Lecture Notes in Computer Science 13059

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

Qiong Huang · Yu Yu (Eds.)

Provable and Practical Security

15th International Conference, ProvSec 2021 Guangzhou, China, November 5–8, 2021 Proceedings

Springer

Editors

Qiong Huang
South China Agricultural University
Guangzhou, China

Yu Yu
Shanghai Jiao Tong University
Shanghai, China

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-90401-2 ISBN 978-3-030-90402-9 (eBook)
https://doi.org/10.1007/978-3-030-90402-9

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

This volume contains the papers presented at ProvSec 2021 - the 15th International Conference on Provable and Practical Security, held during November 5–8, 2021. Due to the global COVID-19 pandemic, this year we organized ProvSec 2021 as a hybrid conference. Attendees from low-risk areas of mainland China were invited to join the conference offline at Guangzhou, while other attendees were invited to join the conference online. The conference was hosted by the College of Mathematics and Informatics, South China Agricultural University, China.

The first ProvSec conference was held in 2007. Until 2018, ProvSec conferences focused on “Provable Security”. Since 2019, “Practical Security” has been added into the theme of the conference to enrich the scope of the conference and to bring together security researchers and practitioners.

This year we received 67 submissions, which were reviewed in a double-blind manner. Each submission was carefully evaluated by three to five reviewers, and then discussed among the Program Committee. Finally, 21 papers were accepted for presentation at the conference. Based on the reviews and votes by Program Committee members, the following paper was given the Best Paper Award:

“Public Key Based Searchable Encryption with Fine-Grained Sender Permission Control”, by Zhongming Wang, Biwen Chen, Tao Xiang, Lu Zhou, Hongyang Yan, and Jin Li.

ProvSec 2021 would not have been possible without the contributions of the many volunteers who freely gave their time and expertise. We would like to thank all the 51 Program Committee members from all over the world and the external reviewers for their substantial work in evaluating the papers. We thank the local organizers for their tremendous efforts in successfully organizing this event. Last but not least, we would like to express our gratitude to all invited speakers and all authors who submitted papers to ProvSec 2021.

November 2021

Qiong Huang
Yu Yu

Organization

General Co-chairs

Rongliang Qiu	South China Agricultural University, China
Fangguo Zhang	Sun Yat-sen University, China

Program Co-chairs

Qiong Huang	South China Agricultural University, China
Yu Yu	Shanghai Jiao Tong University, China

Program Committee

Man Ho Au	University of Hong Kong, China
Shi Bai	Florida Atlantic University, USA
Rishiraj Bhattacharyya	NISER, India
Jie Chen	East China Normal University, China
Cheng-Kang Chu	Huawei, Singapore
Chitchanok	University of Adelaide, Australia
Chuengsatiansup Yi Deng	Institute of Information Engineering, Chinese Academy of Sciences, China
Keita Emura	NICT, Japan
Xiong Fan	University of Maryland, USA
Fei Gao	Beijing University of Posts and Telecommunications, China
Junqing Gong	East China Normal University, China
Swee-Huay Heng	Multimedia University, Malaysia
Xinyi Huang	Fujian Normal University, China
Tetsu Iwata	Nagoya University, Japan
David Jao	University of Waterloo, Canada
Sabyasachi Karati	Indian Statistical Institute, Kolkata, India
Shuichi Katsumata	AIST, Japan
Junzuo Lai	Jinan University, China
Jooyoung Lee	KAIST, South Korea
Hyung Tae Lee	Chung-Ang University, South Korea
Yang Li	University of Electro-Communications, Japan
Kaitai Liang	TU Delft, The Netherlands
Changlu Lin	Fujian Normal University, China
Dongxi Liu	CSIRO, Australia
Shengli Liu	Shanghai Jiao Tong University, China
Zhen Liu	Shanghai Jiao Tong University, China

Kirill Morozov	University of North Texas, USA
Khoa Nguyen	Nanyang Technological University, Singapore
Federico Pintore	University of Oxford, UK
Baodong Qin	Xi'an University of Posts and Telecommunications, China
Somindu C. Ramanna	IIT Kharagpur, India
Amin Sakzad	Monash University, Australia
Olivier Sanders	Orange Labs, France
Daniel Slamanig	Austrian Institute of Technology, Austria
Shi-Feng Sun	Monash University, Australia
Willy Susilo	University of Wollongong, Australia
Atsushi Takayasu	NICT, Japan
Viet Cuong Trinh	Hong Duc University, Vietnam
Lei Wang	Shanghai Jiao Tong University, China
Keita Xagawa	NTT, Japan
Yanhong Xu	University of Calgary, Canada
Haiyang Xue	Institute of Information Engineering, Chinese Academy of Sciences, China
Guomin Yang	University of Wollongong, Australia
Rupeng Yang	Hong Kong Polytechnic University, China
Yong Yu	Shaanxi Normal University, China
Yu Yu	Shanghai Jiao Tong University, China
Fangguo Zhang	Sun Yat-sen University, China
Lei Zhang	East China Normal University, China
Liangfeng Zhang	Shanghai Tech University, China
Cong Zuo	Monash University, Australia

