

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>


Jianying Zhou · Chuadhry Mujeeb Ahmed ·
Lejla Batina · Sudipta Chattopadhyay ·
Olga Gadyatskaya · Chenglu Jin ·
Jingqiang Lin · Eleonora Losiouk ·
Bo Luo · Suryadipta Majumdar ·
Mihalis Maniatakos · Daisuke Mashima ·
Weizhi Meng · Stjepan Picek ·
Masaki Shimaoka · Chunhua Su ·
Cong Wang (Eds.)


Applied Cryptography and Network Security Workshops

ACNS 2021 Satellite Workshops
AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, and SiMLA
Kamakura, Japan, June 21–24, 2021
Proceedings

Editors

Jianying Zhou 
Singapore University of Technology
and Design
Singapore, Singapore

Lejla Batina 
ICIS
Radboud University
Nijmegen, The Netherlands


Olga Gadyatskaya 
LIACS
Leiden University
Leiden, The Netherlands

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


Bo Luo
University of Kansas
Lawrence, KS, USA

Mihalis Maniatakis 
New York University
Abu Dhabi, United Arab Emirates

Weizhi Meng 
Technical University of Denmark
Kongens Lyngby, Denmark


Masaki Shimaoka 
SECOM Co., Ltd.
Tokyo, Japan


Cong Wang 
City University of Hong Kong
Hong Kong, Hong Kong


Chuahdhy Mujeeb Ahmed 
University of Strathclyde
Glasgow, UK

Sudipta Chattopadhyay 
Singapore University of Technology
and Design
Singapore, Singapore

Chenglu Jin 
Centrum Wiskunde & Informatica
Amsterdam, The Netherlands

Eleonora Losiouk 
University of Padua
Padua, Italy

Suryadipta Majumdar 
CIISE
Concordia University
Montréal, Canada

Daisuke Mashima 
Illinois at Singapore Pte Ltd
Singapore, Singapore

Stjepan Picek 
Delft University of Technology
Delft, The Netherlands

Chunhua Su 
University of Aizu
Aizu-Wakamatsu, Japan

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-81644-5

ISBN 978-3-030-81645-2 (eBook)

<https://doi.org/10.1007/978-3-030-81645-2>

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

This proceedings contains the papers selected for presentation at ACNS 2021 satellite workshops, which were held in parallel with the main conference (the 19th International Conference on Applied Cryptography and Network Security) during June 21–24, 2021. The event was planned to be held in Kamakura, Japan. Due to the ongoing COVID-19 crisis, we decided to organize it virtually again to ensure the safety of all participants.

ACNS initiated four satellite workshops successfully in 2019 and expanded to seven in 2020. Each workshop provided a forum to address a specific topic at the forefront of cybersecurity research. In response to this year’s call for workshop proposals, another new workshop was launched besides the existing seven workshops.

- AIBlock: 3rd ACNS Workshop on Application Intelligence and Blockchain Security, chaired by Weizhi Meng and Chunhua Su
- AIHWS: 2nd ACNS Workshop on Artificial Intelligence in Hardware Security, chaired by Stjepan Picek and Lejla Batina
- AIoTS: 3rd ACNS Workshop on Artificial Intelligence and Industrial IoT Security, chaired by Daisuke Mashima and Chuadhry Mujeeb Ahmed
- CIMSS: 1st ACNS Workshop on Critical Infrastructure and Manufacturing System Security, chaired by Chenglu Jin and Michail Maniatakos
- Cloud S&P: 3rd ACNS Workshop on Cloud Security and Privacy, chaired by Suryadipta Majumdar and Cong Wang
- SCI: 2nd ACNS Workshop on Secure Cryptographic Implementation, chaired by Jingqiang Lin and Bo Luo
- SecMT: 2nd ACNS Workshop on Security in Mobile Technologies, chaired by Eleonora Losiouk and Olga Gadyatskaya
- SiMLA: 3rd ACNS Workshop on Security in Machine Learning and its Applications, chaired by Sudipta Chattopadhyay

This year, we received a total of 49 submissions. Each workshop had its own Program Committee (PC) in charge of the review process. These papers were evaluated on the basis of their significance, novelty, and technical quality. The review process was double-blind. In the end, 26 papers were selected for presentation at the eight workshops, resulting in an acceptance rate of 53%.

