

Giuseppe Ateniese
Daniele Venturi (Eds.)

LNCS 13269

Applied Cryptography and Network Security

20th International Conference, ACNS 2022
Rome, Italy, June 20–23, 2022
Proceedings



 Springer

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

Moti Yung 

Columbia University, New York, NY, USA


More information about this series at <https://link.springer.com/bookseries/558>

Giuseppe Ateniese · Daniele Venturi (Eds.)

Applied Cryptography and Network Security

20th International Conference, ACNS 2022
Rome, Italy, June 20–23, 2022
Proceedings

Editors

Giuseppe Ateniese 
Stevens Institute of Technology
Hoboken, NJ, USA

Daniele Venturi 
Sapienza University of Rome
Rome, Italy

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-09233-6

ISBN 978-3-031-09234-3 (eBook)

<https://doi.org/10.1007/978-3-031-09234-3>

© Springer Nature Switzerland AG 2022

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 20th International Conference on Applied Cryptography and Network Security (ACNS 2022). ACNS 2022 was held in Rome, Italy. Due to the ongoing COVID-19 crisis, we decided to have a hybrid conference to face any health risks or travel restrictions for attending the conference. The organization was in the capable hands of Mauro Conti (University of Padua, Italy) and Angelo Spognardi (Sapienza University of Rome, Italy) as general co-chairs, and Massimo Bernaschi (National Research Council, IAC-CNR, Italy) and Fabio De Gaspari (Sapienza University of Rome, Italy) as local organizing chairs. We are deeply indebted to them for their tireless work to ensure the success of the conference even in such complex conditions.

For the third time, ACNS had two rounds of submission cycles, with deadlines in September 2021 and January 2022, respectively. We received a total of 185 submissions from authors in 37 countries. This year's Program Committee (PC) consisted of around 150 members with diverse backgrounds 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. In total, 691 reviews were submitted, with four reviews for most papers. Some papers submitted in the first round received a decision of major revision. The revised versions of those papers were further evaluated in the second round and some of them were accepted. After the review process concluded, a total of 44 papers were accepted to be presented at the conference and included in the proceedings, representing an acceptance rate of around 24%.

Among those papers, we awarded the Best Student Paper Award to Narmeen Shafqat (Northeastern University, Boston, MA, USA) for the paper "ZLeaks: Passive Inference Attacks on Zigbee based Smart Homes" (co-authored with Daniel J. Dubois, David Choffnes, Aaron Schulman, Dinesh Bharadia, and Aanjhan Ranganathan). 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 two outstanding keynote talks: "Chosen Ciphertext Security from Injective Trapdoor Functions" by Prof. Susan Hohenberger Waters (Johns Hopkins University, USA), and "Secure Computation in Practice" by Prof. Raluca Ada Popa (University of California, Berkeley, USA). To them, our heartfelt gratitude for their outstanding presentations.

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, the speakers and session chairs, and everyone who contributed to the success of the

conference. We are also grateful to Riccardo Lazzeretti (Sapienza University of Rome, Italy) for taking care of these proceedings. Last, but certainly not least, we are very grateful to Frontiers for sponsoring the conference, EasyChair for the management of the submissions, and Springer for their help in assembling these proceedings.