Publicity Chair

Hongbo Li	South China Agricultural University, China

Organizing Committee Co-chairs

Sha Ma	South China Agricultural University, China
Ximing Li	South China Agricultural University, China
Cai Zhang	South China Agricultural University, China
Meiyan Xiao	South China Agricultural University, China

External Reviewers

Maxime Buser
Haixia Chen
Valerio Cini
Dung Hoang Duong
Scott Fluhrer
Qingqing Gan
Floyd Johnson
Shangqi Lai
Jiangtao Li
Jianwei Li
Xiaohong Liu
Ji Luo
Tran Ngo
Jianting Ning
Edoardo Persichetti
Christoph Striecks
Erkan Tairi
Shuo Wang
S. J. Yang
Wei-Chuen Yau
Zuoxia Yu
Fei Zhu

Contents

Searchable Encryption

Public Key Based Searchable Encryption with Fine-Grained Sender Permission Control 3
Zhongming Wang, Biwen Chen, Tao Xiang, Lu Zhou, Hongyang Yan, and Jin Li

Improved Security Model for Public-Key Authenticated Encryption with Keyword Search 19
Baodong Qin, Hui Cui, Xiaokun Zheng, and Dong Zheng

Public Key Encryption with Fuzzy Matching 39
Yuanhao Wang, Qiong Huang, Hongbo Li, Meiyan Xiao, Jianye Huang, and Guomin Yang

Partitioned Searchable Encryption 63
Jim Barthel, Marc Beunardeau, Răzvan Roşie, and Rajeev Anand Sahu

Key Exchange and Zero Knowledge Proof

Key Exposure Resistant Group Key Agreement Protocol 83
Tianqi Zhou, Jian Shen, Sai Ji, Yongjun Ren, and Mingwu Zhang

NIKE from Affine Determinant Programs 98
Jim Barthel and Răzvan Roşie

OrBit: OR-Proof Identity-Based Identification with Tight Security for (as Low As) 1-Bit Loss 116
Jason Chia, Ji-Jian Chin, and Sook-Chin Yip

Card-Based Zero-Knowledge Proof Protocols for Graph Problems and Their Computational Model 136
Daiki Miyahara, Hiromichi Haneda, and Takaaki Mizuki

Post Quantum Cryptography

Recovery Attack on Bob's Reused Randomness in CRYSTALS-KYBER and SABER 155
Satoshi Okada and Yuntao Wang

A Lattice Reduction Algorithm Based on Sublattice BKZ 174
Jinzheng Cao, Yanbin Pan, and Qingfeng Cheng

On the (M)iNTRU Assumption in the Integer Case 190
Jim Barthel, Volker Müller, and Răzvan Roşie

Functional Encryption

Verifiable Functional Encryption Using Intel SGX 215
Tatsuya Suzuki, Keita Emura, Toshihiro Ohigashi, and Kazumasa Omote

Fully Secure Unbounded Zero Inner Product Encryption with Short Ciphertexts and Keys 241
Subhranil Dutta, Tapas Pal, and Ratna Dutta

Inner-Product Functional Encryption from Random Linear Codes: Trial and Challenges 259
Zhuoran Zhang, Zheng Zhang, and Fangguo Zhang

Digital Signature

A CCA-Full-Anonymous Group Signature with Verifiable Controllable Linkability in the Standard Model 279
Ru Xiang, Sha Ma, Qiong Huang, and Ximing Li

Cryptanalysis of LRainbow: The Lifted Rainbow Signature Scheme 296
Vikas Srivastava and Sumit Kumar Debnath

Identification Scheme and Forward-Secure Signature in Identity-Based Setting from Isogenies 309
Surbhi Shaw and Ratna Dutta

Linearly Homomorphic Signatures with Designated Combiner 327
Chengjun Lin, Rui Xue, and Xinyi Huang

Efficient Attribute-Based Signature for Monotone Predicates 346
Jixin Zhang, Jiageng Chen, and Weizhi Meng

Practical Security Protocols

Spatial Steganalysis Based on Gradient-Based Neural Architecture Search 365
Xiaoqing Deng, Weiqi Luo, and Yanmei Fang

Turn-Based Communication Channels 376
Carlo Brunetta, Mario Larangeira, Bei Liang, Aikaterini Mitrokotsa, and Keisuke Tanaka

Author Index 393