

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, 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, Zürich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

More information about this series at <http://www.springer.com/series/7410>

Mark Manulis · Ahmad-Reza Sadeghi  
Steve Schneider (Eds.)

# Applied Cryptography and Network Security

14th International Conference, ACNS 2016  
Guildford, UK, June 19–22, 2016  
Proceedings

*Editors*

Mark Manulis  
Department of Computer Science  
University of Surrey  
Guildford  
UK

Steve Schneider  
Department of Computer Science  
University of Surrey  
Guildford  
UK

Ahmad-Reza Sadeghi  
CASED  
Technische Universität Darmstadt  
Darmstadt, Hessen  
Germany

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-39554-8              ISBN 978-3-319-39555-5 (eBook)  
DOI 10.1007/978-3-319-39555-5

Library of Congress Control Number: 2015958852

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing Switzerland 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer International Publishing AG Switzerland

# Preface

The 14th International Conference on Applied Cryptography and Network Security, ACNS 2016, took place June 19–22, 2016, in Guildford, UK, and was organized by the Surrey Centre for Cyber Security (SCCS) at the University of Surrey.

ACNS is an annual conference focusing on original research in applied cryptography, cyber security, and privacy. Both academic research with high relevance to real-world problems and developments in industrial and technical frontiers fall within the scope of the conference.

ACNS 2016 received 183 submissions, all of which were reviewed by the Program Committee. Each of the 49 Program Committee members was assigned an average of 11 submissions for review. Each paper was assigned to at least three reviewers, while submissions co-authored by Program Committee members were assigned to at least four reviewers. The Program Committee was helped by the reports and opinions of 138 external reviewers. The submission process was not anonymous and author names were visible to all reviewers. The review process was organized and managed through EasyChair. The reviewers were asked to declare any conflicts of interest for all submissions in the beginning of the process. The selection process was very competitive and after highly interactive discussions and a careful deliberation, 35 papers were selected by the Program Committee for presentation at the conference. This puts the acceptance rate of ACNS 2016 at 19 %.

The ACNS 2016 program included two invited talks: “Securing Positioning: From GPS to IoT” by Srdjan Capkun from ETH Zurich and “Foundations of Hardware-Based Attested Computation and Applications of SGX” by Bogdan Warinschi from Bristol University. The prize for the Best Student Paper was awarded to Elena Kirshanova and Friedrich Wiemer for their paper “Parallel Implementation of BDD Enumeration for LWE” co-authored with Alexander May.

ACNS 2016 was organized by Mark Manulis and Ahmad-Reza Sadeghi, who served as program chairs, selected the Program Committee, and led their efforts in choosing papers that you will find in this volume, and by Steve Schneider, who served as general chair and was helped in the local organization by Anna-Lisa Ferrara and Shujun Li.

The ACNS 2016 chairs would like to thank everyone who contributed to the success of the conference. We are grateful to the Program Committee and external reviewers for their commitment, hard work, and enthusiasm to ensure that each paper received a thorough and fair review. Last but not least, we wish to thank all conference participants for making ACNS 2016 an enjoyable experience.

June 2016

Mark Manulis  
Ahmad-Reza Sadeghi  
Steve Schneider

# ACNS 2016

## 14th International Conference on Applied Cryptography and Network Security Guildford, UK, June 19–22, 2016

### General Chair

Steve Schneider                      University of Surrey, UK

### Program Chairs

Mark Manulis                          University of Surrey, UK  
Ahmad-Reza Sadeghi                TU Darmstadt, Germany

### Program Committee

Frederik Armknecht	University of Mannheim, Germany
Giuseppe Ateniese	Stevens Institute of Technology, USA
Elias Athanasopoulos	Vrije Universiteit Amsterdam, The Netherlands
Man Ho Au	Hong Kong Polytechnic University, China
Liqun Chen	Hewlett-Packard Laboratories, UK
Sherman S.M. Chow	Chinese University of Hong Kong, China
Mauro Conti	University of Padua, Italy
Lucas Davi	TU Darmstadt, Germany
Alexandra Dmitrienko	ETH Zurich, Switzerland
Michael Franz	University of California, Irvine, USA
Sebastian Gajek	NEC Laboratories Europe, Germany
Jens Groth	University College London, UK
Goichiro Hanaoka	AIST, Japan
Feng Hao	Newcastle University, UK
Michael Huth	Imperial College London, UK
Tibor Jager	Ruhr University Bochum, Germany
Yier Jin	University of Central Florida, USA
Aniket Kate	Purdue University, USA
Stefan Katzenbeisser	TU Darmstadt, Germany
Negar Kiyavash	University of Illinois, USA
Vladimir Kolesnikov	Bell Laboratories, USA
Mark Manulis	University of Surrey, UK
Ivan Martinovic	University of Oxford, UK