June 2022

Daniele Venturi
Giuseppe Ateniese

Organization

General Chairs

Mauro Conti

University of Padua, Italy

Angelo Spognardi

Sapienza University of Rome, Italy

Program Chairs

Giuseppe Ateniese

Stevens Institute of Technology, USA

Daniele Venturi

Sapienza University of Rome, Italy

Workshop Chair

Jianying Zhou

Singapore University of Technology and Design,
Singapore

Poster Chair

Emiliano Casalicchio

Sapienza University of Rome, Italy

Local Organization Chairs

Massimo Bernaschi

National Council of Research, Italy

Fabio De Gaspari

Sapienza University of Rome, Italy

Publicity Chair

Alessandro Brighente

University of Padua, Italy

Publication Chair

Riccardo Lazzeretti

Sapienza University of Rome, Italy

Web Chair

Alicia K. Bidi

Sapienza University of Rome, Italy

Program Committee

Masayuki Abe	NTT, Japan
Mitsuaki Akiyama	NTT, Japan
Cristina Alcaraz	University of Malaga, Spain
Giuseppe Ateniese	George Mason University, USA
Xiaolong Bai	Alibaba Group, China
Lejla Batina	Radboud University, The Netherlands
Carsten Baum	Aarhus University, Denmark
Estuardo Bock	Aalto University, Finland
Matteo Campanelli	Protocol Labs, Denmark
Ignacio Cascudo	IMDEA Software Institute, Spain
Sang Kil Cha	Korea Advanced Institute of Science and Technology, South Korea
Sudipta Chattopadhyay	Singapore University of Technology and Design, Singapore
Sherman S. M. Chow	Chinese University of Hong Kong, Hong Kong
Michele Ciampi	University of Edinburgh, UK
Mauro Conti	University of Padua, Italy
Sandro Coretti	IOHK, Switzerland
Marc Dacier	Qatar Computing Research Institute, Qatar
Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Nico Döttling	Aarhus University, Denmark
Antonio Faonio	EURECOM, France
Prastudy Fauzi	Simula UiB, Norway
Tommaso Gagliardoni	Kudelski Security, Switzerland
Chaya Ganesh	Aarhus University, Denmark
Debin Gao	Singapore Management University, Singapore
Paolo Gasti	New York Institute of Technology, USA
Esha Ghosh	Microsoft, USA
Yong Guan	Iowa State University, USA
Susan Hohenberger	Johns Hopkins University, USA
Hsu-Chun Hsiao	National Taiwan University, China
Hongxin Hu	University at Buffalo, SUNY, USA
Xinyi Huang	Fujian Normal University, China
Sotiris Ioannidis	Technical University of Crete, Greece
Hai Jin	Huazhong University of Science and Technology, China
Stefan Katzenbeisser	University of Passau, Germany
Kwok Yan Lam	Nanyang Technological University, Singapore
Peeter Laud	Cybernetica AS, Estonia
Xiapu Luo	Hong Kong Polytechnic University, Hong Kong

Bernardo Magri	Aarhus University, Denmark
Mark Manulis	Universität der Bundeswehr München, Germany
Giorgia Azzurra Marson	NEC Labs Europe, Germany
Daniel Masny	Meta, USA
Christian Matt	Concordium, Switzerland
Vashek Matyas	Masaryk University, Czech Republic
Veelasha Moonsamy	Ruhr University Bochum, Germany
Pratyay Mukherjee	Hedera Hashgraph/Swirlds, USA
David Naccache	ENS, France
Ariel Nof	Technion, Israel
Sabine Oechsner	University of Edinburgh, UK
Cristina Onete	Université de Limoges, France
Gerardo Pelosi	Politecnico di Milano, Italy
Giuseppe Persiano	Università degli Studi di Salerno, Italy
Thomas Peters	Université catholique de Louvain, Belgium
Josef Pieprzyk	CSIRO/Data61, Australia
Bertram Poettering	IBM Research - Zurich, Switzerland
Divya Ravi	Aarhus University, Denmark
Reihaneh Safavi-Naini	University of Calgary, Canada
Nitesh Saxena	Texas A&M University, USA
Janno Siim	University of Tartu, Finland
Mark Simkin	Ethereum Foundation
Angelo Spognardi	Sapienza Università di Roma, Italy
Purui Su	Institute of Software, CAS, China
Qiang Tang	University of Sydney, Australia
Mehdi Tibouchi	NTT, Japan
Daniel Tschudi	Concordium, Switzerland
Yiannis Tselekounis	University of Edinburgh
Daniele Venturi	Sapienza University of Rome, Italy
Ivan Visconti	University of Salerno, Italy
Cong Wang	City University of Hong Kong, Hong Kong
Zhaoyan Xu	Palo Alto Networks, USA
Chao Zhang	Tsinghua University, China
Fan Zhang	Zhejiang University, China
Kehuan Zhang	Chinese University of Hong Kong, Hong Kong
Yinqian Zhang	Southern University of Science and Technology, China
Hong-Sheng Zhou	Virginia Commonwealth University, USA
Jianying Zhou	Singapore University of Technology and Design, Singapore
Yajin Zhou	Zhejiang University, China

