17th International Conference on Security and Cryptography (SECRYPT 2020)

Online
8 – 10 July 2020

Editors:

Pierangela Samarati
Sabrina De Capitani di Vimercati

Mohammad Obaidat
Jalel Ben-Othman

ISBN: 978-1-7138-4061-9
# BRIEF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INVITED SPEAKERS</td>
<td>IV</td>
</tr>
<tr>
<td>ORGANIZING COMMITTEES</td>
<td>V</td>
</tr>
<tr>
<td>PROGRAM COMMITTEE</td>
<td>VI</td>
</tr>
<tr>
<td>AUXILIARY REVIEWERS</td>
<td>VII</td>
</tr>
<tr>
<td>SELECTED PAPERS BOOK</td>
<td>VII</td>
</tr>
<tr>
<td>FOREWORD</td>
<td>IX</td>
</tr>
<tr>
<td>CONTENTS</td>
<td>XI</td>
</tr>
</tbody>
</table>
INVITED SPEAKERS

Henderik A. Proper
Luxembourg Institute of Science and Technology
Luxembourg

Jaime Lloret Mauri
Universidad Politecnica de Valencia
Spain

Ajith Abraham
Machine Intelligence Research Labs (MIR Labs)
United States

Moti Yung
Columbia University
United States

Ingemar Johansson Cox
University of Copenhagen
United Kingdom
ORGANIZING COMMITTEES

CONFERENCE CO-chairs
Mohammad Obaidat, Fellow of IEEE, Dean of College of Computing & Informatics, University of Sharjah, UAE and with University of Jordan, Jordan and University of Science and Technology Beijing, China
Jalel Ben-Othman, University of Paris 13, France

PROGRAM CO-chairs
Pierangela Samarati, Università degli Studi di Milano, Italy
Sabrina De Capitani di Vimercati, Università degli Studi di Milano, Italy

SECRETARIAT
Mónica Saramago, INSTICC, Portugal

GRAPHICS PRODUCTION AND WEBDESIGNER
André Poeira, INSTICC, Portugal

WEBMASTER
João Francisco, INSTICC, Portugal
Carolina Ribeiro, INSTICC, Portugal
Program Committee

