

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>


Joaquin Garcia-Alfaro · Guillermo Navarro-Arribas ·
Jordi Herrera-Joancomarti (Eds.)


Data Privacy Management, Cryptocurrencies and Blockchain Technology

ESORICS 2020 International Workshops, DPM 2020 and CBT 2020
Guildford, UK, September 17–18, 2020
Revised Selected Papers

Editors

Joaquín García-Alfaro 
Télécom SudParis
Evry Cedex, France

Jordi Herrera-Joancomartí 
Escola d'Enginyeria
Universitat Autònoma de Barcelona
Cerdanyola del Vallès, Barcelona, Spain

Guillermo Navarro-Arribas 
Departament d'Enginyeria de la Informació i
de les Comunicacions
Universitat Autònoma de Barcelona
Bellaterra, Spain

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-66171-7 ISBN 978-3-030-66172-4 (eBook)
<https://doi.org/10.1007/978-3-030-66172-4>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020

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 2020 Program Chairs

This volume contains the post-proceedings of the 15th Data Privacy Management International Workshop (DPM 2020), which was organized within the 25th European Symposium on Research in Computer Security (ESORICS 2020). 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); Wrocław, Poland (2014); Vienna, Austria (2015); Crete, Greece (2016); Oslo, Norway (2017); Barcelona, Spain (2018); and Luxembourg (2019).

This 2020 edition was intended to be held in the University of Surrey, UK, but was finally held virtually due to the COVID-19 pandemic together with the ESORICS main conference and all its workshops.

We received 38 submissions. The Program Committee performed excellent work and all submissions went through a careful review process. Each paper was evaluated on the basis of significance, novelty, and technical quality. After reviewing the submissions, 12 full papers and 5 short papers were accepted for presentation at the event and further publication in these post-proceedings.

We would like to thank everyone who helped in organizing the event, including all the members of the Organizing Committee of both ESORICS and DPM 2020. Our gratitude goes to Mark Manulis, the workshop chair of ESORICS 2020, and to the ESORICS 2020 general chair, Steve Schneider. During the event, we had the valued assistance and help from Kent Leeding. Thanks also go to Sergi Delgado, CEO of Talaia Labs, Spain, and Marc Juarez, from the University of Southern California, USA, for accepting our invitation to conduct the invited talks. Last, but by no means least, we thank all the DPM 2020 Program Committee members, 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: Institut Mines-Telecom and Institut Polytechnique de Paris (Télécom SudParis), France, Universitat Autònoma de Barcelona, Spain, UNESCO Chair in Data Privacy, Cybercat, and projects TIN2017-87211-R and SECURITAS RED2018-102321-T from the Spanish Government.

November 2020

Joaquin Garcia-Alfaro
Guillermo Navarro-Arribas

DPM 2020 Organization

PC Chairs

Joaquin Garcia-Alfaro
Guillermo Navarro-Arribas

Intitut Polytechnique de Paris, France
Universitat Autònoma de Barcelona, Spain

Program Committee

Jordi Casas-Roma
Jordi Castellà-Roca
Mauro Conti
Jorge Cuellar
Sabrina De Capitani di
Vimercati

Universitat Oberta de Catalunya, Spain
Universitat Rovira i Virgili, Spain
University of Padua, Italy
University of Passau, Germany
Università degli Studi di Milano, Italy

Jose Maria de Fuentes
Roberto Di Pietro
Josep Domingo-Ferrer
Sara Foresti
Sebastien Gambs
Javier Herranz
Jordi Herrera-Joancomartí
Marc Juarez
Christos Kalloniatis
Florian Kammüller

Universidad Carlos III de Madrid, Spain
Hamad Bin Khalifa University, Qatar
Universitat Rovira i Virgili, Spain
Università degli Studi di Milano, Italy
Université du Québec à Montréal, Canada
Universitat Politècnica de Catalunya, Spain
Universitat Autònoma de Barcelona, Spain
University of Southern California, USA
University of the Aegean, Greece
Middlesex University London, UK, and TU Berlin,
Germany

Sokratis Katsikas
Hiroaki Kikuchi
Evangelos Kranakis
Alptekin Küpçü
Costas Lambrinoudakis
Maryline Laurent
Giovanni Livraga
Brad Malin
Chris Mitchell
Anna Monreale
Jordi Nin
Martín Ochoa
Melek Önen
Gerardo Pelosi
Silvio Ranise
Kai Rannenberg
Ruben Rios

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
University of Pisa, Italy
ESADE, Universitat Ramon Llull, Spain
AppGate Inc., USA
EURECOM, France
Politecnico di Milano, Italy
Fondazione Bruno Kessler, Italy
Goethe University Frankfurt, Germany
University of Malaga, Spain

Yves Roudier	University of Nice Sophia Antipolis, France
Pierangela Samarati	Università degli Studi di Milano, Italy
David Sanchez	University Rovira i Virgili, Spain
Qiang Tang	Luxembourg Institute of Science and Technology, Luxembourg
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
Nicola Zannone	Eindhoven University of Technology, The Netherlands