ACNS also gave a Best Workshop Paper Award. The winning papers were selected from the nominated candidate papers from each workshop. The following two papers shared the ACNS 2021 Best Workshop Paper Award.

- Abdullah Albalawi, Vassilios Vassilakis, and Radu Calinescu. “Memory Deduplication as a Protective Factor in Virtualized Systems” from the Cloud S&P Workshop

- Aozhuo Sun, Bingyu Li, Huiqing Wan, and Qiongxiao Wang. “PoliCT: Flexible Policy in Certificate Transparency Enabling Lightweight Self-Monitor” from the SCI Workshop

Besides the regular papers being presented at the workshops, there were also 15 invited talks.

- “Towards Better Large-Scale Consensus Protocols” by Pawel Szalachowski from Google, USA, and “Long-term Availability of Crypto Currencies: Security and Privacy against Quantum-Attacks” by Kouichi Sakurai from Kyushu University, Japan, at the AIBlock workshop
- “Internet of Threats: Federated Anomaly Detection in IoT and Challenges” by Ahmad-Reza Sadeghi from TU Darmstadt, Germany, and “Machine Learning for Hardware Security: Standing on the Shoulders of Giants” by Fatemeh Ganji, Worcester Polytechnic Institute, USA, at the AIHWS workshop
- “Sensor and Process Fingerprinting in Industrial Control Systems” by Martin Ochoa from Appgate, Colombia, and “ML-based Assessment of the Resilience of Autonomous Vehicles” by Ravi Iyer from UIUC, USA, at the AIoTS workshop
- “HACKED: Challenges and Solutions for Cybersecurity in Digital Manufacturing” by Nikhil Gupta from New York University, USA, and “Cross-Layer Security of Embedded and Cyber-Physical Systems” by Mohammad Al Faruque from the University of California, Irvine, USA, at the CIMSS Workshop
- “Trusting Outsourced Computation” by Rei Safavi-Naini from the University of Calgary, Canada, and “Secure Network Measurement as a Cloud Service” by Xingliang Yuan from Monash University, Australia, at the Cloud S&P workshop
- “Understanding and Demystifying Bitcoin Mixing Services” by Yajin Zhou from Zhejiang University, China, at the SCI workshop
- “Analyzing and Designing the Security of a Mobile Platform” by Soteris Demetriou from Imperial College London, UK, “Why is Hard to Secure Mobile Proximity Services” by Daniele Antonioli from EURECOM, France, and “From 4G to 5G Security Challenges” by Katharina Kohls from Radboud University, the Netherlands, at the SecMT workshop
- “Adversarial Attacks in ML-Enabled Systems” by Michail Papadakis from Luxembourg University, Luxembourg, at the SiMLA workshop

ANCS included a poster session for the first time in 2021, which was chaired by Masaki Shimaoka. Four posters were included in the proceedings as well, in the form of extended abstracts.

ACNS 2021 workshops were made possible by the joint efforts of many individuals and organizations. We sincerely thank the authors of all submissions. We are grateful to the program chairs and PC members of each workshop for their great effort in providing professional reviews and interesting feedback to authors in a tight time schedule. We thank all the external reviewers for assisting the PC in their particular areas of expertise. We also thank General Chairs Chunhua Su and Kazumasa Omote and the organizing team members of the main conference as well as each workshop for their help in various aspects.

Last but not least, we thank everyone else, speakers and session chairs, for their contribution to the program of ACNS 2021 workshops. We are glad to see that these workshops have become an important part of ACNS and provide a stimulating platform to discuss open problems at the forefront of cybersecurity research.

