

## 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 series at <http://www.springer.com/series/7410>

Cristina Pérez-Solà · Guillermo Navarro-Arribas ·  
Alex Biryukov · Joaquin Garcia-Alfaro (Eds.)


# Data Privacy Management, Cryptocurrencies and Blockchain Technology

ESORICS 2019 International Workshops, DPM 2019  
and CBT 2019, Luxembourg, September 26–27, 2019  
Proceedings

### *Editors*

Cristina Pérez-Solà   
Universitat Oberta de Catalunya  
Barcelona, Spain

Alex Biryukov  
University of Luxembourg  
Esch-sur-Alzette, Luxembourg

Guillermo Navarro-Arribas   
Universitat Autònoma de Barcelona  
Bellaterra, Spain

Joaquín García-Alfaro   
Institut Mines-Télécom  
Evry, France

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-31499-6              ISBN 978-3-030-31500-9 (eBook)  
<https://doi.org/10.1007/978-3-030-31500-9>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2019

Chapters “Integral Privacy Compliant Statistics Computation” and “Graph Perturbation as Noise Graph Addition: A New Perspective for Graph Anonymization” are licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapters.

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 2019 Program Chairs

This volume contains the proceedings of the 14th Data Privacy Management International Workshop (DPM 2017), held in Luxembourg, on September 26, 2019. The workshop, as previous editions, was organized as part of the 24nd European Symposium on Research in Computer Security (ESORICS) 2019. 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); and Barcelona, Spain (2018).

The aim of DPM is to promote and stimulate international collaboration and research exchange on areas related to the management of privacy-sensitive information. This is a very critical and important issue for organizations and end-users. It poses several challenging problems, such as translation of high-level business goals into system-level privacy policies, administration of sensitive identifiers, data integration and privacy engineering, among others.

In this workshop edition we received 26 submission, and each one was evaluated on the basis of significance, novelty, and technical quality. The Program Committee performed an excellent job and all submissions went through a careful review process. In the end, eight full papers, and two short/position papers were accepted for publication and presentation at the event.

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 2019. Our gratitude also goes to Peter Ryan, to the ESORICS 2019 general chair, Peter Roenne and Magali Martin, ESORICS 2019 local organization chairs, and Joaquin Garcia-Alfaro, the workshops chair of ESORICS 2019. Last, but by no means least, we thank all the DPM 2019 Program Committee members, all the additional reviewers, all the authors who submitted papers, and all the workshop attendees.

Finally, we want to acknowledge the support received from the sponsors of the workshop: Universitat Autònoma de Barcelona (UAB), Internet Interdisciplinary Institute (IN3) from the Universitat Oberta de Catalunya (UOC), UNESCO Chair in Data Privacy, Institut Mines-Telecom (Telecom SudParis), CNRS Samovar UMR 5157 (R3S team), and projects TIN2017-87211-R and RTI2018-095094-B-C22 “CONSENT” from the Spanish MINECO.

August 2019

Cristina Pérez-Solà  
Guillermo Navarro-Arribas

# Organization

## 14th International Workshop on Data Privacy Management – DPM 2019

### Program Chairs

Cristina Pérez-Solà	Universitat Oberta de Catalunya, Spain
Guillermo Navarro-Arribas	Universitat Autònoma de Barcelona, Spain

### Program Committee

Archita Agarwal	Brown University, USA
Jordi Casas-Roma	Universitat Oberta de Catalunya, Spain
Jordi Castellà-Roca	Universitat Rovira i Virgili, Spain
Mauro Conti	University of Padua, Italy
Frédéric Cuppens	TELECOM Bretagne, France
Nora Cuppens-Boulahia	IMT Atlantique, France
Sabrina De Capitani di Vimercati	University of Milan, Italy
Jose Maria de Fuentes	Universidad Carlos III de Madrid, Spain
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Christian Duncan	Quinnipiac University, USA
Sebastien Gambs	Université du Québec à Montréal, Canada
Joaquin Garcia-Alfaro	Telecom SudParis, France
Marit Hansen	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Germany
Jordi Herrera-Joancomartí	Universitat Autònoma de Barcelona, Spain
Marc Juarez	Katholieke Universiteit Leuven, Belgium
Christos Kalloniatis	University of the Aegean, Greece
Florian Kammüller	Middlesex University London and TU Berlin, UK/Germany
Sokratis Katsikas	Center for Cyber and Information Security, NTNU, Norway
Hiroaki Kikuchi	Meiji University, Japan
Evangelos Kranakis	Carleton University, Canada
Alptekin Küpçü	Koç University, Turkey
Costas Lambrinoudakis	University of Piraeus, Greece
Maryline Laurent	Institut Mines-Telecom, France
Giovanni Livraga	University of Milan, Italy

