

*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*

Michael Jacobson Michael Locasto  
Payman Mohassel Reihaneh Safavi-Naini (Eds.)

# Applied Cryptography and Network Security

11th International Conference, ACNS 2013  
Banff, AB, Canada, June 25-28, 2013  
Proceedings

 Springer

## Volume Editors

Michael Jacobson  
Michael Locasto  
Payman Mohassel  
Reihaneh Safavi-Naini

University of Calgary, Department of Computer Science  
2500 University Drive NW, Calgary, AB T2N 1N4, Canada

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-38979-5 e-ISBN 978-3-642-38980-1  
DOI 10.1007/978-3-642-38980-1  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013940302

CR Subject Classification (1998): K.6.5, E.3, K.4.4, D.4.6, E.4, C.2, J.1, E.1

LNCS Sublibrary: SL 4 – Security and Cryptology

© Springer-Verlag Berlin Heidelberg 2013

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

*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

ACNS 2013, the 11th International Conference on Applied Cryptography and Network Security, was held during June 25–28 at Banff, Alberta, Canada.

We received 150 submissions of which 33 were accepted as regular papers (22% acceptance rate), and two as short papers. These proceedings contain the revised versions of all the papers. There were three invited talks. Srdjan Capkun, Professor of Computer Science at ETH Zurich, gave a talk entitled “Selected Topics in Wireless Physical Layer Security.” Bryan Parno from Microsoft Research Redmond, gave a talk on “Bootstrapping Cloud Security Speaker,” and Francois Theberge, research mathematician with the Tutte Institute for Mathematics and Computing spoke about “Ensemble Clustering for Graphs-Based Data.”

The Program Committee (PC) consisted of 35 members with diverse research interest and experience. Papers were reviewed double-blind, with each paper assigned to three reviewers. During the discussion phase, when necessary, extra reviews were solicited. We ensured that all papers received fair and objective evaluation by experts and also a broader group of PC members, with particular attention paid to highlighting strengths and weaknesses of papers. The final decisions were made based on the reviews and discussion. The task of paper selection was especially challenging given the high number of strong submissions. In the end, a sizable number of strong papers could not be included in the program owing to lack of space.

We would like to sincerely thank authors of all submissions— those whose papers made it into the program and those whose papers did not. We, and the PC as a whole, were impressed by the quality of submissions contributed from all around the world. Although this made the task of selecting the final list very challenging, it gave us the opportunity to have a strong and diverse program.

We would like to extend our sincere gratitude to the Program Committee. We were very fortunate that so many talented people put such an inordinate amount of time to write reviews and actively participate in discussions for nearly three weeks. They responded to our requests for extra reviews, opinions, comments, comparisons, and inputs. We were impressed by the knowledge, dedication, and integrity of our PC. We also would like to thank many external reviewers, some contacted by us directly and some through PC members, who significantly contributed to the comprehensive evaluation of papers. A list of PC members and external reviewers appears after this note.

We would like to thank Mahabir Jhanwar, the Publicity Chair, for working closely with us throughout the whole process, providing the much needed support in every step. We would also like to thank Tongjie Zhang for handling our social media presence, Coral Burns for her work on the ACNS website, Deb Angus for logistical and administrative support, Camille Sinanan for her help with the local organization and financial administration, and, finally, Hadi Ahmadi and

numerous student volunteers who helped us with the successful organization of the program.

We benefited from advice and feedback from Moti Yung and Jianying Zhou, the ACNS Steering Committee. Alfred Hofmann and his colleagues at Springer provided a meticulous service for the timely production of this volume.

We would like to thank Microsoft Research, the Pacific Institute for Mathematical Sciences (PIMS), Alberta Innovates Technology Future (AITF), and the University of Calgary for their generous support. We also gratefully acknowledge our partnership with the Tutte Institute for Mathematics and Computing (TIMC), in contributing to the success of this conference.

