

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>

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


Security, Privacy, and Applied Cryptography Engineering

10th International Conference, SPACE 2020
Kolkata, India, December 17–21, 2020
Proceedings

Editors

Lejla Batina 
Faculty of Science
Radboud University
Nijmegen, Gelderland, The Netherlands

Stjepan Picek 
Delft University of Technology
Delft, Zuid-Holland, The Netherlands

Mainack Mondal 
Indian Institute of Technology
Kharagpur, India

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-66625-5 ISBN 978-3-030-66626-2 (eBook)
<https://doi.org/10.1007/978-3-030-66626-2>

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

Preface

The 10th International Conference on Security, Privacy and Applied Cryptography Engineering 2020 (SPACE 2020) was held on December 17–20, 2020. 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 the conference at IIT Kharagpur, India, but it took place online due to the worldwide pandemic crisis.

This year we received 48 submissions from 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 52 members from all over the world. After an extensive review process, 13 papers were accepted for presentation at the conference, leading to the acceptance rate of 27%.

The program also included two invited talks and four tutorials on various aspects of applied cryptology, security, and privacy, delivered by world-renowned researchers: Joan Daemen, Patrick Longa, Ahmad-Reza Sadeghi, Peter Schwabe, Ingrid Verbauwhede, and Yuval Yarom. Two of the program chairs also offered a tutorial on side-channel attacks. We sincerely thank the invited speakers for accepting our invitations in spite of their busy schedules. As in previous editions, SPACE 2020 was organized in cooperation with the International Association for Cryptologic Research (IACR). We are grateful to general chairs Indranil Sengupta and Debdeep Mukhopadhyay for their willingness to host the conference physically at IIT Kharagpur and their 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 chairs, Debdeep Mukhopadhyay and Indranil Sengupta, who invested a lot of time and effort in order for the conference to run smoothly. We would like to thank Antriksh Shah and his team from Payatu Technologies for not only partially sponsoring the event, but also being a partner in the organization.

Last, but not least, our sincere thanks go to all the authors who submitted papers to SPACE 2020, and to all of you who attended it virtually. At least due to the COVID-19

virus crisis we were able to have so many of you attending it online and registering for free. We sincerely hope to meet some of you in person next year.

November 2020

Lejla Batina
Mainack Mondal
Stjepan Picek

Organization

General Chairs

Debdeep Mukhopadhyay
Indranil Sengupta

Indian Institute of Technology Kharagpur, India
Indian Institute of Technology Kharagpur, India

Program Committee Chairs

Lejla Batina
Mainack Mondal
Stjepan Picek

Radboud University, The Netherlands
Indian Institute of Technology Kharagpur, India
TU Delft, The Netherlands

Program Committee

Subidh Ali
Lejla Batina
Shivam Bhasin
Sukanta Bhattacharya
Ileana Buhan
Claude Carlet

Indian Institute of Technology Bhilai, India
Radboud University, The Netherlands
Temasek Laboratories @ NTU, Singapore
Indian Institute of Technology Guwahati, India
Radboud University, The Netherlands
The University of Bergen, Norway and Université Paris
8 Vincennes-Saint-Denis, France

Rajat Subhra Chakraborty
Sandip Chakraborty
Rahul Chatterjee
Anupam Chattopadhyay
Lukasz Chmielewski
Chitchanok

Indian Institute of Technology Kharagpur, India
Indian Institute of Technology Kharagpur, India
University of Wisconsin-Madison, USA
Nanyang Technological University, Singapore
Riscure, The Netherlands
University of Adelaide, Australia

Chuengsatiansup
Jean-Luc Danger
Soumyajit Dey
Christian Doerr
Domenic Forte
Fatemeh Ganji
Annelie Heuser
Naofumi Homma
Dirmanto Jap
Salil Kanhere
Jean Peter Kapps
Ramesh Karri
Aniket Kate
Marc Manzano
Luca Mariot
Pedro Maat Massolino

ENST, France
Indian Institute of Technology Kharagpur, India
Hasso Plattner Institute, Germany
University of Florida, USA
Worcester Polytechnic Institute, USA
IRISA, France
Tohoku University, Japan
Nanyang Technological University, Singapore
UNSW Sydney, Australia
George Mason University, USA
New York University, USA
Purdue University, USA
Technology Innovation Institute, Abu Dhabi
TU Delft, The Netherlands
PQShield, UK