Contents

Encryption

Keyed-Fully Homomorphic Encryption Without Indistinguishability Obfuscation	3
<i>Shingo Sato, Keita Emura, and Atsushi Takayasu</i>	
A Performance Evaluation of Pairing-Based Broadcast Encryption Systems	24
<i>Arush Chhatrapati, Susan Hohenberger, James Trombo, and Satyanarayana Vusirikala</i>	
An Optimized GHV-Type HE Scheme: Simpler, Faster, and More Versatile	45
<i>Liang Zhao, Ze Chen, Liqun Chen, and Xinyi Huang</i>	

Attacks

Analyzing the Provable Security Bounds of GIFT-COFB and Photon-Beetle ...	67
<i>Akiko Inoue, Tetsu Iwata, and Kazuhiko Minematsu</i>	
Beware of Your Vibrating Devices! Vibrational Relay Attacks on Zero-Effort Deauthentication	85
<i>Prakash Shrestha and Nitesh Saxena</i>	
ZLeaks: Passive Inference Attacks on Zigbee Based Smart Homes	105
<i>Narmeen Shafqat, Daniel J. Dubois, David Choffnes, Aaron Schulman, Dinesh Bharadia, and Aanijhan Ranganathan</i>	
Passive Query-Recovery Attack Against Secure Conjunctive Keyword Search Schemes	126
<i>Marco Dijkslag, Marc Damie, Florian Hahn, and Andreas Peter</i>	
Gummy Browsers: Targeted Browser Spoofing Against State-of-the-Art Fingerprinting Techniques	147
<i>Zengrui Liu, Prakash Shrestha, and Nitesh Saxena</i>	
Identifying Near-Optimal Single-Shot Attacks on ICSs with Limited Process Knowledge	170
<i>Herson Esquivel-Vargas, John Henry Castellanos, Marco Caselli, Nils Ole Tippenhauer, and Andreas Peter</i>	

RSA Key Recovery from Digit Equivalence Information	193
<i>Chitchanok Chuengsatiansup, Andrew Feutrill, Rui Qi Sim, and Yuval Yarom</i>	
Practical Seed-Recovery of Fast Cryptographic Pseudo-Random Number Generators	212
<i>Florette Martinez</i>	
Autoguess: A Tool for Finding Guess-and-Determine Attacks and Key Bridges	230
<i>Hosein Hadipour and Maria Eichlseder</i>	
Cryptographic Protocols	
KEMTLS with Delayed Forward Identity Protection in (Almost) a Single Round Trip	253
<i>Felix Günther, Simon Rastikian, Patrick Towa, and Thom Wiggers</i>	
Improving the Privacy of Tor Onion Services	273
<i>Edward Eaton, Sajin Sasy, and Ian Goldberg</i>	
Privacy-Preserving Authenticated Key Exchange for Constrained Devices	293
<i>Loïc Ferreira</i>	
Relations Between Privacy, Verifiability, Accountability and Coercion-Resistance in Voting Protocols	313
<i>Alisa Pankova and Jan Willemson</i>	
System Security	
An Approach to Generate Realistic HTTP Parameters for Application Layer Deception	337
<i>Merve Sahin, Cédric Hébert, and Rocio Cabrera Lozoya</i>	
IPSpex: Enabling Efficient Fuzzing via Specification Extraction on ICS Protocol	356
<i>Yue Sun, Shichao Lv, Jianzhou You, Yuyan Sun, Xin Chen, Yaowen Zheng, and Limin Sun</i>	
Probing for Passwords – Privacy Implications of SSIDs in Probe Requests	376
<i>Johanna Ansohn McDougall, Christian Burkert, Daniel Demmler, Monina Schwarz, Vincent Hubbe, and Hannes Federrath</i>	

