

## 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 <https://link.springer.com/bookseries/7410>


Joaquin Garcia-Alfaro · Jose Luis Muñoz-Tapia ·  
Guillermo Navarro-Arribas ·  
Miguel Soriano (Eds.)


# Data Privacy Management, Cryptocurrencies and Blockchain Technology


ESORICS 2021 International Workshops, DPM 2021 and CBT 2021  
Darmstadt, Germany, October 8, 2021  
Revised Selected Papers

### *Editors*

Joaquín García-Alfaro   
Institut Polytechnique de Paris  
Palaiseau, France

Guillermo Navarro-Arribas   
Universitat Autònoma de Barcelona  
Bellaterra, Spain

Jose Luis Muñoz-Tapia   
Universitat Politècnica de Catalunya  
Barcelona, Spain

Miguel Soriano   
Universitat Politècnica de Catalunya  
Barcelona, Spain

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-93943-4

ISBN 978-3-030-93944-1 (eBook)

<https://doi.org/10.1007/978-3-030-93944-1>

LNCS Sublibrary: SL4 – Security and Cryptology

© 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

## Foreword from the DPM 2021 Program Chairs

This volume contains the post-proceedings of the 16th Data Privacy Management International Workshop (DPM 2021), which was organized within the 26th European Symposium on Research in Computer Security (ESORICS 2021). The DPM series started in 2005 when the first workshop took place in Tokyo (Japan). Since then, the event has been held in different venues: Atlanta, USA (2006); Istanbul, Turkey (2007); Saint Malo, France (2009); Athens, Greece (2010); Leuven, Belgium (2011); Pisa, Italy (2012); Egham, UK (2013); Wroclaw, Poland (2014); Vienna, Austria (2015); Crete, Greece (2016); Oslo, Norway (2017); Barcelona, Spain (2018); Luxembourg (2019); and (held virtually) Guildford, UK (2020).

This 2021 edition was intended to be held in Darmstadt, Germany, but was finally held virtually, due to the COVID-19 pandemic, together with the ESORICS main conference and all its workshops.

In response to the call for papers, we received 26 submissions. Each submission was evaluated on the basis of significance, novelty, and technical quality. The Program Committee performed a thorough review process and selected seven full papers, complemented by one position paper and three short papers. The result was a technical program covering topics such as cyber-incident risks involving privacy violations, privacy-preserving location techniques, use of learning approaches to handle privacy management issues, data minimization, policies, and regulation.

We would like to thank everyone who helped at organizing the event, including all the members of the organizing committee of both ESORICS and DPM 2021. Our gratitude goes to Michael Waidner, the general chair of ESORICS 2021. During the event, we had the valued assistance and help of Martina Creutzfeldt. Thanks go as well to all the DPM 2021 Program Committee members, additional reviewers, all the authors who submitted papers, and to all the workshop attendees.

Finally, we want to acknowledge the support received from the sponsoring institutions: Institut Mines-Télécom, Institut Polytechnique de Paris (Telecom SudParis and Samovar Confiance Numérique), Universitat Autònoma de Barcelona (UAB), Universitat Politècnica de Catalunya, the UNESCO Chair in Data Privacy, and Cybercat. We also acknowledge support from the following projects and grants from the Spanish Government: TIN2017-87211-R, SECURITAS RED2018-102321-T, and Beatriz Galindo BG20/00217.

November 2021

Miguel Soriano  
Guillermo Navarro-Arribas  
Joaquín García-Alfaro

# DPM 2021 Organization

## Program Chairs

Joaquin Garcia-Alfaro  
Guillermo Navarro-Arribas  
Miguel Soriano

Institut Polytechnique de Paris, France  
Universitat Autònoma de Barcelona, Spain  
Universitat Politècnica de Catalunya, Spain

## Program Committee

Esma Aïmeur  
Ken Barker  
Elisa Bertino  
Jordi Casas-Roma  
Mauro Conti  
Frédéric Cuppens  
Nora Cuppens-Boulahia  
Nicolas E. Diaz Ferreyra  
Sabrina De Capitani di  
Vimercati