April 2013

Michael Jacobson  
Michael Locasto  
Payman Mohassel  
Reihaneh Safavi-Naini

# ACNS 2013

## 11th International Conference on Applied Cryptography and Network Security

BANFF, Alberta, Canada  
June 25–28, 2013

### General Chairs

Michael Jacobson                      University of Calgary, Canada  
Payman Mohassel                      University of Calgary, Canada

### Program Chairs

Michael Locasto                      University of Calgary, Canada  
Reihaneh Safavi-Naini                      University of Calgary, Canada

### Program Committee

Bill Aiello                      University of British Columbia, Canada  
Giuseppe Ateniese                      Sapienza University of Rome, Italy  
Kevin R.B. Butler                      University of Oregon, USA  
Srdjan Capkun                      ETH Zurich, Switzerland  
Alvaro A. Cárdenas                      University of Texas at Dallas, USA  
Chen-Mou Cheng                      National Taiwan University, Taiwan  
Sherman S.M. Chow                      Chinese University of Hong Kong, Hong Kong  
Ed Dawson                      Queensland University of Technology, Australia  
Roberto Di Pietro                      Università Roma Tre, Italy  
Sara Foresti                      Università degli Studi di Milano, Italy  
Guang Gong                      University of Waterloo, Canada  
Stefanos Gritzalis                      University of the Aegean, Greece  
Guofei Gu                      Texas A&M University, USA  
Angelos D. Keromytis                      Columbia University, USA  
Evangelos Kranakis                      Carleton University, Canada  
Ralf Küsters                      Universität Trier, Germany  
Xuejia Lai                      Shanghai Jiao Tong University, China  
Cédric Lauradoux                      INRIA, France  
Ninghui Li                      Purdue University, USA  
Yingjiu Li                      Singapore Management University, Singapore  
Mark Manulis                      University of Surrey, UK  
Kaisa Nyberg                      Aalto University, Finland  
Josef Pieprzyk                      Macquarie University, Australia  
Bart Preneel                      KU Leuven, Belgium  
Christian Rechberger                      DTU, Denmark

Ahmad-Reza Sadeghi	Technische Universität Darmstadt, Germany
Pierangela Samarati	Università degli Studi di Milano, Italy
Radu Sion	Stony Brook University, USA
Anil Somayaji	Carleton University, Canada
Abhinav Srivastava	AT&T Research, USA
Jessica Staddon	Google, USA
Willy Susilo	University of Wollongong, Australia
Gene Tsudik	UC Irvine, USA
Duncan S. Wong	City University of Hong Kong, Hong Kong
Jianying Zhou	I <sup>2</sup> R, Singapore

### Publicity Chair

Mahabir P. Jhanwar	University of Calgary, Canada
--------------------	-------------------------------

### Steering Committee

Yongfei Han	ONETS, China
Moti Yung	Google, USA
Jianying Zhou	Institute for Infocomm Research, Singapore

### Additional Reviewers

Achara, Jagdish	Chia, Pern	Huang, Jialin
Ahmadi, Hadi	Choi, Seung Geol	Huang, Qiong
Albrecht, Martin R.	Chu, Cheng-Kang	Huang, Xinyi
Alimomeni, Mohsen	Cunche, Mathieu	Huang, Zhengang
Andreeva, Elena	Damopoulos, Dimitrios	Huo, Fei
Androulaki, Elli	De Cristofaro, Emiliano	Jhanwar, Mahabir
Argyros, George	Ding, Jintai	Jiang, Shaoquan
Armknecht, Frederik	Dmitrienko, Alexandra	Kalloniatis, Christos
Athanasopoulos, Elias	Fan, Junfeng	Kambourakis, Georgios
Au, Man Ho	Fan, Xinxin	Kemerlis, Vasileios P.
Bae, Jun-Young	Fang, Liming	Kerschbaum, Florian
Baig, Basim	Fett, Daniel	Kim, Jihye
Bajaj, Sumeet	Fleischhacker, Nils	Konidala, Divyan
Balopoulos, Theodoros	Gagne, Martin	Kontaxis, Georgios
Bernstein, Daniel J.	Gajek, Sebastian	Krell, Fernando
Bloch, Mathieu	Geneiatakis, Dimitris	Krenn, Stephan
Blondeau, Céline	Gervais, Arthur	Kuo, Po-Chun
Boggs, Nathaniel	Ghodosi, Hossein	Lafourcade, Pascal
Boura, Christina	Gong, Zheng	Lange, Tanja
Boyd, Colin	Gorantla, Choudary	Lauridsen, Martin M.
Boyen, Xavier	Groth, Jens	Li, Ming
Cao, Jianneng	Guarino, Stefano	Li, Yan
Chandran, Nishant	Guo, Fuchun	Liang, Kaitai
Chang, Yun-An	Han, Jin	Liu, Joseph

