

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

Rainer Böhme
Philip W.L. Fong
Reihaneh Safavi-Naini (Eds.)

Information Hiding

12th International Conference, IH 2010
Calgary, AB, Canada, June 28-30, 2010
Revised Selected Papers

Volume Editors

Rainer Böhme
International Computer Science Institute
1947 Center Street, Suite 600
Berkeley, CA 94704, USA
E-mail: rainer.boehme@icsi.berkeley.edu

Philip W.L. Fong
University of Calgary
Department of Computer Science
2500 University Drive NW
Calgary, AB, T2N 1N4, Canada
E-mail: pwl.fong@ucalgary.ca

Reihaneh Safavi-Naini
University of Calgary
Department of Computer Science
2500 University Drive NW
Calgary, AB, T2N 1N4, Canada
E-mail: rei@ucalgary.ca

Library of Congress Control Number: 2010936196

CR Subject Classification (1998): E.3, K.6.5, D.4.6, E.4, H.5.1, I.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN	0302-9743
ISBN-10	3-642-16434-X Springer Berlin Heidelberg New York
ISBN-13	978-3-642-16434-7 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

Preface

IH 2010 was the 12th Information Hiding Conference, held in Calgary, Canada, June 28–30, 2010. This series of conferences started with the First Workshop on Information Hiding, held in Cambridge, UK in May 1996. Since then, the conference locations have alternated between Europe and North America. The conference has been held annually since 2005.

For many years, information hiding has captured the imagination of researchers. This conference series aims to bring together a number of closely related research areas, including digital watermarking, steganography and steganalysis, anonymity and privacy, covert and subliminal channels, fingerprinting and embedding codes, multimedia forensics and counter-forensics, as well as theoretical aspects of information hiding and detection. Since its inception, the conference series has been a premier forum for publishing research in these areas. This volume contains the revised versions of 18 accepted papers (incorporating the comments from members of the Program Committee), and extended abstracts of two (out of three) invited talks.

The conference received 39 anonymous submissions for full papers. The task of selecting 18 of them for presentation was not easy. Each submission was reviewed by at least three members of the Program Committee or external reviewers reporting to a member of the Program Committee. In the case of co-authorship by a Program Committee member, five reviews were sought. There is no need to say that no member of the Program Committee reviewed his or her own work. Each paper was carefully discussed until consensus was reached. The contributions of invited speakers were not formally reviewed.

The invited speakers of IH 2010 were:

Gábor Tardos Capacity of collusion-secure fingerprinting—a trade-off between rate and efficiency

Pim Tuyls Hardware intrinsic security

Boris Škorić Security with noisy data

We would like to thank all those who helped with the organization of the conference and in particular the members of the local organizing team whose unrelenting effort ensured a smooth running of the conference. We would like to thank Kris Narayan for his continued effort in maintaining the Web pages and the iChair submission system, and for lending us a hand whenever it was needed. The conference benefitted from the generous financial support of Alberta Innovates, the European Office of Aerospace Research and Development, Technicolor, and the University of Calgary’s Department of Computer Science, Faculty of Science, and Institute for Security, Privacy & Information Assurance (ISPIA).

We gratefully appreciate the work of the 24 external reviewers and 4 shepherds who lent us their experience in shepherding four conditionally accepted papers.

Finally, we would like to thank the authors of all submitted papers for their hard work, and also all presenters and attendees of the conference whose support ensured the success of this conference.

August 2010

Rainer Böhme
Philip W. L. Fong
Reihaneh Safavi-Naini

Organization

Information Hiding 2010 was hosted by the Department of Computer Science, University of Calgary, Alberta, Canada.

Executive Committee

General Chair	Philip W.L. Fong (University of Calgary, Canada)
Program Chairs	Rainer Böhme (ICSI Berkeley, USA) Rei Safavi-Naini (University of Calgary, Canada)

Program Committee

Ross Anderson	University of Cambridge, UK
Mauro Barni	University of Siena, Italy
Patrick Bas	CNRS, France
Francois Cayre	GIPSA-lab Grenoble, France
Ee-Chien Chang	University of Singapore
Christian Collberg	University of Arizona, USA
Ingemar J. Cox	University College London, UK
Gwenaël Doërr	Technicolor, France
Hany Farid	Dartmouth College, USA
Jessica Fridrich	SUNY Binghamton, USA
Teddy Furon	INRIA, France
Neil F. Johnson	Booz Allen Hamilton & JJTC, USA
Stefan Katzenbeisser	TU Darmstadt, Germany
Darko Kirovski	Microsoft Research, USA
John McHugh	Univ. North Carolina & RedJack LLC, USA
Ira S. Moskowitz	Naval Research Lab, USA
Andreas Pfitzmann	TU Dresden, Germany
Ahmad-Reza Sadeghi	Ruhr-University Bochum, Germany
Phil Sallee	Booz Allen Hamilton, USA
Berry Schoenmakers	TU Eindhoven, The Netherlands
Kaushal Solanki	Mayachitra Inc., USA
Kenneth Sullivan	Mayachitra Inc., USA

