

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>

Toru Nakanishi · Ryo Nojima (Eds.)

Advances in Information and Computer Security

16th International Workshop on Security, IWSEC 2021
Virtual Event, September 8–10, 2021
Proceedings

Editors

Toru Nakanishi
Hiroshima University
Hiroshima, Japan

Ryo Nojima
National Institute of Information
and Communications Technology
Tokyo, Japan

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-85986-2

ISBN 978-3-030-85987-9 (eBook)

<https://doi.org/10.1007/978-3-030-85987-9>

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

The 16th International Workshop on Security, IWSEC 2021, was held online (originally scheduled to be held in Tokyo, Japan), during September 8–10, 2021. The workshop was co-organized by ISEC (the Technical Committee on Information Security in Engineering Sciences Society of IEICE) and CSEC (the Special Interest Group on Computer Security of IPSJ).

This year, we categorized topics of interests into two tracks, namely, Cryptography Track (Track A) and Cybersecurity and Privacy Track (Track B); each track was formed by separate Program Committee members. We received 37 submissions, 21 in Track A and 16 in Track B. After extensive reviews and shepherding, we accepted 11 regular papers (7 from Track A and 4 from Track B) and 3 short papers (2 from Track A and 1 from Track B). Each submission was anonymously reviewed by four reviewers on average. These proceedings contain revised versions of the accepted papers. Track A consists of the sessions on lattice-based cryptography, multiparty computation, post-quantum cryptography, and symmetric-key cryptography. Track B consists of the sessions on system security, machine learning and security, and game theory and security.

The Best Paper Awards were given to “Solving the Problem of Blockwise Isomorphism of Polynomials with Circulant Matrices” by Yasufumi Hashimoto and to “KPRM: Kernel Page Restriction Mechanism to Prevent Kernel Memory Corruption” by Hiroki Kuzuno and Toshihiro Yamauchi. The Best Student Paper Award was given to “Evolving Homomorphic Secret Sharing for Hierarchical Access Structures” by Kittiphop Phalakarn, Vorapong Suppakitpaisarn, Nuttapong Attrapadung, and Kanta Matsuura.

Under the COVID-19 pandemic circumstances, a number of people contributed to the success of IWSEC 2021. We would like to thank all authors for submitting their papers to the workshop, and we are also deeply grateful to the members of the Program Committee and to the external reviewers for their in-depth reviews and detailed discussions. Last but not least, we would like to thank the general co-chairs, Tetsuya Izu and Yuji Suga, for leading the Organizing Committee, and we would also like to thank the members of the Organizing Committee for ensuring the smooth running of the workshop.

September 2021

Toru Nakanishi
Ryo Nojima

IWSEC 2021

16th International Workshop on Security Organization

Online, September 8–10, 2021

co-organized by

ISEC in ESS of IEICE

(Technical Committee on Information Security in Engineering Sciences Society of the
Institute of Electronics, Information and Communication Engineers)

and

CSEC of IPSJ

(Special Interest Group on Computer Security of Information Processing
Society of Japan)

General Co-chairs

Tetsuya Izu
Yuji Suga

Fujitsu Laboratories Ltd., Japan
Internet Initiative Japan Inc., Japan

Program Co-chairs

Toru Nakanishi
Ryo Nojima

Hiroshima University, Japan
NICT, Japan

Poster Chair

Mitsuaki Akiyama

NTT, Japan

Publication Chair

Chen-Mou Cheng

Kanazawa University, Japan

Local Organizing Committee

Mitsuaki Akiyama	NTT, Japan
Chen-Mou Cheng	Kanazawa University, Japan
Xuping Huang	Advanced Institute of Industrial Technology, Japan
Yasuhiko Ikematsu	Kyushu University, Japan
Satoru Izumi	National Institute of Technology, Sendai College, Japan
Kaisei Kajita	Japan Broadcasting Corporation, Japan
Kazuya Kakizaki	NEC, Japan
Noboru Kunihiro	University of Tsukuba, Japan
Minako Ogawa	Toshiba Corporation, Japan
Toshiya Shimizu	Fujitsu Laboratories Ltd., Japan
Yuta Takata	Deloitte Tohmatsu Cyber LLC, Japan
Atsushi Takayasu	NICT, Japan
Hiroshi Tsunoda	Tohoku Institute of Technology, Japan
Sven Wohlgenuth	SECOM Co., Ltd., Japan
Masaya Yasuda	Rikkyo University, Japan

Program Committee

Track A: Cryptography Track

Chen-Mou Cheng	Kanazawa University, Japan
Sherman S.M. Chow	The Chinese University of Hong Kong, Hong Kong
Geoffroy Couteau	CNRS, IRIF, Université de Paris, France
Bernardo David	IT University of Copenhagen, Denmark
Antonio Faonio	EURECOM, France
Akinori Hosoyamada	NTT, Japan
Yuichi Komano	Toshiba Corporation, Japan
Florian Mendel	Infineon Technologies, Germany
Kazuhiko Minematsu	NEC, Japan
Khoa Nguyen	Nanyang Technological University, Singapore
Koji Nuida	Kyushu University, Japan
Jae Hong Seo	Hanyang University, Republic of Korea
Yannick Seurin	Agence Nationale de la Securite des Systemes d'Information, France
Daniel Slamanig	AIT Austrian Institute of Technology, Austria
Willy Susilo	University of Wollongong, Australia
Katsuyuki Takashima	Waseda University, Japan
Atsushi Takayasu	NICT, Japan
Mehdi Tibouchi	NTT, Japan
Damien Vergnaud	Sorbonne Université/Institut Universitaire de France, France
Yuyu Wang	University of Electronic Science and Technology of China, China
Yohei Watanabe	The University of Electro-Communications, Japan
Bo-Yin Yang	Academia Sinica, Taiwan
Kazuki Yoneyama	Ibaraki University, Japan

