# Lecture Notes in Computer Science 11273

*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*

Gerhard Weikum
*Max Planck Institute for Informatics, Saarbrücken, Germany*

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

Thomas Peyrin · Steven Galbraith (Eds.)

# Advances in Cryptology – ASIACRYPT 2018

24th International Conference on the Theory
and Application of Cryptology and Information Security
Brisbane, QLD, Australia, December 2–6, 2018
Proceedings, Part II

Springer

*Editors*
Thomas Peyrin
Nanyang Technological University
Singapore, Singapore

Steven Galbraith
University of Auckland
Auckland, New Zealand

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-03328-6 ISBN 978-3-030-03329-3 (eBook)
https://doi.org/10.1007/978-3-030-03329-3

Library of Congress Control Number: 2018959424

LNCS Sublibrary: SL4 – Security and Cryptology

© International Association for Cryptologic Research 2018, corrected publication 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

ASIACRYPT 2018, the 24th Annual International Conference on Theory and Application of Cryptology and Information Security, was held in Brisbane, Australia, during December 2–6, 2018.

The conference focused on all technical aspects of cryptology, and was sponsored by the International Association for Cryptologic Research (IACR).

Asiacrypt 2018 received a total of 234 submissions from all over the world. The Program Committee selected 65 papers for publication in the proceedings of this conference. The review process was made by the usual double-blind peer review by the Program Committee, which consisted of 47 leading experts of the field. Each submission was reviewed by at least three reviewers and five reviewers were assigned to submissions co-authored by Program Committee members. This year, the conference operated a two-round review system with rebuttal phase. In the first-round review the Program Committee selected the 145 submissions that were considered of value for proceeding to the second round. In the second-round phase the Program Committee further reviewed the submissions by taking into account their rebuttal letter from the authors. The selection process was assisted by a total of 347 external reviewers. These three-volume proceedings contain the revised versions of the papers that were selected. The revised versions were not reviewed again and the authors are responsible for their contents.

The program of Asiacrypt 2018 featured three excellent invited talks by Mitsuru Matsui, Melissa Chase, and Vanessa Teague. The conference also featured a traditional rump session that contained short presentations on the latest research results of the field. The Program Committee selected the work "Block Cipher Invariants as Eigenvectors of Correlation Matrices" by Tim Beyne for the Best Paper Award of Asiacrypt 2018. Two more papers, "Learning Strikes Again: the Case of the DRS Signature Scheme" by Yang Yu and Léo Ducas, and "Tighter Security Proofs for GPV-IBE in the Quantum Random Oracle Model" by Shuichi Katsumata, Shota Yamada, and Takashi Yamakawa, were solicited to submit the full versions to the *Journal of Cryptology*. The program chairs selected Chris Brzuska and Bart Mennink for the Best PC Member Award.

Many people contributed to the success of Asiacrypt 2018. We would like to thank the authors for submitting their research results to the conference. We are very grateful to all of the PC members as well as the external reviewers for their fruitful comments and discussions on their areas of expertise. We are greatly indebted to Josef Pieprzyk, the general chair, for his efforts and overall organization. We would also like to thank Waleed Alkalabi, Niluka Arasinghe, Mir Ali Rezazadeh Baee, Lynn Batten, Xavier Boyen, Ed Dawson, Ernest Foo, Mukhtar Hassan, Udyani Herath, Qingyi Li, Georg Lippold, Matthew McKague, Basker Palaniswamy, Anisur Rahman, Leonie Simpson, Shriparen Sriskandarajah, Gabrielle Stephens, and Chathurika Don Wickramage, the

local Organizing Committee for their continuous support. We thank Craig Costello, Léo Ducas, and Pierre Karpman for expertly organizing and chairing the rump session.

Finally we thank Shai Halevi for letting us use his nice software for the paper submission and review process. We also thank Alfred Hofmann, Anna Kramer, and their colleagues for handling the editorial process of the proceedings published in Springer's LNCS series.

