

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

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2020) by SCITEPRESS – Science and Technology Publications, Lda.
All rights reserved.

Printed with permission by Curran Associates, Inc. (2021)

For permission requests, please contact SCITEPRESS – Science and Technology Publications, Lda.
at the address below.

SCITEPRESS – Science and Technology Publications, Lda.
Avenida de S. Francisco Xavier, Lote 7 Cv. C,
2900-616 Setúbal, Portugal

Phone: +351 265 520 185

Fax: +351 265520 186

info@scitepress.org

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

SECRYPT 2020

Proceedings of the
17th International Conference on
Security and Cryptography

July 8 - 10, 2020

Sponsored by
INSTICC - Institute for Systems and Technologies of Information, Control and Communication

Copyright © 2020 by SCITEPRESS – Science and Technology Publications, Lda.
All rights reserved

Edited by Pierangela Samarati, Sabrina De Capitani di Vimercati, Mohammad Obaidat and
Jalel Ben-Othman

ISSN: 2184-7711

<http://www.secrypt.icete.org>
secrypt.secretariat@insticc.org

BRIEF CONTENTS

INVITED SPEAKERS	IV
ORGANIZING COMMITTEES	V
PROGRAM COMMITTEE	VI
AUXILIARY REVIEWERS	VII
SELECTED PAPERS BOOK	VII
FOREWORD	IX
CONTENTS	XI

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
- Luís 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 of 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-Lluís 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**, Università 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
- Yunior 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**, Università 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, Fondazione 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 Tehnology, 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 SECURE 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 SECURE 2020 Program Committee members.

FOREWORD

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 Photonics21. 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 <i>Henderik A. Proper</i>	5
eHealth Monitoring Using Wireless Communication Protocols and Intelligent Systems <i>Jaime Lloret</i>	7
Industry 4.0: Challenges from a Data Science Perspective <i>Ajith Abraham</i>	9
Secure Computation Protocol: A Technology for Our Time <i>Moti Yung</i>	11
Analysing Digital Footprints to Infer the Health of Populations and Individuals <i>Ingemar Johansson Cox</i>	13

PAPERS

FULL PAPERS

Helper-in-the-Middle: Supporting Web Application Scanners Targeting Industrial Control Systems <i>Anne Borcharding, Steffen Pfrang, Christian Haas, Albrecht Weiche and Jürgen Beyerer</i>	19
Termination of Ethereum's Smart Contracts <i>Thomas Genet, Thomas Jensen and Justine Sauvage</i>	31
Avoiding Network and Host Detection using Packet Bit-masking <i>George Stergiopoulos, Eirini Lygerou, Nikolaos Tsalis, Dimitris Tomaras and Dimitris Gritzalis</i>	44
FPGA-based McEliece Cryptosystem using Non-linear Convolutional Codes <i>Michael Ekonde Sone</i>	56
CROOT: Code-based Round-Optimal Oblivious Transfer <i>Nicolas Aragon, Olivier Blazy, Neals Fournaise and Philippe Gaborit</i>	68
DCBC: A Distributed High-performance Block-Cipher Mode of Operation <i>Oussama Trabelsi, Lilia Sfaxi and Riadh Robbana</i>	78
Stay Thrifty, Stay Secure: A VPN-based Assurance Framework for Hybrid Systems <i>Marco Anisetti, Claudio A. Ardagna, Nicola Bena and Ernesto Damiani</i>	90
An Enhanced Lightweight Authentication Scheme for Secure Access to Cloud Data <i>Hamza Hammami, Mohammad S. Obaidat and Sadok Ben Yahia</i>	102
Decentralized Multi-Client Attribute Based Functional Encryption <i>Yuechen Chen, Linru Zhang and Siu-Ming Yiu</i>	110
Optimal Transport Layer for Secure Computation <i>Markus Brandt, Claudio Orlandi, Kris Shrishak and Haya Shulman</i>	122