Brad Malin	Vanderbilt University, USA
Fabio Martinelli	IIT-CNR, Italy
Chris Mitchell	Royal Holloway, University of London, UK
Anna Monreale	University of Pisa, Italy
Jordi Nin	ESADE, Universitat Ramon Llull, Spain
Melek Önen	EURECOM, France
Javier Parra-Arnau	Universitat Rovira i Virgili, Spain
Silvio Ranise	FBK-Irst, Italy
Kai Rannenberg	Goethe University Frankfurt, Germany
Ruben Rios	University of Malaga, Spain
Pierangela Samarati	University of Milan, Italy
David Sanchez	Universitat Rovira i Virgili, Spain
Claudio Soriente	NEC Laboratories Europe, Spain
Iraklis Symeonidis	SnT/APSIA, Luxembourg
Vicenç Torra	Maynooth University, Ireland
Yasuyuki Tsukada	Kanto Gakuin University, Japan
Alexandre Viejo	Universitat Rovira i Virgili, Spain
Isabel Wagner	De Montfort University, UK
Lena Wiese	Georg-August Universität Göttingen, Germany
Nicola Zannone	Eindhoven University of Technology, The Netherlands

### **Additional Reviewers**

Osman Biçer  
 Alberto Blanco-Justicia  
 Majid Hatamian  
 Eleni Laskarina Makri  
 Sergio Martinez  
 Francesca Pratesi  
 Sanaz Taheri Boshrooyeh  
 Federico Turrin  
 Panagiotis Zagouras

## Foreword from the CBT 2019 Program Chairs

This volume contains the proceedings of the Third International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2019) held in Luxembourg, during September 26–27, 2019, in conjunction with the 24th European Symposium on Research in Computer Security (ESORICS) 2019.

Cryptocurrencies and blockchain technology is an area of research which is currently going through rapid development combining progress in IT and security technologies such as novel cryptographic techniques with economic insight and societal needs. As technology matures one can see a move from building blocks and proofs of concept to higher levels and concrete applications. To that end, the CBT workshop aims to provide a forum where researchers in this area can carefully analyze current systems and propose new ones in order to create a scientific background for the solid development of this new field.

In response to the call for papers, we received 32 submissions that were carefully reviewed by the Program Committee of 25 members as well as additional reviewers. Most of the submission received three reviews. The Program Committee selected ten full papers and five short papers for presentation at the workshop. The selected papers cover aspects of smart contracts, second layer and off-chain transactions, economic incentives, privacy, and applications.

Furthermore, the workshop was enhanced with keynote talks sponsored by the Research Institute (cf. <https://researchinstitute.io/>), BART (Blockchain Advanced Research & Technologies), Inria Saclay, Institut Mines-Télécom, and SAMOVAR (URM 5157 of CNRS).

Special thanks to all the authors who submitted papers to CBT 2019, the Program Committee and additional reviewers, who worked hard to review the submissions and discussed the final program. Last but not least, we would like to thank the ESORICS 2019 general chair, Peter Ryan, and the ESORICS 2019 local organization chairs, Peter Roenne and Magali Martin, for all their help and support.

August 2019

Alex Biryukov  
Joaquin Garcia-Alfaro



# Organization

## Third International Workshop on Cryptocurrencies and Blockchain Technology – CBT 2019

### Program Chairs

Alex Biryukov	University of Luxembourg, Luxembourg
Joaquin Garcia-Alfaro	Institut Mines-Telecom, TELECOM SudParis, France

### Program Committee

Daniel Augot	Inria Saclay, France
Jean-Philippe Aumasson	Kudelski, Switzerland
George Bissias	University of Massachusetts at Amherst, USA
Joseph Bonneau	NYU, USA
Rainer Böhme	Universität Innsbruck, Austria
Christian Decker	Blockstream, Switzerland
Sergi Delgado-Segura	UCL, UK
Arthur Gervais	Imperial College London, UK
Hannes Hartenstein	KIT, Germany
Jordi Herrera-Joancomarti	UAB, Spain
Man Ho Au	The Hong Kong Polytechnic University, SAR China
Ghassan Karame	NEC Research, Germany
Aniket Kate	Purdue University, USA
Eleftherios Kokoris-Kogias	EPFL, Switzerland
Patrick McCorry	UCL, UK
Shin'ichiro Matsuo	Georgetown University, USA
Pedro Moreno-Sanchez	TU Wien, Austria
Guillermo Navarro-Arribas	UAB, Spain
Cristina Pérez-Solá	UOC, Spain
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Tim Ruffing	Blockstream, Switzerland
Fatemeh Shirazi	Web3 Foundation, Switzerland
Ewa Syta	Trinity College, USA
Khalifa Toumi	SystemX, France
Edgar Weippl	SBA Research, Austria

**Additional Reviewers**

Sébastien Andreina  
Daniel Feher  
Michael Fröwis  
Jan Grashoefer  
Marc Leinweber  
Wenting Li  
Donghang Lu  
Philipp Schindler

Clara Schneidewind  
Brian Shaft  
Oliver Stengele  
Nicholas Stifter  
Giuseppe Vitto  
Karl Wuest  
Alexei Zamyatin  
Ren Zhang

**Steering Committee**

Rainer Böhme  
Joaquin Garcia-Alfaro  
Hannes Hartenstein  
Jordi Herrera-Joancomartí