Massimiliano Albanese, George Mason University, United States
Cristina Alcaraz, University of Malaga, Spain
Luis Antunes, Universidade do Porto, Portugal
Muhammad Asghar, The University of Auckland, New Zealand
Francesco Buccafurri, University of Reggio Calabria, Italy
Frederic Cuppens, TELECOM Bretagne, France
Nora Cuppens, IMT-Atlantique, France
Sabrina De Capitani di Vimercati, Università degli Studi di Milano, Italy
Roberto Di Pietro, Hamad Bin Khalifa University, Qatar
Mario Di Raimondo, Università di Catania, Italy
Josep Domingo-Ferrer, Rovira i Virgili University, Spain
Ruggero Donida Labati, Università degli Studi di Milano, Italy
Alberto Ferrante, Università della Svizzera Italiana, Switzerland
Josep-Lluis Ferrer-Gomila, Balearic Islands University, Spain
Sara Foresti, Università degli Studi di Milano, Italy
Steven Furnell, University of Plymouth, United Kingdom
Joaquin Garcia-Alfaro, Télécom SudParis, France
Angelo Genovese, Università degli Studi di Milano, Italy
Dimitris Gritzalis, AUEB, Greece
Stefanos Gritzalis, University of Piraeus, Greece
Jinguang Han, Queen’s University Belfast, United Kingdom
Xinyi Huang, Fujian Normal University, China
Vasilis Katos, Bournemouth University, United Kingdom
Sokratis Katsikas, Norwegian University of Science and Technology, Norway
Shinsaku Kiyomoto, KDDI Research Inc., Japan
Albert Levi, Sabanci University, Turkey
Kaitai Liang, University of Surrey, United Kingdom
Jay Ligatti, University of South Florida, United States
Giovanni Livraga, Universita degli Studi di Milano, Italy
Javier Lopez, University of Malaga, Spain
Yunlong Mao, Nanjing University, China
Evangelos Markatos, ICS, Forth, Greece
Fabio Martinelli, Consiglio Nazionale delle Ricerche, Italy
David Megias, Universitat Oberta de Catalunya, Spain
Alessio Merlo, University of Genoa, Italy
Rolf Oppliger, eSECURITY Technologies, Switzerland
Stefano Paraboschi, University of Bergamo, Italy
Joon Park, Syracuse University, United States
Gerardo Pelosi, Politecnico di Milano, Italy
Günther Pernul, University of Regensburg, Germany
Junior Ramirez Cruz, Université du Luxembourg, Luxembourg
Silvio Ranise, Fondazione Bruno Kessler, Italy
Indrakshi Ray, Colorado State University, United States
Ruben Rios del Pozo, Universidad de Málaga, Spain
Nuno Santos, INESC, Portugal
Andreas Schaad, University of Applied Sciences Offenburg, Germany
Fabio Scotti, Universita degli Studi di Milano, Italy
Daniele Sgandurra, Royal Holloway - University of London, United Kingdom
Nicolas Sklavos, University of Patras, Greece
Vicenc Torra, University of Skövde, Sweden
Juan Ramon Troncoso-Pastoriza, EPFL, Switzerland
Corrado Visaggio, Università degli Studi del Sannio, Italy
Roopa Vishwanathan, New Mexico State University, United States
Cong Wang, City University of Hong Kong, Hong Kong
Haining Wang, University of Delaware, United States
Lingyu Wang, Concordia University, Canada
Meng Yu, University of Texas at San Antonio, United States
Mo Yu, Google, United States
Jiawei Yuan, University of Massachusetts Dartmouth, United States
Qiang Zeng, University of South Carolina, United States
Lei Zhang, Refinitiv, United States
Shengzhi Zhang, Boston University, Metropolitan College, United States
Yongjun Zhao, The Chinese University of Hong Kong, Hong Kong

AUXILIARY REVIEWERS

Tahir Ahmad, Foundazione Bruno Kessler, Italy
Stefano Berlato, FBK, Italy
Bruhadeshwar Bezawada, Colorado State University, United States
Vasiliki Diamantopoulou, University of the Aegean, Greece
Dimitra Georgiou, Greece
Giacomo Giorgi, CNR-IIT, Italy
Emauela Marasco, George Mason University, United States
Luca Mariot, Uni. MIB, Italy
Christina Michailidou, IIT-CNR, Italy
Umberto Morelli, FBK, Italy
Jianting Ning, Nanyang Technological University, Singapore
Pankaj Pandey, Norwegian University of Science and Technology, Norway
Panagiotis Rizomiliotis, Harokopio University, Greece
Alessandro Tomasi, Fondazione Bruno Kessler, Italy
Theodoros Tzouramanis, University of Thessaly, Greece
Luca Verderame, University of Genova, Italy
Xu Yang, RMIT University, Australia
Yuexin Zhang, Xidian University, China
Fei Zhu, RMIT, Australia

SELECTED PAPERS BOOK

A number of selected papers presented at SECRYPT 2020 will be published by Springer in a CCIS Series book. This selection will be done by the Conference Co-chairs and Program Co-chairs, among the papers actually presented at the conference, based on a rigorous review by the SECRYPT 2020 Program Committee members.
This book contains the proceedings of the 17th International Conference on Security and Cryptography (SECRYPT 2020) which is part of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020). This year ICETE 2020 was, exceptionally, held as an online web-based event, due to the COVID-19 pandemic, from 8 - 10 July, 2020.

