

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 series at <http://www.springer.com/series/7410>

Nuttapong Attrapadung ·
Takeshi Yagi (Eds.)

Advances in Information and Computer Security

14th International Workshop on Security, IWSEC 2019
Tokyo, Japan, August 28–30, 2019
Proceedings

Editors

Nuttapong Attrapadung 
National Institute of Advanced Industrial
Science and Technology
Tokyo, Japan

Takeshi Yagi
NTT Security (Japan) KK
Tokyo, Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-26833-6 ISBN 978-3-030-26834-3 (eBook)
<https://doi.org/10.1007/978-3-030-26834-3>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2019

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 14th International Workshop on Security, IWSEC 2019, was held at the Multi-Purpose Digital Hall, Ookayama Campus, Tokyo Institute of Technology, Tokyo, Japan, during August 28–30, 2019. 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 is formed by separate Program Committee members. We received 63 submissions, 42 in Track A and 21 in Track B, out of which two papers were withdrawn before the review process. After extensive reviews and shepherding, we accepted 18 regular papers (12 from Track A and six from Track B) and five short papers (three from Track A and two from Track B). Each submission was anonymously reviewed by four reviewers. These proceedings contain revised versions of the accepted papers. Track A consists of the sessions on public-key primitives, symmetric-key primitives, cryptanalysis, and cryptographic protocols. Track B consists of the sessions on malware detection and classification, intrusion detection and prevention, Web and usable security, and forensics.

The Best Paper Awards were given to “An Efficient F4-style Based Algorithm to Solve MQ Problems” by Takuma Ito, Naoyuki Shinohara, and Shigenori Uchiyama, and to “Towards Efficient Detection of Malicious VBA Macros with LSI” by Mamoru Mimura and Taro Ohnami. The Best Student Paper Award was given to “CCA-Secure Leakage-Resilient Identity-Based Key-Encapsulation from Simple (not q -type) Assumptions” by Toi Tomita, Wakaha Ogata, and Kaoru Kurosawa. In addition to the presentations of the accepted papers, the workshop also featured two keynote talks, a poster session, and invited talk sessions from domestic symposiums, namely, SCIS (Symposium on Cryptography and Information Security) and CSS (Computer Security Symposium). We also included a special session organized by AIMaP (Advanced Innovation powered by Mathematics Platform).

A number of people contributed to the success of IWSEC 2019. We would like to thank all authors for submitting their papers to the workshop, and also we are deeply grateful to the members of the Program Committee and to the external reviewers for their in-depth reviews and detailed discussions. We must mention that the selection of the papers was an extremely challenging task.

Last but not least, we would like to thank the General Co-Chairs, Toshihiro Yamauchi and Shiho Moriai, 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.

June 2019

Nuttapong Attrapadung
Takeshi Yagi

IWSEC 2019

14th International Workshop on Security Organization

Tokyo, Japan, August 28–30, 2019

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

Shiho Moriai	National Institute of Information and Communications Technology, Japan
Toshihiro Yamauchi	Okayama University, Japan

Advisory Committee

Hideki Imai	University of Tokyo, Japan
Kwangjo Kim	Korea Advanced Institute of Science and Technology, the Republic of Korea
Christopher Kruegel	University of California, Santa Barbara, USA
Günter Müller	University of Freiburg, Germany
Yuko Murayama	Tsuda University, Japan
Koji Nakao	National Institute of Information and Communications Technology, Japan
Eiji Okamoto	University of Tsukuba, Japan
C. Pandu Rangan	Indian Institute of Technology Madras, India
Kai Rannenberg	Goethe University Frankfurt, Germany
Ryoichi Sasaki	Tokyo Denki University, Japan

Program Co-chairs

Nuttapong Attrapadung	AIST, Japan
Takeshi Yagi	NTT Security (Japan) KK, Japan

Local Organizing Committee

Kazumaro Aoki	Nippon Telegraph and Telephone Corporation, Japan
Keita Emura	National Institute of Information and Communications Technology, Japan
Shota Fujii	Hitachi, Ltd., Japan
Masahiro Fujita	Mitsubishi Electric Corporation, Japan
Yuichi Hayashi	Nara Institute of Science and Technology, Japan
Shoichi Hirose	The University of Fukui, Japan
Makoto Iguchi	Kii Corporation, Japan
Akira Kanaoka	Toho University, Japan
Ryo Kikuchi	Nippon Telegraph and Telephone Corporation, Japan
Yoshihiro Mizoguchi	Institute of Mathematics for Industry, Kyusyu University, Japan
Ken Naganuma	Hitachi, Ltd., Japan
Satsuya Ohata	AIST, Japan
Kazuma Ohara	NEC Corporation, Japan
Yuji Suga	Internet Initiative Japan Inc., Japan
Nobuyuki Sugio	NTT DOCOMO, Inc., Japan
Atsushi Takayasu	The University of Tokyo, Japan
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Yohei Watanabe	National Institute of Information and Communications Technology, Japan
Sven Wohlgemuth	Hitachi, Ltd., Japan
Dai Yamamoto	Fujitsu Limited, Japan
Masaya Yasuda	Institute of Mathematics for Industry, Kyusyu University, Japan