December 2018

Thomas Peyrin
Steven Galbraith

# ASIACRYPT 2018

**The 24th Annual International Conference on Theory and Application of Cryptology and Information Security**

Sponsored by the International Association for Cryptologic Research (IACR)

December 2–6, 2018, Brisbane, Australia

## General Chair

| | |
|---|---|
| Josef Pieprzyk | CSIRO, Data61, Australia |

## Program Co-chairs

| | |
|---|---|
| Thomas Peyrin | Nanyang Technological University, Singapore |
| Steven Galbraith | University of Auckland, New Zealand |

## Program Committee

| | |
|---|---|
| Martin Albrecht | Royal Holloway University of London, UK |
| Prabhanjan Ananth | MIT, USA |
| Lejla Batina | Radboud University, The Netherlands |
| Sonia Belaïd | CryptoExperts, France |
| Daniel J. Bernstein | University of Illinois at Chicago, USA |
| Chris Brzuska | Aalto University, Finland |
| Bernardo David | Tokyo Institute of Technology, Japan |
| Nico Döttling | Friedrich-Alexander University Erlangen-Nürnberg, Germany |
| Léo Ducas | CWI, The Netherlands |
| Jens Groth | University College London, UK |
| Dawu Gu | Shanghai Jiao Tong University, China |
| Goichiro Hanaoka | AIST, Japan |
| Viet Tung Hoang | Florida State University, USA |
| Takanori Isobe | University of Hyogo, Japan |
| Jérémy Jean | ANSSI, France |
| Stefan Kölbl | Technical University of Denmark, Denmark |
| Ilan Komargodski | Cornell Tech, USA |
| Kaoru Kurosawa | Ibaraki University, Japan |
| Virginie Lallemand | Ruhr-Universität Bochum, Germany |
| Gaëtan Leurent | Inria, France |
| Benoît Libert | CNRS and ENS de Lyon, France |
| Helger Lipmaa | University of Tartu, Estonia |

| | |
|---|---|
| Atul Luykx | Visa Research, USA |
| Stefan Mangard | TU Graz, Austria |
| Bart Mennink | Radboud University, The Netherlands |
| Brice Minaud | Royal Holloway University of London, UK |
| Mridul Nandi | Indian Statistical Institute, India |
| Khoa Nguyen | Nanyang Technological University, Singapore |
| Svetla Nikova | KU Leuven, Belgium |
| Elisabeth Oswald | University of Bristol, UK |
| Arpita Patra | Indian Institute of Science, India |
| Giuseppe Persiano | Università di Salerno, Italy and Google, USA |
| Carla Ràfols | Universitat Pompeu Fabra, Spain |
| Amin Sakzad | Monash University, Australia |
| Jae Hong Seo | Hanyang University, Korea |
| Ling Song | Institute of Information Engineering, Chinese Academy of Sciences, China<br>Nanyang Technological University, Singapore |
| Douglas Stebila | University of Waterloo, Canada |
| Marc Stevens | CWI, The Netherlands |
| Qiang Tang | New Jersey Institute of Technology, USA |
| Mehdi Tibouchi | NTT laboratories, Japan |
| Yosuke Todo | NTT Secure Platform Laboratories, Japan |
| Dominique Unruh | University of Tartu, Estonia |
| Gilles Van Assche | STMicroelectronics, Belgium |
| Frederik Vercauteren | KU Leuven, Belgium |
| Bo-Yin Yang | Academia Sinica, Taiwan |
| Yu Yu | Shanghai Jiao Tong University, China |
| Aaram Yun | UNIST, Korea |

## External Reviewers

Behzad Abdolmaleki
Aysajan Abidin
Shweta Agrawal
Estuardo Alpirez Bock
Joël Alwen
Abdelrahaman Aly
Andris Ambainis
Elena Andreeva
Jan-Pieter d'Anvers
Kazumaro Aoki
Nuttapong Attrapadung
Karim Baghery
Shi Bai
Gustavo Banegas
Subhadeep Banik
Paulo Barreto
Gilles Barthe
Hridam Basu
Aurélie Bauer
Carsten Baum
Christof Beierle
Adi Ben-Zvi
Ela Berners-Lee
David Bernhard
Pauline Bert
Ward Beullens
Rishiraj Bhattacharyya
Jean-Francois Biasse
Nina Bindel
Bruno Blanchet