ICETE 2020 is sponsored by INSTICC (the Institute for Systems and Technologies of Information, Control and Communication) and held in cooperation with the ACM SIGMIS (Special Interest Group on Management Information Systems), the ACM SIGMM (Special Interest Group on Multimedia), the European Association for Signal Processing (EURASIP), the Japan Society of Applied Physics (JSAP), the International Association of Business Process Management Professionals International (ABPMP) and the Photonics 21. Moreover, ICETE 2020 has WfMC (Workflow Management Coalition), OMG (Object Management Group) and FIPA (the Foundation for Intelligent Physical Agents) as Organizational Co-Sponsors.

The purpose of the International Joint Conference on e-Business and Telecommunications is to bring together researchers and practitioners interested in the dissemination of new results in the fields of information and communication technologies, including data communication networking, e-business, optical communication systems, security and cryptography, signal processing and multimedia applications, and wireless networks and mobile systems. These are the main conference areas that define the six component conferences, namely: DCNET, ICE-B, OPTICS, SECRYPT, SIGMAP, and WINSYS, which together form the ICETE joint international conference.

ICETE 2020 includes five distinguished keynote lectures, delivered by experts in their fields, including (alphabetically): Ajith Abraham (Machine Intelligence Research Labs (MIR Labs), USA), Henderik Proper (Luxembourg Institute of Science and Technology, Luxembourg), Ingemar Johansson Cox (University of Copenhagen, United Kingdom), Jaime Lloret Mauri (Universidad Politecnica de Valencia, Spain) and Moti Yung (Columbia University, USA).

With its six segments, we expect the conference to appeal to a global audience of the engineers, scientists, business practitioners and policy experts, interested in R&D on Telecommunication Systems and Services. All tracks focus on research related to real world applications and rely on contributions not only from academia, but also from industry, business and government, with different solutions for end-user applications and enabling technologies, in a diversity of communication environments. The accepted papers demonstrate a number of new and innovative solutions and the vitality of these research areas.

In response to the call for papers, SECRYPT has received 123 papers in total, with contributions from 39 different countries in all continents, confirming the success and global dimension of SECRYPT 2020. To evaluate each submission, a double blind paper evaluation method was used: each paper was reviewed by at least two experts from the International Program Committee in a double-blind review process. The selection process followed strict criteria. So, only 19 papers were accepted and orally presented at SECRYPT as full papers (15% of submissions) and 32 as short papers (26% of submissions). Additionally, 18 papers were accepted for poster presentations.

With this acceptance ratio, SECRYPT 2020 continues the tradition of previous conferences as a distinguished and high-quality conference. Extended versions of selected best papers of the conference will be invited to appear in a post-conference book that will be published by Springer.

We would like to express our thanks to all colleagues involved in supporting the conference. We would like to thank in particular: the members of the Program Committee and the external reviewers, who really did a great job, devoting expertise and time in reviewing the papers and participating in the discussion process. We would like to thank all the authors who submitted papers, whether or not the paper was eventually included in the program. We would also like to thank the invited speakers for their invaluable contribution, in sharing their vision, knowledge and research outcomes.

Finally, we gratefully acknowledge the professional support of the INSTICC team for all organizational
processes, especially given the need to introduce online streaming, forum management, direct messaging facilitation and other web-based activities in order to make it possible for SECRYPT 2020 authors to present their work and share ideas with colleagues in spite of the logistic difficulties caused by the current pandemic situation.

We hope that the papers accepted and included in the proceedings will be helpful references in future works for all those who need to address topics in the SECRYPT and all the other ICETE knowledge areas.

Pierangela Samarati  
Università degli Studi di Milano, Italy

Sabrina De Capitani di Vimercati  
Università degli Studi di Milano, Italy

Mohammad Obaidat  
Fellow of IEEE, Dean of College of Computing & Informatics, University of Sharjah, UAE and with University of Jordan, Jordan and University of Science and Technology Beijing, China

Jalel Ben-Othman  
University of Paris 13, France
# CONTENTS

## INVITED SPEAKERS

### KEYNOTE SPEAKERS

Enterprise Systems Architecture - Essentials  
*Henderik A. Proper*  
5

eHealth Monitoring Using Wireless Communication Protocols and Intelligent Systems  
*Jaime Lloret*  
7

