

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, Zurich, 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, Chennai, 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>


Bart Preneel · Frederik Vercauteren (Eds.)

Applied Cryptography and Network Security

16th International Conference, ACNS 2018
Leuven, Belgium, July 2–4, 2018
Proceedings

Editors

Bart Preneel 
imec-COSIC
KU Leuven
Heverlee
Belgium

Frederik Vercauteren 
imec-COSIC
KU Leuven
Heverlee
Belgium

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-93386-3 ISBN 978-3-319-93387-0 (eBook)
<https://doi.org/10.1007/978-3-319-93387-0>

Library of Congress Control Number: 2018944429

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG, part of Springer Nature 2018

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG
part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

ACNS 2018, the 16th International Conference on Applied Cryptography and Network Security, was held during July 2–4, 2018, at KU Leuven, Belgium. The local organization was in the capable hands of the COSIC team at KU Leuven and we are deeply indebted to them for their support and smooth collaboration.

We received 173 paper submissions, out of which 36 were accepted, resulting in an acceptance rate of 20%. These proceedings contain revised versions of all the papers. The invited keynotes were delivered by Gilles Barthe, who spoke on formal verification of side-channel resistance and Haya Shulman who shared with the audience her perspective on RPKI’s Deployment and Security of BGP.

The Program Committee consisted of 52 members with diverse backgrounds and broad research interests. The review process was double-blind. Each paper received at least three reviews; for submissions by Program Committee members, this was increased to five. During the discussion phase, additional reviews were solicited when necessary. An intensive discussion was held to clarify issues and to converge toward decisions. The selection of the program was challenging; in the end some high-quality papers had to be rejected owing to lack of space. The committee decided to give the Best Student Paper Award to the paper “Non-interactive zaps of knowledge” by Georg Fuchsbauer and Michele Orrù.

We would like to sincerely thank the authors of all submissions for contributing high-quality submissions and giving us the opportunity to compile a strong and diverse program. We know that the Program Committee’s decisions can be very disappointing, especially rejections of good papers that did not find a slot in the sparse number of accepted papers.

Special thanks go to the Program Committee members; we value their hard work and dedication to write careful and detailed reviews and to engage in interesting discussions. A few Program Committee members, whom we asked to serve as shepherds, spent additional time in order to help the authors improve their works. More than 160 external reviewers contributed to the review process; we would like to thank them for their efforts.

Finally, we thank everyone else — speakers and session chairs — for their contribution to the program of ACNS 2018. We would also like to thank the sponsors for their generous support.

We hope that the papers in this volume prove valuable for your research and professional activities and that ACNS will continue to play its unique role in bringing together researchers and practitioners in the area of cryptography and network security.

April 2018

Bart Preneel
Frederik Vercauteren

ACNS 2018

Applied Cryptography and Network Security 2018

KU Leuven, Belgium

July 2–4, 2018

General Chair

Bart Preneel KU Leuven, Belgium

Program Chairs

Bart Preneel KU Leuven, Belgium

Frederik Vercauteren KU Leuven, Belgium

Program Committee

Michel Abdalla	ENS and CNRS, France
Masayuki Abe	NTT, Japan
Elli Androulaki	IBM Research, Switzerland
Alex Biryukov	University of Luxembourg, Luxembourg
Marina Blanton	University at Buffalo, The State University of New York, USA
Jan Camenisch	IBM Research, Switzerland
Liqun Chen	University of Surrey, UK
Chen-Mou Cheng	National Taiwan University, Taiwan
Naccache David	ENS, France
Dieter Gollmann	Hamburg University of Technology, Germany
Peter Gutmann	University of Auckland, New Zealand
Shai Halevi	IBM Research, USA
Goichiro Hanaoka	AIST, Japan
Amir Herzberg	University of Connecticut, USA
Tibor Jager	Paderborn University, Germany
Marc Joye	NXP Semiconductors, USA
Aniket Kate	Purdue University, USA
Stefan Katzenbeisser	TU Darmstadt, Germany
Florian Kerschbaum	University of Waterloo, Canada
Aggelos Kiyias	University of Edinburgh, UK
Kwangjo Kim	KAIST, Korea
Kaoru Kurosawa	Ibaraki University, Japan
Ralf Kusters	University of Stuttgart, Germany