Program Committee

Track A: Cryptography Track

Kazumaro Aoki	NTT, Japan
Nuttapong Attrapadung	AIST, Japan
Olivier Blazy	University of Limoges, France
Bernardo David	Tokyo Institute of Technology, Japan
Itai Dinur	Ben-Gurion University, Israel
Antonio Faonio	IMDEA Software Institute, Spain
Takahiro Matsuda	AIST, Japan
Florian Mendel	Graz University of Technology, Austria
Kazuhiko Minematsu	NEC, Japan
Kirill Morozov	University of North Texas, USA
Fabrice Mouhartem	ENS Lyon, France and Microsoft Research, India
Thomas Peters	Université catholique de Louvain, Belgium
Yusuke Sakai	AIST, Japan
Jae Hong Seo	Hanyang University, Republic of Korea

Yannick Seurin	Agence Nationale de la Sécurité des Systemes d'Information, France
Willy Susilo	University of Wollongong, Australia
Katsuyuki Takashima	Mitsubishi Electric Corporation, Japan
Atsushi Takayasu	The University of Tokyo, Japan
Qiang Tang	New Jersey Institute of Technology, USA
Mehdi Tibouchi	NTT, Japan
Damien Vergnaud	Sorbonne Université, UPMC, CNRS, France
Yuyu Wang	Tokyo Institute of Technology, Japan
Yohei Watanabe	NICT, Japan
Rui Zhang	Chinese Academy of Sciences, China

Track B: Cybersecurity and Privacy Track

Mitsuaki Akiyama	Nippon Telegraph and Telephone Corporation, Japan
Josep Balasch	KU Leuven, Belgium
Gregory Blanc	Telecom SudParis, France
Yue Chen	Palo Alto Networks, USA
Daiki Chiba	Nippon Telegraph and Telephone Corporation, Japan
Herve Debar	Telecom SudParis, France
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Catalonia
Kimmo Halunen	VTT Technical Research Centre of Finland Ltd., Finland
Yuichi Hayashi	Nara Institute of Science and Technology, Japan
Akira Kanaoka	Toho University, Japan
Yuhei Kawakoya	Nippon Telegraph and Telephone Corporation, Japan
Frederic Majorczyk	DGA-MI/CentraleSupélec, France
Yoshihiro Oyama	University of Tsukuba, Japan
Hajime Shimada	Nagoya University, Japan
Junko Takahashi	Nippon Telegraph and Telephone Corporation, Japan
Yuta Takata	PwC Cyber Services LLC, Japan
Giorgos Vasiliadis	Qatar Computing Research Institute HBKU, Greece
Takeshi Yagi	NTT Security (Japan) KK, Japan
Takumi Yamamoto	Mitsubishi Electric Corporation, Japan

Additional Reviewers

Miguel Ambrona	Michalis Diamantaris	Koki Hamada
Carles Anglés-Tafalla	Maria Eichlseder	Keisuke Hara
Sarah Azouvi	Keita Emura	Junichirou Hayata
Michael Bamiloshin	Daniel Escudero	Ehsan Hesamifard
Pascal Bemmman	Scott Fluhrer	Takato Hirano
Alberto Blanco-Justicia	Daisuke Fujimoto	Atsunori Ichikawa
George Christou	Atsushi Fujioka	Akiko Inoue
Pratish Datta	Kaiwen Guo	Toshiyuki Isshiki

Mitsugu Iwamoto
Maxim Jourenko
Saqib A. Kakvi
Shuichi Katsumata
Craig Kenney
Suhri Kim
Michael Klooss
Takuma Koyama
Stefan Kölbl
Wen-Jie Lu
Sergio Martinez
Michael Meyer

Luca Nizzardo
Yasuyuki Nogami
Koji Nuida
Satsuya Ohata
Toshihiro Ohigashi
Javier Parra-Arnau
Arnab Roy
Jacob Schuldt
Vladimir Soukharev
Xiangyu Su
Koutarou Suzuki
Tadanori Teruya

Masayuki Tezuka
Guanyu Tian
Yacheng Wang
Erich Wenger
Friedrich Wiemer
Keita Xagawa
Takashi Yamakawa
Takanori Yasuda
Yusuke Yoshida
Masaya Yoshikawa