Josep Domingo-Ferrer  
Sara Foresti  
Jose Maria de Fuentes  
Sebastien Gambs  
Javier Herranz  
Marc Juarez  
Christos Kalloniatis  
Florian Kammüller  
Sokratis Katsikas  
Hiroaki Kikuchi  
Evangelos Kranakis  
Alptekin Küpçü  
Costas Lambrinoudakis  
Maryline Laurent  
Giovanni Livraga  
Brad Malin  
Chris Mitchell  
Martín Ochoa  
Melek Önen  
Gerardo Pelosi  
Silvio Ranise  
Kai Rannenberg  
Ruben Rios

University of Montreal, Canada  
University of Calgary, Canada  
Purdue University, USA  
Universitat Oberta de Catalunya, Spain  
University of Padua, Italy  
Polytechnique Montreal, Canada  
Polytechnique Montreal, Canada  
University of Duisburg-Essen, Germany  
Università degli Studi di Milano, Italy  
  
Universitat Rovira i Virgili, Spain  
Università degli Studi di Milano, Italy  
Universidad Carlos III de Madrid, Spain  
Université du Québec à Montréal, Canada  
Universitat Politècnica de Catalunya, Spain  
University of Southern California, USA  
University of the Aegean, Greece  
Middlesex University London and TU Berlin, Germany  
Open University of Cyprus, Cyprus  
Meiji University, Japan  
Carleton University, Canada  
Koç University, Turkey  
University of Piraeus, Greece  
Institut Mines-Télécom, France  
University of Milan, Italy  
Vanderbilt University, USA  
Royal Holloway, University of London, UK  
AppGate Inc., Colombia  
EURECOM, France  
Politecnico di Milano, Italy  
Fondazione Bruno Kessler, Italy  
Goethe University Frankfurt, Germany  
University of Malaga, Spain

Pierangela Samarati	Università degli Studi di Milano, Italy
Vicenç Torra	Umeå University, Sweden
Yasuyuki Tsukada	Kanto Gakuin University, Japan
Alexandre Viejo	Universitat Rovira i Virgili, Spain
Isabel Wagner	De Montfort University, UK
Jens Weber	University of Victoria, Canada
Lena Wiese	University of Göttingen, Germany
Nicola Zannone	Eindhoven University of Technology, The Netherlands

## **Steering Committee**

Joaquin Garcia-Alfaro	Institut Polytechnique de Paris, France
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Vicenç Torra	Umeå University, Sweden

## **Additional Reviewers**

Alessandro Brighente	Riccardo Longo
David Harborth	Utku Tefek
Stefano Berlato	Osman Biçer
Fred Tronnier	Ehsan Nowroozi
Ziqi Zhang	

## **Foreword from the CBT 2021 Program Chairs**

The 5th International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2021) was held in collaboration with the 26th European Symposium on Research in Computer Security (ESORICS 2021) and the 16th International Workshop on Data Privacy Management (DPM 2021). Due to the COVID-19 outbreak, the event was held virtually.

We wish to thank all of the authors who submitted their work. This year, CBT received 31 submissions. The review process was conducted virtually, using the EasyChair platform, by the Program Chairs and all the members of the Program Committee, with the help of some external reviewers. Based on the reviews and the discussion, six papers were accepted for presentation at the workshop as full papers, complemented by six short papers.

We would like to thank all of the people involved in CBT 2021. We are grateful to the Program Committee members and the external reviewers for their help in providing detailed and timely reviews of the submissions. We also thank all the members of the ESORICS 2021 local organization team for all their help and support. Thanks go as well to Springer for their support throughout the entire process. Last but by no means least, we thank all the authors who submitted papers and all the workshop attendees.