Xuejia Lai	Shanghai Jiaotong University, China
Benoit Libert	CNRS and ENS de Lyon, France
Dongdai Lin	SKLOIS, Chinese Academy of Sciences, China
Michael Locasto	SRI International, USA
Javier Lopez	University of Malaga, Spain
Mark Manulis	University of Surrey, UK
Atefeh Mashatan	Ryerson University, Canada
Bart Mennink	Radboud University, The Netherlands
Atsuko Miyaji	JAIST, Japan
Refik Molva	Eurecom, France
Michael Naehrig	Microsoft Research, USA
Miyako Ohkubo	NICT, Japan
Panos Papadimitratos	KTH Royal Institute of Technology, Sweden
Thomas Peyrin	Nanyang Technological University, Singapore
Josef Pieprzyk	QUT, Australia
Benny Pinkas	Bar-Ilan University, Israel
Bart Preneel	KU Leuven, Belgium
Christian Rechberger	TU Graz, Austria
Matt Robshaw	Impinj, USA
Ahmad Sadeghi	TU Darmstadt, Germany
Yu Sasaki	NTT Secure Platform Laboratories, Japan
Willy Susilo	University of Wollongong, Australia
Mehdi Tibouchi	NTT Secure Platform Laboratories, Japan
Damien Vergnaud	ENS, France
Ivan Visconti	University of Salerno, Italy
Frederik Vercauteren	KU Leuven, Belgium
Avishai Wool	Tel Aviv University, Israel
Moti Yung	Columbia University, USA
Jiaying Zhou	Singapore University of Technology and Design, Singapore

Additional Reviewers

Aydin Abadi	Pascal Bemmam	Jiageng Chen
Mai Ben Adar-Bessos	Fabrice Benhamouda	Rongmao Chen
Megha Agrawal	Cecilia Boschini	Yu Chen
Hyeongcheol Ahn	Florian Bourse	Céline Chevalier
Muhamad Erza Aminanto	Ferdinand Brasser	Rakyong Choi
Hassan Asghar	Niklas Büscher	Tung Chou
Nuttapong Attrapadung	Seyit Camtepe	Sherman S. M. Chow
Joonsang Baek	Luigi Catuogno	Peter Chvojka
Anubhab Baksi	Avik Chakraborti	Michele Ciampi
Josep Balasch	Jagmohan Chauhan	Craig Costello
Harry Barlett	Hao Chen	Angelo De Caro

