

## 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>


Kazue Sako · Nils Ole Tippenhauer (Eds.)

# Applied Cryptography and Network Security

19th International Conference, ACNS 2021  
Kamakura, Japan, June 21–24, 2021  
Proceedings, Part I

*Editors*

Kazue Sako  
Waseda University  
Tokyo, Japan

Nils Ole Tippenhauer   
CISPA Helmholtz Center  
for Information Security  
Saarbrücken, Germany

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-78371-6              ISBN 978-3-030-78372-3 (eBook)  
<https://doi.org/10.1007/978-3-030-78372-3>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021

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

We are pleased to present the proceedings of the 19th International Conference on Applied Cryptography and Network Security (ACNS 2021).

ACNS 2021 was planned to be held in Kamakura, Japan. Due to the ongoing COVID-19 crisis, we decided to have a virtual conference again to ensure the safety of all participants. The organization was in the capable hands of Chunhua Su (University of Aizu, Japan) and Kazumasa Omote (University of Tsukuba, Japan) as general co-chairs, and Ryoma Ito (NICT, Japan) as local organizing chair. We are deeply indebted to them for their tireless work to ensure the success of the conference even in such complex conditions.

For the second time, ACNS had two rounds of submission cycles, with deadlines in September 2020 and January 2021, respectively. We received a total of 186 submissions from authors in 43 countries. This year's Program Committee (PC) consisted of 69 members with diverse backgrounds (among them, 27% female experts) and broad research interests. The review process was double-blind and rigorous, and papers were evaluated on the basis of research significance, novelty, and technical quality. 539 reviews were submitted in total, with at least 3 reviews for most papers.

Some papers submitted in the first round received a decision of major revision. The revised version of those papers were further evaluated in the second round and most of them were accepted. After the review process concluded, a total of 37 papers were accepted to be presented at the conference and included in the proceedings, representing an acceptance rate of around 20%.

Among those papers, 27 were co-authored and presented by full-time students. From this subset, we awarded the Best Student Paper Award to Angèle Bossuat (IRISA, France) for the paper “Unlinkable and Invisible  $\gamma$ -Sanitizable Signatures” (co-authored with Xavier Bultel). The reviewers particularly appreciated its clear and convincing motivation and explanation of the intuition behind the approach, and the strong properties achieved by the proposed sanitizable signature scheme. The monetary prize of 1,000 euro was generously sponsored by Springer.

We had a rich program including eight satellite workshops in parallel with the main event, providing a forum to address specific topics at the forefront of cybersecurity research. The papers presented at those workshops were published in separate proceedings.

This year we had three outstanding keynote talks: “Privacy-Preserving Authentication: Concepts, Applications, and New Advances” by Prof. Anja Lehmann (Hasso Plattner Institute, Germany), “Digital Being” presented by Nat Sakimura (OpenID Foundation, Japan), and “Cryptography and the Changing Landscape of Payment Fraud” by Prof. Ross Anderson (University of Cambridge and University of Edinburgh, UK). To them, our heartfelt gratitude for their outstanding presentations.

In this very unusual year, the conference was made possible by the untiring efforts of many individuals and organizations. We are grateful to all the authors for their

submissions. We sincerely appreciate the outstanding work of all the PC members and the external reviewers, who selected the papers after reading, commenting, and debating them. Finally, we thank all the people who volunteered their time and energy to put together the conference, speakers and session chairs, and everyone who contributed to the success of the conference.

Last, but certainly not least, we are very grateful to Mitsubishi Electric for sponsoring the conference, and Springer for their help in assembling these proceedings.