Steering Committee

Joaquin Garcia-Alfaro	Intitut 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

Tahir Ahmad	Salimeh Dashti
Stefano Berlato	Angeliki Kitsiou
Osman Biçer	Katerina Mavroeidi
Matteo Cardaioli	Luca Pajola
Marco Casagrande	Argyri Pattakou

Foreword from the CBT 2020 Program Chairs

The 4th International Workshop on Cryptocurrencies and Blockchain Technology (CBT 2020) was held in collaboration with the 25th European Symposium on Research in Computer Security (ESORICS 2020) and the 15th International Workshop on Data Privacy Management (DPM 2020). 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 24 submissions, out of which, 8 papers were accepted for presentation as full papers, complemented by 4 short papers, 2 invited talks, and a discussion panel. The review process was conducted virtually, involving a rigorous process conducted by the Technical Program Committee (TPC) chairs, all the members of the TPC, and the help of some external reviewers.

The CBT 2020 program was organized in three sessions grouping the contributions into the following topics: Transactions, Mining, Second Layer, Signature Schemes, Formal Methods, Privacy, SNARKs, and Anonymity. The sessions were chaired by members of the TCP, and authors and attendees engaged in exciting discussions on new frontiers in the field of cryptocurrencies and blockchain technology.

We would like to thank all of the people involved in CBT 2020. We are grateful to the TPC members and the external reviewers for their help in providing detailed and timely reviews of the submissions; to Sergi Delgado, CEO of Talaia Labs, Spain, and Marc Juarez, from the University of Southern California, USA, for accepting our invitation to conduct two keynotes, and for their presence during the event and talks; to Shin'ichiro Matsuo (Georgetown University, USA), Pindar Wong (VeriFi Ltd., Hong Kong), Nat Sakimura (OpenID Foundation), Julien Bringer (Convenor of ISO TC307/WG2), Patrick McCorry (PISA Research), and Florian Kammueßer (Middlesex University London, UK, and TU Berlin, Germany) for accepting our invitation to conduct a discussion panel on "How cryptocurrency and blockchain technology will become a trust foundation for the New Normal while ensuring data privacy management?" We also thank all the members of the Surrey team, especially to Steve Schneider, Mark Manulis, Kent Leeding, and Mohammed Alsadi, for all their help and support. Thanks also go to Springer for their great support throughout the entire process.

Finally, the organization was made possible through the strong help of our supporters: Institut Mines-Télécom and Institut Polytechnique de Paris, SAMOVAR, France, Universitat Autònoma de Barcelona, Spain, Cybercat, BART (Inria, IRT SYSTEMX, Télécom SudParis, and Télécom Paris, France). A special thank you to all of them. Last, but by no means least, we thank all the authors who submitted papers and talks, and all the workshop attendees.

November 2020

Joaquín García-Alfaro
Jordi Herrera-Joancomartí

CBT 2020 Organization

Program Committee Chairs

Joaquin Garcia-Alfaro	Intitut Polytechnique de Paris, France
Jordi Herrera-Joancomart	Universitat Autònoma de Barcelona, Spain

Program Committee

Daniel Augot	Inria Saclay, France
Alex Biryukov	University of Luxembourg, Luxembourg
Rainer Böhme	Universität Innsbruck, Austria
Joseph Bonneau	New York University, USA
Alexander Chepur	IOHK Research, Russia
Mauro Conti	University of Padua, Italy
Vanesa Daza	Universitat Pompeu Fabra, Spain
Sergi Delgado-Segura	Talaia Labs, Spain
Arthur Gervais	Imperial College London, UK
Hannes Hartenstein	Karlsruhe Institute of Technology, Germany
Ghassan Karame	NEC Research, Germany
Eleftherios Kokoris-Kogias	Novi, Switzerland
Shin'ichiro Matsuo	Georgetown University, USA
Andrew Miller	University of Illinois at Urbana-Champaign, USA
Pedro Moreno-Sanchez	IMDEA, Spain
Guillermo Navarro	Universitat Autònoma de Barcelona, Spain
Cristina Pérez-Solà	Universitat Oberta de Catalunya, Spain
Matteo Signorini	Nokia Bell Labs France, France
Khalifa Toumi	IRT SystemX, France

Steering Committee

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

Additional Reviewers

Florian Jacob
Sébastien Andreina
Rahul Saha
Ankit Gangwal
Arantxa Zapico
Oliver Stengele

Federico Franzoni
Daniel Feher
Gulshan Kumar
Alexei Zamyatin
Matthias Grundmann
Abhimanyu Rawat

Contents

DPM Workshop: Fairness, Differential Privacy and Scalability

Fairness-Aware Privacy-Preserving Record Linkage.	3
<i>Dinusha Vatsalan, Joyce Yu, Wilko Henecka, and Brian Thorne</i>	
Differentially Private Profiling of Anonymized Customer Purchase Records	19
<i>Hiroaki Kikuchi</i>	
P-Signature-Based Blocking to Improve the Scalability of Privacy-Preserving Record Linkage	35
<i>Dinusha Vatsalan, Joyce Yu, Brian Thorne, and Wilko Henecka</i>	