An Identity-matching Process to Strengthen Trust in Federated-identity Architectures <i>Paul Marillonnet, Mikaël Ates, Maryline Laurent and Nesrine Kaaniche</i>	134
Ensuring the Integrity of Outsourced Web Scripts <i>Josselin Mignerey, Cyrille Mucchietto and Jean-Baptiste Orfila</i>	147
Authentication and Key Management Automation in Decentralized Secure Email and Messaging via Low-entropy Secrets <i>Itzel Vazquez Sandoval, Arash Atashpendar and Gabriele Lenzini</i>	159
FALCO: Detecting Superfluous JavaScript Injection Attacks using Website Fingerprints <i>Chih-Chun Liu, Hsu-Chun Hsiao and Tiffany Hyun-Jin Kim</i>	172
Beyond Black and White: Combining the Benefits of Regular and Incognito Browsing Modes <i>John Korniotakis, Panagiotis Papadopoulos and Evangelos P. Markatos</i>	184
Practically Efficient Attribute-based Encryption for Compartmented Access Structures <i>Ferucio Laurentiu Tiplea, Alexandru Ionitã and Anca Maria Nica</i>	193
Round-optimal Constant-size Blind Signatures <i>Olivier Blazy, Brouilhet Laura, Céline Chevalier and Neals Fournaise</i>	205
Prov-Trust: Towards a Trustworthy SGX-based Data Provenance System <i>Nesrine Kaaniche, Sana Belguith, Maryline Laurent, Ashish Gehani and Giovanni Russello</i>	217
A Failure Rate Model of Bit-flipping Decoders for QC-LDPC and QC-MDPC Code-based Cryptosystems <i>Marco Baldi, Alessandro Barengi, Franco Chiaraluce, Gerardo Pelosi and Paolo Santini</i>	230
SHORT PAPERS	
Exploring Current E-mail Cyber Threats using Authenticated SMTP Honeypot <i>Lukáš Zobal, Dušan Kolář and Jakub Křoustek</i>	245
Optimizing <i>dm-crypt</i> for XTS-AES: Getting the Best of Atmel Cryptographic Co-processors <i>Levent Demir, Mathieu Thiery, Vincent Roca, Jean-Michel Tenkes and Jean-Louis Roch</i>	255
<i>cipherPath</i> : Efficient Traversals over Homomorphically Encrypted Paths <i>Georg Bramm and Julian Schütte</i>	263
A White-Box Encryption Scheme using Physically Unclonable Functions <i>Sandra Rasoamiamanana, Marine Minier and Gilles Macario-Rat</i>	271
Towards Understanding Man-on-the-Side Attacks (MotS) in SCADA Networks <i>Peter Maynard and Kieran McLaughlin</i>	279
Towards Secure Edge-assisted Image Sharing for Timely Disaster Situation Awareness <i>Jing Yao, Yifeng Zheng, Cong Wang and Surya Nepal</i>	287
Evasive Windows Malware: Impact on Antiviruses and Possible Countermeasures <i>Cédric Herzog, Valérie Viet Triem Tong, Pierre Wilke, Arnaud Van Straaten and Jean-Louis Lanet</i>	294
Security Analysis of ElGamal Implementations <i>Mohamad El Laz, Benjamin Grégoire and Tamara Rezk</i>	302

Efficient Constructions of Non-interactive Secure Multiparty Computation from Pairwise Independent Hashing <i>Satoshi Obana and Maki Yoshida</i>	314
Signatures to Go: A Framework for Qualified PDF Signing on Mobile Devices <i>Emina Ahmetovic, Thomas Lenz and Christian Kollmann</i>	322
Privacy-Preserving Greater-Than Integer Comparison without Binary Decomposition <i>Sigurd Eskeland</i>	332
Multi-Stakeholder Cybersecurity Risk Assessment for Data Protection <i>Majid Mollaefar, Alberto Siena and Silvio Ranise</i>	341
A Novel Anonymous Authentication and Key Agreement Scheme for Smart Grid <i>Hamza Hammami, Mohammad S. Obaidat and Sadok Ben Yahia</i>	349
SENSSE: Simple, Efficient Searchable Symmetric Encryption for Sensor Networks <i>Bojan Spasić, Olivier Markowitch and Philippe Thiran</i>	355
Linear Generalized ElGamal Encryption Scheme <i>Pascal Lafourcade, Léo Robert and Demba Sow</i>	364
Accelerating Homomorphic Encryption using Approximate Computing Techniques <i>Shabnam Khanna and Ciara Rafferty</i>	372
This Selfie Does Not Exist: On the Security of Electroneum Cloud Mining <i>Alexander Marsalek, Edona Faslija and Dominik Ziegler</i>	380
ProteiNN: Privacy-preserving One-to-Many Neural Network Classifications <i>Beyza Bozdemir, Orhan Ermis and Melek Önen</i>	389
Privacy-preserving Content-based Publish/Subscribe with Encrypted Matching and Data Splitting <i>Nathanaël Denis, Pierre Chaffardon, Denis Conan, Maryline Laurent, Sophie Chabridon and Jean Leneutre</i>	397
Differentially Private Graph Publishing and Randomized Response for Collaborative Filtering <i>Julián Salas and Vicenç Torra</i>	407
A Machine-learning based Unbiased Phishing Detection Approach <i>Hossein Shirazi, Landon Zweigle and Indrakshi Ray</i>	415
Beyond Administration: A Modeling Scheme Supporting the Dynamic Analysis of Role-based Access Control Policies <i>Marius Schlegel and Peter Amthor</i>	423
Solving Set Relations with Secure Bloom Filters Keeping Cardinality Private <i>Louis Tajan, Dirk Westhoff and Frederik Armknecht</i>	435
Identity Verification and Fraud Detection During Online Exams with a Privacy Compliant Biometric System <i>M. A. Haytom, C. Rosenberger, C. Charrier, C. Zhu and C. Regnier</i>	443
VIP Blowfish Privacy in Communication Graphs <i>Mohamed Nassar, Elie Chicha, Bechara Al Bouna and Richard Chbeir</i>	451
Droppix: Towards More Realistic Video Fingerprinting <i>Przemysław Błażkiewicz, Marek Klonowski and Piotr Syga</i>	460