June 2021

Kazuo Sako  
Nils Ole Tippenhauer

# Organization

## General Co-chairs

Chunhua Su	University of Aizu, Japan
Kazumasa Omote	University of Tsukuba, Japan

## Program Co-chairs

Kazue Sako	Waseda University, Japan
Nils Ole Tippenhauer	CISPA, Germany

## Publicity Chair

Keita Emura	NICT, Japan
-------------	-------------

## Workshop Chair

Jianying Zhou	Singapore University of Technology and Design, Singapore
---------------	---

## Poster Chair

Masaki Shimaoka	University of Tsukuba/SECOM, Japan
-----------------	------------------------------------

## Local Organizing Chair

Ryoma Ito	NICT, Japan
-----------	-------------

## Program Committee

Mitsuaki Akiyama	NTT, Japan
Cristina Alcaraz	UMA, Spain
Giuseppe Ateniese	Stevens Institute of Technology, USA
Man Ho Au	The University of Hong Kong, Hong Kong
Lejla Batina	Radboud University, the Netherlands
Alex Biryukov	University of Luxembourg, Luxembourg
Ferdinand Brasser	TU Darmstadt, Germany
Christopher Brzuska	Aalto University, Finland
Alvaro Cardenas	The University of Texas at Dallas, USA
Sudipta Chattopadhyay	SUTD, Singapore
Liqun Chen	University of Surrey, UK
Xiaofeng Chen	Xidian University, China

Jiska Classen	TU Darmstadt, Germany
Hervé Debar	Télécom SudParis, France
Stephanie Delaune	IRISA, France
Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Christian Doerr	Delft University of Technology, the Netherlands
F. Betül Durak	Ecole Polytechnique Fédérale de Lausanne, Switzerland
Nico Döttling	CISPA Helmholtz Center for Information Security, Germany
Karim Eldefrawy	SRI International, USA
Zekeriya Erkin	Delft University of Technology, the Netherlands
Olga Gadyatskaya	Leiden University, the Netherlands
Joaquin Garcia-Alfaro	Institut Polytechnique de Paris, France
Paolo Gasti	New York Institute of Technology, USA
Dieter Gollmann	Hamburg University of Technology, Germany
Stefanos Gritzalis	University of Piraeus, Greece
Xinyi Huang	Fujian Normal University, China
Antoine Joux	Fondation Partenariale de l'UPMC/IMJ-PRG, France
Ghassan Karame	NEC Laboratories Europe, Germany
Stefan Katzenbeisser	University of Passau, Germany
Hiroaki Kikuchi	Meiji University, Japan
Qi Li	Tsinghua University, China
Zhiqiang Lin	Ohio State University, USA
Joseph Liu	Monash University, Australia
Xiapu Luo	The Hong Kong Polytechnic University, Hong Kong
Emil Lupu	Imperial College London, UK
Di Ma	University of Michigan, USA
Mark Manulis	University of Surrey, UK
Takahiro Matsuda	National Institute of Advanced Industrial Science and Technology, Japan
Sjouke Mauw	University of Luxembourg, Luxembourg
Catherine Meadows	NRL, USA
Nele Mentens	Leiden University, the Netherlands
Kazuhiko Minematsu	NEC Corporation, Japan
Veelasha Moonsamy	Ruhr University Bochum, Germany
Toru Nakanishi	Hiroshima University, Japan
Satoshi Obana	Hosei University, Japan
Martín Ochoa	AppGate Inc., Columbia
Wakaha Ogata	Tokyo Institute of Technology, Japan
Miyako Ohkubo	NICT, Japan
Christina Pöpper	New York University, USA
Aanjhan Ranganathan	Northeastern University, USA
Joel Reardon	University of Calgary, Canada
Ruben Rios	University of Malaga, Spain
Sushmita Ruj	CSIRO, Australia
Mark Ryan	University of Birmingham, UK



Reihaneh Safavi-Naini	University of Calgary, Canada
Kazue Sako	Waseda University, Japan
Steve Schneider	University of Surrey, UK
Sooel Son	Korea Advanced Institute of Science and Technology, South Korea
Hung-Min Sun	National Tsing Hua University, Taiwan
Willy Susilo	University of Wollongong, Australia
Pawel Szalachowski	Google, USA
Qiang Tang	University of Sydney, Australia
Vanessa Teague	Thinking Cybersecurity, Australia
Nils Ole Tippenhauer	CISPA Helmholtz Center for Information Security, Germany
A. Selcuk Uluagac	Florida International University, USA
Edgar Weippl	University of Vienna, Austria
Christian Wressnegger	Karlsruhe Institute of Technology, Germany
Kehuan Zhang	The Chinese University of Hong Kong, Hong Kong

