

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 for Informatics, Saarbruecken, Germany

Steven Galbraith Mridul Nandi (Eds.)

Progress in Cryptology - INDOCRYPT 2012

13th International Conference on Cryptology in India
Kolkata, India, December 9-12, 2012
Proceedings



Springer

Volume Editors

Steven Galbraith
University of Auckland
Department of Mathematics
Private Bag 92019
Auckland 1142, New Zealand
E-mail: s.galbraith@math.auckland.ac.nz

Mridul Nandi
Indian Statistical Institute
Applied Statistics Unit
203 B.T. Road
Kolkata 700108, West Bengal, India
E-mail: mridul@isical.ac.in

ISSN 0302-9743
ISBN 978-3-642-34930-0
DOI 10.1007/978-3-642-34931-7
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-34931-7

Library of Congress Control Number: 2012951708

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

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Indocrypt 2012, the 13th International Conference on Cryptology in India, took place during December 9–12, 2012. It was hosted by the Indian Statistical Institute in Kolkata. The Indocrypt series of conferences began in 2000 under the leadership of Bimal Roy. This series is now well established as an international forum for presenting high-quality cryptography research.

This year 99 papers were submitted for consideration. The authors of the submitted papers were from institutions across 25 countries and five continents.

As in previous years, the submission deadline was split into two: authors were required to register titles and abstracts by July 23, 2012, while final versions of papers had to be submitted by July 28. During that week the titles and abstracts were made available to the Program Committee (PC) to enable them to select their preferred articles for review. Most papers were refereed by three committee members, and papers co-authored by a PC member were refereed by five committee members. We thank Tanja Lange for hosting the ichair system, which was used to manage submissions and online discussions, on her Web server.

The review stage was very tight, with only three weeks for reviewing papers and only two weeks (August 20 to September 1) for the online discussions. It was a difficult challenge for the 33 PC members and 86 sub-reviewers to give every paper a fair assessment in such a short time. A total of 313 referee reports were written, and 314 comments were posted on the online discussions. At the end of the discussion process 28 papers were accepted for the proceedings (five of them conditionally accepted subject to successful revision according to referee suggestions). Authors were notified on September 3 and had around 2 weeks to revise their papers according to the suggestions of the referees.

We would like to thank all the authors of submitted papers for supporting the Indocrypt conference. The best way to support a conference is to submit papers to it and attend it. We also wish to thank the members of the PC and their sub-reviewers (a list is given here) for devoting their time and knowledge to the selection of papers.

The proceedings include the revised versions of the 28 selected papers. Revisions were not checked by the PC and the authors bear the full responsibility for the contents of the respective papers. The proceedings also contain invited papers by Nigel Smart and Vinod Vaikuntanathan, as well as a one-page abstract of the invited lecture by Orr Dunkelman.

The organization of the conference involved many individuals. We express our heart-felt gratitude to the General Chair, Bimal Roy, Director of Indian

Statistical Institute, Kolkata, and Subhamoy Maitra for taking care of the actual hosting of the conference. Members of the Cryptology Research Group at the Indian Statistical Institute provided invaluable secretarial support. Finally, we would like to acknowledge Springer for their active cooperation and timely production of the proceedings.

December 2012

Steven Galbraith
Mridul Nandi

Manoj M. Prabhakaran	University of Illinois, Urbana-Champaign, USA
Bart Preneel	Katholieke Universiteit Leuven, Belgium
C. Pandu Rangan	Indian Statistical Institute, Chennai, India
Christian Rechberger	Danish Technical University, Denmark
Phillip Rogaway	University of California, Davis, USA
Dipanwita Roy Chowdhury	Indian Institute of Technology, Kharagpur, India
Palash Sarkar	Indian Statistical Institute, Kolkata, India
Nicolas Sendrier	INRIA Rocquencourt, France
Damien Stehle	Ecole Normale Superieure de Lyon, France
Dominique Unruh	University of Tartu, Estonia
Fre Vercauteren	Katholieke Universiteit Leuven, Belgium