Contents

Public-Key Primitives 1

CCA-Secure Leakage-Resilient Identity-Based Key-Encapsulation from Simple (Not q -type) Assumptions	3
<i>Toi Tomita, Wakaha Ogata, and Kaoru Kurosawa</i>	
(Short Paper) A Faster Constant-Time Algorithm of CSIDH Keeping Two Points.	23
<i>Hiroshi Onuki, Yusuke Aikawa, Tsutomu Yamazaki, and Tsuyoshi Takagi</i>	

Cryptanalysis on Public-Key Primitives

An Efficient F_4 -style Based Algorithm to Solve MQ Problems	37
<i>Takuma Ito, Naoyuki Shinohara, and Shigenori Uchiyama</i>	
How to Solve Multiple Short-Exponent Discrete Logarithm Problem	53
<i>Kaoru Kurosawa, Akinaga Ueda, Hayato Matsubishi, and Yusuke Sakagami</i>	

Cryptographic Protocols 1

Secure Multiparty Matrix Multiplication Based on Strassen-Winograd Algorithm.	67
<i>Jean-Guillaume Dumas, Pascal Lafourcade, Julio Lopez Fenner, David Lucas, Jean-Baptiste Orfila, Clément Pernet, and Maxime Puys</i>	
An Anonymous Credential System with Constant-Size Attribute Proofs for CNF Formulas with Negations.	89
<i>Ryo Okishima and Toru Nakanishi</i>	

Symmetric-Key Primitives

More Results on Shortest Linear Programs	109
<i>Subhadeep Banik, Yuki Funabiki, and Takanori Isobe</i>	
Tweakable TWINE: Building a Tweakable Block Cipher on Generalized Feistel Structure	129
<i>Kosei Sakamoto, Kazuhiko Minematsu, Nao Shibata, Maki Shigeri, Hiroyasu Kubo, Yuki Funabiki, Andrey Bogdanov, Sumio Morioka, and Takanori Isobe</i>	

Malware Detection and Classification

Correlating High- and Low-Level Features: Increased Understanding of Malware Classification.	149
<i>Sergii Banin and Geir Olav Dyrkolbotn</i>	
Towards Efficient Detection of Malicious VBA Macros with LSI	168
<i>Mamoru Mimura and Taro Ohminami</i>	

Intrusion Detection and Prevention

IDS Alert Priority Determination Based on Traffic Behavior.	189
<i>Shohei Hiruta, Satoshi Ikeda, Shigeyoshi Shima, and Hiroki Takakura</i>	
(Short Paper) Effectiveness of Entropy-Based Features in High- and Low-Intensity DDoS Attacks Detection.	207
<i>Abigail Koay, Ian Welch, and Winston K. G. Seah</i>	

Web and Usable Security

API Usability of Stateful Signature Schemes	221
<i>Alexander Zeier, Alexander Wiesmaier, and Andreas Heinemann</i>	
(Short Paper) Method for Preventing Suspicious Web Access in Android WebView	241
<i>Masaya Sato, Yuta Imamura, Rintaro Orito, and Toshihiro Yamauchi</i>	

Public-Key Primitives 2

Equivalence Between Non-malleability Against Replayable CCA and Other RCCA-Security Notions	253
<i>Junichiro Hayata, Fuyuki Kitagawa, Yusuke Sakai, Goichiro Hanaoka, and Kanta Matsuura</i>	
Cocks' Identity-Based Encryption in the Standard Model, via Obfuscation Techniques (Short Paper)	273
<i>Xin Wang, Shimin Li, and Rui Xue</i>	

Cryptanalysis on Symmetric-Key Primitives

Finding Ordinary Cube Variables for Keccak-MAC with Greedy Algorithm. . .	287
<i>Fukang Liu, Zhenfu Cao, and Gaoli Wang</i>	
Preimage Attacks on Reduced Troika with Divide-and-Conquer Methods. . .	306
<i>Fukang Liu and Takanori Isobe</i>	

Cryptographic Protocols 2

VSS Made Simpler 329
 Yvo Desmedt and Kirill Morozov

Bidirectional Asynchronous Ratcheted Key Agreement
with Linear Complexity 343
 F. Betül Durak and Serge Vaudenay

A New Approach to Constructing Digital Signature Schemes (Short Paper) . . . 363
 Ahto Buldas, Denis Firsov, Risto Laanoja, Henri Lakk, and Ahto Truu

Forensics

GRYPHON: Drone Forensics in Dataflash and Telemetry Logs 377
 Evangelos Mantas and Constantinos Patsakis

Toward the Analysis of Distributed Code Injection
in Post-mortem Forensics 391
 *Yuto Otsuki, Yuhei Kawakoya, Makoto Iwamura, Jun Miyoshi,
 Jacob Faires, and Terrence Lillard*

Author Index 411