## Additional Reviewers

Akand, Mamun	Florez, Johana
Amjad, Ghous	Gan, Qingqing
Anada, Hiroaki	Gardham, Daniel
Anagnostopoulos, Marios	Genise, Nicholas
Banik, Subhadeep	Gerault, David
Blazy, Olivier	Ghesmati, Simin
Booth, Roland	Ghosh, Koustabh
Braeken, An	Gontier, Arthur
Briongos, Samira	Grassi, Lorenzo
Bultel, Xavier	Guo, Kaiwen
Buser, Maxime	Gálvez, Rafa
Chen, Long	Hameed, Muhammad Zaid
Chen, Xihui	Han, Jinguang
Chen, Yi	Hashimoto, Keitaro
Chengjun Lin	Hirano, Takato
Co, Kenneth	Homoliak, Ivan
Cui, Tingting	Hoshino, Fumitaka
Dekker, F. W.	Hou, Zhenduo
Diao, Wenrui	Hsu, Chingfang
Diugan, Raluca	Hu, Kexin
Duong, Dung Hoang	Huguenin-Dumittan, Loïs
Dutta, Sabyasachi	Hülsing, Andreas
El Hirsch, Solane	Ichikawa, Atsunori
Eliyan, Lubna	Isobe, Takanori
Ersoy, Oguzhan	Issiki, Toshiyuki
Feng, Hanwen	Jangid, Mohit
Fentham, Daniel	Jiang, Shaoquan
Ferreira Torres, Christof	Jiang, Yuting

Judmayer, Aljosha	Schuldt, Jacob
Kannwischer, Matthias J.	Schwabe, Peter
Kasra, Shabnam	Shen, Jun
Kim, Joongyum	Shirase, Masaaki
Laing, Thalia May	Sideri, Maria
Larangeira, Mario	Smith, Zach
Leurent, Gaëtan	Song, Ling
Li, Jiguo	Song, Yongcheng
Li, Tianyu	Song, Zirui
Li, Xinyu	Stifter, Nicholas
Li, Yanan	Sun, Siwei
Libert, Benoît	Suzuki, Koutarou
Liu, Jia	Tang, Di
Lopez, Christian	Tengana, Lizzy
Lu, Xingye	Terner, Ben
Lu, Yuan	Tiepelt, Marcel
Ma, Jinhua	Tikhomirov, Sergei
Mahawaga Arachchige, Pathum Chamikara	Tomita, Toui
Marotzke, Adrian	Tsohou, Aggeliki
Mazumdar, Subhra	van Bruggen, Christian
McMurtry, Eleanor	van Tetering, Daphne
Mirza, Shujaat	Vaudenay, Serge
Miteloudi, Konstantina	Vitto, Giuseppe
Moreau, Solène	Vliegen, Jo
Niederhagen, Ruben	Wang, Jianfeng
Ning, Jianting	Wang, Qingju
Nishide, Takashi	Wang, Yongqi
Orsini, Emmanuela	Weiqlang Wen
Pan, Jiaxin	Wi, Seongil
Pan, Jing	Wu, Jiaojiao
Pang, Bo	Xu, Yanhong
Papamartzivanos, Dimitrios	Xue, Haiyang
Park, Sunnyeo	Yamakawa, Takashi
Pasquini, Dario	Yan, Hailun
Pereira, Vitor	Yang, Guomin
Pilgun, Aleksandr	Yang, Rupeng
Prabel, Lucas	Yang, S. J.
Qiu, Tian	Yang, Wenjie
Rabbani, Md Masoom	Yin, Qilei
Ramírez-Cruz, Yuniór	Yoneyama, Kazuki
Reijsbergen, Daniel	Yuan, Xingliang
Rivera, Esteban	Zeilberger, Hadas
Roenne, Peter	Zhang, Peng
Sato, Masaya	Zhang, Xiaoyu
Schindler, Philipp	Zhang, Yuexin
	Zhang, Zeyu