Olivier Blazy
Xavier Bonnetain
Charlotte Bonte
Carl Bootland
Jonathan Bootle
Cecilia Boschini
Raphael Bost
Christina Boura
Florian Bourse
Dusan Bozilov
Andreas Brasen Kidmose
Jacqueline Brendel
Ignacio Cascudo
Dario Catalano
Andrea Cerulli
Avik Chakraborty
Debrup Chakraborty
Long Chen
Yu Chen
Yu Long Chen
Wonhee Cho
Ashish Choudhury
Chitchanok Chuengsatiansup
Michele Ciampi
Sandro Coretti
Alain Couvreur
Ben Curtis
Dana Dachman-Soled
Joan Daemen
Nilanjan Datta
Pratish Datta
Alex Davidson
Thomas De Cnudde
Luca De Feo
Lauren De Meyer
Gabrielle de Micheli
Fabrizio De Santis
Rafael Del Pino
Cyprien Delpech de Saint Guilhem
Yi Deng
Amit Deo
David Derler
Apoorvaa Deshpande
Lin Ding
Ning Ding
Christoph Dobraunig
Rafael Dowsley
Alexandre Duc
Avijit Dutta
Ratna Dutta
Sébastien Duval
Edward Eaton
Maria Eichlseder
Ali El Kaafarani
Keita Emura
Naomi Ephraim
Muhammed Esgin
Thomas Espitau
Martianus Frederic Ezerman
Leo (Xiong) Fan
Antonio Faonio
Oriol Farràs
Prastudy Fauzi
Serge Fehr
Dario Fiore
Tore Frederiksen
Thomas Fuhr
Eiichiro Fujisaki
Benjamin Fuller
Philippe Gaborit
Clemente Galdi
Nicolas Gama
Chaya Ganesh
Si Gao
Luke Garratt
Romain Gay
Nicholas Genise
Rosario Gennaro
Essam Ghadafi
Anirban Ghatak
Satrajit Ghosh
Junqing Gong
Alonso González
Hannes Gross
Paul Grubbs
Charles Guillemet
Siyao Guo
Qian Guo
Kyoohyung Han
Javier Herranz
Julia Hesse
Harunaga Hiwatari

Thang Hoang
Dennis Hofheinz
Seungwan Hong
Akinori Hosoyamada
Kathrin Hövelmanns
James Howe
Andreas Huelsing
Ilia Iliashenko
Ai Ishida
Masahito Ishizaka
Mitsugu Iwamoto
Tetsu Iwata
Håkon Jacobsen
Christian Janson
Dirmanto Jap
Jinhyuck Jeong
Ashwin Jha
Luke Johnson
Antoine Joux
Pierre Karpman
Shuichi Katsumata
Andrey Kim
Dongwoo Kim
Duhyeong Kim
Jeongsu Kim
Jihye Kim
Jiseung Kim
Myungsun Kim
Elena Kirshanova
Fuyuki Kitagawa
Susumu Kiyoshima
Yashvanth Kondi
Ben Kreuter
Toomas Krips
Veronika Kuchta
Marie-Sarah Lacharite
Junzuo Lai
Esteban Landerreche
Tanja Lange
Joohee Lee
Iraklis Leontiadis
Tancrède Lepoint
Jie Li
Qinyi Li
Shun Li
Wei Li
Xiangyu Li
Fuchun Lin
Donxi Liu
Fukang Liu
Hanlin Liu
Junrong Liu
Shengli Liu
Ya Liu
Zhen Liu
Zhiqiang Liu
Victor Lomne
Yu Long
Xianhui Lu
Yuan Lu
Chen Lv
Shunli Ma
Xuecheng Ma
Rusydi Makarim
Giulio Malavolta
Mary Maller
Alex Malozemoff
Yoshifumi Manabe
Avradip Mandal
Mark Manulis
Marco Martinoli
Daniel Masny
Pedro Maat Costa Massolino
Takahiro Matsuda
Alexander May
Sogol Mazaheri
Patrick McCorry
Florian Mendel
Peihan Miao
Vincent Migliore
Kazuhiko Minematsu
Matthias Minihold
Takaaki Mizuki
Andrew Morgan
Paz Morillo
Fabrice Mouhartem
Pratyay Mukherjee
Alireza Naghipour
Yusuke Naito
Maria Naya-Plasencia
Ryo Nishimaki
Ariel Nof