Finally, we want to acknowledge the support received from the sponsoring institutions: Universitat Politècnica de Catalunya, Institut Polytechnique de Paris (Telecom SudParis and Samovar Confiance Numérique), Universitat Autònoma de Barcelona (UAB), BART (Inria, IRT SYSTEMX, Institut Mines-Télécom), Cybercat, and Bandit. We acknowledge support as well from the Beatriz Galindo grant BG20/00217.

November 2021

Jose Luis Muñoz-Tapia  
Guillermo Navarro-Arribas  
Joaquin Garcia-Alfaro



# CBT 2021 Organization

## Program Chairs

Joaquin Garcia-Alfaro  
Guillermo Navarro  
Jose Luis Muñoz-Tapia

Institut Polytechnique de Paris, France  
Universitat Autònoma de Barcelona, Spain  
Universitat Politècnica de Catalunya, Spain

## Program Committee

Shashank Agrawal	Western Digital Research, USA
Daniel Augot	Inria Saclay, France
Georgia Avarikioti	ETH Zurich, Switzerland
Spiridon Bakiras	Hamad Bin Khalifa University, Qatar
Iddo Bentov	Cornell Tech, USA
Alex Biryukov	University of Luxembourg, Luxembourg
George Bissias	University of Massachusetts at Amherst, USA
Joseph Bonneau	New York University, USA
Karima Boudaoud	University of Nice, France
Jeremy Clark	Concordia University, Canada
Mauro Conti	University of Padua, Italy
Sanchari Das	University of Denver, USA
Vanesa Daza	Universitat Pompeu Fabra, Spain
Matteo Dell'Amico	EURECOM, France
Sven Dietrich	City University of New York, USA
Kaoutar Elkhiyaoui	EURECOM, France
Esha Ghosh	Microsoft Research, USA
Hannes Hartenstein	Karlsruhe Institute of Technology, Germany
Ethan Heilman	Boston University, USA
Ryan Henry	University of Calgary, Canada
Antonio Faonio	EURECOM, France
Jordi Herrera-Joancomarti	Universitat Autònoma de Barcelona, Spain
Ghassan Karame	NEC Research, Germany
Jiasun Li	George Mason University, USA
Daniel Xiapu Luo	Hong Kong Polytechnic University, Hong Kong
Giorgia Marson	University of Bern, Switzerland
Shin'ichiro Matsuo	Georgetown University, USA
Pedro Moreno-Sanchez	IMDEA, Spain
Cristina Pérez-Solà	Universitat Oberta de Catalunya, Spain
Simon Oya	University of Waterloo, Canada
Elizabeth Quaglia	Royal Holloway, University of London, UK

Alfredo Rial	University of Luxembourg, Luxembourg
Alessandra Scafuro	North Carolina State University, USA
Edgar Weippl	SBA Research, Austria

### **Steering Committee**

Rainer Böhme	Universität Innsbruck, Austria
Joaquin Garcia-Alfaro	Institut Polytechnique de Paris, France
Hannes Hartenstein	Karlsruher Institut für Technologie, Germany
Jordi Herrera-Joancomart	Universitat Autònoma de Barcelona, Spain

### **Additional Reviewers**

Alessandro Brighente	Maryam Ehsanpour
Héctor Masip Ardevol	Rahul Saha
Giuseppe Vitto	Abhimanyu Rawat
Saskia Bayreuther	Lukas Aumayr
Oliver Stengele	Marc Leinweber
Maja Schwarz	Aljosha Judmayer

# Contents

## DPM Workshop: Risks and Privacy Preservation

Best Security Measures to Reduce Cyber-Incident and Data Breach Risks . . .	3
<i>Hiroaki Kikuchi, Michihiro Yamada, Kazuki Ikegami, and Koji Inui</i>	
Synthesizing Privacy-Preserving Location Traces Including Co-locations . . . .	20
<i>Jun Narita, Yayoi Suganuma, Masakatsu Nishigaki, Takao Murakami, and Tetsushi Ohki</i>	