Industry 4.0: Challenges from a Data Science Perspective  
*Ajith Abraham*  
9

Secure Computation Protocol: A Technology for Our Time  
*Moti Yung*  
11

Analysing Digital Footprints to Infer the Health of Populations and Individuals  
*Ingemar Johansson Cox*  
13

## PAPERS

### FULL PAPERS

Helper-in-the-Middle: Supporting Web Application Scanners Targeting Industrial Control Systems  
*Anne Borcherding, Steffen Pfrang, Christian Haas, Albrecht Weiche and Jürgen Beyerer*  
19

Termination of Ethereum’s Smart Contracts  
*Thomas Genet, Thomas Jensen and Justine Sauvage*  
31

Avoiding Network and Host Detection using Packet Bit-masking  
*George Stergioupolos, Eirini Lygerou, Nikolaos Tsalis, Dimitris Tomaras and Dimitris Gritzalis*  
44

FPGA-based McEliece Cryptosystem using Non-linear Convolutional Codes  
*Michael Ekonde Sone*  
56

CROOT: Code-based Round-Optimal Oblivious Transfer  
*Nicolas Aragon, Olivier Blazy, Neals Fournaise and Philippe Gaborit*  
68

DCBC: A Distributed High-performance Block-Cipher Mode of Operation  
*Oussama Trabelsi, Lilia Sfaxi and Riadh Robbana*  
78

Stay Thrifty, Stay Secure: A VPN-based Assurance Framework for Hybrid Systems  
*Marco Anisetti, Claudio A. Ardagna, Nicola Bena and Ernesto Damiani*  
90

An Enhanced Lightweight Authentication Scheme for Secure Access to Cloud Data  
*Hanza Hammami, Mohammad S. Obaidat and Sadok Ben Yahia*  
102

Decentralized Multi-Client Attribute Based Functional Encryption  
*Yuechen Chen, Linru Zhang and Siu-Ming Yu*  
110