Yi Deng	Qiqi Lai	Yusuke Sakai
David Derler	Ben Lapid	Katerina Samari
Christoph Dobraunig	Jeeun Lee	John Schanck
Manu Drijvers	Qi Li	Guido Schmitz
Li Duan	Christopher Liebchen	Jacob Schuldt
Maria Eichlseder	Tingting Lin	Hwajeong Seo
Kaoutar Elkhyaoui	Helger Lipmaa	Mike Simon
Keita Emura	Patrick Longa	Luisa Siniscalchi
Oguzhan Ersoy	Xiapu Luo	Chunhua Su
Thomas Espitau	Yiyuan Luo	Koutarou Suzuki
Gerardo Fernandez	Xuecheng Ma	Akira Takahashi
Carmen Fernandez	Takahiro Matsuda	Katsuyuki Takashima
Daniel Fett	Matthew McKague	Harry Chandra
Dario Fiore	Siang Meng Sim Meng	Tanuwidjaja
Steven Galbraith	Weizhi Meng	Tadanori Teruya
Adria Gascon	Markus Miettinen	Yosuke Todo
Romain Gay	Takaaki Mizuki	Junichi Tomida
Kai Gellert	Kirill Morozov	Patrick Towa
Junqing Gong	Fabrice Mouhartem	Yiannis Tselekounis
Zheng Gong	Johannes Mueller	Ida Tucker
Alonso Gonzalez	Zakaria Najm	Aleksei Udovenko
Lorenzo Grassi	Toru Nakanishi	Cédric Van Rompay
Clémentine Gritti	Surya Nepal	Dimitrios Vasilopoulos
Jian Guo	Khoa Nguyen	Vesselin Velichkov
Jinguang Han	David Niehues	Nikita Veshchikov
Yoshikazu Hanatani	Ana Nieto	Haoyang Wang
Lin Hou	Ariel Nof	Qingju Wang
Guifang Huang	David Nuñez	Yohei Watanabe
Jialin Huang	Kazuma Ohara	Keita Xagawa
Iliia Iliashenko	Shinya Okumura	Weijia Xue
Vincenzo Iovino	Kazumasa Omote	Shota Yamada
Ai Ishida	Melek Önen	Takashi Yamakawa
Dirmanto Jap	Leo Perrin	Hailun Yan
Saqib Kakvi	Thomas Peters	Guomin Yang
Daniel Kales	Le Trieu Phong	Kazuki Yoneyama
Jean-Gabriel Kammerer	Tran Viet Xuan Phuong	Hirotaaka Yoshida
Julien Keuffer	Thomas Pöppelmann	Hongbo Yu
Jongkil Kim	Jeyavijayan Rajendran	Zheng Yuan
Markulf Kohlweiss	Sebastian Ramacher	Thomas Zacharias
Florian Kohnhäuser	Somindu Ramanna	Rina Zeitoun
Takeshi Koshiba	Daniel Rausch	Bingsheng Zhang
Hugo Krawczyk	Joost Renes	Lei Zhang
Po-Chun Kuo	Sietse Ringers	Tao Zhang
Rafael Kurek	Ruben Rios	Vincent Zucca
Jianchang Lai	Rodrigo Roman	

Contents

Cryptographic Protocols

A Cryptographic Analysis of the WireGuard Protocol	3
<i>Benjamin Dowling and Kenneth G. Paterson</i>	
Distributed SSH Key Management with Proactive RSA Threshold Signatures	22
<i>Yotam Harchol, Ittai Abraham, and Benny Pinkas</i>	
Non-interactive Zaps of Knowledge.	44
<i>Georg Fuchsbauer and Michele Orrù</i>	

Side Channel Attacks and Tamper Resistance

Formal Verification of Side-Channel Countermeasures via Elementary Circuit Transformations	65
<i>Jean-Sébastien Coron</i>	
Drive-By Key-Extraction Cache Attacks from Portable Code	83
<i>Daniel Genkin, Lev Pachmanov, Eran Tromer, and Yuval Yarom</i>	
On the Ineffectiveness of Internal Encodings - Revisiting the DCA Attack on White-Box Cryptography.	103
<i>Estuardo Alpirez Bock, Chris Brzuska, Wil Michiels, and Alexander Treff</i>	
Continuously Non-malleable Codes with Split-State Refresh.	121
<i>Antonio Faonio, Jesper Buus Nielsen, Mark Simkin, and Daniele Venturi</i>	

Digital Signatures

Efficient Unconditionally Secure Signatures Using Universal Hashing	143
<i>Ryan Amiri, Aysajan Abidin, Petros Wallden, and Erika Andersson</i>	
Floppy-Sized Group Signatures from Lattices	163
<i>Cecilia Boschini, Jan Camenisch, and Gregory Neven</i>	
On the Security Notions for Homomorphic Signatures	183
<i>Dario Catalano, Dario Fiore, and Luca Nizzardo</i>	
Invisible Sanitizable Signatures and Public-Key Encryption are Equivalent. . .	202
<i>Marc Fischlin and Patrick Harasser</i>	