DPM Workshop: Utility, Diversity and Leakage Resistance

Utility Promises of <i>Self-Organising Maps</i> in Privacy Preserving Data Mining.	55
<i>Kabiru Mohammed, Aladdin Ayeshe, and Eerke Boiten</i>	
Multi-criteria Optimization Using <i>l</i> -diversity and <i>t</i> -closeness for <i>k</i> -anonymization.	73
<i>Clémence Mauger, Gaël Le Mahec, and Gilles Dequen</i>	
ArchiveSafe: Mass-Leakage-Resistant Storage from Proof-of-Work	89
<i>Moe Sabry, Reza Samavi, and Douglas Stebila</i>	

DPM Workshop: Obfuscation, Contact Tracing and Engineering

Joint Obfuscation for Privacy Protection in Location-Based Social Networks	111
<i>Behnaz Bostanipour and George Theodorakopoulos</i>	
Modeling and Analyzing the Corona-Virus Warning App with the Isabelle Infrastructure Framework	128
<i>Florian Kammüller and Bianca Lutz</i>	
Extracting Speech from Motion-Sensitive Sensors	145
<i>Safaa Azzakhnini and Ralf C. Staudemeyer</i>	

PDP-ReqLite: A Lightweight Approach for the Elicitation of Privacy and Data Protection Requirements	161
<i>Nicolás E. Díaz Ferreyra, Patrick Tessier, Gabriel Pedroza, and Maritta Heisel</i>	
Towards Multiple Pattern Type Privacy Protection in Complex Event Processing Through Event Obfuscation Strategies	178
<i>Saravana Murthy Palanisamy</i>	
GPS-Based Behavioral Authentication Utilizing Distance Coherence	195
<i>Tran Phuong Thao and Rie Shigetomi Yamaguchi</i>	
DPM Workshop: Short Papers	
Short Paper: Integrating the Data Protection Impact Assessment into the Software Development Lifecycle	219
<i>Christopher Irvine, Dharini Balasubramaniam, and Tristan Henderson</i>	
Citizens as Data Donors: Maximizing Participation Through Privacy Assurance and Behavioral Change	229
<i>Mohamad Gharib</i>	
Tracking the Invisible: Privacy-Preserving Contact Tracing to Control the Spread of a Virus	240
<i>Didem Demirag and Erman Ayday</i>	
Privacy Policy Classification with XLNet (Short Paper)	250
<i>Majd Mustapha, Katsiaryna Krasnashchok, Anas Al Bassit, and Sabri Skhiri</i>	
Every Query Counts: Analyzing the Privacy Loss of Exploratory Data Analyses	258
<i>Saskia Nuñez von Voigt, Mira Pauli, Johanna Reichert, and Florian Tschorsch</i>	
CBT Workshop: Transactions, Mining, Second Layer and Inter-bank Payments	
TxChain: Efficient Cryptocurrency Light Clients via Contingent Transaction Aggregation	269
<i>Alexei Zamyatin, Zeta Avarikioti, Daniel Perez, and William J. Knottenbelt</i>	
VRF-Based Mining Simple Non-outsourcable Cryptocurrency Mining	287
<i>Runchao Han, Haoyu Lin, and Jiangshan Yu</i>	

On the Selection of the LN Client Implementation Parameters	305
<i>Luis E. Oleas-Chávez, Cristina Pérez-Solà, and Jordi Herrera-Joacomartí</i>	
Privacy Preserving Netting Protocol for Inter-bank Payments	319
<i>Hisham S. Galal and Amr M. Youssef</i>	
CBT Workshop: Signature Schemes, Formal Methods and Incentivization	
Triptych: Logarithmic-Sized Linkable Ring Signatures with Applications . . .	337
<i>Sarang Noether and Brandon Goodell</i>	
Moderated Redactable Blockchains: A Definitional Framework with an Efficient Construct.	355
<i>Mohammad Sadeq Dousti and Alptekin Küpçü</i>	
Radium: Improving Dynamic PoW Targeting	374
<i>George Bissias</i>	
Proof of No-Work: How to Incentivize Individuals to Stay at Home	390
<i>Michael Bartholic, Jianan Su, Ryosuke Ushida, Yusuke Ikeno, Zhengrong Gu, and Shin'ichiro Matsuo</i>	
CBT Workshop: Short Papers	
Fundamental Properties of the Layer Below a Payment Channel Network . . .	409
<i>Matthias Grundmann and Hannes Hartenstein</i>	
Zerojoin: Combining Zerocoin and CoinJoin	421
<i>Alexander Chepurnoy and Amitabh Saxena</i>	
Who Let the DOGS Out: Anonymous but Auditable Communications Using Group Signature Schemes with Distributed Opening.	437
<i>Marina Dehez-Clementi, Jean-Christophe Deneuville, Jérôme Lacan, Hassan Asghar, and Dali Kaafar</i>	
Tracking Mixed Bitcoins	447
<i>Tin Tironasakul, Manuel Maarek, Andrea Eross, and Mike Just</i>	
Author Index	459