Lecture Notes in Computer Science 11049

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

More information about this series at http://www.springer.com/series/7410

Atsuo Inomata · Kan Yasuda (Eds.)

Advances in Information and Computer Security

13th International Workshop on Security, IWSEC 2018
Sendai, Japan, September 3–5, 2018
Proceedings

Springer

Editors
Atsuo Inomata
Tokyo Denki University
Tokyo
Japan

Kan Yasuda
Nippon Telegraph and Telephone Corporation
Tokyo
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-97915-1 ISBN 978-3-319-97916-8 (eBook)
https://doi.org/10.1007/978-3-319-97916-8

Library of Congress Control Number: 2018950103

LNCS Sublibrary: SL4 – Security and Cryptology

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 13th International Workshop on Security, IWSEC 2018, was held at Sakura Hall of Tohoku University in Sendai, Japan, during September 3–5, 2018. The workshop was co-organized by ISEC (the Technical Committee on Information Security in Engineering Sciences Society of IEICE), CSEC (the Special Interest Group on Computer Security of IPSJ), and Cyberscience Center, Tohoku University.

This year, the workshop received 64 submissions, out of which two papers were withdrawn before the review process, and two other papers were withdrawn during the process. After extensive reviews and shepherding, we eventually accepted 18 regular papers and two short papers. Each submission was anonymously reviewed by four reviewers, and four (out of the 18) regular papers were accepted after revision under shepherding. These proceedings contain revised versions of the accepted papers.

The Best Paper Award was given to "Chosen Message Attack on Multivariate Signature ELSA at Asiacrypt 2017" by Yasufumi Hashimoto, Yasuhiko Ikematsu, and Tsuyoshi Takagi, and the Best Student Paper Award was given to "Estimated Cost for Solving Generalized Learning with Errors Problem via Embedding Techniques" by Weiyao Wang, Yuntao Wang, Atsushi Takayasu, and Tsuyoshi Takagi. In addition to the presentations of the accepted papers, the workshop also featured a poster session, SCIS/CSS invited talks, and two keynote talks. The keynote talks were given by Naofumi Homma and by Vasaka Visoottiviseth.

A number of people contributed to the success of IWSEC 2018. 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. 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, Atsushi Fujioka and Masayuki Terada, 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 2018

Atsuo Inomata
Kan Yasuda

IWSEC 2018
13th International Workshop on Security
Organization

Sendai, Japan, September 3–5, 2018

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)
and
Cyberscience Center, Tohoku University

General Co-chairs

Atsushi Fujioka	Kanagawa University, Japan
Masayuki Terada	NTT DOCOMO, Inc., Japan

Advisory Committee

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

Program Co-chairs

Atsuo Inomata	Tokyo Denki University, Japan
Kan Yasuda	Nippon Telegraph and Telephone Corporation, Japan

Organizing Committee

Hiroaki Anada	University of Nagasaki, Japan
Nuttapong Attrapadung	National Institute of Advanced Industrial Science and Technology, Japan
Keita Emura	National Institute of Information and Communications Technology, Japan
Takuya Hayashi	National Institute of Information and Communications Technology, Japan
Makoto Iguchi	Kii Corporation, Japan
Shuji Isobe	Tohoku University, Japan
Satoru Izumi	Tohoku University, Japan
Ryo Kikuchi	Nippon Telegraph and Telephone Corporation, Japan
Takaaki Mizuki	Tohoku University, Japan
Shiho Moriai	National Institute of Information and Communications Technology, Japan
Ken Naganuma	Hitachi, Ltd., Japan
Yoshitaka Nakamura	Future University Hakodate, Japan
Tetsushi Ohki	Shizuoka University, Japan
Yuji Suga	Internet Initiative Japan Inc., Japan
Nobuyuki Sugio	NTT DOCOMO, Inc., Japan
Keisuke Tanaka	Tokyo Institute of Technology, Japan
Yohei Watanabe	The University of Electro-Communications, Japan
Sven Wohlgemuth	Hitachi, Ltd., Japan
Takeshi Yagi	NTT Security (Japan) KK, Japan
Dai Yamamoto	Fujitsu Limited, Japan
Toshihiro Yamauchi	Okayama University, Japan

Program Committee

Mohamed Abid	University of Gabes, Tunisia
Mitsuaki Akiyama	Nippon Telegraph and Telephone Corporation, Japan
Nuttapong Attrapadung	National Institute of Advanced Industrial Science and Technology, Japan
Josep Balasch	KU Leuven, Belgium
Gregory Blanc	Telecom SudParis, France
Olivier Blazy	Université de Limoges, France
Yue Chen	Palo Alto Networks, USA
Celine Chevalier	Université Pantheon-Assas, France
Sabrina De Capitani di Vimercati	DI - Università degli Studi di Milano, Italy
Herve Debar	Telecom SudParis, France
Itai Dinur	Ben-Gurion University, Israel
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Catalonia
Dawu Gu	Shanghai Jiao Tong University, China
Florian Hahn	SAP, Germany

Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Atsuo Inomata	Tokyo Denki University, Japan
Akira Kanaoka	Toho University, Japan
Yuichi Komano	Toshiba Corporation, Japan
Noboru Kunihiro	The University of Tokyo, Japan
Maryline Laurent	Telecom SudParis, France
Zhou Li	RSA Labs, USA
Atul Luykx	Visa Inc., USA
Frederic Majorczyk	DGA-MI/CentraleSupelec, France
Florian Mendel	Graz University of Technology, Austria
Bart Mennink	Radboud University, The Netherlands
Kirill Morozov	University of North Texas, USA
Ivica Nikolic	Nanyang Technological University, Singapore
Yin Minn Pa Pa	PwC Japan, Japan
Reza Reyhanitabar	KU Leuven, Belgium
Yusuke Sakai	National Institute of Advanced Industrial Science and Technology, Japan
Yu Sasaki	Nippon Telegraph and Telephone Corporation, Japan
Dominique Schroeder	Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany
Yannick Seurin	Agence Nationale de la Securite des Systemes d'Information, France
Willy Susilo	University of Wollongong, Australia
Katsuyuki Takashima	Mitsubishi Electric Corporation, Japan
Mehdi Tibouchi	Nippon Telegraph and Telephone Corporation, Japan
Giorgos Vasiliadis	Qatar Computing Research Institute HBKU, Qatar
Sven Wohlgemuth	Hitachi, Ltd., Japan
Takeshi Yagi	NTT Security (Japan) KK, Japan
Kan Yasuda	Nippon Telegraph and Telephone Corporation, Japan
Rui Zhang	Chinese Academy of Sciences, China

Additional Reviewers

Anglès-Tafalla, Carles
Azaiez, Ikbel
Ben Amor, Arij
Benletaief, Nedra
Blanco-Justicia, Alberto
Cheng, Chen-Mou
de Saint Guilhem, Cyprien
Del Vasto, Luis
Deneuville, Jean-Christophe
Ding, Ning
Dobraunig, Christoph
Dramé-Maigné, Sophie
Eichlseder, Maria
Fech, Katharina
Gaborit, Philippe
Grujic, Milos
Hassan, Fadi
Hiromasa, Ryo
Jebri, Sarra
Kaaniche, Nesrine
Kakvi, Saqib A.
Kim, Jon-Lark

Lai, Russell W. F.
Lequesne, Matthieu
Long, Yu
Malavolta, Giulio
Matsuda, Takahiro
Matsuo, Kazuto
Morita, Hiraku
Ogata, Wakaha
Ricci, Sara
Ronge, Viktoria
Schläffer, Martin
Schuldt, Jacob
Shen, Yaobin
Shu, Jiang
Viguier, Benoît
Wouters, Lennert
Xu, Rui
Yamada, Shota
Yasuda, Takanori
Zhang, Chi

Contents

Cryptanalysis

Chosen Message Attack on Multivariate Signature ELSA at Asiacrypt 2017 . . . 3
Yasufumi Hashimoto, Yasuhiko Ikematsu, and Tsuyoshi Takagi

Key Recovery Attack on McNie Based on Low Rank Parity Check Codes and Its Reparation . . . 19
Terry Shue Chien Lau and Chik How Tan

Inference Attacks on Encrypted Databases Based on Order Preserving Assignment Problem . . . 35
Sota Onozawa, Noboru Kunihiro, Masayuki Yoshino, and Ken Naganuma

Implementation Security

Entropy Reduction for the Correlation-Enhanced Power Analysis Collision Attack . . . 51
Andreas Wiemers and Dominik Klein

Safe Trans Loader: Mitigation and Prevention of Memory Corruption Attacks for Released Binaries . . . 68
Takamichi Saito, Masahiro Yokoyama, Shota Sugawara, and Kuniyasu Suzaki

Public-Key Primitives

Estimated Cost for Solving Generalized Learning with Errors Problem via Embedding Techniques . . . 87
Weiyao Wang, Yuntao Wang, Atsushi Takayasu, and Tsuyoshi Takagi

(Short Paper) How to Solve DLOG Problem with Auxiliary Input . . . 104
Akinaga Ueda, Hayato Tada, and Kaoru Kurosawa

(Short Paper) Parameter Trade-Offs for NFS and ECM . . . 114
Kazumaro Aoki

Security in Practice

Is Java Card Ready for Hash-Based Signatures? . . . 127
Ebo van der Laan, Erik Poll, Joost Rijneveld, Joeri de Ruiter, Peter Schwabe, and Jan Verschuren

Detecting Privacy Information Abuse by Android Apps from API Call Logs . . . 143
Katsutaka Ito, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada

Verification of LINE Encryption Version 1.0 Using ProVerif 158
Cheng Shi and Kazuki Yoneyama

The Anatomy of the HIPAA Privacy Rule: A Risk-Based Approach as a Remedy for Privacy-Preserving Data Sharing 174
Makoto Iguchi, Taro Uematsu, and Tatsuro Fujii

Secret Sharing

Improvements to Almost Optimum Secret Sharing with Cheating Detection . . . 193
Louis Cianciullo and Hossein Ghodosi

XOR-Based Hierarchical Secret Sharing Scheme 206
Koji Shima and Hiroshi Doi

Symmetric-Key Primitives

Integer Linear Programming for Three-Subset Meet-in-the-Middle Attacks: Application to GIFT 227
Yu Sasaki

Symbolic-Like Computation and Conditional Differential Cryptanalysis of QUARK 244
Jingchun Yang, Meicheng Liu, Dongdai Lin, and Wenhao Wang

Lightweight Recursive MDS Matrices with Generalized Feistel Network 262
Qiuping Li, Baofeng Wu, and Zhuojun Liu

Provable Security

How to Prove KDM Security of BHHO 281
Hayato Tada, Akinaga Ueda, and Kaoru Kurosawa

From Identification Using Rejection Sampling to Signatures via the Fiat-Shamir Transform: Application to the BLISS Signature 297
Pauline Bert and Adeline Roux-Langlois

Universal Witness Signatures 313
Chen Qian, Mehdi Tibouchi, and Rémi Géraud

Author Index 331