# Contents – Part I

## Cryptographic Protocols

Adaptive-ID Secure Hierarchical ID-Based Authenticated Key Exchange Under Standard Assumptions Without Random Oracles . . . . .	3
<i>Ren Ishibashi and Kazuki Yoneyama</i>	
Analysis of Client-Side Security for Long-Term Time-Stamping Services. . . .	28
<i>Long Meng and Liqun Chen</i>	
Towards Efficient and Strong Backward Private Searchable Encryption with Secure Enclaves. . . . .	50
<i>Viet Vo, Shangqi Lai, Xingliang Yuan, Surya Nepal, and Joseph K. Liu</i>	

## Secure and Fair Protocols

CECMLP: New Cipher-Based Evaluating Collaborative Multi-layer Perceptron Scheme in Federated Learning . . . . .	79
<i>Yuqi Chen, Xiaoyu Zhang, Yi Xie, Meixia Miao, and Xu Ma</i>	
Blind Polynomial Evaluation and Data Trading. . . . .	100
<i>Yi Liu, Qi Wang, and Siu-Ming Yiu</i>	
Coin-Based Multi-party Fair Exchange . . . . .	130
<i>Handan Kılınç Alper and Alptekin Küpçü</i>	

## Cryptocurrency and Smart Contracts

P2DEX: Privacy-Preserving Decentralized Cryptocurrency Exchange. . . . .	163
<i>Carsten Baum, Bernardo David, and Tore Kasper Frederiksen</i>	
W-OTS <sup>+</sup> Up My Sleeve! A Hidden Secure Fallback for Cryptocurrency Wallets. . . . .	195
<i>David Chaum, Mario Larangeira, Mario Yaksetig, and William Carter</i>	
Terrorist Attacks for Fake Exposure Notifications in Contact Tracing Systems . . . . .	220
<i>Gennaro Avitabile, Daniele Friolo, and Ivan Visconti</i>	

## Digital Signatures

Unlinkable and Invisible $\gamma$ -Sanitizable Signatures . . . . .	251
<i>Angèle Bossuat and Xavier Bultel</i>	

Partially Structure-Preserving Signatures: Lower Bounds, Constructions and More . . . . .	284
<i>Essam Ghadafi</i>	
An Efficient Certificate-Based Signature Scheme in the Standard Model . . . .	313
<i>Guoqiang Wang and Yanmei Cao</i>	
<b>Embedded System Security</b>	
SnakeGX: A Sneaky Attack Against SGX Enclaves . . . . .	333
<i>Flavio Toffalini, Mariano Graziano, Mauro Conti, and Jianying Zhou</i>	
Telepathic Headache: Mitigating Cache Side-Channel Attacks on Convolutional Neural Networks . . . . .	363
<i>Hervé Chabanne, Jean-Luc Danger, Linda Guiga, and Ulrich Kühne</i>	
Efficient FPGA Design of Exception-Free Generic Elliptic Curve Cryptosystems . . . . .	393
<i>Kiyofumi Tanaka, Atsuko Miyaji, and Yaoan Jin</i>	
<b>Lattice Cryptography</b>	
Access Control Encryption from Group Encryption . . . . .	417
<i>Xiuhua Wang, Harry W. H. Wong, and Sherman S. M. Chow</i>	
Password Protected Secret Sharing from Lattices. . . . .	442
<i>Partha Sarathi Roy, Sabyasachi Dutta, Willy Susilo, and Reihaneh Safavi-Naini</i>	
Efficient Homomorphic Conversion Between (Ring) LWE Ciphertexts . . . . .	460
<i>Hao Chen, Wei Dai, Miran Kim, and Yongsoo Song</i>	
<b>Author Index</b> . . . . .	481

