Lecture Notes in Computer Science 11405

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

Mitsuru Matsui (Ed.)

Topics in Cryptology – CT-RSA 2019

The Cryptographers' Track at the RSA Conference 2019
San Francisco, CA, USA, March 4–8, 2019
Proceedings

Springer

Editor
Mitsuru Matsui
Mitsubishi Electric Corporation
Kamakura, Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-12611-7 ISBN 978-3-030-12612-4 (eBook)
https://doi.org/10.1007/978-3-030-12612-4

Library of Congress Control Number: 2019930584

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 RSA conference has been a major international event for information security experts since its inception in 1991. It is an annual event that attracts several hundreds of vendors and over 40,000 participants from industry, government, and academia. Since 2001, the RSA conference has included the Cryptographer's Track (CT-RSA), which provides a forum for current research in cryptography. CT-RSA has become a major publication venue for cryptographers.

This volume represents the proceedings of the 2019 RSA Conference Cryptographer's Track, which was held in San Francisco, California, during March 4–8, 2019. A total of 75 submissions were received for review, of which 28 papers were selected for presentation and publication. As chair of the Program Committee, I would like to deeply thank all the authors who contributed the results of their innovative research.

My appreciation also goes to all the members of the Program Committee and their designated external reviewers who carefully read and reviewed these submissions. The selection process was a difficult task since each contribution had its own merits. At least three reviewers were assigned to each submission (four if the work included a Program Committee member as an author), and the selection process was carried out with great professionalism and transparency.

The submission process as well as the review process and the editing of the final proceedings were greatly simplified by the software written by Shai Halevi. I would like to thank him for his kind support throughout the entire process. In addition to the contributed talks, the program included a panel discussion moderated by Bart Preneel on "Cryptography and AI."

March 2019 Mitsuru Matsui

CT-RSA 2019

RSA Conference Cryptographer's Track 2019

Moscone Center, San Francisco, California, USA
March 4–8, 2019

Program Chair

Mitsuru Matsui	Mitsubishi Electric Corporation, Japan

Program Committee

Josh Benaloh	Microsoft Research, USA
Alex Biryukov	University of Luxembourg, Luxembourg
Alexandra Boldyreva	Georgia Institute of Technology, USA
Joppe Bos	NXP, Belgium
David Cash	University of Chicago, USA
Jung Hee Cheon	Seoul National University, South Korea
Jean-Sébastien Coron	University of Luxembourg, Luxembourg
Henri Gilbert	ANSSI, France
Helena Handschuh	Rambus Cryptography Research, USA
Tibor Jager	Paderborn University, Germany
Stanislaw Jarecki	University of California at Irvine, USA
Marc Joye	OneSpan, Belgium
Florian Kerschbaum	University of Waterloo, Canada
Xuejia Lai	Shanghai Jiao Tong University, China
Tancrède Lepoint	SRI International, USA
Michael Naehrig	Microsoft Research, USA
Miyako Ohkubo	NICT, Japan
Elisabeth Oswald	University of Bristol, UK
Léo Perrin	Inria, France
David Pointcheval	CNRS and Ecole Normale Supérieure, France
Bart Preneel	KU Leuven and iMinds, Belgium
Reihaneh Safavi-Naini	University of Calgary, Canada
Kazue Sako	NEC, Japan
Peter Scholl	Aarhus University, Denmark
Nigel Smart	KU Leuven, Belgium and University of Bristol, UK
François-Xavier Standaert	Université Catholique de Louvain, Belgium
Takeshi Sugawara	The University of Electro-Communications, Japan
Mehdi Tibouchi	NTT Corporation, Japan
Huaxiong Wang	Nanyang Technological University, Singapore

Additional Reviewers

Masayuki Abe
Mamun Akand
James Bartusek
Carsten Baum
Pascal Bemmann
Ritam Bhaumik
Jan Bobolz
Jie Chen
Hang Cheng
Wonhee Cho
Peter Chvojka
Jan Pieter Denvers
Keita Emura
Prastudy Fauzi
Kai Gellert
Benedikt Gierlichs
Johann Großschädl
Cyprien Delpech de Saint Guilhem
Chun Guo
Mike Hamburg
Kyoohyung Han
Minki Hhan
Viet Tung Hoang
Seungwan Hong
James Howe
Jingwei Hu
Takanori Isobe
Toshiyuki Isshiki
Jeremy Jean
Jinhyuck Jeong
Shaoquan Jiang
Zhang Juanyang
Saqib Kakvi
Sabyasachi Karati
Andrey Kim
Dongwoo Kim
Duhyeong Kim
Jaeyun Kim
Jiseung Kim
Rafael Kurek
Virginie Lallemand
Joohee Lee
Keewoo Lee
Yang Li
Benoît Libert
Fuchun Lin
Tingting Lin
Ximeng Liu
Yunwen Liu
Yiyuan Luo
Fermi Ma
Mark Marson
Marco Martinoli
Alexander May
Rui Meng
Rebekah Mercer
Yusuke Naito
Sanami Nakagawa
Khoa Nguyen
David Niehues
Ventzi Nikov
Ryo Nishimaki
Sabine Oechsner
Kazuma Ohara
Jiaxin Pan
Louiza Papachristodoulou
Romain Poussier
Emmanuel Prouff
Matt Robshaw
Dragos Rotaru
Vladimir Rozic
Yusuke Sakai
Luan Cardoso dos Santos
Tobias Schneider
André Schrottenloher
Peter Schwabe
Jae Hong Seo
Yongha Son
Koutarou Suzuki
Hiroto Tamiya
Hikaru Tsuchida
Mike Tunstall
Aleksei Udovenko
Rei Ueno
Fre Vercauteren
Giuseppe Vitto
Hendrik Waldner
Qingju Wang
Carolyn Whitnall
Keita Xagawa
Hailun Yan
Donggeon Yhee
Kazuki Yoneyama
Liang Feng Zhang

Contents