External Referees

Mohamed Ahmed	Carmit Hazay	Yusuke Sakai
Abdelraheem	Javier Herranz	Subhabrata Samajdar
Elena Andreeva	Huseyin Hisil	Somitra Sanadhya
Diego F. Aranha	Chethan Kamath	Yu Sasaki
Subhadeep Banik	Ferhat Karakoc	Jacob C.N. Schuldt
Guido Bertoni	Sandip Karmakar	Gautham Sekar
Rishiraj Bhattacharyya	Kouhei Kasamatsu	Sharmila Deva Selvi
Zeeshan Bilal	Simon Knellwolf	Sourav Sengupta
Begül Bilgin	Ozgul Kucuk	Jae Hong Seo
Praloy Biswas	Fabien Laguillaumie	Kyoji Shibutani
Julia Borghoff	Gregory Landais	Francesco Sica
Joppe Bos	Cédric Lauradoux	Alice Silverberg
Charles Bouillaguet	Anh Le	Shashank Singh
Christina Boura	Gregor Leander	Ben Smith
Stanislav Bulygin	Benoit Libert	Valentin Suder
Donghoon Chang	Changshe Ma	Enrico Thomae
Yun-An Chang	Subhamoy Maitra	Michael Tunstall
Melissa Chase	Preetha Mathews	Berkant Ustaoglu
Anupam Chattopadhyay	Takahiro Matsuda	Vinod Vaikuntanathan
Ashish Choudhury	Filippo Melzani	Ayineedi Venkateswarlu
Sherman S.M. Chow	Miodrag Mihaljevic	Sree Vivek
Craig Costello	Nicky Mouha	Colin Walter
Abhijit Das	Sean Murphy	Carolyn Whitnall
Christophe Doche	Michael Naehrig	Christopher Wolf
Keita Emura	Souradyuti Paul	Marcin Wójcik
Reza Rezaeian Farashahi	Roel Peeters	Shota Yamada
Thomas Fuhr	Albrecht Petzoldt	Naoto Yanai
David Galindo	Maria Naya Plasencia	Bo-Yin Yang
Sugata Gangopadhyay	Sukhendu Quila	Wei Zhang
Gerhard Hancke	Dhiman Saha	

Sponsoring Institutions

Defence Research and Development Organization (D.R.D.O.), India

Google Inc., India

Microsoft Research, Bangalore

National Board of Higher Mathematics (N.B.H.M.), Mumbai

Reserve Bank of India (R.B.I.), Kolkata

Tata Consultancy Services (T.C.S.), Kolkata

Table of Contents

Invited Papers

How to Compute on Encrypted Data	1
<i>Vinod Vaikuntanathan</i>	
From Multiple Encryption to Knapsacks – Efficient Dissection of Composite Problems	16
<i>Orr Dunkelman</i>	
Using the Cloud to Determine Key Strengths	17
<i>Thorsten Kleinjung, Arjen K. Lenstra, Dan Page, and Nigel P. Smart</i>	

Protocol

A Unified Characterization of Completeness and Triviality for Secure Function Evaluation	40
<i>Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek</i>	
On the Non-malleability of the Fiat-Shamir Transform	60
<i>Sebastian Faust, Markulf Kohlweiss, Giorgia Azzurra Marson, and Daniele Venturi</i>	
Another Look at Symmetric Incoherent Optimal Eavesdropping against BB84	80
<i>Arpita Maitra and Goutam Paul</i>	
On-Line/Off-Line Leakage Resilient Secure Computation Protocols	100
<i>Chaya Ganesh, Vipul Goyal, and Satya Lokam</i>	

Side Channel

Leakage Squeezing of Order Two	120
<i>Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Housseem Maghrebi</i>	
ROSETTA for Single Trace Analysis: Recovery Of Secret Exponent by Triangular Trace Analysis	140
<i>Christophe Clavier, Benoit Feix, Georges Gagnerot, Christophe Giraud, Mylène Roussellet, and Vincent Verneuil</i>	

