Lecture Notes in Computer Science 10681

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

Junji Shikata (Ed.)

Information Theoretic Security

10th International Conference, ICITS 2017
Hong Kong, China, November 29 – December 2, 2017
Proceedings

Springer

Editor
Junji Shikata
Yokohama National University
Yokohama
Japan

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-72088-3 ISBN 978-3-319-72089-0 (eBook)
https://doi.org/10.1007/978-3-319-72089-0

Library of Congress Control Number: 2017959633

LNCS Sublibrary: SL4 – Security and Cryptology

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

ICITS 2017, the 10th International Conference on Information Theoretic Security, was held in Hong Kong, China, during November 29 – December 2, 2017. The conference took place on the campus of The Chinese University of Hong Kong. ICITS 2017 was held in cooperation with the International Association for Cryptologic Research (IACR), and supported by IEEE Information Theory Society Hong Kong Chapter. The General Chair of the conference was Kenneth Shum.

ICITS is the successor conference to the 2005 IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security, held on Awaji Island, Japan. It is now an international conference which deals with all aspects of information-theoretic security and brings together researchers from various areas including cryptography, information theory, and quantum computing. Information-theoretic security is the cryptographic security that does not depend on computational assumptions, and it is achieved by utilizing techniques or methods from various fields such as information theory, discrete mathematics, and quantum physics.

ICITS 2017 had two tracks, a conference track and a workshop track, as did the previous ICITS. This two-track format was started with ICITS 2012, and it has the advantage of bringing together researchers from various areas with different publication cultures. The proceedings contain the accepted papers for the conference track. The accepted works for the workshop track were presented at the conference but do not appear in this volume. The list of the contributions in the workshop track is given before the Table of Contents.

The Program Committee received a total of 42 submissions, of which 12 were accepted for the conference track and 7 for the workshop track. All submitted papers were reviewed by at least 3 members of the Program Committee, who sometimes were assisted by external reviewers.

In addition to the 19 contributed presentations, there were 6 invited talks:

- "Randomness Extraction in the Quantum World" by Kai-Min Chung, Academia Sinica, Taiwan
- "Sufficiently Myopic Adversaries Are Blind" by Sidharth Jaggi, The Chinese University of Hong Kong, Hong Kong
- "Quantum Wiretap Channel Coding and Information Spectrum Methods" by Tomohiro Ogawa, The University of Electro-Communications, Japan
- "A Unified Paradigm of Organized Complexity and Semantic Information Theory" by Tatsuaki Okamoto, NTT, Japan
- "Physical Assumptions for Long-Term Secure Communication" by Rei Safavi-Naini, University of Calgary, Canada
- "Secret Sharing Schemes: Some New Approaches and Problems" by Huaxiong Wang, Nanyang Technological University, Singapore

I would like to thank all the people who have contributed to the success of ICITS 2017. First of all, I would like to thank all the authors who submitted their papers to ICITS 2017. I would also like to thank all members of the Program Committee, who completed the reviews in a timely and professional manner. It was a great honor for me to work together with them. Moreover, I would like to thank the Steering Committee of ICITS, in particular Yvo Desmedt and Rei Safavi-Naini, for their kind support from the initial stage of the conference. I am grateful to the Program Chairs of previous conferences for their advice and assistance, in particular Anderson Nascimento, Stefan Wolf, and Anja Lehmann. I would especially like to thank the General Chair, Kenneth Shum, for organizing and managing the wonderful conference ICITS 2017, and the Treasurer, Chee Wei, for financial management, Wei Kang for taking charge of publicity, and Hoover Yin for designing the website of the conference. I would also like to thank the CANS 2017 program co-chairs, Sran Čapkun and Sherman S. M. Chow, and the CANS 2017 General Chair, Kehuan Zhang, for the collaboration, because ICITS and CANS were co-located in the campus of The Chinese University of Hong Kong from November 29 to December 2, 2017. Finally, I would like to thank Alfred Hofmann, Elke Werner, and Anna Kramer and other LNCS staff at Springer for their help in publishing the proceedings. Our sponsor was the Institute of Network Coding, The Chinese University of Hong Kong.

October 2017 Junji Shikata

ICITS 2017

The 10th International Conference on Information Theoretic Security

Hong Kong, China, November 29 – December 2, 2017

In cooperation with the International Association for Cryptologic Research (IACR)
Supported by IEEE Information Theory Society Hong Kong Chapter

General Chair

Kenneth Shum	The Chinese University of Hong Kong, Hong Kong

Program Chair

Junji Shikata	Yokohama National University, Japan

Program Committee

Divesh Aggarwal	National University of Singapore, Singapore
Paulo Barreto	University of Washington, Tacoma, USA
Mario Berta	Imperial College London, UK
Matthieu Bloch	Georgia Institute of Technology, USA
Ignacio Cascudo	Aalborg University, Denmark
Paolo D'Arco	University of Salerno, Italy
Frédéric Dupuis	CNRS, LORIA, Université de Lorraine, France
Benjamin Fuller	University of Connecticut, USA
Peter Gazi	IOHK Research, Hong Kong
Goichiro Hanaoka	AIST, Japan
Masahito Hayashi	Nagoya University, Japan
Mitsugu Iwamoto	The University of Electro-Communications, Japan
Takeshi Koshiba	Waseda University, Japan
Yuan Luo	Shanghai Jiao Tong University, China
Hemanta Maji	Purdue University, USA
Keith Martin	University of London, Royal Holloway, UK
Kirill Morozov	The University of Tokyo, Japan
Anderson Nacimento	University of Washington, USA
Frédérique Oggier	Nanyang Technological University, Singapore
Carles Padró	Universitat Politècnica de Catalunya, Spain
Vinod M. Prabhakaran	Tata Institute of Fundamental Research, India
Rei Safavi-Naini	University of Calgary, Canada
Rafael Schaefer	Technische Universität Berlin, Germany
Vincent Tan	National University of Singapore, Singapore