June 2021

Jianying Zhou
ACNS 2021 Workshop Chair

Organization

AIBlock 2021

Third ACNS Workshop on Application Intelligence and Blockchain Security

June 22, 2021

General Chair

Man Ho Au

The University of Hong Kong, China

Program Chairs

Weizhi Meng

Technical University of Denmark, Denmark

Chunhua Su

University of Aizu, Japan

Program Committee

Konstantinos Chalkias

Novi/Facebook, USA

Mauro Conti

University of Padua, Italy

Jintai Ding

University of Cincinnati, USA

Dieter Gollmann

Hamburg University of Technology, Germany

Georgios Kambourakis

University of the Aegean, Greece

Debiao He

Wuhan University, China

Mario Larangeira

Tokyo Institute of Technology/IOHK, Japan

Wenjuan Li

The Hong Kong Polytechnic University, China

Jiqiang Lu

Beihang University, China

Felix Gomez Marmol

University of Murcia, Spain

Kouichi Sakurai

Kyushu University, Japan

Jun Shao

Zhejiang Gongshang University, China

Claudio Juan Tessone

Swiss Federal Institute of Technology, Switzerland

Ding Wang

Nankai University, China

Qianhong Wu

Beihang University, China

AIHWS 2021

Second ACNS Workshop on Artificial Intelligence in Hardware Security

June 21, 2021

Program Chairs

Lejla Batina	Radboud University, the Netherlands
Stjepan Picek	Delft University of Technology, the Netherlands

Program Committee

Shivam Bhasin	Nanyang Technological University, Singapore
Ileana Buhan	Radboud University, the Netherlands
Chitchanok Chuengsatiansup	The University of Adelaide, Australia
Lukasz Chmielewski	Radboud University, the Netherlands
Elena Dubrova	KTH Royal Institute of Technology, Sweden
Fatemeh Ganji	Worcester Polytechnic Institute, USA
Naofumi Homma	Tohoku University, Japan
Dirmanto Jap	Nanyang Technological University, Singapore
Alan Jovic	University of Zagreb, Croatia
Liran Lerman	Thales Belgium, Belgium
Eleonora Losiouk	University of Padova, Italy
Luca Mariot	Delft University of Technology, the Netherlands
Nele Mentens	Katholieke Universiteit Leuven, Belgium, and Leiden University, the Netherlands
Debdeep Mukhopadhyay	IIT Kharagpur, India
Naila Mukhtar	Macquarie University, Australia
Kostas Papagiannopoulos	NXP Semiconductors, Germany
Guilherme Perin	Delft University of Technology, the Netherlands
Kazuo Sakiyama	The University of Electro-Communications, Japan
Shahin Tajik	Worcester Polytechnic Institute, USA
Vincent Verneuil	NXP Semiconductors, Germany
Nikita Veshchikov	NXP Semiconductors, Belgium

Publicity Chair

Marina Krcek	Delft University of Technology, the Netherlands
--------------	---

AIoTS 2021

Third ACNS Workshop on Artificial Intelligence and Industrial IoT Security

June 22, 2021

Program Chairs

Daisuke Mashima
Chuadhry Mujeeb Ahmed

Illinois at Singapore Pte Ltd, Singapore
University of Strathclyde, UK

Organizing Chairs

Sridhar Adepu
John Henry Castellanos
Xin Lou

SUTD, Singapore
SUTD, Singapore
Illinois at Singapore Pte Ltd, Singapore

Program Committee

Anand Agrawal
Yao Chen
Yao Cheng
Mina S. Guirguis
Zhongyuan Hau
Venkata Reddy
Jorjeta Jetcheva
Chitra Javali
Nandha Kumar Kandasamy
Eunsuk Kang
Eleonora Losiouk
Kazuhiro Minami
Takashi Onoda
Tohid Shekari
Ryan Shah
Yoriyuki Yamagata
Riccardo Taormina
Takeshi Sugawara

NYU Abu Dhabi, UAE
Illinois at Singapore Pte Ltd, Singapore
Huawei International Pte Ltd, Singapore
Texas State University, USA
Imperial College London, UK
IIPE-Visakhapatnam, India
San Jose State University, USA
Institute for Infocomm Research (I2R), Singapore
SUTD, Singapore
CMU, USA
University of Padua, Italy
The Institute of Statistical Mathematics, Japan
Aoyama Gakuin University, Japan
Georgia Tech, USA
University of Strathclyde, UK
AIST, Japan
TU Delft, the Netherlands
The University of Electro-Communications, Japan

