

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>

Shlomi Dolev · Oded Margalit · Benny Pinkas ·
Alexander Schwarzmnn (Eds.)

Cyber Security Cryptography and Machine Learning

5th International Symposium, CSCML 2021
Be'er Sheva, Israel, July 8–9, 2021
Proceedings

Editors

Shlomi Dolev
Ben-Gurion University of the Negev
Be'er Sheva, Israel

Oded Margalit
Ben-Gurion University of the Negev
Be'er Sheva, Israel

Benny Pinkas
Bar-Ilan University
Tel Aviv, Israel

Alexander Schwarzmann
Augusta University
Augusta, GA, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-78085-2

ISBN 978-3-030-78086-9 (eBook)

<https://doi.org/10.1007/978-3-030-78086-9>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021

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

Preface

CSCML, the International Symposium on Cyber Security Cryptography and Machine Learning, is an international forum for researchers, entrepreneurs, and practitioners in the theory, design, analysis, implementation, or application of cyber security, cryptography, and machine learning systems and networks, and, in particular, of conceptually innovative topics in these research areas.

Information technology has become crucial to our everyday lives, an indispensable infrastructure of our society and therefore a target for attacks by malicious parties. Cyber security is one of the most important fields of research these days because of these developments. Two of the (sometimes competing) fields of research, cryptology and machine learning, are the most important building blocks of cyber security.

Topics of interest for CSCML include cyber security design; secure software development methodologies; formal methods, semantics and verification of secure systems; fault tolerance, reliability, and availability of distributed secure systems; game-theoretic approaches to secure computing; automatic recovery self-stabilizing and self-organizing systems; communication, authentication, and identification security; cyber security for mobile systems and the Internet of Things; cyber security of corporations; security and privacy for cloud, Edge and Fog computing; cryptocurrency; blockchain; cryptography; cryptographic implementation analysis and construction; secure multi-party computation; privacy-enhancing technologies and anonymity; post-quantum cryptology and security; machine learning and big data; anomaly detection and malware identification; business intelligence and security; digital forensics, digital rights management; trust management and reputation systems; and information retrieval, risk analysis, and DoS.

The 5th CSCML took place during July 8–9, 2021, in Beer-Sheva, Israel. The keynote speakers were Steve Blank, serial entrepreneur and one of the founding fathers of Silicon Valley; Bruce Schneier, Fellow of the Harvard Kennedy School of Government and internationally renowned security technologist; and Nir Zuk, founder and CTO of Palo Alto Networks. This year the conference was organized in cooperation with the International Association for Cryptologic Research (IACR) and selected papers will appear in a dedicated special issue of the Information and Computation Journal. This volume contains 22 contributions selected by the Program Committee from 48 submissions, and also includes 13 short papers (of at most 8 pages). All submitted papers were read and evaluated by Program Committee members, assisted by external reviewers. We are grateful to the EasyChair system in assisting the reviewing process. The support of Ben-Gurion University of the Negev (BGU), in particular BGU-NHSA, the BGU Lynne and William

Frankel Center for Computer Science, the BGU Cyber Security Research Center, and the Department of Computer Science, and IBM is also gratefully acknowledged.

March 2021

Shlomi Dolev
Oded Margalit
Benny Pinkas
Alexander Schwarzmann

Organization

CSCML, the International Symposium on Cyber Security Cryptography and Machine Learning, is an international forum for researchers, entrepreneurs and practitioners in the theory, design, analysis, implementation, or application of cyber security, cryptology, and machine learning systems and networks, and, in particular, of conceptually innovative topics in the scope.

Founding Steering Committee

Orna Berry	DELLEMC, Israel
Shlomi Dolev (Chair)	Ben-Gurion University, Israel
Yuval Elovici	Ben-Gurion University, Israel
Bezalel Gavish	Southern Methodist University, USA
Ehud Gudes	Ben-Gurion University, Israel
Jonathan Katz	University of Maryland, USA
Rafail Ostrovsky	UCLA, USA
Jeffrey D. Ullman	Stanford University, USA
Kalyan Veeramachaneni	MIT, USA
Yaron Wolfsthal	IBM, Israel
Moti Yung	Columbia University and Google, USA

Organizing Committee

General Chair

Shlomi Dolev	Ben-Gurion University, Israel
--------------	-------------------------------

Program Chairs

Oded Margalit	Ben-Gurion University, Israel
Benny Pinkas	Bar-Ilan University, Israel
Alexander Schwarzmann	Augusta University, USA

Organizing Chair

Amanda Lapidot	Ben-Gurion University, Israel
----------------	-------------------------------

