halevi, Hugo Krawczyk, and Tal Rabin

Towards Key-Dependent Message Security in the Standard Model 108
Dennis Hofheinz and Dominique Unruh

The Twin Diffie-Hellman Problem and Applications 127
David Cash, Eike Kiltz, and Victor Shoup

Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products 146
Jonathan Katz, Amit Sahai, and Brent Waters

Isogenies and the Discrete Logarithm Problem in Jacobians of Genus 3 Hyperelliptic Curves 163
Benjamin Smith

On the Indifferentiability of the Sponge Construction 181
Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche

A New Mode of Operation for Block Ciphers and Length-Preserving MACs 198
Yevgeniy Dodis, Krzysztof Pietrzak, and Prashant Puniya

Security/Efficiency Tradeoffs for Permutation-Based Hashing 220
Phillip Rogaway and John Steinberger

New Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5 237
Lei Wang, Kazuo Ohta, and Noboru Kunihiro

Collisions for the LPS Expander Graph Hash Function 254
Jean-Pierre Tillich and Gilles Zémor

Second Preimage Attacks on Dithered Hash Functions 270
Elena Andreeva, Charles Bouillaguet, Pierre-Alain Fouque, Jonathan J. Hoch, John Kelsey, Adi Shamir, and Sebastien Zimmer

Efficient Two Party and Multi Party Computation Against Covert Adversaries 289
Vipul Goyal, Payman Mohassel, and Adam Smith

Almost-Everywhere Secure Computation 307
Juan A. Garay and Rafail Ostrovsky

Truly Efficient 2-Round Perfectly Secure Message Transmission Scheme 324
Kaoru Kurosawa and Kazuhiro Suzuki

Protocols and Lower Bounds for Failure Localization in the Internet 341
Boaz Barak, Sharon Goldberg, and David Xiao

$HB^{\#}$: Increasing the Security and Efficiency of HB^{+} 361
Henri Gilbert, Matthew J.B. Robshaw, and Yannick Seurin

Sub-linear Zero-Knowledge Argument for Correctness of a Shuffle 379
Jens Groth and Yuval Ishai

Precise Concurrent Zero Knowledge 397
Omkant Pandey, Rafael Pass, Amit Sahai, Wei-Lung Dustin Tseng, and Muthuramakrishnan Venkitasubramaniam

Efficient Non-interactive Proof Systems for Bilinear Groups 415
Jens Groth and Amit Sahai

Zero-Knowledge Sets with Short Proofs 433
Dario Catalano, Dario Fiore, and Mariagrazia Messina

Strongly Multiplicative Ramp Schemes from High Degree Rational Points on Curves 451
Hao Chen, Ronald Cramer, Robbert de Haan, and Ignacio Cascudo Pueyo

Detection of Algebraic Manipulation with Applications to Robust Secret Sharing and Fuzzy Extractors 471
Ronald Cramer, Yevgeniy Dodis, Serge Fehr, Carles Padró, and Daniel Wichs

Obfuscating Point Functions with Multibit Output 489
Ran Canetti and Ronny Ramzi Dakdouk

Isolated Proofs of Knowledge and Isolated Zero Knowledge 509
Ivan Damgård, Jesper Buus Nielsen, and Daniel Wichs

David and Goliath Commitments: UC Computation for Asymmetric Parties Using Tamper-Proof Hardware 527
Tal Moran and Gil Segev

New Constructions for UC Secure Computation Using Tamper-Proof Hardware 545
Nishanth Chandran, Vipul Goyal, and Amit Sahai

Author Index 563