Cryptographic Primitives

A Cryptographic View of Deep-Attestation, or How to Do Provably-Secure Layer-Linking	399
<i>Ghada Arfaoui, Pierre-Alain Fouque, Thibaut Jacques, Pascal Lafourcade, Adina Nedelcu, Cristina Onete, and Léo Robert</i>	
Don't Tamper with Dual System Encryption: Beyond Polynomial Related-Key Security of IBE	419
<i>Tsz Hon Yuen, Cong Zhang, and Sherman S. M. Chow</i>	
Progressive and Efficient Verification for Digital Signatures	440
<i>Cecilia Boschini, Dario Fiore, and Elena Pagnin</i>	
Revocable Hierarchical Attribute-Based Signatures from Lattices	459
<i>Daniel Gardham and Mark Manulis</i>	
Covert Authentication from Lattices	480
<i>Rajendra Kumar and Khoa Nguyen</i>	
Spreading the Privacy Blanket: Differentially Oblivious Shuffling for Differential Privacy	501
<i>Dov Gordon, Jonathan Katz, Mingyu Liang, and Jiayu Xu</i>	
Bootstrapping for Approximate Homomorphic Encryption with Negligible Failure-Probability by Using Sparse-Secret Encapsulation	521
<i>Jean-Philippe Bossuat, Juan Troncoso-Pastoriza, and Jean-Pierre Hubaux</i>	
(Commit-and-Prove) Predictable Arguments with Privacy	542
<i>Hamidreza Khoshakhlagh</i>	
MPC	
Communication-Efficient Proactive MPC for Dynamic Groups with Dishonest Majorities	565
<i>Karim Eldefrawy, Tancrede Lepoint, and Antonin Leroux</i>	
PSI-Stats: Private Set Intersection Protocols Supporting Secure Statistical Functions	585
<i>Jason H. M. Ying, Shuwei Cao, Geong Sen Poh, Jia Xu, and Hoon Wei Lim</i>	
Efficient Oblivious Evaluation Protocol and Conditional Disclosure of Secrets for DFA	605
<i>Kittiphop Phalakarn, Nuttapong Attrapadung, and Kanta Matsuura</i>	

Efficient and Tight Oblivious Transfer from PKE with Tight Multi-user Security	626
<i>Saikrishna Badrinarayanan, Daniel Masny, and Pratyay Mukherjee</i>	
Efficient Two-Party Exponentiation from Quotient Transfer	643
<i>Yi Lu, Keisuke Hara, Kazuma Ohara, Jacob Schuldt, and Keisuke Tanaka</i>	
Efficient Compiler to Covert Security with Public Verifiability for Honest Majority MPC	663
<i>Thomas Attema, Vincent Dunning, Maarten Everts, and Peter Langenkamp</i>	
How Byzantine is a Send Corruption?	684
<i>Karim Eldefrawy, Julian Loss, and Ben Terner</i>	
Blockchain	
Babel Fees via Limited Liabilities	707
<i>Manuel M. T. Chakravarty, Nikos Karayannidis, Aggelos Kiayias, Michael Peyton Jones, and Polina Vinogradova</i>	
FAST: Fair Auctions via Secret Transactions	727
<i>Bernardo David, Lorenzo Gentile, and Mohsen Pourpouneh</i>	
Astrape: Anonymous Payment Channels with Boring Cryptography	748
<i>Yuhao Dong, Ian Goldberg, Sergey Gorbunov, and Raouf Boutaba</i>	
Block-Cyphers	
A White-Box Speck Implementation Using Self-equivalence Encodings	771
<i>Joachim Vandersmissen, Adrián Ranea, and Bart Preneel</i>	
Improved Differential-Linear Attack with Application to Round-Reduced Speck _{32/64}	792
<i>Feifan Wang and Gaoli Wang</i>	
Deep Neural Networks Aiding Cryptanalysis: A Case Study of the Speck Distinguisher	809
<i>Norica Băcuieti, Lejla Batina, and Stjepan Picek</i>	
Post-quantum Cryptography	
Carry-Less to BIKE Faster	833
<i>Ming-Shing Chen, Tim Güneysu, Markus Krausz, and Jan Philipp Thoma</i>	

Faster Kyber and Dilithium on the Cortex-M4 853
*Amin Abdulrahman, Vincent Hwang, Matthias J. Kannwischer,
and Daan Sprenkels*

**Quantum-Resistant Software Update Security on Low-Power Networked
Embedded Devices** 872
*Gustavo Banegas, Koen Zandberg, Emmanuel Baccelli,
Adrian Herrmann, and Benjamin Smith*

Post-quantum ID-Based Ring Signatures from Symmetric-Key Primitives 892
Maxime Buser, Joseph K. Liu, Ron Steinfeld, and Amin Sakzad

Author Index 913