Delegatable Attribute-Based Anonymous Credentials from Dynamically Malleable Signatures 221
Johannes Blömer and Jan Bobolz

Privacy Preserving Computation

Privacy-Preserving Ridge Regression with only Linearly-Homomorphic Encryption. 243
Irene Giacomelli, Somesh Jha, Marc Joye, C. David Page, and Kyonghwan Yoon

Privacy-Preserving Plaintext-Equality of Low-Entropy Inputs 262
Sébastien Canard, David Pointcheval, Quentin Santos, and Jacques Traoré

Nothing Refreshes Like a RePSI: Reactive Private Set Intersection 280
Andrea Cerulli, Emiliano De Cristofaro, and Claudio Soriente

Multi-party Computation

New Protocols for Secure Equality Test and Comparison 303
Geoffroy Couteau

Minimising Communication in Honest-Majority MPC by Batchwise Multiplication Verification 321
Peter Sebastian Nordholt and Meilof Veeningen

Best of Both Worlds in Secure Computation, with Low Communication Overhead 340
Daniel Genkin, S. Dov Gordon, and Samuel Ranellucci

3PC ORAM with Low Latency, Low Bandwidth, and Fast Batch Retrieval . . . 360
Stanislaw Jarecki and Boyang Wei

Symmetric Key Primitives

MERGE MAC: A MAC for Authentication with Strict Time Constraints and Limited Bandwidth 381
Ralph Ankele, Florian Böhl, and Simon Friedberger

KANGAROOTWELVE: Fast Hashing Based on KECCAK- p 400
Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, Ronny Van Keer, and Benoît Viguier

Symmetric Key Cryptanalysis

Related-Key Boomerang Attacks on Full ANU Lightweight Block Cipher . . . 421
Yu Sasaki

Generic Round-Function-Recovery Attacks for Feistel Networks
over Small Domains 440
F. Betül Durak and Serge Vaudenay

Differential Cryptanalysis of Round-Reduced Sparx-64/128 459
Ralph Ankele and Eik List

Can Caesar Beat Galois? Robustness of CAESAR Candidates Against
Nonce Reusing and High Data Complexity Attacks 476
Serge Vaudenay and Damian Vizár

Public Key Encryption

Improved Anonymous Broadcast Encryptions: Tight Security
and Shorter Ciphertext 497
Jiangtao Li and Junqing Gong

Time-Based Direct Revocable Ciphertext-Policy Attribute-Based
Encryption with Short Revocation List 516
Joseph K. Liu, Tsz Hon Yuen, Peng Zhang, and Kaitai Liang

Almost Tight Multi-Instance Multi-Ciphertext Identity-Based
Encryption on Lattices 535
Xavier Boyen and Qinyi Li

Authentication and Biometrics

In-Region Authentication 557
Mamunur Rashid Akand and Reihaneh Safavi-Naini

Formal Analysis of Distance Bounding with Secure Hardware 579
Handan Kılınç and Serge Vaudenay

KRB-CCN: Lightweight Authentication and Access Control for Private
Content-Centric Networks 598
Ivan O. Nunes and Gene Tsudik

Assentication: User De-authentication and Lunchtime Attack Mitigation
with Seated Posture Biometric 616
Tyler Kaczmarek, Ercan Ozturk, and Gene Tsudik

Cloud and Peer-to-Peer Security

Stateful Multi-client Verifiable Computation 637
*Christian Cachin, Esha Ghosh, Dimitrios Papadopoulos,
and Björn Tackmann*

VERICOUNT: Verifiable Resource Accounting Using Hardware
and Software Isolation 657
Shruti Tople, Soyeon Park, Min Suk Kang, and Prateek Saxena

Message-Locked Encryption with File Update 678
Suyash Kandeale and Souradyuti Paul

DogFish: Decentralized Optimistic Game-theoretic File SHaring 696
Seny Kamara and Alptekin Küpçü

Author Index 715