CIMSS 2021

First ACNS Workshop on Critical Infrastructure and Manufacturing System Security

June 21, 2021

Program Chairs

Chenglu Jin
Michail Maniatakos

CWI Amsterdam, the Netherlands
New York University Abu Dhabi, UAE

Publicity Chair

Zheng Yang

SUTD, Singapore

Program Committee

Irfan Ahmed	Virginia Commonwealth University, USA
Mohammad Al Faruque	University of California Irvine, USA
Cristina Alcaraz	University of Malaga, Spain
Binbin Chen	SUTD, Singapore
Long Cheng	Clemson University, USA
Soumyajit Dey	Indian Institute of Technology, Kharagpur, India
Jairo Giraldo	University of Utah, USA
Charalambos Konstantinou	Florida State University, USA
Andres Murillo	SUTD, Singapore
Awais Rashid	University of Bristol, UK
Marco Rocchetto	V-Research, Italy
Carlos Rubio-Medrano	Texas A&M University - Corpus Christi, USA
Alexandru Stefanov	Delft University of Technology, the Netherlands
Riccardo Taormina	Delft University of Technology, the Netherlands
Richard J. Thomas	University of Birmingham, UK
Nektarios Tsoutsos	University of Delaware, USA
Edgar Weippl	SBA Research, Austria
Mark Yampolskiy	Auburn University, USA
Zheng Yang	SUTD, Singapore
Stefano Zanero	Politecnico di Milano, Italy
Saman Zonouz	Rutgers University, USA

CLOUD S&P 2021

Third ACNS Workshop on Cloud Security and Privacy

June 24, 2021

Program Chairs

Suryadipta Majumdar
Cong Wang

Concordia University, Canada
City University of Hong Kong, HK SAR, China

Program Committee

Prabir Bhattacharya
Mauro Conti
Helei Cui
Nora Cuppens
Sabrina De Capitani di
Vimercati
Yosr Jarraya
Kallol Krishna Karmaker
Rongxing Lu
Eduard Marin
Nicolae Paladi
Makan Pourzandi
Pierangela Samarati
Paria Shirani
Lingyu Wang
Xingliang Yuan
Mengyuan Zhang

Thomas Edison State University, USA
University of Padua, Italy
Northwestern Polytechnical University, China
École Polytechnique de Montréal, Canada
Università degli studi di Milano, Italy
Ericsson Security, Canada
University of Newcastle, UK
University of New Brunswick, Canada
Telefonica Research, Spain
RISE Research Institutes of Sweden, Sweden
Ericsson Security, Canada
Università degli studi di Milano, Italy
Concordia University, Canada
Concordia University, Canada
Monash University, Australia
Hong Kong Polytechnic University, HK SAR, China

SCI 2021

Second ACNS Workshop on Secure Cryptographic Implementation

June 23, 2021

Program Chairs

Jingqiang Lin	University of Science and Technology of China, China
Bo Luo	The University of Kansas, USA

Publication Chair

Jun Shao	Zhejiang Gongshang University, China
----------	--------------------------------------

Publicity Chairs

Le Guan	University of Georgia, USA
Debiao He	Wuhan University, China

Program Committee

Bo Chen	Michigan Technological University, USA
Fu Chen	Central University of Finance and Economics, China
Jiankuo Dong	Nanjing University of Posts and Telecommunications, China
Johann Großschädl	University of Luxembourg, Luxembourg
Le Guan	University of Georgia, USA
Debiao He	Wuhan University, China
Bingyu Li	Beihang University, China
Fengjun Li	The University of Kansas, USA
Di Ma	ZDNS, China
Yuan Ma	Chinese Academy of Sciences, China
Jun Shao	Zhejiang Gongshang University, China
Ruisheng Shi	Beijing University of Posts and Telecommunications, China
Zhiguo Wan	Shandong University, China
Ding Wang	Nankai University, China
Juan Wang	Wuhan University, China
Jun Xu	Stevens Institute of Technology, USA
Li Yang	Xidian University, China
Fan Zhang	Zhejiang University, China
Fangyu Zheng	Chinese Academy of Sciences, China

