

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

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

Stephan Krenn · Haya Shulman ·
Serge Vaudenay (Eds.)

Cryptology and Network Security

19th International Conference, CANS 2020
Vienna, Austria, December 14–16, 2020
Proceedings

Editors

Stephan Krenn
AIT Austrian Institute of Technology GmbH
Vienna, Austria

Haya Shulman
Fraunhofer SIT
Darmstadt, Germany

Serge Vaudenay
IC LASEC
EPFL
Lausanne, Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-65410-8 ISBN 978-3-030-65411-5 (eBook)
<https://doi.org/10.1007/978-3-030-65411-5>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020

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, expressed 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.

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

Preface

The 19th International Conference on Cryptology and Network Security (CANS 2020) was held during December 14–16, 2020, as an online conference, due to the COVID-19 pandemic. CANS 2020 was held in cooperation with the International Association for Cryptologic Research (IACR).

CANS is a recognized annual conference focusing on cryptology, computer and network security, and data security and privacy, attracting cutting-edge research findings from scientists around the world. Previous editions of CANS were held in Taipei ('01), San Francisco ('02), Miami ('03), Xiamen ('05), Suzhou ('06), Singapore ('07), Hong Kong ('08), Kanazawa ('09), Kuala Lumpur ('10), Sanya ('11), Darmstadt ('12), Parary ('13), Crete ('14), Marrakesh ('15), Milan ('16), Hong Kong ('17), Naples ('18), and Fuzhou ('19).

In 2020, the conference received 118 submissions. The submission and review process was done using the EasyChair Web-based software system. We were helped by 40 Program Committee members and 110 external reviewers. The submissions went through a doubly-anonymous review process and 30 papers were selected. This volume represents the revised version of the accepted papers.

Following the CANS tradition, the Program Committee awarded some authors. This year, the Best Paper Award was given for three papers:

- Daniel Kales and Greg Zaverucha for “An Attack on Some Signature Schemes Constructed From Five-Pass Identification Schemes”
- Andrea Caforio, Fatih Balli, and Subhadeep Banik for “Energy Analysis of Lightweight AEAD Circuits”
- Bar Meyuhas, Nethanel Gelernter, and Amir Herzberg for “Cross-Site Search Attacks: Unauthorized Queries over Private Data”

We were honored to have four keynote speakers: Atsuko Miyaji, Kenny Paterson, Mathias Payer, and Zhiyun Qian. We also had a tutorial by Amir Herzberg.

We would like to thank the ATHENE National Research Center for Applied Cybersecurity, as well as the H2020 initiative CyberSec4Europe, for their support during the planning of the conference. We would also like to thank Springer for their support with producing the proceedings. We heartily thank the authors of all submitted papers. Moreover, we are grateful to the members of the Program Committee and the external sub-reviewers for their diligent work, as well as all members of the Organizing Committee for their kind help. We would also like to acknowledge the Steering Committee for supporting us.

November 2020

Stephan Krenn
Haya Shulman
Serge Vaudenay

Organization

Steering Committee

Yvo G. Desmedt (Chair)	The University of Texas at Dallas, USA
Juan A. Garay	Texas A&M University, USA
Amir Herzberg	Bar-Ilan University, Israel
Yi Mu	Fujian Normal University, China
Panos Papadimitratos	KTH, Sweden
David Pointcheval	CNRS, ENS Paris, France
Huaxiong Wang	Nanyang Technological University, Singapore

PC Chairs

Haya Shulman	Fraunhofer SIT, Germany
Serge Vaudenay	Ecole Polytechnique Fédérale de Lausanne, Switzerland

General Chair

Stephan Krenn	AIT Austrian Institute of Technology, Austria
---------------	---

Organizing Committee

Manuela Kos	AIT Austrian Institute of Technology, Austria
Michael Mürling	AIT Austrian Institute of Technology, Austria
Krzysztof Pietrzak (Publicity Chair)	IST Austria, Austria
Hervais Simo	Fraunhofer SIT, Germany

Program Committee

Yehuda Afek	Tel-Aviv University, Israel
Steven Arzt	Fraunhofer, Germany
Xavier Boyen	Queensland University of Technology, Australia
Bremner Bremner-Barr	IDC, Israel
Sherman S. M. Chow	The Chinese University of Hong Kong, Hong Kong
Ran Cohen	Northeastern University, USA
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
F. Betül Durak	Robert Bosch LLC, USA
Michael Franz	University of California, Irvine, USA
Flavio D. Garcia	University of Birmingham, UK