Universität Innsbruck, Austria  
Institut Mines-Telecom, France  
Karlsruher Institut für Technologie, Germany  
Universitat Autònoma de Barcelona, Spain

# Contents

## DPM Workshop: Privacy Preserving Data Analysis

PINFER: Privacy-Preserving Inference: Logistic Regression, Support Vector Machines, and More, over Encrypted Data. . . . .	3
<i>Marc Joye and Fabien Petitcolas</i>	
Integral Privacy Compliant Statistics Computation. . . . .	22
<i>Navoda Senavirathne and Vicenç Torra</i>	
Towards Data Anonymization in Data Mining via Meta-heuristic Approaches . . . . .	39
<i>Fatemeh Amiri, Gerald Quirchmayr, Peter Kieseberg, Edgar Weippl, and Alessio Bertone</i>	
Skiplist Timing Attack Vulnerability . . . . .	49
<i>Eyal Nussbaum and Michael Segal</i>	

## DPM Workshop: Field/Lab Studies

A Study on Subject Data Access in Online Advertising After the GDPR . . . .	61
<i>Tobias Urban, Dennis Tatang, Martin Degeling, Thorsten Holz, and Norbert Pohlmann</i>	
On Privacy Risks of Public WiFi Captive Portals . . . . .	80
<i>Suzan Ali, Tousif Osman, Mohammad Mannan, and Amr Youssef</i>	
User Perceptions of Security and Usability of Mobile-Based Single Password Authentication and Two-Factor Authentication . . . . .	99
<i>Devriş İşler, Alptekin Küpçü, and Aykut Coskun</i>	

## DPM Workshop: Privacy by Design and Data Anonymization

Graph Perturbation as Noise Graph Addition: A New Perspective for Graph Anonymization. . . . .	121
<i>Vicenç Torra and Julián Salas</i>	
Towards Minimising Timestamp Usage In Application Software: A Case Study of the Mattermost Application . . . . .	138
<i>Christian Burkert and Hannes Federrath</i>	

Card-Based Cryptographic Protocols with the Minimum Number of Rounds Using Private Operations . . . . .	156
<i>Hibiki Ono and Yoshifumi Manabe</i>	

## **CBT Workshop: Lightning Networks and Level 2**

TEE-Based Distributed Watchtowers for Fraud Protection in the Lightning Network. . . . .	177
<i>Marc Leinweber, Matthias Grundmann, Leonard Schönborn, and Hannes Hartenstein</i>	

Payment Networks as Creation Games. . . . .	195
<i>Georgia Avarikioti, Rolf Scheuner, and Roger Wattenhofer</i>	

An Efficient Micropayment Channel on Ethereum. . . . .	211
<i>Hisham S. Galal, Muhammad ElSheikh, and Amr M. Youssef</i>	

Extending Atomic Cross-Chain Swaps. . . . .	219
<i>Jean-Yves Zie, Jean-Christophe Deneuville, Jérémy Briffaut, and Benjamin Nguyen</i>	

## **CBT Workshop: Smart Contracts and Applications**

A Minimal Core Calculus for Solidity Contracts . . . . .	233
<i>Massimo Bartoletti, Letterio Galletta, and Maurizio Murgia</i>	

Multi-stage Contracts in the UTXO Model. . . . .	244
<i>Alexander Chepurinov and Amitabh Saxena</i>	

The Operational Cost of Ethereum Airdrops. . . . .	255
<i>Michael Fröwis and Rainer Böhme</i>	

Blockchain Driven Platform for Energy Distribution in a Microgrid . . . . .	271
<i>Arjun Choudhry, Ikechukwu Dimobi, and Zachary M. Isaac Gould</i>	

Practical Mutation Testing for Smart Contracts . . . . .	289
<i>Joran J. Honig, Maarten H. Everts, and Marieke Huisman</i>	

## **CBT Workshop: Payment Systems, Privacy and Mining**

Online Payment Network Design . . . . .	307
<i>Georgia Avarikioti, Kenan Besic, Yuyi Wang, and Roger Wattenhofer</i>	

A Multi-protocol Payment System to Facilitate Financial Inclusion . . . . .	321
<i>Kazım Rifat Özyilmaz, Nazmi Berhan Kongel, Ali Erhat Nalbant, and Ahmet Özcan</i>	

Simulation Extractability in Groth’s zk-SNARK . . . . .	336
<i>Shahla Atapoor and Karim Baghery</i>	
Auditable Credential Anonymity Revocation Based on Privacy-Preserving Smart Contracts. . . . .	355
<i>Rujia Li, David Galindo, and Qi Wang</i>	
Bonded Mining: Difficulty Adjustment by Miner Commitment . . . . .	372
<i>George Bissias, David Thibodeau, and Brian N. Levine</i>	
12 Angry Miners . . . . .	391
<i>Aryaz Eghbali and Roger Wattenhofer</i>	
<b>Author Index . . . . .</b>	<b>399</b>