Liu, Zhen	Radomirovic, Sasa	Vogt, Andreas
Lombardi, Flavio	Ranganathan, Aanjhan	Wachsmann, Christian
Long, Yu	Rasmussen, Kasper	Wu, Jong-Shian
Ma, Di	Bonne	Wu, Teng
Malisa, Luka	Rial, Alfredo	Xie, Xiang
Mandal, Kalikinkar	Rizomiliotis, Panagiotis	Xu, Hong
Miettinen, Markus	Rouselakis, Yannis	Xu, Jia
Mohassel, Payman	Salim, Farzad	Xu, Zhaoyan
More, Sara	Schmitz, Guido	Xue, Weijia
Mouha, Nicky	Schneider, Michael	Yang, Chao
Nergiz, Ahmet Erhan	Sepehrdad, Pouyan	Yang, Guomin
Nguyen, Lan	Shahandashti, Siamak	Yang, Yanjiang
Niederhagen, Ruben	Soleimany, Hadi	Yu, Ching-Hua
Nikolic, Ivica	Soriente, Claudio	Yuen, Tsz Hon
Nikova, Svetla	Su, Dong	Zhang, Cong
Nishide, Takashi	Tan, Xiao	Zhang, Haibin
Núñez, David	Tuengerthal, Max	Zhang, Jialong
Olejnik, Lukasz	Tzouramanis, Theodoros	Zhang, Liangfeng
Pappas, Vasilis	Ustaoglu, Berkant	Zhang, Tao
Peeters, Roel	Vahlis, Yevgeniy	Zhou, Xuhua
Peikert, Chris	Van Herrewege, Anthony	Zhu, Bo
Pointcheval, David	Varici, Kerem	
Polychronakis, Michalis	Villani, Antonio	
Popper, Christina	Vo, Binh	



# Table of Contents

## Cloud Cryptography

Transparent, Distributed, and Replicated Dynamic Provable Data Possession .....	1
<i>Mohammad Etemad and Alptekin Küpçü</i>	
Client-Controlled Cryptography-as-a-Service in the Cloud .....	19
<i>Sören Bleikertz, Sven Bugiel, Hugo Ideler, Stefan Nürnberger, and Ahmad-Reza Sadeghi</i>	
CloudHKA: A Cryptographic Approach for Hierarchical Access Control in Cloud Computing .....	37
<i>Yi-Ruei Chen, Cheng-Kang Chu, Wen-Guey Tzeng, and Jianying Zhou</i>	
Computing on Authenticated Data for Adjustable Predicates .....	53
<i>Björn Deiseroth, Victoria Fehr, Marc Fischlin, Manuel Maasz, Nils Fabian Reimers, and Richard Stein</i>	

## Secure Computation

Towards Efficient Private Distributed Computation on Unbounded Input Streams (Extended Abstract) .....	69
<i>Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov, and Yelena Yuditsky</i>	
From Oblivious AES to Efficient and Secure Database Join in the Multiparty Setting .....	84
<i>Sven Laur, Riivo Talviste, and Jan Willemson</i>	
Private Database Queries Using Somewhat Homomorphic Encryption ...	102
<i>Dan Boneh, Craig Gentry, Shai Halevi, Frank Wang, and David J. Wu</i>	

## Hash Function and Block Cipher

BLAKE2: Simpler, Smaller, Fast as MD5 .....	119
<i>Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O’Hearn, and Christian Winnerlein</i>	
Cryptophia’s Short Combiner for Collision-Resistant Hash Functions ...	136
<i>Arno Mittelbach</i>	

Generic Attacks for the Xor of  $k$  Random Permutations . . . . . 154  
*Jacques Patarin*

Preimage Attacks on Feistel-SP Functions: Impact of Omitting the  
 Last Network Twist . . . . . 170  
*Yu Sasaki*

**Signature**

Constructing Practical Signcryption KEM from Standard Assumptions  
 without Random Oracles . . . . . 186  
*Xiangxue Li, Haifeng Qian, Yu Yu, Yuan Zhou, and Jian Weng*

Sequential Aggregate Signatures Made Shorter . . . . . 202  
*Kwangsu Lee, Dong Hoon Lee, and Moti Yung*