## DPM Workshop: Policies and Regulation

Quantitative Rubric for Privacy Policy Analysis . . . . .	39
<i>Paul O'Donnell, Joe Harrison, Joshua Lyons, Lauren Anderson, Lauren Maunder, Sarah Ramboyong, and Alan J. Michaels</i>	
Rethinking the Limits of Mobile Operating System Permissions . . . . .	55
<i>Brian Krupp</i>	
Interdependent Privacy Issues Are Pervasive Among Third-Party Applications . . . . .	70
<i>Shuaishuai Liu, Barbara Herendi, and Gergely Biczók</i>	

## DPM Workshop: Privacy and Learning

SPGC: An Integrated Framework of Secure Computation and Differential Privacy for Collaborative Learning . . . . .	89
<i>Kazuki Iwahana, Naoto Yanai, Jason Paul Cruz, and Toru Fujiwara</i>	
A $k$ -Anonymised Federated Learning Framework with Decision Trees . . . . .	106
<i>Saloni Kwatra and Vicenç Torra</i>	
Anonymizing Machine Learning Models . . . . .	121
<i>Abigail Goldstein, Gilad Ezov, Ron Shmelkin, Micha Moffie, and Ariel Farkash</i>	

## DPM Workshop: Short Papers

A New Privacy Enhancing Beacon Scheme in V2X Communication . . . . .	139
<i>Takahito Yoshizawa, Dave Singelée, and Bart Preneel</i>	
Next Generation Data Masking Engine . . . . .	152
<i>Micha Moffie, Dan Mor, Sigal Asaf, and Ariel Farkash</i>	

Towards a Formal Approach for Data Minimization in Programs (Short Paper) . . . . .	161
<i>Florian Lanzinger and Alexander Weigl</i>	
<b>CBT Workshop: Mining, Consensus and Market Manipulation</b>	
Virtual ASICs: Generalized Proof-of-Stake Mining in Cryptocurrencies . . . . .	173
<i>Chaya Ganesh, Claudio Orlandi, Daniel Tschudi, and Aviv Zohar</i>	
Asymmetric Asynchronous Byzantine Consensus . . . . .	192
<i>Christian Cachin and Luca Zanolini</i>	
Using Degree Centrality to Identify Market Manipulation on Bitcoin. . . . .	208
<i>Daiane M. Pereira and Rodrigo S. Couto</i>	
<b>CBT Workshop: Smart Contracts and Anonymity</b>	
Augmenting MetaMask to Support TLS-endorsed Smart Contracts . . . . .	227
<i>Ulrich Gellersdörfer, Jonas Ebel, and Florian Matthes</i>	
Smart Contracts for Incentivized Outsourcing of Computation . . . . .	245
<i>Alptekin Küpçü and Reihaneh Safavi-Naini</i>	
Anonymous Sidechains . . . . .	262
<i>Foteini Baldimtsi, Ian Miers, and Xinyuan Zhang</i>	
<b>CBT Workshop: Short Papers</b>	
Filling the Tax Gap via Programmable Money . . . . .	281
<i>Dimitris Karakostas and Aggelos Kiayias</i>	
Impact of Delay Classes on the Data Structure in IOTA. . . . .	289
<i>Andreas Penzkofer, Olivia Saa, and Daria Dziubaltowska</i>	
Secure Static Content Delivery for CDN Using Blockchain Technology. . . . .	301
<i>Mauro Conti, P. Vinod, and Pier Paolo Tricomi</i>	
Lattice-Based Proof-of-Work for Post-Quantum Blockchains . . . . .	310
<i>Rouzbeh Behnia, Eamonn W. Postlethwaite, Muslum Ozgur Ozmen, and Attila Altay Yavuz</i>	
Blockchain-Based Two-Factor Authentication for Credit Card Validation . . . . .	319
<i>Suat Mercan, Mumin Cebe, Kemal Akkaya, and Julian Zuluaga</i>	

Homomorphic Decryption in Blockchains via Compressed Discrete-Log Lookup Tables . . . . .	328
<i>Panagiotis Chatzigiannis, Konstantinos Chalkias, and Valeria Nikolaenko</i>	
<b>Author Index</b> . . . . .	341