Bodhisatwa Mazumdar	Indian Institute of Technology Indore, India
Nele Mentens	KU Leuven, Belgium
Mainack Mondal	Indian Institute of Technology Kharagpur, India
Debdeep Mukhopadhyay	Indian Institute of Technology Kharagpur, India
Sikhar Patranabis	ETH Zurich, Switzerland
Guilherme Perin	TU Delft, The Netherlands
Stjepan Picek	TU Delft, The Netherlands
Ilai Polian	University of Stuttgart, Germany
Chester Rebeiro	Indian Institute of Technology Madras, India
Sujoy Sinha Roy	University of Birmingham, UK
Dipanwita Roychowdhury	Indian Institute of Technology Kharagpur, India
Kazuo Sakiyama	The University of Electro-Communications, Japan
Somitra Sanadhya	Indian Institute of Technology Ropar, India
Vishal Saraswat	Robert Bosch Engineering and Business Solutions, India
Peter Schwabe	Radboud University, The Netherlands
Rijurekha Sen	Indian Institute of Technology Delhi, India
Johanna Sepulveda	Airbus, Germany
Sandeep Shukla	Indian Institute of Technology Kanpur, India
Eran Toch	Tel Aviv University, Israel
Christine van Vredendaal	NXP Semiconductors, The Netherlands
Jason Xue	University of Adelaide, Australia
Bohan Yang	Tsinghua University, China
Yuval Yarom	University of Adelaide, Australia; Data61
Amr Youssef	Concordia University, Canada
Fan Zhang	Zhejiang University, China

Additional Reviewers

Ayantika Chatterjee	Shayan Mohammed
Durba Chatterjee	Rijoy Mukherjee
Nandish Chattopadhyay	Ruchira Naskar
Siddhartha Chowdhury	Hammond Pearce
Soumyadyuti Ghosh	Duy-Phuc Pham
Aritra Hazra	Romain Poussier
Jiaji He	Prasanna Ravi
Matthias J. Kannwischer	Rajat Sadhukhan
Chandan Karfa	Pranesh Santikellur
Samuel Karumba	Deepraj Soni
Mustafa Khairallah	Benjamin Tan
Manas Khatua	Imdad Ullah
Ipsita Koley	Léo Weissbart
Anushree Mahapatra	Yoo-Seung Won
Regio Michelin	Wanli Xue
Debasis Mitra	Wenping Zhu

Contents

Systems Security

tPAKE: Typo-Tolerant Password-Authenticated Key Exchange	3
<i>Thitikorn Pongmorrakot and Rahul Chatterjee</i>	
PAS-TA-U: PASsword-Based Threshold Authentication with Password Update	25
<i>Rachit Rawat and Mahabir Prasad Jhanwar</i>	
Re-markable: Stealing Watermarked Neural Networks Through Synthesis . . .	46
<i>Nandish Chattopadhyay, Chua Sheng Yang Viroy, and Anupam Chattopadhyay</i>	
Robust Adaptive Cloud Intrusion Detection System Using Advanced Deep Reinforcement Learning	66
<i>Kamalakanta Sethi, Rahul Kumar, Dinesh Mohanty, and Padmalochan Bera</i>	
A Forensic Technique to Detect Copy-Move Forgery Based on Image Statistics	86
<i>Ayush Nirwal, Raghav Khandelwal, Smit Patel, and Priyanka Singh</i>	

Cryptography

ExtPFA: Extended Persistent Fault Analysis for Deeper Rounds of Bit Permutation Based Ciphers with a Case Study on GIFT	101
<i>Priyanka Joshi and Bodhisatwa Mazumdar</i>	
On Configurable SCA Countermeasures Against Single Trace Attacks for the NTT: A Performance Evaluation Study over Kyber and Dilithium on the ARM Cortex-M4.	123
<i>Prasanna Ravi, Romain Poussier, Shivam Bhasin, and Anupam Chattopadhyay</i>	
HEDrone: Privacy-Preserving Proof-of-Alibi for Drone Compliance Based on Homomorphic Encryption	147
<i>Ganeshsai Garikipati, Roshani, Anish Mathuria, and Priyanka Singh</i>	
Fiat-Shamir with Aborts: From Identification Schemes to Linkable Ring Signatures	167
<i>Dipayan Das</i>	

An Insecurity Study of Ethereum Smart Contracts.	188
<i>Bishwas C. Gupta, Nitesh Kumar, Anand Handa, and Sandeep K. Shukla</i>	
Cryptographically Secure Multi-tenant Provisioning of FPGAs	208
<i>Arnab Bag, Sikhar Patranabis, Debapriya Basu Roy, and Debdeep Mukhopadhyay</i>	
Experimental Results on Higher-Order Differential Spectra of 6 and 8-bit Invertible S-Boxes.	226
<i>Subhamoy Maitra, Bimal Mandal, Manmatha Roy, and Deng Tang</i>	
Quantum Resource Estimates of Grover’s Key Search on ARIA	238
<i>Amit Kumar Chauhan and Somitra Kumar Sanadhya</i>	
Author Index	259