Stefano Tessaro	University of California, Santa Barbara, USA
Huaxiong Wang	Nanyang Technological University, Singapore
Shun Watanabe	Tokyo University of Agriculture and Technology, Japan

ICITS Steering Committee

Carlo Blundo	University of Salerno, Italy
Yvo Desmedt (Chair)	University College London, UK and University of Texas at Dallas, USA
Yuval Ishai	Technion, Israel
Kaoru Kurosawa	Ibaraki University, Japan
Ueli Maurer	ETH Zurich, Switzerland
C. Pandu Rangan	Indian Institute of Technology, Madras, India
Rei Safavi-Naini	University of Calgary, Canada
Junji Shikata	Yokohama National University, Japan
Stefan Wolf	Università della Svizzera italiana, Switzerland
Moti Yung	Snapchat and Columbia University, USA
Yuliang Zheng	University of Alabama at Birmingham, USA

External Reviewers

Carsten Baum	Fuyuki Kitagawa	David Sutter
Christopher Chubb	Fuchun Lin	Mingyuan Wang
Romar Dela Cruz	Tomoyuki Morimae	Yohei Watanabe
Deepesh Data	Varun Narayanan	Sophia Yakoubov
Rafael Dowsley	Ali Poostindouz	Kenji Yasunaga
Serge Fehr	Manoj Prabhakaran	Lei Yu
Christoph Hirche	Varun Raj	Yun Zhang
Andreas Hülsing	Kaushik Seshadreesan	Lin Zhou
Shaoquan Jiang	Setareh Sharifian	Sufang Zhou
Chethan Kamath	Kazumasa Shinagawa	
Akinori Kawachi	Noah Stephens-Davidowitz	

Sponsor

Institute of Network Coding, The Chinese University of Hong Kong

Workshop Track Presentations

The following papers were accepted to the workshop track of ICITS 2017. They were presented at the conference but do not appear as papers in these proceedings.

1. On Secure Asymmetric Multilevel Diversity Coding Systems
   Congduan Li, Xuan Guang, Chee Wei Tan, and Raymond W. Yeung
2. Secure Wireless Communication under Spatial and Local Gaussian Noise Assumptions
   Masahito Hayashi
3. Secrecy and Robustness for Active Attack in Secure Network Coding and its Application to Network Quantum Key Distribution
   Masahito Hayashi, Masaki Owari, Go Kato, and Ning Cai
4. Information-theoretic Physical Layer Security for Satellite Channels
   Angeles Vazquez-Castro and Masahito Hayashi
5. Compressed Secret Key Agreement
   Chung Chan
6. Computing on Quantum Shared Secrets
   Yingkai Ouyang, Si-Hui Tan, Liming Zhao, and Joseph Fitzsimons
7. Worst-Case Guessing Secrecy Is Meaningful in Secret Sharing Schemes
   Mitsugu Iwamoto

Contents

Linear-Time Non-Malleable Codes in the Bit-Wise Independent Tampering Model 1
Ronald Cramer, Ivan Damgård, Nico Döttling, Irene Giacomelli, and Chaoping Xing

Disproving the Conjectures from "On the Complexity of Scrypt and Proofs of Space in the Parallel Random Oracle Model" 26
Daniel Malinowski and Karol Żebrowski

Broadcast Encryption with Guessing Secrecy 39
Yohei Watanabe

Contrast Optimal XOR Based Visual Cryptographic Schemes 58
Sabyasachi Dutta and Avishek Adhikari

Verifiably Multiplicative Secret Sharing 73
Maki Yoshida and Satoshi Obana

Round and Communication Efficient Unconditionally-Secure MPC with $t < n/3$ in Partially Synchronous Network 83
Ashish Choudhury, Arpita Patra, and Divya Ravi

Catching MPC Cheaters: Identification and Openability 110
Robert Cunningham, Benjamin Fuller, and Sophia Yakoubov

Secure Grouping Protocol Using a Deck of Cards 135
Yuji Hashimoto, Kazumasa Shinagawa, Koji Nuida, Masaki Inamura, and Goichiro Hanaoka

Four Cards Are Sufficient for a Card-Based Three-Input Voting Protocol Utilizing Private Permutations 153
Takeshi Nakai, Satoshi Shirouchi, Mitsugu Iwamoto, and Kazuo Ohta

Single-Shot Secure Quantum Network Coding for General Multiple Unicast Network with Free Public Communication 166
Go Kato, Masaki Owari, and Masahito Hayashi

Secure Network Coding for Multiple Unicast: On the Case of Single Source 188
Gaurav Kumar Agarwal, Martina Cardone, and Christina Fragouli

Rényi Resolvability and Its Applications to the Wiretap Channel 208
Lei Yu and Vincent Y. F. Tan

Author Index 235