Hash Functions and Stream Cipher

Collision Attack on the Hamsi-256 Compression Function	156
<i>Mario Lamberger, Florian Mendel, and Vincent Rijmen</i>	
Generalized Iterated Hash Functions Revisited: New Complexity Bounds for Multicollision Attacks	172
<i>Tuomas Kortelainen, Ari Vesanen, and Juha Kortelainen</i>	
A Differential Fault Attack on the Grain Family under Reasonable Assumptions	191
<i>Subhadeep Banik, Subhamoy Maitra, and Santanu Sarkar</i>	
Cryptanalysis of Pseudo-random Generators Based on Vectorial FCSRs	209
<i>Thierry P. Berger and Marine Minier</i>	

Cryptanalysis of Block Ciphers

Faster Chosen-Key Distinguishers on Reduced-Round AES	225
<i>Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean</i>	
The Higher-Order Meet-in-the-Middle Attack and Its Application to the Camellia Block Cipher (Extended Abstract)	244
<i>Jiqiang Lu, Yongzhuang Wei, Jongsung Kim, and Enes Pasalic</i>	
Double-SP Is Weaker Than Single-SP: Rebound Attacks on Feistel Ciphers with Several Rounds	265
<i>Yu Sasaki</i>	
Automatic Search of Truncated Impossible Differentials for Word-Oriented Block Ciphers	283
<i>Shengbao Wu and Mingsheng Wang</i>	

Time Memory Trade-Off

High-Speed Parallel Implementations of the Rainbow Method in a Heterogeneous System	303
<i>Jung Woo Kim, Jungjoo Seo, Jin Hong, Kunsoo Park, and Sung-Ryul Kim</i>	
Computing Small Discrete Logarithms Faster	317
<i>Daniel J. Bernstein and Tanja Lange</i>	

Hardware

Embedded Syndrome-Based Hashing	339
<i>Ingo von Maurich and Tim Güneysu</i>	

Compact Hardware Implementations of the Block Ciphers mCrypton, NOEKEON, and SEA	358
<i>Thomas Plos, Christoph Dobraunig, Markus Hofinger, Alexander Oprisnik, Christoph Wiesmeier, and Johannes Wiesmeier</i>	

Elliptic Curve

Efficient Arithmetic on Elliptic Curves in Characteristic 2	378
<i>David Kohel</i>	
A New Model of Binary Elliptic Curves	399
<i>Hongfeng Wu, Chunming Tang, and Rongquan Feng</i>	
Analysis of Optimum Pairing Products at High Security Levels	412
<i>Xusheng Zhang and Dongdai Lin</i>	
Constructing Pairing-Friendly Genus 2 Curves with Split Jacobian	431
<i>Robert Drylo</i>	

Digital Signature

Faster Batch Forgery Identification	454
<i>Daniel J. Bernstein, Jeroen Doumen, Tanja Lange, and Jan-Jaap Oosterwijk</i>	
Implementing CFS	474
<i>Gregory Landais and Nicolas Sendrier</i>	

Symmetric Key Design and Provable Security

SipHash: A Fast Short-Input PRF	489
<i>Jean-Philippe Aumasson and Daniel J. Bernstein</i>	
A Novel Permutation-Based Hash Mode of Operation FP and the Hash Function SAMOSA	509
<i>Souradyuti Paul, Ekawat Homsirikamol, and Kris Gaj</i>	
Resistance against Adaptive Plaintext-Ciphertext Iterated Distinguishers	528
<i>Ash Bay, Atefeh Mashatan, and Serge Vaudenay</i>	
Sufficient Conditions on Padding Schemes of Sponge Construction and Sponge-Based Authenticated-Encryption Scheme	545
<i>Donghoon Chang</i>	
Author Index	565