Optimal Transport Layer for Secure Computation  
*Markus Brandt, Claudio Orlandi, Kris Shrishak and Haya Shulman*  
122
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Identity-matching Process to Strengthen Trust in Federated-identity Architectures</td>
<td>134</td>
</tr>
<tr>
<td>Paul Marillonnet, Mikaël Ates, Maryline Laurent and Nesrine Kaaniche</td>
<td></td>
</tr>
<tr>
<td>Ensuring the Integrity of Outsourced Web Scripts</td>
<td>147</td>
</tr>
<tr>
<td>Josselin Mignerey, Cyrille Mucchietto and Jean-Baptiste Orfila</td>
<td></td>
</tr>
<tr>
<td>Authentication and Key Management Automation in Decentralized Secure Email and Messaging via Low-entropy Secrets</td>
<td>159</td>
</tr>
<tr>
<td>Itzel Vazquez Sandoval, Arash Atashpendar and Gabriele Lenzini</td>
<td></td>
</tr>
<tr>
<td>FALCO: Detecting Superfluous JavaScript Injection Attacks using Website Fingerprints</td>
<td>172</td>
</tr>
<tr>
<td>Chih-Chun Liu, Hsu-Chun Hsiao and Tiffany Hyun-Jin Kim</td>
<td></td>
</tr>
<tr>
<td>Beyond Black and White: Combining the Benefits of Regular and Incognito Browsing Modes</td>
<td>184</td>
</tr>
<tr>
<td>John Korniotakis, Panagiotis Papadopoulos and Evangelos P. Markatos</td>
<td></td>
</tr>
<tr>
<td>Practically Efficient Attribute-based Encryption for Compartmented Access Structures</td>
<td>193</td>
</tr>
<tr>
<td>Ferucio Laurentiu Tiplea, Alexandru Ionită and Anca Maria Nica</td>
<td></td>
</tr>
<tr>
<td>Round-optimal Constant-size Blind Signatures</td>
<td>205</td>
</tr>
<tr>
<td>Olivier Blazy, Brouilhet Laura, Céline Chevalier and Neals Fournaise</td>
<td></td>
</tr>
<tr>
<td>Prov-Trust: Towards a Trustworthy SGX-based Data Provenance System</td>
<td>217</td>
</tr>
<tr>
<td>Nesrine Kaaniche, Sana Belguith, Maryline Laurent, Ashish Gehani and Giovanni Russello</td>
<td></td>
</tr>
<tr>
<td>A Failure Rate Model of Bit-flipping Decoders for QC-LDPC and QC-MDPC Code-based Cryptosystems</td>
<td>230</td>
</tr>
<tr>
<td>Marco Baldi, Alessandro Bareghi, Franco Chiaramonte, Gerardo Pelosi and Paolo Santini</td>
<td></td>
</tr>
<tr>
<td><strong>SHORT PAPERS</strong></td>
<td></td>
</tr>
<tr>
<td>Exploring Current E-mail Cyber Threats using Authenticated SMTP Honeypot</td>
<td>245</td>
</tr>
<tr>
<td>Lukáš Zobal, Dušan Kolář and Jakub Kroutek</td>
<td></td>
</tr>
<tr>
<td>Optimizing dm-crypt for XTS-AES: Getting the Best of Atmel Cryptographic Co-processors</td>
<td>255</td>
</tr>
<tr>
<td>Levent Demir, Mathieu Thiery, Vincent Roca, Jean-Michel Tenkes and Jean-Louis Roch</td>
<td></td>
</tr>
<tr>
<td>cipherPath: Efficient Traversals over Homomorphically Encrypted Paths</td>
<td>263</td>
</tr>
<tr>
<td>Georg Bramm and Julian Schütte</td>
<td></td>
</tr>
<tr>
<td>A White-Box Encryption Scheme using Physically Unclonable Functions</td>
<td>271</td>
</tr>
<tr>
<td>Sandra Rasoamiharanana, Marine Minier and Gilles Macario-Rat</td>
<td></td>
</tr>
<tr>
<td>Towards Understanding Man-on-the-Side Attacks (MotS) in SCADA Networks</td>
<td>279</td>
</tr>
<tr>
<td>Peter Maynard and Kieran McLaughlin</td>
<td></td>
</tr>
<tr>
<td>Towards Secure Edge-assisted Image Sharing for Timely Disaster Situation Awareness</td>
<td>287</td>
</tr>
<tr>
<td>Jing Yao, Yifeng Zheng, Cong Wang and Surya Nepal</td>
<td></td>
</tr>
<tr>
<td>Evasive Windows Malware: Impact on Antiviruses and Possible Countermeasures</td>
<td>294</td>
</tr>
<tr>
<td>Cédric Herzog, Valérie Viet Triem Tong, Pierre Wilke, Arnaud Van Straaten and Jean-Louis Lanet</td>
<td></td>
</tr>
<tr>
<td>Security Analysis of ElGamal Implementations</td>