**Group-Oriented Cryptography**

How to Share a Lattice Trapdoor: Threshold Protocols for Signatures  
 and (H)IBE . . . . . 218  
*Rikke Bendlin, Sara Krehbiel, and Chris Peikert*

Toward Practical Group Encryption . . . . . 237  
*Laila El Aimagi and Marc Joye*

**System Attack I**

Experimental Analysis of Attacks on Next Generation Air Traffic  
 Communication . . . . . 253  
*Matthias Schäfer, Vincent Lenders, and Ivan Martinovic*

Launching Generic Attacks on iOS with Approved Third-Party  
 Applications . . . . . 272  
*Jin Han, Su Mon Kywe, Qiang Yan, Feng Bao, Robert Deng,  
 Debin Gao, Yingjiu Li, and Jianying Zhou*

**Secure Implementation – Hardware**

Hardware Architectures for MSP430-Based Wireless Sensor Nodes  
 Performing Elliptic Curve Cryptography . . . . . 290  
*Erich Wenger*

Beyond Full Disk Encryption: Protection on Security-Enhanced  
 Commodity Processors . . . . . 307  
*Michael Henson and Stephen Taylor*

## Secure Implementation – Software

NEON Implementation of an Attribute-Based Encryption Scheme . . . . .	322
<i>Ana Helena Sánchez and Francisco Rodríguez-Henríquez</i>	
Fast and Maliciously Secure Two-Party Computation Using the GPU . . .	339
<i>Tore Kasper Frederiksen and Jesper Buus Nielsen</i>	
Comparing the Pairing Efficiency over Composite-Order and Prime-Order Elliptic Curves . . . . .	357
<i>Aurore Guillevic</i>	

## System Attack II

FROST: Forensic Recovery of Scrambled Telephones . . . . .	373
<i>Tilo Müller and Michael Spreitzenbarth</i>	
Attacking Atmel’s CryptoMemory EEPROM with Special-Purpose Hardware . . . . .	389
<i>Alexander Wild, Tim Güneysu, and Amir Moradi</i>	
Keystroke Timing Analysis of on-the-fly Web Apps . . . . .	405
<i>Chee Meng Tey, Payas Gupta, Debin Gao and Yan Zhang</i>	
Terrorism in Distance Bounding: Modeling Terrorist-Fraud Resistance . . . . .	414
<i>Marc Fischlin and Cristina Onete</i>	

## Group-Oriented Systems

CrowdShare: Secure Mobile Resource Sharing . . . . .	432
<i>N. Asokan, Alexandra Dmitrienko, Marcin Nagy, Elena Reshetova, Ahmad-Reza Sadeghi, Thomas Schneider, and Stanislaus Stelle</i>	
Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System . . . . .	441
<i>Filip Zagórski, Richard T. Carback, David Chaum, Jeremy Clark, Aleksander Essex, and Poorvi L. Vora</i>	

## Key Exchange and Leakage Resilience

Exposure-Resilient One-Round Tripartite Key Exchange without Random Oracles . . . . .	458
<i>Koutarou Suzuki and Kazuki Yoneyama</i>	
Public Key Exchange Using Semidirect Product of (Semi)Groups . . . . .	475
<i>Maggie Habeeb, Delaram Kahrobaei, Charalambos Koupparis, and Vladimir Shpilrain</i>	

Leakage Resilient IBE and IPE under the DLIN Assumption ..... 487  
*Kaoru Kurosawa and Le Trieu Phong*

**Cryptographic Proof**

Batch Proofs of Partial Knowledge ..... 502  
*Ryan Henry and Ian Goldberg*

Efficient Signatures of Knowledge and DAA in the Standard Model .... 518  
*David Bernhard, Georg Fuchsbauer, and Essam Ghadafi*

**Cryptosystems**

Analysis and Improvement of Lindell’s UC-Secure Commitment  
Schemes ..... 534  
*Olivier Blazy, Céline Chevalier, David Pointcheval, and  
Damien Vergnaud*

Primeless Factoring-Based Cryptography – Solving the Complexity  
Bottleneck of Public-Key Generation– ..... 552  
*Sonia Bogos, Ioana Boureanu, and Serge Vaudenay*

**Author Index** ..... 571