



Delft University of Technology

Preface

Batina, Lejla; Picek, Stjepan; Mondal, Mainack

Publication date
2022

Document Version
Final published version

Published in
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)

Citation (APA)
Batina, L., Picek, S., & Mondal, M. (2022). Preface. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 13162 LNCS, v.

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

Green Open Access added to TU Delft Institutional Repository

'You share, we take care!' - Taverne project

<https://www.openaccess.nl/en/you-share-we-take-care>

Otherwise as indicated in the copyright section: the publisher is the copyright holder of this work and the author uses the Dutch legislation to make this work public.

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>

Lejla Batina · Stjepan Picek ·
Mainack Mondal (Eds.)

Security, Privacy, and Applied Cryptography Engineering

11th International Conference, SPACE 2021
Kolkata, India, December 10–13, 2021
Proceedings

Editors

Lejla Batina 
Radboud University
Nijmegen, The Netherlands

Stjepan Picek 
Radboud University
Nijmegen, The Netherlands

Mainack Mondal 
Indian Institute of Technology Kharagpur
Kharagpur, India

TU Delft
Delft, The Netherlands

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-95084-2 ISBN 978-3-030-95085-9 (eBook)
<https://doi.org/10.1007/978-3-030-95085-9>

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

Preface

The 11th International Conference on Security, Privacy, and Applied Cryptography Engineering 2021 (SPACE 2021) was held during December 10–13, 2021. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is a challenging field, requiring expertise from diverse domains ranging from mathematics and computer science to circuit design. It was first planned to host SPACE 2021 at IIT Kharagpur, India, but it took place online due to the worldwide COVID-19 crisis.

This year we received 42 submissions from authors in many different countries, mainly from Asia and Europe. The submissions were evaluated based on their significance, novelty, technical quality, and relevance to the SPACE conference. The submissions were reviewed in a double-blind mode by at least three members of the Program Committee, which consisted of 51 members from all over the world. After an extensive review process, 13 papers were accepted for presentation at the conference, leading to an acceptance rate of 30.95%.

The program also included two invited talks and three tutorials on various aspects of applied cryptology, security, and privacy, delivered by world-renowned researchers: Christof Paar, Ahmad-Reza Sadeghi, Nele Mentens, Peter Schwabe, and Blase Ur. We sincerely thank the invited speakers for accepting our invitations in spite of their busy schedules. As in previous editions, SPACE 2021 was organized in cooperation with the International Association for Cryptologic Research (IACR). We are grateful to the general chair, Debdeep Mukhopadhyay, for his willingness to host it physically at IIT Kharagpur and his assistance with turning it into an online event.

There is a long list of volunteers who invested their time and energy to put together the conference. We are grateful to all the members of the Program Committee and their sub-reviewers for all their hard work in the evaluation of the submitted papers. We thank our publisher, Springer, for agreeing to continue to publish the SPACE proceedings as a volume in the Lecture Notes in Computer Science (LNCS) series. We are grateful to the local Organizing Committee, especially to the general chair, Debdeep Mukhopadhyay, who invested a lot of time and effort in order for the conference to run smoothly.

Last but not least, our sincere thanks go to all the authors who submitted papers to SPACE 2021, and to all of you who attended it virtually. At least due to the COVID-19 crisis we were able to have so many of you attending the conference online and registering for free. We sincerely hope to meet some of you in person next year.

December 2021

Lejla Batina
Stjepan Picek
Mainack Mondal

Organization

General Chair

Debdeep Mukhopadhyay Indian Institute of Technology, Kharagpur, India

Program Committee Chairs

Lejla Batina Radboud University, The Netherlands
Stjepan Picek Radboud University and TU Delft, The Netherlands
Mainack Mondal Indian Institute of Technology, Kharagpur, India

Program Committee

Amr Youssef	Concordia University, Canada
Aniket Kate	Purdue University, USA
Anupam Chattopadhyay	Nanyang Technological University, Singapore
Bodhisatwa Mazumdar	Indian Institute of Technology, Indore, India
Bohan Yang	Tsinghua University, China
Chester Rebeiro	Indian Institute of Technology, Madras, India
Chitchanok	University of Adelaide, Australia
Chuengsatiansup	
Claude Carlet	University of Bergen, Norway, and University of Paris 8, France
Daniel Moghimi	University of California, San Diego, USA
Diego Aranha	Aarhus University, Denmark
Dirmanto Jap	Nanyang Technological University, Singapore
Domenic Forte	University of Florida, USA
Eran Toch	Tel Aviv University, Israel
Fan Zhang	Zhejiang University, China
Fatemeh Ganji	Worcester Polytechnic Institute, USA
Guilherme Perin	TU Delft, The Netherlands
Ilia Polian	Stuttgart University, Germany
Ileana Buhan	Radboud University, The Netherlands
Jakub Breier	Silicon Austria Labs, Austria
Jean-Luc Danger	Télécom Paris, France
Johanna Sepulveda	Airbus, Germany
Kazuo Sakiyama	University of Electro-Communications, Japan
Kerstin Lemke-Rust	Bonn-Rhein-Sieg University of Applied Sciences, Germany
Kostas Papagiannopoulos	University of Amsterdam, The Netherlands
Luca Mariot	TU Delft, The Netherlands
Lukasz Chmielewski	Radboud University, The Netherlands

