The Tenth International Conference on Provable Security (ProvSec2016)
November 10-12, 2016, Nanjing, 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 2016. More details will be announced later.

Important Dates:
Paper submission deadline: June 3, 2016
Notification of acceptance: August 3, 2016
Camera ready deadline: August 14, 2016
Conference date: November 10-12, 2016

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Submitted papers must be original, unpublished, and not submitted to another conference or journal for consideration for publication.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=provsec2016

Please send any enquiry to: provsec2016@163.com

Stipends:
ProvSec 2016 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 2016. More information about stipends, including instructions about how to apply, will appear at the conference website.

Keynote Speakers:
TBA

Conference Venue:
Nanjing is the capital of Jiangsu province and the second largest city in eastern China (after Shanghai). ProvSec 2016 will be hosted in Shuangmenlou Hotel which is the former address of British Embassy in China. It has a long history dating back to 1916. More information about Nanjing and Shuangmenlou hotel can be found: https://en.wikipedia.org/wiki/Nanjing; http://www.smlhotel.com/

General Chair:
Jie Cao (Nanjing University of Finance and Economic, China)

Program Committee Co-Chairs:
Liqun Chen (Hewlett Packard (HP) Labs, Bristol, UK)
Jinguang Han (Nanjing University of Finance and Economics, China)

Program Committee:

Man Ho Au (Hong Kong Polytechnic University, Hong Kong)
Joonsang Baek (Khalifa University of Science, Technology and Research, Arab)
Zhenfu Cao (Shanghai Jiao Tong University, China)
Liqun Chen (Hewlett-Packard Laboratories, UK)
Yu Chen (Chinese Academy of Sciences, China)
Xiaofeng Chen (Xidian University, China)
Kim-Kwang Raymond Choo (University of South Australia, Australia)
Sherman S.M Chow (Chinese University of Hong Kong, Hong Kong)
Nico Döttling (Aarhus University, Denmark)
Georg Fuchsbauer (IST Austria, Austria)
David Galindo (University of Birmingham, UK)
Jinguang Han (Nanjing University of Finance and Economics, China)
Qiong Huang (South China Agricultural University, China)
Xinyi Huang (Fujian Normal University, China)
Sorina Ionica (University of Picardie Jules Verne, France)
Kwangjo Kim (KAIST, Korea)
Alptekin Küpçü (Koç University, Turkey)
Jiguo Li (Hohai University, China)
Yingjiu Li (Singapore Management University, Singapore)
Kaitai Liang (Aalto University, Finland)
Xiaodong Lin (University of Ontario Institute of Technology, Canada)
Joseph Liu (Monash University, Australia)
Rongxing Lu (Nanyang Technological University, Singapore)
Masahiro Mambo (Kanazawa University, Japan)
Mark Manulis (University of Surrey, UK)
Bart Mennink (KU Leuven, Belgium)
Chris Mitchell (Royal Holloway, University of London, UK)
Atsuko Miyaji (Osaka University, Japan)
Yi Mu (University of Wollongong, Australia)
Tatsuaki Okamoto (NTT, Japan)
Thomas Peters (Ecole normale supérieure, France)
Christophe Petit (University of Oxford, UK)
Josef Pieprzyk (Queensland University of Technology, Australia)
Yogachandran Rahulamathavan (City University London, UK)
Kui Ren (State University of New York at Buffalo, USA)
Reza Reyhanitabar (EPFL, Lausanne, Switzerland)
Willy Susilo (University of Wollongong, Australia)
Qiang Tang (University of Luxembourg, Luxembourg)
Cong Wang (City University of Hong Kong, Hong Kong)
Huaxiong Wang (Nanyang Technological University, Singapore)
Jian Weng (Jinan University, China)
Qianhong Wu (Beihang University, China)
Shouhuai Xu (University of Texas at San Antonio, USA)
Guomin Yang (University of Wollongong, Australia)
Chung-Huang Yang (National Kaohsiung Normal University, Taiwan)
Wun-She Yap (Universiti Tunku Abdul Rahman, Malaysia)
Xun Yi (RMIT University, Australia)
Siu Ming Yiu (The University of Hong Kong, Hong Kong)
Yong Yu (University of Electronic Science and Technology of China, China)
Tsz Hon Yuen (Huawei Singapore,Singapore)
Fangguo Zhang (Sun Yat-sen University, China)
Futai Zhang (Nanjing Normal University, China)

Rui Zhang (Chinese Academy of Sciences, China)
Yuan Zhang (Nanjing University, China)
Zongyang Zhang (AIST, Japan)
Jianying Zhou (Institute for infocomm research, Singapore)

Organizing Chair:
Zhiang Wu (Nanjing University of Finance and Economics, China)

Publication Chair:
Zhan Bu (Nanjing University of Finance and Economics, China)
Muhammad Khurram Khan (King Saud University, Kingdom of Saudi Arabia)

Publicity Chair:
Jiageng Chen (Huazhong Normal Unversity, China)
Ali El Kaafarani (Oxford University, UK)

Registration Chair:
Jianchang Fang (Nanjing University of Finance and Economics, China)

For more detailed information of the conference, please access to the conference website at http://provsec2016.njue.edu.cn/index.html.