Program Committee

Adi Akavia	University of Haifa, Israel
Don Beaver	FOR.ai, USA
Carlo Blundo	Università degli Studi di Salerno, Italy
Christina Boura	University of Versailles, France
Lucas Davi	University of Duisburg-Essen, Germany
Camil Demetrescu	Sapienza University of Rome, Italy
Itai Dinur	Ben-Gurion University, Israel
Orr Dunkelman	University of Haifa, Israel
Eman El-Sheikh	University of West Florida, USA
Chen Feng	University of British Columbia Okanagan, Canada
Rosario Gennaro	City University of New York, USA
Shay Gueron	University of Haifa and Intel Corporation, Israel
David Hay	The Hebrew University, Israel
Amir Herzberg	University of Connecticut, USA
Çetin Kaya Koç	University of California, Santa Barbara, USA
Vladimir Kolesnikov	Georgia Institute of Technology, USA
Łukasz Krzywiecki	Wrocław University of Science and Technology, Poland
Ana Milanova	Rensselaer Polytechnic Institute, USA
Tal Moran	IDC Herzliya, Israel
David Naccache	ENS, France
Ariel Nof	Technion, Israel
Nisha Panwar	Augusta University, USA
Giuseppe Persiano	Università degli Studi di Salerno, Italy
Leo Reyzin	Boston University, USA
Eyal Ronen	Tel Aviv University, Israel
Tirza Routtenberg	Ben-Gurion University, Israel
Alexander Russell	University of Connecticut, USA
Baruch Schieber	New Jersey Institute of Technology, USA
Sandeep Shukla	IIT Kanpur, India
Moshe Sipser	Ben-Gurion University, Israel
Yannis Stamatiou	University of Patras, Greece
Uri Stemmer	Ben-Gurion University, Israel
Daniel Takabi	Georgia State University, USA
Qiang Tang	New Jersey Institute of Technology, USA
Nikos Triandopoulos	Stevens Institute of Technology, USA
Eran Tromer	Tel Aviv University, Israel
Qianhong Wu	Beihang University, China
Marten van Dijk	CWI, Netherlands
Thijs Veugen	TNO and CWI, Netherlands

External Reviewers

Alexander Binun
Nishanth Chandran
Long Chen
Jins de Jong
Philip Derbeko
Hanwen Feng
Guillermo Francia Iii
Fangyu Gai
Kaiwen Guo
Maanak Gupta
Sheng Hu
Jin Jin
Walter Krawec
Ximing Li
Yin Li

Vikas Maurya
Christian Niesler
Jianyu Niu
Primal Pappachan
Rami Puzis
Tian Qiu
Menachem Sadigurschi
Ramprasad Saptharishi
Shantanu Sharma
Moshe Shechner
Sebastian Surminski
Guoxi Wang
Kun Wang
Masaya Yasuda
Yan Zhu

Sponsors



In cooperation with



Contents

Programmable Bootstrapping Enables Efficient Homomorphic Inference of Deep Neural Networks	1
<i>Ilaria Chillotti, Marc Joye, and Pascal Paillier</i>	
Adversaries Strike Hard: Adversarial Attacks Against Malware Classifiers Using Dynamic API Calls as Features	20
<i>Hariom, Anand Handa, Nitesh Kumar, and Sandeep Kumar Shukla</i>	
Privacy-Preserving Coupling of Vertically-Partitioned Databases and Subsequent Training with Gradient Descent	38
<i>Thijs Veugen, Bart Kamphorst, Natasja van de L'Isle, and Marie Beth van Egmond</i>	
Principal Component Analysis Using CKKS Homomorphic Scheme	52
<i>Samavaya Panda</i>	
DepthStAr: Deep Strange Arguments Detection	71
<i>Michael Berlin, Oded Margalit, and Gera Weiss</i>	
Robust Multivariate Anomaly-Based Intrusion Detection System for Cyber-Physical Systems	86
<i>Aneet Kumar Dutta, Rohit Negi, and Sandeep Kumar Shukla</i>	
Privacy-Preserving Password Strength Meters with FHE	94
<i>Nitesh Emmadi, Imtiyazuddin Shaik, Harshal Tupsamudre, Harika Narumanchi, Rajan Mindigal Alasingara Bhattachar, and Sachin Premsukh Lodha</i>	
Automatic Detection of Water Stress in Corn Using Image Processing and Deep Learning	104
<i>Mor Soffer, Ofer Hadar, and Naftali Lazarovitch</i>	
Tortoise and Hares Consensus: The Meshcash Framework for Incentive-Compatible, Scalable Cryptocurrencies	114
<i>Iddo Bentov, Pavel Hubáček, Tal Moran, and Asaf Nadler</i>	
Game of Drones - Detecting Spying Drones Using Time Domain Analysis	128
<i>Ben Nassi, Raz Ben-Netanel, Adi Shamir, and Yuval Elovici</i>	

