The Eleventh International Conference on Provable Security (ProvSec2017)
October 23 - 25, 2017, Xi'an, China

----------Call for Papers----------

General Information:

Provable security is an important research area in modern cryptography. Cryptographic primitives or protocols without a rigorous proof cannot be regarded as secure in practice. In fact, there are many schemes that were originally thought as secure but eventually broken, which clearly indicates the need of formal security assurance. With provable security, we are confident in using cryptographic schemes and protocols in various real-world applications. Meanwhile, schemes with provable security sometimes give only theoretical feasibility rather than a practical construction, and correctness of the proofs may be difficult to verify. ProvSec conference thus provides a platform for researchers, scholars and practitioners to exchange new ideas for solving these problems in the provable security area.

Conference Topics:

All aspects of provable security for cryptographic primitives or protocols, include but are not limited to the following areas:

- Asymmetric provably secure cryptography
- Cryptographic primitives
- Lattice-based security reductions
- Leakage-resilient cryptography
- Pairing-based provably secure cryptography
- Privacy and anonymity technologies
- Provable secure hash functions
- Provable security of key management
- Secure cryptographic protocols and applications
- Security notions, approaches, and paradigms
- Steganography and steganalysis
- Symmetric provably secure cryptography

Publication and Awards:

The conference proceedings will be published by Springer-Verlag in the Lecture Notes in Computer Science series (see www.springer.com/lncs). The best paper(s) and best student

paper(s) will be selected and awarded a prize.

Special Issues:
We are discussing with some journals for special issues of selected papers published in ProvSec 2017. More details will be announced later.

Important Dates:
Paper submission deadline: ~~June 3, 2017~~ ; June 17, 2017 (UTC 24:00)
Notification of acceptance: August 3, 2017
Camera ready deadline: August 14, 2017
Conference date: October 23 - 25, 2017

Instructions for authors:
Submitted papers must be original, unpublished, and not submitted to another conference or journal for consideration for publication. Papers must be written in English; they should be at most 15 pages (excluding bibliography and appendices).

At least one author of each accepted paper is required to register for the conference and present the paper.

All submissions will be blind-reviewed. Papers must be anonymous, with no author names, affiliations, acknowledgements, or obvious references. A submitted paper should begin with a title, a short abstract, and a list of keywords.

Clear instructions for the preparation of a final proceedings version will be sent to the authors of accepted papers. Authors are strongly recommended to submit their papers in the standard LNCS format (see the Springer web page http://www.springer.com/computer/lncs?SGWID=0-164-0-0-0 for details).

Papers must be submitted using the EasyChair conference management system at
https://easychair.org/conferences/?conf=provsec2017

Please send any enquiry to: provsec2017@163.com

Stipends:
ProvSec 2017 provides a limited number of stipends to help partially cover travel and accommodation expenses for full-time students whose papers are accepted and presented at ProvSec 2017. More information about stipends, including instructions about how to apply, will appear at the conference website.

Keynote Speakers:
TBA

Conference Venue:
TBA

Honorary Co-Chairs:

Jianfeng Ma, (Xidian University, China)

Xiaoming Wang, (Shaanxi Normal University, China)

General Co-Chairs:

Bo Yang (Shaanxi Normal University, China)

Hui Li (Xidian University, China)

Dong Zheng (Xi'an University of Posts & Telecommunications, China)

Program Co-Chairs:

Tatsuaki Okamoto (NTT, Japan)

Yong Yu (Shaanxi Normal University, China)

Organizing Co-Chairs:

Zhenqiang Wu (Shaanxi Normal University, China)

Qiqi Lai (Shaanxi Normal University, China)

Yanwei Zhou (Shaanxi Normal University, China)

Publication Co-Chairs:

Man Ho Au (The Hong Kong Polytechnic University, Hong Kong)

Yannan Li (University of Electronic Science and Technology of China, China)

Publicity Co-Chairs:

Jianfeng Wang (Xidian University, China)

Kaitai Liang (Manchester Metropolitan University, UK)

Jianbing Ni (University of Waterloo, Canada)

Website Co-Chairs:

Yanqi Zhao (Shaanxi Normal University, China)

Ru Meng (Shaanxi Normal University, China)

Registration Co-Chairs:

Yujie Ding (Shaanxi Normal University, China)

Yuanxiao Li (Shaanxi Normal University, China)

Program Committee:

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, Norwegian)

Aniello Castiglione (University of Salerno, Italy)

Xiaofeng Chen (Xidian University, China)

Liqun Chen (University of Surrey, UK)

Rongmao Chen (National University of Defense Technology, China)

Céline Chevalier (École normale supérieure, France)

Kim-Kwang Raymond Choo (The University of Texas at San Antonio, USA)

Hongzhen Du (Baoji University of Arts and Sciences, China)

Christian Esposito (University of Salerno, Italy)

Jinguang Han (Nanjing University of Finance and Economics, China)

Debiao He (Wuhan University, China)

Qiong Huang (South China Agricultural University, China)

Xinyi Huang (Fujian Normal University, China)

Ryo Kikuchi (NTT, Japan)

Junzuo Lai (Jinan University, China)

Fagen Li (University of Electronic Science and Technology of China, China)

Jin Li (Guangzhou University, China)

Shundong Li (Shaanxi Normal University, China)
Xiaodong Lin (University of Ontario Institute of Technology, Canada)
Feng Liu (The State Key Laboratory of Information Security, China)
Joseph Liu (Monash University, Australia)
Zhe Liu (University of Waterloo, Canada)
Jiqiang Liu (Beijing Jiaotong University, China)
Vincenzo Iovino (University of Luxembourg, Luxembourg)
Bernardo M. David (Aarhus University, Denmark)
Mark Manulis (University of Surrey, UK)
Barbara Masucci (University of Salerno, Italy)
Mitsuru Matsui (Mitsubishi Electric, Japan)
Bart Mennink (Radboud University Nijmegen, Netherlands)
Yi Mu (University of Wollongong, Australia)
Pratyay Mukherjee (University of California, Berkley, USA)
Josef Pieprzyk (Queensland University of Technology, Australia)
Jae Hong Seo (Myongji University, Republic of Korea)
Jun Shao (Zhejiang Gongshang University, China)
Chunhua Su (Osaka University, Japan)
Willy Susilo (University of Wollongong, Australia)
Qiang Tang (New Jersey Institute of Technology, USA)
Mehdi Tibouchi (NTT, Japan)
Ding Wang (Peking University, China)
Baocang Wang (Xidian University, China)
Qian Wang (Wuhan University, China)
Huaxiong Wang (Nanyang Technological University, Singapore)
Qianhong Wu (Beihang University, China)
Shota Yamada (AIST, Japan)
Chung-Huang Yang (National Kaohsiung Normal University, Taiwan)
Guomin Yang (University of Wollongong, Australia)
Xun Yi (RMIT University, Australia)
Siu Ming Yiu (The University of Hong Kong, Hong Kong)
Yu Yu (Shanghai Jiaotong University, China)
Fangguo Zhang (Sun Yat-sen University, China)
Lei Zhang (East China Normal University, China)
Mingwu Zhang (Hubei University of Technology, China)
Rui Zhang (Chinese Academy of Sciences, China)
Wenzheng Zhang (National Laboratory for Modern Communications, China)
Fucai Zhou (Northeastern University, China)

For more detailed information of the conference, please access to the conference website at http://it.snnu.edu.cn/index.html.