Marc Stoettinger	Hessen3C, Germany
Marc Manzano	Sandbox@Alphabet, Spain
Martin Henze	Fraunhofer FKIE, Germany
Md Masoom Rabbani	KU Leuven, Belgium
Naofumi Homma	Tohoku University, Japan
Oğuzhan Ersoy	TU Delft, The Netherlands
Olga Gadyatskaya	Leiden University, The Netherlands
Pedro Maat C. Massolino	PQShield, Oxford, UK
Peter Schwabe	MPI-SP, Germany, and Radboud University, The Netherlands
Rajat Subhra Chakraborty	Indian Institute of Technology, Kharagpur, India
Ruben Niederhagen	University of Southern Denmark, Denmark
Sandeep Shukla	Indian Institute of Technology, Kanpur, India
Sandip Chakraborty	Indian Institute of Technology, Kharagpur, India
Shahram Rasoolzadeh	Radboud University, The Netherlands
Shivam Bhasin	Nanyang Technological University, Singapore
Sikhar Patranabis	Visa Research, USA
Silvia Mella	STMicroelectronics, Italy
Somitra Sanadhya	Indian Institute of Technology, Jodhpur, India
Soumyajit Dey	Indian Institute of Technology, Kharagpur, India
Sk Subidh Ali	Indian Institute of Technology, Bhilai, India
Vishal Saraswat	Bosch Engineering and Business Solutions, Bengaluru, India

Additional Reviewers

Anirban Chakraborty	Nikhilesh Kumar Singh
Soumyadyuti Ghosh	Sayandeep Saha
Arnab Bag	Vikas Maurya
Ipsita Koley	Reetwik Das
Arpan Jati	Aneet Kumar Dutta
Manaar Alam	

Contents

Symmetric Cryptography

Computing the Distribution of Differentials over the Non-linear Mapping χ	3
<i>Joan Daemen, Alireza Mehrdad, and Silvia Mella</i>	
Light-OCB: Parallel Lightweight Authenticated Cipher with Full Security . . .	22
<i>Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-López, and Mridul Nandi</i>	
MILP Based Differential Attack on Round Reduced WARP.	42
<i>Manoj Kumar and Tarun Yadav</i>	

Post-Quantum Cryptography and Homomorphic Encryption

SHELBRS: Location-Based Recommendation Services Using Switchable Homomorphic Encryption	63
<i>Mishel Jain, Priyanka Singh, and Balasubramanian Raman</i>	
On Threat of Hardware Trojan to Post-Quantum Lattice-Based Schemes: A Key Recovery Attack on SABER and Beyond	81
<i>Prasanna Ravi, Suman Deb, Anubhab Baksi, Anupam Chattopadhyay, Shivam Bhasin, and Avi Mendelson</i>	
Safe-Error Attacks on SIKE and CSIDH	104
<i>Fabio Campos, Juliane Krämer, and Marcel Müller</i>	

Hardware Security and Side-Channel Attacks

Network Data Remanence Side Channel Attack on SPREAD, H-SPREAD and Reverse AODV	129
<i>Pushpraj Naik and Urbi Chatterjee</i>	
Parasite: Mitigating Physical Side-Channel Attacks Against Neural Networks.	148
<i>Hervé Chabanne, Jean-Luc Danger, Linda Guiga, and Ulrich Kühne</i>	
Reinforcement Learning-Based Design of Side-Channel Countermeasures . . .	168
<i>Jorai Rijdsdijk, Lichao Wu, and Guilherme Perin</i>	

Deep Freezing Attacks on Capacitors and Electronic Circuits	188
<i>Jalil Morris, Obi Nnorom Jr., Anisul Abedin, Ferhat Erata, and Jakub Szefer</i>	
AI and Cloud Security	
Encrypted SQL Arithmetic Functions Processing for Secure Cloud Database.	207
<i>Tanusree Parbat and Ayantika Chatterjee</i>	
Robustness Against Adversarial Attacks Using Dimensionality	226
<i>Nandish Chattopadhyay, Subhrojyoti Chatterjee, and Anupam Chattopadhyay</i>	
SoK - Network Intrusion Detection on FPGA.	242
<i>Laurens Le Jeune, Arish Sateesan, Md Masoom Rabbani, Toon Goedemé, Jo Vliegen, and Nele Mentens</i>	
Author Index	263