Peter Gaži	IOHK Research, Slovakia
Niv Gilboa	Ben-Gurion University, Israel
Dieter Gollmann	Hamburg University of Technology, Germany
Louis Goubin	Versailles Saint-Quentin-en-Yvelines University, France
Amir Herzberg	Department of Computer Science and Engineering, Israel
Sotiris Ioannidis	Technical University of Crete, Greece
Alptekin Küpçü	Koç University, Turkey
Atefeh Mashatan	Ryerson University, Canada
Kazuhiko Minematsu	NEC Corporation, Japan
Chris Mitchell	Royal Holloway, UK
Max Mühlhäuser	TU Darmstadt, Germany
Mridul Nandi	Indian Statistical Institute, India
Raphael C.-W. Phan	Monash University, Malaysia
Thomas Pornin	NCC Group, Canada
Neta Rozen-Schiff	Hebrew University of Jerusalem, Israel
Mark Ryan	University of Birmingham, UK
Peter Y. A. Ryan	University of Luxembourg, Luxembourg
Simona Samardjiska	Radboud University, The Netherlands
Gil Segev	Hebrew University of Jerusalem, Israel
Jean-Pierre Seifert	Technical University of Berlin, Germany
Haya Shulman	Fraunhofer, Germany
Cristian-Alexandru Staicu	CISPA Helmholtz Center for Information Security, Germany
Nikhil Tripathi	TU Darmstadt, Germany
Serge Vaudenay	Ecole Polytechnique Fédérale de Lausanne, Switzerland
Damien Vergnaud	Sorbonne Université, Institut Universitaire de France, France
Ivan Visconti	Università degli Studi di Salerno, Italy
Damian Vizár	CSEM, Switzerland
Edgar Weippl	University of Vienna, Austria
Matthias Wählisch	Freie Universität Berlin, Germany
Avishay Yanai	VMware Research, Israel

External Reviewers

Abdulla Aldoseri	Augustin Bariant
Nikolaos Alexopoulos	Khashayar Barooti
Gennaro Avitabile	Andrea Basso
Shahar Azulay	Rishabh Bhaduria
Fatih Balli	Rishiraj Bhattacharyya
Subhadeep Banik	Osman Bıçer

Leon Böck
Vincenzo Botta
Andrea Caforio
Fabio Campos
Avik Chakraborti
Gwangbae Choi
Daniel Collins
Sandro Coretti
Hila Dahari
Nilanjan Datta
Mohammad Sadeq Dousti
Cansu Döğanyay
Alexandre Duc
Sonia Duc
Minxin Du
Ehsan Ebrahimi
Rolf Egert
Keita Emura
Daniel Fentham
Georgios Fotiadis
Daniele Friolo
Sarah Gaballah
Reza Ghasemi
Anirban Ghatak
Simin Ghesmati
Satrajit Ghosh
Tim Grube
Mathias Gusenbauer
Ariel Hamlin
Yahya Hassanzadeh-Nazarabadi
Philipp Holzinger
Lois Huguenin-Dumittan
Vincenzo Iovino
Novak Kaluderovic
Shankar Karuppayah
Handan Kılınç Alper
Maria Kober
Philip Kolvenbach
Veronika Kuchta
Mario Larangeira
Eysa Lee
Wanpeng Li
Fukang Liu
Jack P. K. Ma

Alexandra Mai
Lukas Malina
Karola Marky
Adrian Marotzke
Zdenek Martinasek
Soundes Marzougui
Marc Miltenberger
Jose Moreira
Johannes Mueller
Sayantan Mukherjee
Kit Murdock
Alon Noy (Neuhaus)
Lucien K. L. Ng
Mihai Ordean
Shinjo Park
Guillermo Pascual-Perez
Francesco Pasquale
Leo Perrin
Katharina Pfeffer
Niklas Pirnay
Andreea-Ina Radu
Eyal Ronen
Yann Rotella
Lior Rotem
Sujoy Sinha Roy
Pratik Sarkar
Liron Schiff
Philipp Schindler
Gili Schul-Ganz
Henning Seidler
Kris Shrishak
Rajiv Ranjan Singh
Marjan Skrobot
Najmeh Soroush
Aikaterini Sotiraki
Sanaz Taheri-Boshrooyeh
Hiroto Tamiya
Sam L. Thomas
Bénédict Tran
Itay Tsabary
Andrea Tundis
Rei Ueno
Bogdan Ursu
Jeroen van Wier

Benoit Viguiers
Aidmar Wainakh
Jiafan Wang
Thom Wiggers
Nils Wisiol

Donald P. H. Wong
Harry W. H. Wong
Zohar Yakhini
Hailun Yan
Yongjun Zhao

Contents

Best Papers

An Attack on Some Signature Schemes Constructed from Five-Pass Identification Schemes	3
<i>Daniel Kales and Greg Zaverucha</i>	
Energy Analysis of Lightweight AEAD Circuits	23
<i>Andrea Caforio, Fatih Balli, and Subhadeep Banik</i>	
Cross-Site Search Attacks: Unauthorized Queries over Private Data.	43
<i>Bar Meyuhas, Nethanel Gelernter, and Amir Herzberg</i>	