<td>302</td>
</tr>
<tr>
<td>Mohamad El Laz, Benjamin Grégoire and Tamara Rezk</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Efficient Constructions of Non-interactive Secure Multiparty Computation from Pairwise Independent Hashing</td>
<td>314</td>
</tr>
<tr>
<td>Satoshi Obana and Maki Yoshida</td>
<td></td>
</tr>
<tr>
<td>Signatures to Go: A Framework for Qualified PDF Signing on Mobile Devices</td>
<td>322</td>
</tr>
<tr>
<td>Emina Ahmetovic, Thomas Lenz and Christian Kollmann</td>
<td></td>
</tr>
<tr>
<td>Privacy-Preserving Greater-Than Integer Comparison without Binary Decomposition</td>
<td>332</td>
</tr>
<tr>
<td>Sigurd Eskeland</td>
<td></td>
</tr>
<tr>
<td>Multi-Stakeholder Cybersecurity Risk Assessment for Data Protection</td>
<td>341</td>
</tr>
<tr>
<td>Majid Mollaeefar, Alberto Siena and Silvio Ranise</td>
<td></td>
</tr>
<tr>
<td>A Novel Anonymous Authentication and Key Agreement Scheme for Smart Grid</td>
<td>349</td>
</tr>
<tr>
<td>Hamza Hammami, Mohammad S. Obaidat and Sadok Ben Yahia</td>
<td></td>
</tr>
<tr>
<td>SENSSE: Simple, Efficient Searchable Symmetric Encryption for Sensor Networks</td>
<td>355</td>
</tr>
<tr>
<td>Bojan Spasic', Olivier Markowitch and Philippe Thiran</td>
<td></td>
</tr>
<tr>
<td>Linear Generalized ElGamal Encryption Scheme</td>
<td>364</td>
</tr>
<tr>
<td>Pascal Lafourcade, Léo Robert and Demba Sow</td>
<td></td>
</tr>
<tr>
<td>Accelerating Homomorphic Encryption using Approximate Computing Techniques</td>
<td>372</td>
</tr>
<tr>
<td>Shahnam Khanna and Ciara Rafferty</td>
<td></td>
</tr>
<tr>
<td>This Selfie Does Not Exist: On the Security of Electroneum Cloud Mining</td>
<td>380</td>
</tr>
<tr>
<td>Alexander Marsalek, Edona Fasllija and Dominik Ziegler</td>
<td></td>
</tr>
<tr>
<td>ProteiNN: Privacy-preserving One-to-Many Neural Network Classifications</td>
<td>389</td>
</tr>
<tr>
<td>Beyza Bozdemir, Orhan Ermis and Melek Önen</td>
<td></td>
</tr>
<tr>
<td>Privacy-preserving Content-based Publish/Subscribe with Encrypted Matching and Data Splitting</td>
<td>397</td>
</tr>
<tr>
<td>Nathanaël Denis, Pierre Chaffardon, Denis Conan, Maryline Laurent, Sophie Chabridon and Jean Leneutre</td>
<td></td>
</tr>
<tr>
<td>Differentially Private Graph Publishing and Randomized Response for Collaborative Filtering</td>
<td>407</td>
</tr>
<tr>
<td>Julián Salas and Vicenç Torra</td>
<td></td>
</tr>
<tr>
<td>A Machine-learning based Unbiased Phishing Detection Approach</td>
<td>415</td>
</tr>
<tr>
<td>Hossein Shirazi, Landon Zweigle and Indrakshi Ray</td>
<td></td>
</tr>
<tr>
<td>Beyond Administration: A Modeling Scheme Supporting the Dynamic Analysis of Role-based Access Control Policies</td>
<td>423</td>
</tr>
<tr>
<td>Marius Schlegel and Peter Amthor</td>
<td></td>
</tr>
<tr>
<td>Solving Set Relations with Secure Bloom Filters Keeping Cardinality Private</td>
<td>435</td>
</tr>
<tr>
<td>Louis Tajan, Dirk Westhoff and Frederik Armknecht</td>
<td></td>
</tr>
<tr>
<td>Identity Verification and Fraud Detection During Online Exams with a Privacy Compliant Biometric System</td>
<td>443</td>
</tr>
<tr>
<td>M. A. Haytom, C. Rosenberger, C. Charrier, C. Zhu and C. Regnier</td>
<td></td>
</tr>
<tr>
<td>VIP Blowfish Privacy in Communication Graphs</td>
<td>451</td>
</tr>
<tr>
<td>Mohamed Nassar, Elie Chicha, Bechara Al Bouna and Richard Chbeir</td>
<td></td>
</tr>
<tr>
<td>Droppix: Towards More Realistic Video Fingerprinting</td>
<td>460</td>
</tr>
<tr>
<td>Przemysław Blaśkiewicz, Marek Klonowski and Piotr Syga</td>
<td></td>
</tr>
</tbody>
</table>