Organizing Team

Local Organizers	Mohd Anwar, Mina Askari, Martin Gagné, Kris Narayan, Camille Sinanan
External Advice	Stefan Katzenbeisser (TU Darmstadt)
Volunteers	Mohsen Alimomeni, Hoi Le, Mohammed Tuhin

External Reviewers

André Adelsbach

Hadi Ahmadi

Gerard Allwein

Manuela Berg

Stefan Berthold

Tomas Filler

Elke Franz

Martin Gagne

Steven J. Greenwald

Christian Grothoff

Stefan Köpsell

Matthias Kirchner

Yali Liu

Hans Löhr

Cathy Meadows

Bartolomeo Montrucchio

Kris Narayan

Richard E. Newman

Dagmar Schönfeld

Haya Shulman

Boris Škorić

Robin Sommer

Andreas Westfeld

Antje Winkler

Shepherds

Rainer Böhme

Christian Grothoff

Teddy Furon

Matthias Kirchner

ICSI Berkeley, USA

TU München, Germany

INRIA, France

TU Dresden, Germany

Sponsoring Institutions

Alberta Innovates — Technology Future, Edmonton, Canada

European Office of Aerospace Research and Development, London, UK

Technicolor S. A., France

University of Calgary (Department of CS, Faculty of Science, ISPIA)

Table of Contents

FPGA Time-Bounded Unclonable Authentication	1
<i>Mehrdad Majzoobi, Ahmed Elnably, and Farinaz Koushanfar</i>	
A Unified Submodular Framework for Multimodal IC Trojan Detection	17
<i>Farinaz Koushanfar, Azalia Mirhoseini, and Yousra Alkabani</i>	
A Secure and Robust Approach to Software Tamper Resistance	33
<i>Sudeep Ghosh, Jason D. Hiser, and Jack W. Davidson</i>	
Security with Noisy Data (Extended Abstract of Invited Talk)	48
<i>Boris Škorić</i>	
Detection of Copy-Rotate-Move Forgery Using Zernike Moments	51
<i>Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee</i>	
Scene Illumination as an Indicator of Image Manipulation	66
<i>Christian Riess and Elli Angelopoulou</i>	
Capacity of Collusion Secure Fingerprinting — A Tradeoff Between Rate and Efficiency (Extended Abstract of Invited Talk)	81
<i>Gábor Tardos</i>	
Short Collusion-Secure Fingerprint Codes Against Three Pirates	86
<i>Koji Nuida</i>	
Tardos's Fingerprinting Code over AWGN Channel	103
<i>Minoru Kuribayashi</i>	
Steganalysis Using Partially Ordered Markov Models	118
<i>Jennifer Davidson and Jaikishan Jalan</i>	
The Influence of the Image Basis on Modeling and Steganalysis Performance	133
<i>Valentin Schwamberger, Pham Hai Dang Le, Bernhard Schölkopf, and Matthias O. Franz</i>	
The Square Root Law in Stegosystems with Imperfect Information	145
<i>Andrew D. Ker</i>	
Using High-Dimensional Image Models to Perform Highly Undetectable Steganography	161
<i>Tomáš Pevný, Tomáš Filler, and Patrick Bas</i>	
Obtaining Higher Rates for Steganographic Schemes While Maintaining the Same Detectability	178
<i>Anindya Sarkar, Kaushal Solanki, and B.S. Manjunath</i>	

Robust and Undetectable Steganographic Timing Channels for i.i.d. Traffic	193
<i>Yali Liu, Dipak Ghosal, Frederik Armknecht, Ahmad-Reza Sadeghi, Steffen Schulz, and Stefan Katzenbeisser</i>	
STBS: A Statistical Algorithm for Steganalysis of Translation-Based Steganography	208
<i>Peng Meng, Liusheng Hang, Zhili Chen, Yuchong Hu, and Wei Yang</i>	
The Reverse Statistical Disclosure Attack	221
<i>Nayantara Malleesh and Matthew Wright</i>	
Security Analysis of ISS Watermarking Using Natural Scene Statistics	235
<i>Dong Zhang, Jiangqun Ni, Qiping Zeng, Dah-Jye Lee, and Jiwu Huang</i>	
Provably Secure Spread-Spectrum Watermarking Schemes in the Known Message Attack Framework	249
<i>Jian Cao and Jiwu Huang</i>	
A New Spread Spectrum Watermarking Scheme to Achieve a Trade-Off between Security and Robustness	262
<i>Jian Cao, Jiwu Huang, and Jiangqun Ni</i>	
Author Index	277