Cybersecurity

Stronger Targeted Poisoning Attacks Against Malware Detection	65
<i>Shintaro Narisada, Shoichiro Sasaki, Seira Hidano, Toshihiro Uchibayashi, Takuo Suganuma, Masahiro Hiji, and Shinsaku Kiyomoto</i>	
STDNeut: Neutralizing Sensor, Telephony System and Device State Information on Emulated Android Environments.	85
<i>Saurabh Kumar, Debadatta Mishra, Biswabandan Panda, and Sandeep K. Shukla</i>	
HMAC and “Secure Preferences”: Revisiting Chromium-Based Browsers Security	107
<i>Pablo Picazo-Sanchez, Gerardo Schneider, and Andrei Sabelfeld</i>	
Detecting Word Based DGA Domains Using Ensemble Models	127
<i>P. V. Sai Charan, Sandeep K. Shukla, and P. Mohan Anand</i>	

Credentials

Distance-Bounding, Privacy-Preserving Attribute-Based Credentials.	147
<i>Daniel Bosk, Simon Bouget, and Sonja Buchegger</i>	
Trenchcoat: Human-Computable Hashing Algorithms for Password Generation	167
<i>Ruthu Hulikal Rooparaghunath, T. S. Harikrishnan, and Debayan Gupta</i>	
Provably Secure Scalable Distributed Authentication for Clouds	188
<i>Andrea Huszti and Norbert Oláh</i>	

Forward-Secure 0-RTT Goes Live: Implementation and Performance Analysis in QUIC	211
<i>Fynn Dallmeier, Jan P. Drees, Kai Gellert, Tobias Handirk, Tibor Jager, Jonas Klauke, Simon Nachtigall, Timo Renzelmann, and Rudi Wolf</i>	
Elliptic Curves	
Semi-commutative Masking: A Framework for Isogeny-Based Protocols, with an Application to Fully Secure Two-Round Isogeny-Based OT	235
<i>Cyprien Delpéch de Saint Guilhem, Emmanuela Orsini, Christophe Petit, and Nigel P. Smart</i>	
Optimized and Secure Pairing-Friendly Elliptic Curves Suitable for One Layer Proof Composition	259
<i>Youssef El Housni and Aurore Guillevic</i>	
Curves with Fast Computations in the First Pairing Group	280
<i>Rémi Clarisse, Sylvain Duquesne, and Olivier Sanders</i>	
Revisiting ECM on GPUs	299
<i>Jonas Wloka, Jan Richter-Brockmann, Colin Stahlke, Thorsten Kleinjung, Christine Priplata, and Tim Güneysu</i>	
Payment Systems	
Arcula: A Secure Hierarchical Deterministic Wallet for Multi-asset Blockchains	323
<i>Adriano Di Luzio, Danilo Francati, and Giuseppe Ateniese</i>	
Detecting Covert Cryptomining Using HPC	344
<i>Ankit Gangwal, Samuele Giuliano Piazzetta, Gianluca Lain, and Mauro Conti</i>	
Lightweight Virtual Payment Channels	365
<i>Maxim Jourenko, Mario Larangeira, and Keisuke Tanaka</i>	
Privacy-Enhancing Tools	
Chosen-Ciphertext Secure Multi-identity and Multi-attribute Pure FHE	387
<i>Tapas Pal and Ratna Dutta</i>	
Linear Complexity Private Set Intersection for Secure Two-Party Protocols	409
<i>Ferhat Karakoç and Alptekin Küpçü</i>	

Compact Multi-Party Confidential Transactions.	430
<i>Jayamine Alupotha, Xavier Boyen, and Ernest Foo</i>	
Simulation Extractable Versions of Groth’s zk-SNARK Revisited	453
<i>Karim Baghery, Zaira Pindado, and Carla Ràfols</i>	
Efficient Composable Oblivious Transfer from CDH in the Global Random Oracle Model	462
<i>Bernardo David and Rafael Dowsley</i>	
Lightweight Cryptography	
Integral Cryptanalysis of Reduced-Round Tweakable TWINE.	485
<i>Muhammad ElSheikh and Amr M. Youssef</i>	
RiCaSi: Rigorous Cache Side Channel Mitigation via Selective Circuit Compilation.	505
<i>Heiko Mantel, Lukas Scheidel, Thomas Schneider, Alexandra Weber, Christian Weinert, and Tim Weißmantel</i>	
Assembly or Optimized C for Lightweight Cryptography on RISC-V?.	526
<i>Fabio Campos, Lars Jellema, Mauk Lemmen, Lars Müller, Amber Sprenkels, and Benoit Viguier</i>	
Codes and Lattices	
Attack on LAC Key Exchange in Misuse Situation	549
<i>Aurélien Greuet, Simon Montoya, and Guénaél Renault</i>	
Enhancing Code Based Zero-Knowledge Proofs Using Rank Metric	570
<i>Emanuele Bellini, Philippe Gaborit, Alexandros Hasikos, and Victor Mateu</i>	
A Secure Algorithm for Rounded Gaussian Sampling	593
<i>Séamus Brannigan, Maire O'Neill, Ayesha Khalid, and Ciara Rafferty</i>	
Accelerating Lattice Based Proxy Re-encryption Schemes on GPUs	613
<i>Gyana Sahu and Kurt Rohloff</i>	
Author Index	633