Additional Reviewers

Yanbin Li
Zhen Zhou
Haoyang An

Nanjing Agricultural University, China
Wuhan University, China
Wuhan University, China

SecMT 2021

Second ACNS Workshop on Security in Mobile Technologies

June 23, 2021

Program Chairs

Eleonora Losiouk
Olga Gadyatskaya

University of Padua, Italy
Leiden University, the Netherlands

Program Committee

Kevin Allix
Marco Casagrande
Lorenzo Cavallaro
Guozhu Meng

University of Luxembourg, Luxembourg
University of Padua, Italy
King's College London, UK
Institute of Information Engineering, Chinese Academy
of Sciences, China

Veelasha Moonsamy
Georgios Portokalidis
Giovanni Russello
Andrea Saracino
Riccardo Spolaor
Flavio Toffalini

Ruhr University Bochum, Germany
Stevens Institute of Technology, USA
University of Auckland, New Zealand
Consiglio Nazionale delle Ricerche, Italy
Shandong University, China
Singapore University of Technology and Design,
Singapore

Rolando Trujillo
Luca Verderame

Deakin University, Australia
University of Genova, Italy

SiMLA 2021

Third ACNS Workshop on Security in Machine Learning and its Applications

June 24, 2021

Program Chair

Sudipta Chattopadhyay

Singapore University of Technology and Design,
Singapore

Web Chair

Sakshi Udeshi

Singapore University of Technology and Design,
Singapore

Program Committee

Chris Poskitt

Shuhao Zhang

Singapore Management University, Singapore

Singapore University of Technology and Design,
Singapore

Wenrui Diao

Jingyi Wang

Ezekiel Soremekun

Shuang Liu

Kehuan Zhang

Shandong University, China

Zhejiang University, China

University of Luxembourg, Luxembourg

Tianjin University, China

The Chinese University of Hong Kong, Hong Kong

Contents

AIBlock - Application Intelligence and Blockchain Security

Shaping Blockchain Technology for Securing Supply Chains	3
<i>Yong Zhi Lim, Jianying Zhou, and Martin Saerbeck</i>	
The Obfuscation Method of User Identification System	19
<i>Jing Xu, Fei Xu, and Chi Xu</i>	
Proof of Assets in the Diem Blockchain.	27
<i>Panagiotis Chatzigiannis and Konstantinos Chalkias</i>	
An Identity-Based Blind Signature Scheme with Message Recovery from Pairings	42
<i>Yihong Wen, Cong Peng, Shicheng Wang, Li Li, and Min Luo</i>	

AIHWS - Artificial Intelligence in Hardware Security

A Good Anvil Fears No Hammer: Automated Rowhammer Detection Using Unsupervised Deep Learning.	59
<i>Anirban Chakraborty, Manaar Alam, and Debdeep Mukhopadhyay</i>	
Model Evasion Attacks Against Partially Encrypted Deep Neural Networks in Isolated Execution Environment	78
<i>Kota Yoshida and Takeshi Fujino</i>	
On Reverse Engineering Neural Network Implementation on GPU	96
<i>Łukasz Chmielewski and Léo Weissbart</i>	
On the Importance of Pooling Layer Tuning for Profiling Side-Channel Analysis.	114
<i>Lichao Wu and Guilherme Perin</i>	
Towards Real-Time Deep Learning-Based Network Intrusion Detection on FPGA	133
<i>Laurens Le Jeune, Toon Goedemé, and Nele Mentens</i>	
Towards Trained Model Confidentiality and Integrity Using Trusted Execution Environments	151
<i>Tsunato Nakai, Daisuke Suzuki, and Takeshi Fujino</i>	

AIoTS - Artificial Intelligence and Industrial IoT Security

Quantum Computing Threat Modelling on a Generic CPS Setup.	171
<i>Cher Chye Lee, Teik Guan Tan, Vishal Sharma, and Jianying Zhou</i>	
Cyber-Attack Case Studies on Dynamic Voltage Restorer in Smart Grid	191
<i>Muhammad M. Roomi, Daisuke Mashima, Nandhakumar Kandasamy, and Partha P. Biswas</i>	
Attacklets to Test Anomaly Detectors for Critical Infrastructure	209
<i>Salimah Liyakkathali, Gayathri Sugumar, and Aditya Mathur</i>	