Wakaha Ogata
Emmanuela Orsini
Rafail Ostrovsky
Carles Padró
Tapas Pandit
Louiza Papachristodoulou
Alain Passelègue
Kenny Paterson
Goutam Paul
Michaël Peeters
Chris Peikert
Massimo Perillo
Léo Perrin
Edoardo Persichetti
Peter Pessl
Thomas Peters
Christophe Petit
Stjepan Picek
Zaira Pindado
Bertram Poettering
Eamonn Postlethwaite
Thomas Prest
Emmanuel Prouff
Elizabeth Quaglia
Adrián Ranea
Shahram Rasoolzadeh
Divya Ravi
Ling Ren
Guénaël Renault
Joost Renes
Joost Rijneveld
Thomas Roche
Paul Rösler
Mélissa Rossi
Dragos Rotaru
Yann Rotella
Arnab Roy
Sujoy Sinha Roy
Sylvain Ruhault
Mohammad Sabt
Mohammad Reza Sadeghi
Yusuke Sakai
Simona Samardzijska
Olivier Sanders
John Schanck
Peter Scholl
André Schrottenloher
Jacob Schuldt
Peter Schwabe
Danping Shi
Kyoji Shibutani
SeongHan Shin
Ferdinand Sibleyras
Janno Siim
Javier Silva
Thierry Simon
Luisa Siniscalchi
Kit Smeets
Yongha Son
Gabriele Spini
Christoph Sprenger
Martijn Stam
Damien Stehle
Ron Steinfeld
Joshua Stock
Ko Stoffelen
Shifeng Sun
Siwei Sun
Moon Sung Lee
Koutarou Suzuki
Alan Szepieniec
Akira Takahashi
Katsuyuki Takashima
Benjamin Tan
Adrian Thillard
Jean-Pierre Tillich
Elmar Tischhauser
Radu Titiu
Junichi Tomida
Ni Trieu
Boaz Tsaban
Thomas Unterluggauer
Christine Van Vredendaal
Prashant Vasudevan
Serge Vaudenay
Philip Vejre
Muthuramakrishnan Venkitasubramaniam
Daniele Venturi
Benoît Viguier
Jorge L. Villar
Srinivas Vivek

Antonia Wachter-Zeh
Alexandre Wallet
Michael Walter
Peng Wang
Ping Wang
Yuyu Wang
Man Wei
Zihao Wei
Friedrich Wiemer
Tim Wood
Joanne Woodage
Thomas Wunderer
Keita Xagawa
Haiyang Xue
Shota Yamada
Takashi Yamakawa
Avishay Yanai
Kang Yang
Qianqian Yang
Kan Yasuda
Kevin Yeo
Scott Yilek
Kazuki Yoneyama
Jingyue Yu
Yang Yu
Xingliang Yuan
Thomas Zacharias
Michal Zajac
Rina Zeitoun
Mark Zhandry
Bin Zhang
Cong Zhang
Fan Zhang
Jiang Zhang
Juanyang Zhang
Ren Zhang
Yingjie Zhang
Raymond K. Zhao
Shuoyao Zhao
Linfeng Zhou
Vincent Zucca

## Local Organizing Committee

### General Chair

| | |
|---|---|
| Josef Pieprzyk | CSIRO, Data61, Australia |

### Advisors

| | |
|---|---|
| Lynn Batten | Deakin University, Australia |
| Ed Dawson | QUT, Australia |

### Members

| | |
|---|---|
| Waleed Alkalabi | QUT, Australia |
| Niluka Arasinghe | QUT, Australia |
| Mir Ali Rezazadeh Baee | QUT, Australia |
| Xavier Boyen | QUT, Australia |
| Ernest Foo | QUT, Australia |
| Mukhtar Hassan | QUT, Australia |
| Udyani Herath | QUT, Australia |
| Qingyi Li | QUT, Australia |
| Georg Lippold | Mastercard, Australia |
| Matthew McKague | QUT, Australia |
| Basker Palaniswamy | QUT, Australia |
| Anisur Rahman | QUT, Australia |

| | |
|---|---|
| Leonie Simpson | QUT, Australia |
| Shriparen Sriskandarajah | QUT, Australia |
| Gabrielle Stephens | QUT, Australia |
| Chathurika Don Wickramage | QUT, Australia |

# Contents – Part II


**Symmetric-Key Cryptanalysis**

Programming the Demirci-Selçuk Meet-in-the-Middle Attack with Constraints . . . . . 3
*Danping Shi, Siwei Sun, Patrick Derbez, Yosuke Todo, Bing Sun, and Lei Hu*

Cryptanalysis of MORUS . . . . . 35
*Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki, and Benoît Viguier*

