

Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering

448

Editorial Board Members

Ozgur Akan

Middle East Technical University, Ankara, Turkey

Paolo Bellavista

University of Bologna, Bologna, Italy

Jiannong Cao

Hong Kong Polytechnic University, Hong Kong, China

Geoffrey Coulson

Lancaster University, Lancaster, UK

Falko Dressler

University of Erlangen, Erlangen, Germany

Domenico Ferrari

Università Cattolica Piacenza, Piacenza, Italy

Mario Gerla

UCLA, Los Angeles, USA

Hisashi Kobayashi

Princeton University, Princeton, USA

Sergio Palazzo

University of Catania, Catania, Italy

Sartaj Sahni

University of Florida, Gainesville, USA

Xuemin Shen 

University of Waterloo, Waterloo, Canada

Mircea Stan

University of Virginia, Charlottesville, USA

Xiaohua Jia

City University of Hong Kong, Kowloon, Hong Kong

Albert Y. Zomaya

University of Sydney, Sydney, Australia


More information about this series at <https://link.springer.com/bookseries/8197>

Jingqiang Lin · Qiang Tang (Eds.)

Applied Cryptography in Computer and Communications

Second EAI International Conference, AC3 2022
Virtual Event, May 14–15, 2022
Proceedings

Editors

Jingqiang Lin 
University of Science and Technology
of China
Hefei, Anhui, China

Qiang Tang
The University of Sydney
Sydney, NSW, Australia

ISSN 1867-8211

ISSN 1867-822X (electronic)

Lecture Notes of the Institute for Computer Sciences, Social Informatics
and Telecommunications Engineering

ISBN 978-3-031-17080-5

ISBN 978-3-031-17081-2 (eBook)

<https://doi.org/10.1007/978-3-031-17081-2>

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 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 delighted to introduce the proceedings of the 2022 European Alliance for Innovation (EAI) International Conference on Applied Cryptography in Computer and Communications (AC3 2022). This conference brought together researchers, developers, and practitioners around the world who focus on all technical aspects of applied cryptography including, but not limited to, cryptographic algorithms, protocols, implementations, standards and practices, and applications of cryptography in computer, information, and system security. Some of the works presented at AC3 2022 also applied cryptographic technologies to solve security problems in real-world systems, including cloud services, the Internet of Things, cyber-physical systems, distributed systems, edge computing, information-centric networks, databases, data centers, etc.

The technical program of AC3 2022 consisted of 14 papers in oral presentation sessions at six main conference tracks: Track 1 – Quantum-Safe Cryptographic Solution; Track 2 – Applied Cryptography for IoT; Track 3 – Authentication Protocol; Track 4 – Real-World Applied Cryptography; Track 5 – Network Attack and Defense; and Track 6 – Security Application. Aside from the high-quality technical paper presentations, the technical program also featured two keynote speeches delivered by Juan A. Garay from Texas A&M University, USA, and Meiqin Wang from Shandong University, China.

Coordination with the steering committee, including Imrich Chlamtac (chair), Bo Chen, and Bo Luo, was essential for the success of the conference. We sincerely appreciate their constant support and guidance. It was also a great pleasure to work with such an excellent organizing committee team for their hard work in organizing and supporting the conference. In particular, we are grateful to the Technical Program Committee, who completed the peer-review process for the technical papers and helped to put together a high-quality technical program. We are also grateful to Conference Managers Martin Vojtek and Lucia Sedlarova for their support and all the authors who submitted their papers to the AC3 2022 conference.

We strongly believe that the AC3 conference provides a good forum for all researchers, developers, and practitioners to discuss all science and technology aspects that are relevant to applied cryptography. We also expect that the future AC3 conferences will be as successful and stimulating as this year's, as indicated by the contributions presented in this volume.

May 2021

Jingqiang Lin
Qiang Tang

Organization

Steering Committee

Imrich Chlamtac	University of Trento, Italy
Bo Chen	Michigan Technological University, USA
Jingqiang Lin	University of Science and Technology of China, China
Bo Luo	University of Kansas, USA

Organizing Committee

Honorary Chair

Yongbiao Liu	Jinling Institute of Technology, China
--------------	--

General Chairs

Bo Luo	University of Kansas, USA
Zheng Zhang	Jinling Institute of Technology, China

Technical Program Committee Chairs

Jingqiang Lin	University of Science and Technology of China, China
Qiang Tang	University of Sydney, Australia

Sponsorship and Exhibit Chair

Huimin You	Jiangsu Computer Society, China
------------	---------------------------------

Local Chair

Aiyan Qu	Jinling Institute of Technology, China
----------	--

Workshops Chair

Le Guan	University of Georgia, USA
---------	----------------------------

Publicity and Social Media Chairs

Jun Dai	California State University, USA
Jun Shao	Zhejiang Gongshang University, China
Chenglu Jin	CWI Amsterdam, The Netherlands