Software Emulation of Quantum Resistant Trusted Platform Modules <i>Luis Fiolhais, Paulo Martins and Leonel Sousa</i>	469
Formal Accuracy Analysis of a Biometric Data Transformation and Its Application to Secure Template Generation <i>Shoukat Ali, Koray Karabina and Emrah Karagoz</i>	477
SwaNN: Switching among Cryptographic Tools for Privacy-preserving Neural Network Predictions <i>Gamze Tillem, Beyza Bozdemir and Melek Önen</i>	489
Deconstructing the Decentralization Trilemma <i>Harry Halpin</i>	497
Towards Language Support for Model-based Security Policy Engineering <i>Peter Amthor and Marius Schlegel</i>	505
Exploiting Hot Spots in Heuristic Safety Analysis of Dynamic Access Control Models <i>Marius Schlegel and Winfried E. Kühnhauser</i>	514
POSTERS	
CP-ABE Scheme Satisfying Constant-size Keys based on ECC <i>Nishant Raj and Alwyn Roshan Pais</i>	527
Privacy Enhanced DigiLocker using Ciphertext-Policy Attribute-Based Encryption <i>Puneet Bakshi and Sukumar Nandi</i>	533
Efficient Access-control in the IIoT through Attribute-Based Encryption with Outsourced Decryption <i>Dominik Ziegler, Alexander Marsalek, Bernd Prünster and Josef Sabongui</i>	539
Practical Predicate Encryption for Inner Product <i>Yi-Fan Tseng, Zi-Yuan Liu and Raylin Tso</i>	545
Securing Device-to-Cloud Interactions in the Internet of Things Relying on Edge Devices <i>Elías Grande and Marta Beltrán</i>	551
Under Pressure: Pushing Down on Me – Touch Sensitive Door Handle to Identify Users at Room Entry <i>Christian Tietz, Eric Klieme, Rachel Brabender, Teresa Lasarow, Lukas Rambold and Christoph Meinel</i>	557
Practical Hash-based Anonymity for MAC Addresses <i>Junade Ali and Vladimir Dyo</i>	564
Defender-centric Conceptual Cyber Exposure Ontology for Adaptive Cyber Risk Assessment <i>Lamine Aouad and Muhammad Rizwan Asghar</i>	572
Performance Comparison of Two Generic MPC-frameworks with Symmetric Ciphers <i>Thomas Lorünser and Florian Wohner</i>	579
A Fine-grained Access Control Model for Knowledge Graphs <i>Marco Valzelli, Andrea Maurino and Matteo Palmonari</i>	587
A Trend-following Trading Indicator on Homomorphically Encrypted Data <i>Haotian Weng and Artem Lenskiy</i>	594

SMART: Shared Memory based SDN Architecture to Resist DDoS Attacks <i>Sana Belguith, Muhammad Rizwan Asghar, Song Wang, Karina Gomez and Giovanni Russello</i>	600
QSOR: Quantum-safe Onion Routing <i>Zsolt Tujner, Thomas Rooijackers, Maran van Heesch and Melek Önen</i>	610
Attribute-Based Encryption and Its Application to a Software-Distributed Shared Memory <i>Oana Stan, Loïc Cudennec and Louis Syoën</i>	617
Address-bit Differential Power Analysis on Boolean Split Exponent Counter-measure <i>Christophe Negre</i>	624
Providing Secured Access Delegation in Identity Management Systems <i>Abubakar-Sadiq Shehu, António Pinto and Manuel E. Correia</i>	630
An Innovative Self-Healing Approach with STIX Data Utilisation <i>Arnolnt Spyros, Konstantinos Rantos, Alexandros Papanikolaou and Christos Ilioudis</i>	637
A Comprehensive Quantified Approach for Security Risk Management in e-Health Systems <i>Sondes Ksibi, Faouzi Jaidi and Adel Bouhoula</i>	644
AUTHOR INDEX	651