

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology Madras, Chennai, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

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

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

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

Contents

Structure-Preserving Certificateless Encryption and Its Application	1
<i>Tao Zhang, Huangting Wu, and Sherman S. M. Chow</i>	
Public Key Encryption Resilient to Post-challenge Leakage and Tampering Attacks	23
<i>Suvradip Chakraborty and C. Pandu Rangan</i>	
Downgradable Identity-Based Encryption and Applications	44
<i>Olivier Blazy, Paul Germouty, and Duong Hieu Phan</i>	
Large Universe Subset Predicate Encryption Based on Static Assumption (Without Random Oracle)	62
<i>Sanjit Chatterjee and Sayantan Mukherjee</i>	
An Improved RNS Variant of the BFV Homomorphic Encryption Scheme. . .	83
<i>Shai Halevi, Yuriy Polyakov, and Victor Shoup</i>	
New Techniques for Multi-value Input Homomorphic Evaluation and Applications	106
<i>Sergiu Carpov, Malika Izabachène, and Victor Mollimard</i>	
Efficient Function-Hiding Functional Encryption: From Inner-Products to Orthogonality	127
<i>Manuel Barbosa, Dario Catalano, Azam Soleimanian, and Bogdan Warinschi</i>	
Robust Encryption, Extended	149
<i>Rémi Géraud, David Naccache, and Răzvan Roşie</i>	
Tight Reductions for Diffie-Hellman Variants in the Algebraic Group Model	169
<i>Taiga Mizuide, Atsushi Takayasu, and Tsuyoshi Takagi</i>	
Doubly Half-Injective PRGs for Incompressible White-Box Cryptography . .	189
<i>Estuardo Alpirez Bock, Alessandro Amadori, Joppe W. Bos, Chris Brzuska, and Wil Michiels</i>	
Error Detection in Monotone Span Programs with Application to Communication-Efficient Multi-party Computation	210
<i>Nigel P. Smart and Tim Wood</i>	
Lossy Trapdoor Permutations with Improved Lossiness	230
<i>Benedikt Auerbach, Eike Kiltz, Bertram Poettering, and Stefan Schoenen</i>	

Post-quantum EPID Signatures from Symmetric Primitives.	251
<i>Dan Boneh, Saba Eskandarian, and Ben Fisch</i>	
Assessment of the Key-Reuse Resilience of NewHope.	272
<i>Aurélié Bauer, Henri Gilbert, Guénaél Renault, and Mélissa Rossi</i>	
Universal Forgery and Multiple Forgeries of MergeMAC and Generalized Constructions	293
<i>Tetsu Iwata, Virginie Lallemand, Gregor Leander, and Yu Sasaki</i>	
Linking Stam’s Bounds with Generalized Truncation.	313
<i>Bart Mennink</i>	
Poly-Logarithmic Side Channel Rank Estimation via Exponential Sampling	330
<i>Liron David and Avishai Wool</i>	
Efficient Fully-Leakage Resilient One-More Signature Schemes	350
<i>Antonio Faonio</i>	
MILP-Based Differential Attack on Round-Reduced GIFT	372
<i>Baoyu Zhu, Xiaoyang Dong, and Hongbo Yu</i>	
Quantum Chosen-Ciphertext Attacks Against Feistel Ciphers	391
<i>Gembu Ito, Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki, and Tetsu Iwata</i>	
Automatic Search for a Variant of Division Property Using Three Subsets . . .	412
<i>Kai Hu and Meiqin Wang</i>	
Constructing TI-Friendly Substitution Boxes Using Shift-Invariant Permutations	433
<i>Si Gao, Arnab Roy, and Elisabeth Oswald</i>	
Fast Secure Comparison for Medium-Sized Integers and Its Application in Binarized Neural Networks.	453
<i>Mark Abspoel, Niek J. Bouman, Berry Schoenmakers, and Niels de Vreede</i>	
EPIC: Efficient Private Image Classification (or: Learning from the Masters)	473
<i>Eleftheria Makri, Dragos Rotaru, Nigel P. Smart, and Frederik Vercauteren</i>	
Context Hiding Multi-key Linearly Homomorphic Authenticators	493
<i>Lucas Schabhüser, Denis Butin, and Johannes Buchmann</i>	

Revisiting the Secret Hiding Assumption Used in Verifiable (Outsourced) Computation	514
<i>Liang Zhao</i>	
Delegatable Anonymous Credentials from Mercurial Signatures	535
<i>Elizabeth C. Crites and Anna Lysyanskaya</i>	
Accountable Tracing Signatures from Lattices.	556
<i>San Ling, Khoa Nguyen, Huaxiong Wang, and Yanhong Xu</i>	
Author Index	577