Publications Chairs

Yuan Hong	Illinois Institute of Technology, USA
Shucheng Yu	Stevens Institute of Technology, USA

Web Chair

Zeyan Liu	University of Kansas, USA
-----------	---------------------------

Posters and PhD Track Chairs

Alex Bardas	University of Kansas, USA
Drew Davidson	University of Kansas, USA

Demos Chair

Shuhui Yang	Purdue University Northwest, USA
-------------	----------------------------------

Technical Program Committee

Anjia Yang	Jinan University, China
Bernardo David	IT University of Copenhagen, Denmark
Bingyu Li	Beihang University, China
Debiao He	Wuhan University, China
Ding Wang	Nankai University, China
Fei Gao	Beijing University of Posts and Communications, China
Guangquan Xu	Tianjin University, China
Haixin Duan	Tsinghua University, China
Jiageng Chen	Central China Normal University, China
Jian Shen	Nanjing University of Information Science and Technology, China
Jing Chen	Wuhan University, China
Josef Pieprzyk	CSIRO Data61, Australia
Jun Shao	Zhejiang Gongshang University, China
Khoa Nguyen	University of Wollongong, Australia
Le Guan	University of Georgia, USA

Li Yang	Xidian University, China
Long Chen	Institute of Software, Chinese Academy of Sciences, China
Ping Chen	Fudan University, China
Qiong Xiao Wang	Institute of Information Engineering, Chinese Academy of Sciences, China
Sherman S. M. Chow	The Chinese University of Hong Kong, Hong Kong
Shijie Jia	Institute of Information Engineering, Chinese Academy of Sciences, China
Tianqi Zhou	Nanjing University of Information Science and Technology, China
Ximeng Liu	Fuzhou University, China
Xiuhua Wang	Huazhong University of Science and Technology, China
Xuyun Nie	University of Electronic Science and Technology of China, China
Yongjun Zhao	Nanyang Technological University, Singapore
Yueqiang Cheng	NIO Security Research, USA

Contents

Quantum-Safe Cryptographic Solution

DU-QS22: A Dataset for Analyzing QC-MDPC-Based Quantum-Safe Cryptosystems	3
<i>Mohammad Reza Nosouhi, Syed W. Shah, Lei Pan, and Robin Doss</i>	

Quantum-Safe Signing of Notification Messages in Intelligent Transport Systems	11
<i>Sara Nikula, Kimmo Halunen, and Visa Vallivaara</i>	

Applied Cryptography for IoT

WB-GWS: An IoT-Oriented Lightweight Gateway System Based on White-Box Cryptography	29
<i>Jinfu Hao, Yongbao Wang, Weijie Deng, Nanjiang Xie, and Zheng Gong</i>	

Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment	46
<i>Keyan Abdul-Aziz Mutlaq, Vincent Omollo Nyangaresi, Mohd Adib Omar, and Zaid Ameen Abduljabbar</i>	

Resource Consumption Evaluation of C++ Cryptographic Libraries on Resource-Constrained Devices	65
<i>Razvan Raducu, Ricardo J. Rodríguez, and Pedro Álvarez</i>	

Authentication Protocol

A Secure Lightweight RFID Mutual Authentication Protocol Without Explicit Challenge-Response Pairs	79
<i>Keke Huang, Changlu Lin, and Yali Liu</i>	

bisAUTH: A Blockchain-Inspired Secure Authentication Protocol for IoT Nodes	108
<i>Cherif Diallo</i>	

Real-World Applied Cryptography

X-FTPC: A Fine-Grained Trust Propagation Control Scheme for Cross-Certification Utilizing Certificate Transparency	123
<i>Shushang Wen, Bingyu Li, Ziqiang Ma, Qianhong Wu, and Nenghai Yu</i>	

The Block-Based Mobile PDE Systems are Not Secure - Experimental Attacks 139
Niusen Chen, Bo Chen, and Weisong Shi

Black-Box Testing of Cryptographic Algorithms Based on Data Characteristics 153
Haoling Fan, Lingjia Meng, Fangyu Zheng, Mingyu Wang, and Bowen Xu

Network Attack and Defense

IoT Devices Classification Base on Network Behavior Analysis 173
Lingan Chen, Xiaobin Tan, Chuang Peng, Mingye Zhu, Zhenghuan Xu, and Shuangwu Chen

Semi-supervised False Data Injection Attacks Detection in Smart Grid 189
Yasheng Zhou, Li Yang, and Yang Cao

Security Application

A Novel Logistics Scheme Based on Zero-Trust Model 203
Haobo Wang, Wei Ou, and Wenbao Han

ALFLAT: Chinese NER Using ALBERT, Flat-Lattice Transformer, Word Segmentation and Entity Dictionary 216
Haifeng Lv and Yong Ding

Author Index 229