Privacy Vulnerability of NeNDS Collaborative Filtering	145
<i>Eyal Nussbaum and Michael Segal</i>	
Lawful Interception in WebRTC Peer-To-Peer Communication	153
<i>Assaf Wagner and Rami Puzis</i>	
Hierarchical Ring Signatures Immune to Randomness Injection Attacks	171
<i>Łukasz Krzywiecki, Mirosław Kutylowski, Rafał Rothenberger, and Bartosz Drzazga</i>	
Theoretical Aspects of a Priori On-Line Assessment of Data Predictability in Applied Tasks	187
<i>Sergey Frenkel</i>	
Randomly Rotate Qubits, Compute and Reverse for Weak Measurements Resilient QKD and Securing Entanglement: (Extended Abstract)	196
<i>Dor Bitan and Shlomi Dolev</i>	
Warped Input Gaussian Processes for Time Series Forecasting	205
<i>Igor Vinokur and David Tolpin</i>	
History Binding Signature: (Extended Abstract)	221
<i>Shlomi Dolev and Matan Liber</i>	
Effective Enumeration of Infinitely Many Programs that Evade Formal Malware Analysis	230
<i>Vasiliki Liagkou, Panagiotis E. Nastou, Paul Spirakis, and Yannis C. Stamatiou</i>	
DNS-Morph: UDP-Based Bootstrapping Protocol for Tor	244
<i>Rami Ailabouni, Orr Dunkelman, and Sara Bitan</i>	
Polynomial Time k -Shortest Multi-criteria Prioritized and All-Criteria-Disjoint Paths: (Extended Abstract)	266
<i>Yefim Dinitz, Shlomi Dolev, and Manish Kumar</i>	
Binding BIKE Errors to a Key Pair	275
<i>Nir Drucker, Shay Gueron, and Dusan Kostic</i>	
Fast and Error-Free Negacyclic Integer Convolution Using Extended Fourier Transform	282
<i>Jakub Klemsa</i>	

Efficient Secure Ridge Regression from Randomized Gaussian Elimination	301
<i>Frank Blom, Niek J. Bouman, Berry Schoenmakers, and Niels de Vreede</i>	
POLYDNN Polynomial Representation of NN for Communication-Less SMPC Inference	317
<i>Philip Derbeko and Shlomi Dolev</i>	
Use of Blockchain for Ensuring Data Integrity in Cloud Databases	325
<i>Yakov Vainshtein and Ehud Gudes</i>	
Invited Talk: The Coming AI Hackers	336
<i>Bruce Schneier</i>	
Turning HATE into LOVE: Compact Homomorphic Ad Hoc Threshold Encryption for Scalable MPC	361
<i>Leonid Reyzin, Adam Smith, and Sophia Yakoubov</i>	
Fully Dynamic Password Protected Secret Sharing: Simplifying PPSS Operation and Maintenance	379
<i>Akif Patel and Moti Yung</i>	
Early Detection of In-Memory Malicious Activity Based on Run-Time Environmental Features	397
<i>Dorel Yaffe and Danny Hendler</i>	
Software Integrity and Validation Using Cryptographic Composability and Computer Vision	405
<i>Donald Beaver</i>	
Efficient Generic Arithmetic for KKW: Practical Linear MPC-in-the-Head NIZK on Commodity Hardware Without Trusted Setup	414
<i>David Heath, Vladimir Kolesnikov, and Jiahui Lu</i>	
Trust and Verify: A Complexity-Based IoT Behavioral Enforcement Method	432
<i>Kyle Haefner and Indrakshi Ray</i>	
Using a Neural Network to Detect Anomalies Given an N-gram Profile	451
<i>Byunggu Yu and Junwhan Kim</i>	
Meta-X: A Technique for Reducing Communication in Geographically Distributed Computations	467
<i>Foto Afrati, Shlomi Dolev, Shantanu Sharma, and Jeffrey D. Ullman</i>	

BLINDLY FOLLOW: SITS CRT and FHE for DCLSMPC of DUFSM (Extended Abstract)	487
<i>Shlomi Dolev and Stav Doolman</i>	
Implementing GDPR in Social Networks Using Trust and Context	497
<i>Nadav Voloch, Ehud Gudes, and Nurit Gal-Oz</i>	
Author Index	505