Azalia Mirhoseini	Rice University, USA
Atsuko Miyaji	JAIST, Japan
Payman Mohassel	University of Calgary, Canada
Jörn Müller-Quade	Karlsruhe Institute of Technology, Germany
David Naccache	Ecole Normale Supérieure, France
Michael Naehrig	Microsoft Research Redmond, USA
Hamed Okhravi	MIT Lincoln Laboratory, USA
Claudio Orlandi	Aarhus University, Denmark
Panos Papadimitratos	KTH Royal Institute of Technology, Sweden
Thomas Peyrin	Nanyang Technological University, Singapore
Bertram Poettering	Ruhr University Bochum, Germany
Bart Preneel	KU Leuven, Belgium
Jeyavijayan Rajendran	University of Texas at Dallas, USA
Christian Rechberger	Technical University of Denmark, Denmark
Peter Y. Ryan	University of Luxembourg, Luxembourg
Rei Safavi-Naini	University of Calgary, Canada
Thomas Schneider	TU Darmstadt, Germany
Ozgur Sinanoglu	NYU Abu Dhabi, UAE
Douglas Stebila	McMaster University, Canada
Thorsten Strufe	TU Dresden, Germany
Gang Tan	Penn State University, USA
Vanessa Teague	University of Melbourne, Australia
Mehdi Tibouchi	NTT Secure Platform Laboratories, Japan
Ivan Visconti	University of Salerno, Italy
Wenyuan Xu	University of South Carolina, USA
Moti Yung	Snapchat, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

## External Reviewers

Dirk Achenbach	Colin Boyd
Sk Subidh Ali	Ferdinand Brasser
Moreno Ambrosini	Brandon Broadnax
Kanishka Ariyapala	Luigi Catuogno
Afonso Arriaga	Andrea Cerulli
Tomer Ashur	Pyrros Chaidos
Nuttapong Attrapadung	Sze Yiu Chau
Saikrishna Badrinarayanan	Zhuo Chen
David Barrera	Michele Ciampi
Marc Beunardeau	Alberto Compagno
David Bigelow	Heng Cui
Begül Bilgin	Daniel Demmler
Kaidel Bjoern	Alexander Detrano
Jonathan Bootle	Fraser Dickin
Joppe Bos	Christoph Dobraunig

Benjamin Dowling  
Maria Eichelseder  
Keita Emura  
Hossein Fereidooni  
Manuel Fersch  
Houda Ferradi  
Yuichi Futa  
Rémi Géraud  
Essam Ghadafi  
Lorenzo Grassi  
Stefano Guarino  
Gus Gutoski  
Britta Hale  
Stephan Häuser  
Matt Henriksen  
Felix Heuer  
Jialin Huang  
Matthias Huber  
Siam Hussain  
Jean-Louis Huynen  
Chandrakumar Holenarasipursuresh  
Panagiotis Ilia  
Vincenzo Iovino  
Morshed Islam  
Hakon Jacobsen  
Angela Jäschke  
Dirmanto Jap  
Mahavir Jhawar  
Sachhidh Kannan  
Bhavana Kanukurthi  
Arun Kanuparthi  
Ghassan Karame  
Pierre Karpman  
Nikolaos Karvelas  
Taechan Kim  
Ágnes Kiss  
Alexander Koch  
Stefan Koelbl  
Matthias Krause  
Russell W.F. Lai  
Kim Laine  
Chhagan Lal  
Charles Lamech  
Sebastian Lauer  
Hoon Wei Lim  
Shen Liu