# Contents – Part II

## Analysis of Applied Systems

Breaking and Fixing Third-Party Payment Service for Mobile Apps . . . . .	3
<i>Shangcheng Shi, Xianbo Wang, and Wing Cheong Lau</i>	
DSS: Discrepancy-Aware Seed Selection Method for ICS Protocol Fuzzing . . . . .	27
<i>Shuangpeng Bai, Hui Wen, Dongliang Fang, Yue Sun, Puzhuo Liu, and Limin Sun</i>	
Threat for the Secure Remote Password Protocol and a Leak in Apple’s Cryptographic Library . . . . .	49
<i>Andy Russon</i>	

## Secure Computations

Privacy-Preserving Data Aggregation with Probabilistic Range Validation . . .	79
<i>F. W. Dekker and Zekeriya Erkin</i>	
LLVM-Based Circuit Compilation for Practical Secure Computation . . . . .	99
<i>Tim Heldmann, Thomas Schneider, Oleksandr Tkachenko, Christian Weinert, and Hossein Yalame</i>	
An Efficient Passive-to-Active Compiler for Honest-Majority MPC over Rings . . . . .	122
<i>Mark Abspoel, Anders Dalskov, Daniel Escudero, and Ariel Nof</i>	

## Cryptanalysis

Experimental Review of the IKK Query Recovery Attack: Assumptions, Recovery Rate and Improvements . . . . .	155
<i>Ruben Groot Roessink, Andreas Peter, and Florian Hahn</i>	
Efficient Methods to Search for Best Differential Characteristics on SKINNY . . . . .	184
<i>Stéphanie Delaune, Patrick Derbez, Paul Huynh, Marine Minier, Victor Mollimard, and Charles Prud’homme</i>	
Towards Efficient LPN-Based Symmetric Encryption . . . . .	208
<i>Sonia Bogos, Dario Korolija, Thomas Locher, and Serge Vaudenay</i>	

## System Security

A Differentially Private Hybrid Approach to Traffic Monitoring . . . . .	233
<i>Rogério V. M. Rocha, Pedro P. Libório, Harsh Kupwade Patil, and Diego F. Aranha</i>	
Proactive Detection of Phishing Kit Traffic . . . . .	257
<i>Qian Cui, Guy-Vincent Jourdan, Gregor V. Bochmann, and Iosif-Viorel Onut</i>	
VESTIGE: Identifying Binary Code Provenance for Vulnerability Detection . . .	287
<i>Yuede Ji, Lei Cui, and H. Howie Huang</i>	
SoK: Auditability and Accountability in Distributed Payment Systems. . . . .	311
<i>Panagiotis Chatzigiannis, Foteini Baldimtsi, and Konstantinos Chalkias</i>	
Defending Web Servers Against Flash Crowd Attacks. . . . .	338
<i>Rajat Tandon, Abhinav Palia, Jaydeep Ramani, Brandon Paulsen, Genevieve Bartlett, and Jelena Mirkovic</i>	

## Cryptography and Its Applications

TurboIKOS: Improved Non-interactive Zero Knowledge and Post-quantum Signatures . . . . .	365
<i>Yaron Gvili, Julie Ha, Sarah Scheffler, Mayank Varia, Ziling Yang, and Xinyuan Zhang</i>	
Cryptanalysis of the Binary Permuted Kernel Problem. . . . .	396
<i>Thales Bandiera Paiva and Routo Terada</i>	
Security Comparisons and Performance Analyses of Post-quantum Signature Algorithms. . . . .	424
<i>Manohar Raavi, Simeon Wuthier, Pranav Chandramouli, Yaroslav Balytskyi, Xiaobo Zhou, and Sang-Yoon Chang</i>	
Tighter Proofs for the SIGMA and TLS 1.3 Key Exchange Protocols . . . . .	448
<i>Hannah Davis and Felix Günther</i>	
Improved Structured Encryption for SQL Databases via Hybrid Indexing. . . .	480
<i>David Cash, Ruth Ng, and Adam Rivkin</i>	
Author Index . . . . .	511