New MILP Modeling: Improved Conditional Cube Attacks on Keccak-Based Constructions . . . . . 65
*Ling Song, Jian Guo, Danping Shi, and San Ling*

On the Concrete Security of Goldreich's Pseudorandom Generator . . . . . 96
*Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi, and Yann Rotella*

**Public Key and Identity-Based Encryption**

A Framework for Achieving KDM-CCA Secure Public-Key Encryption . . . . 127
*Fuyuki Kitagawa and Keisuke Tanaka*

Understanding and Constructing AKE via Double-Key Key Encapsulation Mechanism . . . . . 158
*Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang, and Jingnan He*

Identity-Based Encryption Tightly Secure Under Chosen-Ciphertext Attacks . . . . . 190
*Dennis Hofheinz, Dingding Jia, and Jiaxin Pan*

Short Digital Signatures and ID-KEMs via Truncation Collision Resistance . . . . . 221
*Tibor Jager and Rafael Kurek*

**Asiacrypt 2018 Award Paper I**

Tighter Security Proofs for GPV-IBE in the Quantum Random Oracle Model . . . . . 253
*Shuichi Katsumata, Shota Yamada, and Takashi Yamakawa*

**Side-Channels**

New Instantiations of the CRYPTO 2017 Masking Schemes . . . . . 285
*Pierre Karpman and Daniel S. Roche*

Statistical Ineffective Fault Attacks on Masked AES with Fault Countermeasures . . . . . 315
*Christoph Dobraunig, Maria Eichlseder, Hannes Gross, Stefan Mangard, Florian Mendel, and Robert Primas*

Tight Private Circuits: Achieving Probing Security with the Least Refreshing . . . . . 343
*Sonia Belaïd, Dahmun Goudarzi, and Matthieu Rivain*

Attacks and Countermeasures for White-box Designs . . . . . 373
*Alex Biryukov and Aleksei Udovenko*

**Signatures**

Signatures with Flexible Public Key: Introducing Equivalence Classes for Public Keys. . . . . 405
*Michael Backes, Lucjan Hanzlik, Kamil Kluczniak, and Jonas Schneider*

Compact Multi-signatures for Smaller Blockchains . . . . . 435
*Dan Boneh, Manu Drijvers, and Gregory Neven*

Multi-key Homomorphic Signatures Unforgeable Under Insider Corruption. . . . . 465
*Russell W. F. Lai, Raymond K. H. Tai, Harry W. H. Wong, and Sherman S. M. Chow*

Attribute-Based Signatures for Unbounded Languages from Standard Assumptions . . . . . 493
*Yusuke Sakai, Shuichi Katsumata, Nuttapong Attrapadung, and Goichiro Hanaoka*

**Asiacrypt 2018 Award Paper II**

Learning Strikes Again: The Case of the DRS Signature Scheme . . . . . 525
*Yang Yu and Léo Ducas*

**Leakage-Resilient Cryptography**

How to Securely Compute with Noisy Leakage in Quasilinear Complexity . . . . . 547
*Dahmun Goudarzi, Antoine Joux, and Matthieu Rivain*

Leakage-Resilient Cryptography from Puncturable Primitives and Obfuscation . . . . . 575
*Yu Chen, Yuyu Wang, and Hong-Sheng Zhou*

**Functional/Inner Product/Predicate Encryption**

Unbounded Inner Product Functional Encryption from Bilinear Maps . . . . . 609
*Junichi Tomida and Katsuyuki Takashima*

Adaptively Simulation-Secure Attribute-Hiding Predicate Encryption . . . . . 640
*Pratish Datta, Tatsuaki Okamoto, and Katsuyuki Takashima*

Improved Inner-Product Encryption with Adaptive Security and Full Attribute-Hiding . . . . . 673
*Jie Chen, Junqing Gong, and Hoeteck Wee*

Decentralized Multi-Client Functional Encryption for Inner Product. . . . . 703
*Jérémy Chotard, Edouard Dufour Sans, Romain Gay, Duong Hieu Phan, and David Pointcheval*

Practical Fully Secure Unrestricted Inner Product Functional Encryption Modulo $p$ . . . . . 733
*Guilhem Castagnos, Fabien Laguillaumie, and Ida Tucker*

Correction to: Cryptanalysis of MORUS . . . . . C1
*Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki, and Benoît Viguier*

**Author Index** . . . . . 765