CIMSS - Critical Infrastructure and Manufacturing System Security

WiP: Distributed Intrusion Detection System for TCP/IP-Based Connections in Industrial Environments Using Self-organizing Maps.	231
<i>Aleksei Kharitonov and Axel Zimmermann</i>	
Demand Manipulation Attack Resilient Privacy Aware Smart Grid Using PUFs and Blockchain	252
<i>Soumyadyuti Ghosh, Urbi Chatterjee, Durba Chatterjee, Rumia Masburah, Debdeep Mukhopadhyay, and Soumyajit Dey</i>	

Cloud S&P - Cloud Security and Privacy

BFV, CKKS, TFHE: Which One is the Best for a Secure Neural Network Evaluation in the Cloud?	279
<i>Pierre-Emmanuel Clet, Oana Stan, and Martin Zuber</i>	
Memory Deduplication as a Protective Factor in Virtualized Systems	301
<i>Abdullah Albalawi, Vassilios Vassilakis, and Radu Calinescu</i>	

SCI -Secure Cryptographic Implementation

A (Bit)slice of Rainbow.	321
<i>Florian Caullery</i>	
Cryptanalysis of a Lattice-Based Group Signature with Verifier-Local Revocation Achieving Full Security.	332
<i>Yanhua Zhang, Ximeng Liu, Yupu Hu, Qikun Zhang, and Huiwen Jia</i>	
An Efficient Proactive Secret Sharing Scheme for Cloud Storage	346
<i>Shuihai Zhang, Jingfu Wang, Yan Zhang, Bei Pei, and Chunli Lyu</i>	

PoliCT: Flexible Policy in Certificate Transparency Enabling Lightweight Self-monitor	358
<i>Aozhuo Sun, Bingyu Li, Huiqing Wan, and Qiong Xiao Wang</i>	
Aggregate Signature with Traceability of Devices Dynamically Generating Invalid Signatures	378
<i>Ryu Ishii, Kyosuke Yamashita, Yusuke Sakai, Takahiro Matsuda, Tadanori Teruya, Goichiro Hanaoka, Kanta Matsuura, and Tsutomu Matsumoto</i>	
Combating the OS-Level Malware in Mobile Devices by Leveraging Isolation and Steganography	397
<i>Niusen Chen, Wen Xie, and Bo Chen</i>	
SecMT - Security in Mobile Technologies	
Pass-As-You-Go: A Direct Anonymous Attestation-Based Untraceable Contactless Transit Pass	417
<i>Aïda Diop, Nicolas Desmoulins, and Jacques Traoré</i>	
SiMLA - Security in Machine Learning and Its Applications	
Towards Demystifying Adversarial Robustness of Binarized Neural Networks	439
<i>Zihao Qin, Hsiao-Ying Lin, and Jie Shi</i>	
Kryptonite: An Adversarial Attack Using Regional Focus	463
<i>Yogesh Kulkarni and Krisha Bhambani</i>	
Posters	
POSTER: Resistance Analysis of Two AES-Like Against the Boomerang Attack	485
<i>Laetitia Debesse, Sihem Mesnager, and Mounira Msahli</i>	
POSTER: LHSa: Lightweight Hardware Security Arbitrator	490
<i>Yongjin Kim</i>	
POSTER: Another Look at Boyar-Peralta's Algorithm	495
<i>Anubhab Baksi, Banashri Karmakar, and Vishnu Asutosh Dasu</i>	
POSTER: Optimizing Device Implementation of Linear Layers with Automated Tools	500
<i>Anubhab Baksi, Banashri Karmakar, and Vishnu Asutosh Dasu</i>	

Short Paper

Long-term Availability of Crypto Currencies: Security and Privacy Against
Quantum-Attacks 507
 Kouichi Sakurai

Author Index 511