Xiruo Liu  
Patrick Longa  
Jiqiang Lu  
Stefan Lucks  
Daniel Masny  
Takahiro Matsuda  
Bodhisatwa Mazumdar  
Florian Mendel  
Alfred Menezes  
Vasily Mikhalev  
Vladislav Mladlenov  
Paweł Morawiecki  
Pedro Moreno-Sanchez  
Matthias Nagel  
Ivica Nikolic  
Go Ohtake  
Kazumasa Omote  
Cristina Onete  
Jiaxin Pan  
Panagiotis Papadopoulos  
Arpita Patra  
Umberto Ferraro Petrillo  
Antigoni Polychroniadou  
Ivan Pryvalov  
Kim Ramchen  
Sadegh Riazi  
Peter B. Roenne  
Stefanie Roos  
Arnab Roy  
Sujoy Sinha Roy  
Bita Rouhani  
Vladimir Rozic  
Tim Ruffing  
Yusuke Sakai  
Hani Salah  
Jacob Schuldt  
Alexander Senior  
Hwajeong Seo  
Setareh Sharifian  
Siang Meng Sim  
Luisa Siniscalchi  
Juraj Somorovsky  
Ebrahim Songhori  
Riccardo Spolaor  
Richard Skowyra  
Marjan Skrobot



Chunhua Su  
Somayeh Taheri  
Katsuyuki Takashima  
Qiang Tang  
Tyge Tiessen  
Elmar Tischhauser  
Thao Tran  
Pengwei Wang  
Qingju Wang  
Xiuhua Wang  
Xueyang Wang  
Marcel Winandy  
Miao Xu

Jia Xu  
Shota Yamada  
Rupeng Yang  
Muhammad Yasin  
Shaza Zeitouni  
Dongrui Zeng  
Liang Feng Zhang  
Tao Zhang  
Zongyang Zhang  
Yongjun Zhao  
Luying Zhou  
Michael Zohner

# Contents

## Authentication and Key Establishment

On the Security of the Algebraic Eraser Tag Authentication Protocol . . . . .	3
<i>Simon R. Blackburn and M.J.B. Robshaw</i>	
A Cryptographic Analysis of UMTS/LTE AKA . . . . .	18
<i>Stephanie Alt, Pierre-Alain Fouque, Gilles Macario-rat, Cristina Onete, and Benjamin Richard</i>	
Low-Cost Mitigation Against Cold Boot Attacks for an Authentication Token . . . . .	36
<i>Ian Goldberg, Graeme Jenkinson, and Frank Stajano</i>	
Two More Efficient Variants of the J-PAKE Protocol . . . . .	58
<i>Jean Lancrenon, Marjan Škrobot, and Qiang Tang</i>	
Hash-Based TPM Signatures for the Quantum World . . . . .	77
<i>Megumi Ando, Joshua D. Guttman, Alberto R. Papaleo, and John Scire</i>	

## Signatures with Advanced Properties

Fuzzy Signatures: Relaxing Requirements and a New Construction . . . . .	97
<i>Takahiro Matsuda, Kenta Takahashi, Takao Murakami, and Goichiro Hanaoka</i>	
Foundations of Fully Dynamic Group Signatures . . . . .	117
<i>Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Essam Ghadafi, and Jens Groth</i>	
A Lattice-Based Group Signature Scheme with Message-Dependent Opening . . . . .	137
<i>Benoît Libert, Fabrice Mouhartem, and Khoa Nguyen</i>	
Threshold-Optimal DSA/ECDSA Signatures and an Application to Bitcoin Wallet Security . . . . .	156
<i>Rosario Gennaro, Steven Goldfeder, and Arvind Narayanan</i>	
Legally Fair Contract Signing Without Keystones . . . . .	175
<i>Houda Ferradi, Rémi Géraud, Diana Maimuț, David Naccache, and David Pointcheval</i>	

**DoS Attacks and Network Anomaly Detection**

Why Software DoS Is Hard to Fix: Denying Access in Embedded Android Platforms . . . . . 193  
*Ryan Johnson, Mohamed Elsabagh, and Angelos Stavrou*

Network Anomaly Detection Using Unsupervised Feature Selection and Density Peak Clustering. . . . . 212  
*Xiejun Ni, Daojing He, Sammy Chan, and Farooq Ahmad*

