Journal of Universal Computer Science, vol. 25, no. 3 (2019), 154-157
submitted: 16/3/19, accepted: 20/3/19, appeared: 28/3/19 © J.UCS

Advances of Provable Security Techniques

J.UCS Special Issue

Yong Yu
(School of Computer Science, Shaanxi Normal University, Xi'an, China
yuyong@snnu.edu.cn)

Yi Mu
(Fujian Provincial Key Laboratory of Network Security and Cryptology
Fujian Normal University, Fuzhou, China
yimu@fjnu.edu.cn)

1 Introduction and Motivation

Provable security techniques are regarded as being of utmost importance in modern cryptography as security proofs give useful confidence in an algorithm's security. Cryptographic primitives or protocols without a rigorous proof cannot be regarded as secure in practice. In fact, there is a number of schemes that were originally thought as secure but eventually broken, which clearly indicates the need of formal security proofs. With provable security, we are confident in using cryptographic schemes and protocols in various real-world applications. Security proofs are actually a kind of reduction proofs which show that within some defined mathematical world, if an adversary is able to break the algorithm then the adversary can solve a well-known intractable problem. In a security proof, we are reducing the problem of attacking the algorithm to solving a hard problem and may conclude that breaking the algorithm is at least an equally hard problem. New ideas for security reductions in the provable security area appear every day. The objective of this special issue is to promote research in provable security.

We solicited papers through two ways: conference and open call-for-papers. The conference is the 11th International Conference on Provable Security (ProvSec 2017). We also publicized an open call-for-papers at J.UCS website as well as in major academic announcement mailing lists/websites.

2 Contributions

Specifically, 24 submissions were received for this special issue. Each paper was reviewed by at least three international experts, and in most cases a second reviewing found for minor or major revisions was performed. Finally, eight quality research papers were selected for this special issue. The articles presented in this special issue deal with a variety of important topics within provable security scope. We offer a brief description of each paper below.

2.1 Natural sd-RCCA Secure Public-key Encryptions from Hybrid Paradigms

In this paper, Yuan Chen, Qingkuan Dong, Yannan Li, Qiqi Lai and Zhedong Wang formalize the related notions of natural public-key encryption, and also other variants of KEM plus DEM hybrid paradigm since MACs are commonly used in them. Then they show natural examples of desired probabilistic MACs under the standard DDH assumption, and find appropriate KEMs to match the message space for those MACs and then obtain natural instances of sd-RCCA secure hybrid PKEs.

2.2 Provably Secure Ciphertext-Policy Attribute-Based Encryption from Identity-Based Encryption

In this paper, Yi-Fan Tseng, Chun-I Fan and Chih-Wen Lin show a relation between CP-ABE and identity-based encryption (IBE), and present a bi-directional conversion between an access structure and identities. By the proposed conversion, the CP-ABE scheme constructed from an IBE scheme will inherit the features, such as constant-size ciphertexts and anonymity, from the IBE scheme, and vice versa. It turns out that the proposed conversion also gives the first CP-ABE achieving access structures with wildcard and constant-size ciphertexts/private keys. Finally, authors prove the CCA security for confidentiality and anonymity.

2.3 Ontology and Weighted D-S Evidence Theory-based Vulnerability Data Fusion Method

In this paper, Xiaoling Tao, Liyan Liu, Feng Zhao, Yan Huang, Yi Liang and Saide Zhu propose an ontology and weighted D-S evidence theory-based vulnerability data fusion method. In this method, authors utilize ontology to describe the network vulnerability semantically and construct the network vulnerability ontology hierarchically. Then authors use weighted D-S evidence theory to perform the operation of probability distribution and fusion processing. Authors also simulate the proposed method on MapReduce parallel computing platform.

2.4 Towards Multi-user Searchable Encryption Supporting Boolean Query and Fast Decryption

In this paper, Yunling Wang, Jianfeng Wang, Shi-Feng Sun, Joseph K. Liu, Willy Susilo, Joonsang Baek, Ilsun You and Xiaofeng Chen present a novel SMSE scheme based on server-side match technique, where the cloud can filter the documents that cannot be decrypted by the user and only return the matched ones. In addition, the decryption is also efficient, independent with the access policy structure. Security and efficiency evaluation show that the proposed scheme can achieve the desired security goals, while dramatically reducing the communication and computation overhead.

2.5 CCA-Secure Deterministic Identity-Based Encryption Scheme

In this paper, Meijuan Huang, Bo Yang, Yi Zhao, Kaitai Liang, Liang Xue and Xiaoyi Yang introduce the notion of identity-based all-but-one trapdoor functions (IB-ABO-TDF), which is an extension of all-but-one lossy trapdoor function in the public-key

setting. Authors give an instantiation of IB-ABO-TDF under decisional linear assumption. Based on an identity-based lossy trapdoor function and the IB-ABO-TDF, authors present a generic construction of CCA-secure DIBE scheme.

2.6 Combination Model of Heterogeneous Data for Security Measurement

In this paper, considering implication relationship of metrics, Xiuze Dong, Yunchuan Guo, Fenghua Li, Liju Dong and Arshad Khan propose a combination model and combination policy for security measurement. Several examples demonstrate the effectiveness of our model.

2.7 An Identity-Based Signcryption on Lattice without Trapdoor

In this paper, Xianmin Wang, Yu Zhang, Brij Bhooshan Gupta, Hongfei Zhu and Dingxi Liu propose an identity-based signcryption on lattice, which does not need to rely on a trapdoor. Meanwhile, the proposed scheme achieves IND-CCA2 and sUF-CMA security, and it is also secure against the current quantum algorithm attacks based on LWE problem for lattice. Furthermore, authors demonstrate that the newly proposed scheme has much shorter secret key size, and higher speeds in signcryption and unsigncryption stages, compared with some exiting identity-based signcryption schemes.

2.8 A New Identification Scheme based on Syndrome Decoding Problem with Provable Security against Quantum Adversaries

In this paper, Bagus Santoso and Chunhua Su propose a novel four-pass code-based identification scheme. By using quantum random oracle model, authors provide a security proof for the proposed scheme against quantum adversaries which aim to impersonate the prover under concurrent active attacks, based on the hardness assumption of syndrome decoding (SD) problem. The security proof only requires a non-programmable quantum random oracle, in contrast to existing security proofs of digital signatures generated from ID scheme via Fiat-Shamir transform which require programmable quantum random oracles.

3 Reviewers

We would like to take this opportunity to thank the reviewers involved in this special issue for their valuable comments and suggestions. Most of them are program members of ProvSec 2017.

Janaka Alawatugoda, University of Peradeniya, Sri Lanka
Elena Andreeva, KU Leuven, Belgium
Man Ho Au, Hong Kong Polytechnic University, Hong Kong
Colin Boyd, Norwegian University of Science and Technology, Norway
Aniello Castiglione, University of Salerno, Italy
Liqun Chen, University of Surrey, UK
Rongmao Chen, National University of Defense Technology, China

Yong Yu
Yi Mu
China, March 2019