XIII
Software Emulation of Quantum Resistant Trusted Platform Modules
Luís Fiolhais, Paulo Martins and Leonel Sousa

Formal Accuracy Analysis of a Biometric Data Transformation and Its Application to Secure Template Generation
Shoukat Ali, Koray Karabina and Emrah Karagoz

SwaNN: Switching among Cryptographic Tools for Privacy-preserving Neural Network Predictions
Gamze Tillem, Beyza Bozdemir and Melek Önen

Deconstructing the Decentralization Trilemma
Harry Halpin

Towards Language Support for Model-based Security Policy Engineering
Peter Amthor and Marius Schlegel

Exploiting Hot Spots in Heuristic Safety Analysis of Dynamic Access Control Models
Marius Schlegel and Winfried E. Künnhauser

POSTERS

CP-ABE Scheme Satisfying Constant-size Keys based on ECC
Nishant Raj and Abwyn Roshan Pais

Privacy Enhanced DigiLocker using Ciphertext-Policy Attribute-Based Encryption
Puneet Bakshi and Sukumar Nandi

Efficient Access-control in the IIoT through Attribute-Based Encryption with Outsourced Decryption
Dominik Ziegler, Alexander Marsalek, Bernd Prünster and Josef Sabongui

Practical Predicate Encryption for Inner Product
Yi-Fan Tseng, Zi-Yuan Liu and Raylin Tso

Securing Device-to-Cloud Interactions in the Internet of Things Relying on Edge Devices
Elias Grande and Marta Beltrán

Under Pressure: Pushing Down on Me – Touch Sensitive Door Handle to Identify Users at Room Entry
Christian Tietz, Eric Klieme, Rachel Brabender, Teresa Lasarow, Lukas Rambold and Christoph Meinel

Practical Hash-based Anonymity for MAC Addresses
Junade Ali and Vladimir Dyo

Defender-centric Conceptual Cyber Exposure Ontology for Adaptive Cyber Risk Assessment
Lamine Aouad and Muhammad Rizwan Asghar

Performance Comparison of Two Generic MPC-frameworks with Symmetric Ciphers
Thomas Lorünser and Florian Wohner

A Fine-grained Access Control Model for Knowledge Graphs
Marco Valzelli, Andrea Maurino and Matteo Palmonari

A Trend-following Trading Indicator on Homomorphically Encrypted Data
Haotian Weng and Artem Lenskiy

XIV
<table>
<thead>
<tr>
<th>Title</th>
<th>Authors</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMART: Shared Memory based SDN Architecture to Resist DDoS ATtacks</td>
<td>Sana Belguith, Muhammad Rizwan Asghar, Song Wang, Karina Gomez and Giovanni Russello</td>
<td>600</td>
</tr>
<tr>
<td>QSOR: Quantum-safe Onion Routing</td>
<td>Zsolt Tujner, Thomas Rooijakkers, Maran van Heesch and Melek Önen</td>
<td>610</td>
</tr>
<tr>
<td>Attribute-Based Encryption and Its Application to a Software-Distributed Shared Memory</td>
<td>Oana Stan, Loic Cudennec and Louis Syoen</td>
<td>617</td>
</tr>
<tr>
<td>Address-bit Differential Power Analysis on Boolean Split Exponent Counter-measure</td>
<td>Christophe Negre</td>
<td>624</td>
</tr>
<tr>
<td>Providing Secured Access Delegation in Identity Management Systems</td>
<td>Abubakar-Sadiq Shehu, Antonio Pinto and Manuel E. Correia</td>
<td>630</td>
</tr>
<tr>
<td>An Innovative Self-Healing Approach with STIX Data Utilisation</td>
<td>Arnolnt Spyros, Konstantinos Rantos, Alexandros Papanikolaou and Christos Ilioudis</td>
<td>637</td>
</tr>
<tr>
<td><strong>AUTHOR INDEX</strong></td>
<td></td>
<td>651</td>
</tr>
</tbody>
</table>