**Deterministic and Functional Encryption**

More Efficient Constructions for Inner-Product Encryption. . . . . 231  
*Somindu C. Ramanna*

Attribute Based Encryption with Direct Efficiency Tradeoff . . . . . 249  
*Nuttapong Attrapadung, Goichiro Hanaoka, Tsutomu Matsumoto, Tadanori Teruya, and Shota Yamada*

Turing Machines with Shortcuts: Efficient Attribute-Based Encryption for Bounded Functions . . . . . 267  
*Xavier Boyen and Qinyi Li*

Offline Witness Encryption . . . . . 285  
*Hamza Abusalah, Georg Fuchsbauer, and Krzysztof Pietrzak*

Deterministic Public-Key Encryption Under Continual Leakage . . . . . 304  
*Venkata Koppula, Omkant Pandey, Yannis Rouselakis, and Brent Waters*

**Computing on Encrypted Data**

Better Preprocessing for Secure Multiparty Computation . . . . . 327  
*Carsten Baum, Ivan Damgård, Tomas Toft, and Rasmus Zakarias*

Trinocchio: Privacy-Preserving Outsourcing by Distributed Verifiable Computation. . . . . 346  
*Berry Schoenmakers, Meilof Veeningen, and Niels de Vreede*

Verifiable Multi-party Computation with Perfectly Private Audit Trail . . . . . 367  
*Édouard Cuvelier and Olivier Pereira*

Practical Fault-Tolerant Data Aggregation . . . . . 386  
*Krzysztof Grining, Marek Klonowski, and Piotr Syga*

Accelerating Homomorphic Computations on Rational Numbers . . . . . 405  
*Angela Jäschke and Frederik Armknecht*

**Non-Interactive Proofs and PRFs**

New Techniques for Non-interactive Shuffle and Range Arguments . . . . . 427  
*Alonso González and Carla Ráfols*

Constrained PRFs for Unbounded Inputs with Short Keys . . . . . 445  
*Hamza Abusalah and Georg Fuchsbauer*

**Symmetric Ciphers**

Wide Trail Design Strategy for Binary MixColumns: Enhancing Lower Bound of Number of Active S-boxes. . . . . 467  
*Yosuke Todo and Kazumaro Aoki*

Automatic Search of Linear Trails in ARX with Applications to SPECK and Chaskey. . . . . 485  
*Yunwen Liu, Qingju Wang, and Vincent Rijmen*

Square Attack on 7-Round Kiasu-BC . . . . . 500  
*Christoph Dobraunig, Maria Eichlseder, and Florian Mendel*

On the Design Rationale of SIMON Block Cipher: Integral Attacks and Impossible Differential Attacks against SIMON Variants . . . . . 518  
*Kota Kondo, Yu Sasaki, and Tetsu Iwata*

Correlation Power Analysis of Lightweight Block Ciphers: From Theory to Practice . . . . . 537  
*Alex Biryukov, Daniel Dinu, and Johann Großschädl*

**Cryptography in Software**

Assisted Identification of Mode of Operation in Binary Code with Dynamic Data Flow Slicing . . . . . 561  
*Pierre Lestrinant, Frédéric Guihéry, and Pierre-Alain Fouque*

Parallel Implementation of BDD Enumeration for LWE. . . . . 580  
*Elena Kirshanova, Alexander May, and Friedrich Wiemer*

Memory Carving in Embedded Devices: Separate the Wheat from the Chaff. . . 592  
*Thomas Gougeon, Morgan Barbier, Patrick Lacharme, Gildas Avoine, and Christophe Rosenberger*

**Security for Human Use**

CAPTCHaStar! A Novel CAPTCHA Based on Interactive Shape Discovery . . . 611  
*Mauro Conti, Claudio Guarisco, and Riccardo Spolaor*

TMGuard: A Touch Movement-Based Security Mechanism for Screen  
Unlock Patterns on Smartphones . . . . . 629  
*Weizhi Meng, Wenjuan Li, Duncan S. Wong, and Jianying Zhou*

Gesture-Based Continuous Authentication for Wearable Devices:  
The Smart Glasses Use Case . . . . . 648  
*Jagmohan Chauhan, Hassan Jameel Asghar, Anirban Mahanti,  
and Mohamed Ali Kaafar*

**Author Index** . . . . . 667