Track B: Cybersecurity and Privacy Track

Mitsuaki Akiyama	NTT, Japan
Josep Balasch	KU Leuven, Belgium
Gregory Blanc	Telecom SudParis, France
Herve Debar	Telecom SudParis, France
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Catalonia
Koki Hamada	NTT, Japan
Yuichi Hayashi	Nara Institute of Science and Technology, Japan
Hiroaki Kikuchi	Meiji University, Japan
Frederic Majorczyk	DGA-MI/CentraleSupélec, France
Yuji Suga	Internet Initiative Japan Inc., Japan
Giorgos Vasiliadis	Qatar Computing Research Institute HBKU, Greece
Takeshi Yagi	NTT Security (Japan) KK, Japan
Akira Yamada	KDDI Research, Inc., Japan
Takumi Yamamoto	Mitsubishi Electric Corporation, Japan

External Reviewers

Behzad Abdolmaleki	Yuto Otsuki
Yusuke Aikawa	Sebastian Ramacher
Ming-Shing Chen	Bagus Santoso
Nariyoshi Chida	Martin Schläffer
Heewon Chung	Kazumasa Shinagawa
Valerio Cini	Chuanjie Su
Reo Eriguchi	Xiangyu Su
Daisuke Fujimoto	Erkan Tairi
Jingnan He	Junko Takahashi
Jingwei Hu	Xiuhua Wang
Yasuhiko Ikematsu	Takuya Watanabe
Toshiyuki Isshiki	Huangting Wu
Tezuka Masayuki	Takanori Yasuda
William H.Y. Mui	Quan Yuan

Contents

Lattice-Based Cryptography

A Trace Map Attack Against Special Ring-LWE Samples	3
<i>Yasuhiko Ikematsu, Satoshi Nakamura, and Masaya Yasuda</i>	
Shortest Vectors in Lattices of Bai-Galbraith's Embedding Attack on the LWR Problem	23
<i>Shusaku Uemura, Kazuhide Fukushima, Shinsaku Kiyomoto, Momonari Kudo, and Tsuyoshi Takagi</i>	

System Security

KPRM: Kernel Page Restriction Mechanism to Prevent Kernel Memory Corruption	45
<i>Hiroki Kuzuno and Toshihiro Yamauchi</i>	
(Short Paper) Evidence Collection and Preservation System with Virtual Machine Monitoring	64
<i>Toru Nakamura, Hiroshi Ito, Shinsaku Kiyomoto, and Toshihiro Yamauchi</i>	

Multiparty Computation

Evolving Homomorphic Secret Sharing for Hierarchical Access Structures	77
<i>Kittiphop Phalakarn, Vorapong Suppakitpaisarn, Nuttapong Attrapadung, and Kanta Matsuura</i>	

Machine Learning and Security

Understanding Update of Machine-Learning-Based Malware Detection by Clustering Changes in Feature Attributions	99
<i>Yun Fan, Toshiki Shibahara, Yuichi Ohsita, Daiki Chiba, Mitsuaki Akiyama, and Masayuki Murata</i>	
Proposal of Jawi CAPTCHA Using Digraphia Feature of the Malay Language	119
<i>Hisaaki Yamaba, Ahmad Saiful Aqmal Bin Ahmad Sohaimi, Shotaro Usuzaki, Kentaro Aburada, Masayuki Mukunoki, Mirang Park, and Naonobu Okazaki</i>	

Post-Quantum Cryptography (1)

Solving the Problem of Blockwise Isomorphism of Polynomials
with Circulant Matrices 137
Yasufumi Hashimoto

FFT Program Generation for Ring LWE-Based Cryptography 151
Masahiro Masuda and Yuki Yoshi Kameyama

Symmetric-Key Cryptography

Optimum Attack on 3-Round Feistel-2 Structure 175
Takanori Daiza and Kaoru Kurosawa

Post-Quantum Cryptography (2)

An Intermediate Secret-Guessing Attack on Hash-Based Signatures 195
Roland Booth, Yanhong Xu, Sabyasachi Karati, and Reihaneh Safavi-Naini

(Short Paper) Analysis of a Strong Fault Attack on Static/Ephemeral CSIDH ... 216
Jason T. LeGrow and Aaron Hutchinson

(Short Paper) Simple Matrix Signature Scheme 227
Changze Yin, Yacheng Wang, and Tsuyoshi Takagi

Game Theory and Security

Moving Target Defense for the CloudControl Game 241
Koji Hamasaki and Hitoshi Hohjo

Author Index 253