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

General Information:

Provable security is an essential tool for analyzing security of modern cryptographic primitives. The research community has witnessed the great contributions that the provable security methodology made to the analysis of cryptographic schemes and protocols. Nowadays cryptographic primitives without a rigorous "proof" cannot be regarded as sound. Also, the methodology has been used to discover security flaws in the cryptographic schemes and protocols, which were considered seemingly secure without formal analysis. On the one hand, provable security provides confidence in using cryptographic schemes and protocols for various real-world applications, but on the other hand, schemes with provable security are sometimes not efficient enough to be used in practice, and correctness of the proofs may be difficult to verify. Therefore, ProvSec conference is to provide a platform for researchers, scholars and practitioners to exchange new ideas on diverse problems in provable security.

Conference Topics:

All aspects of provable security in constructing and analyzing cryptographic primitives, including but are not limited to:

- Provably secure asymmetric primitives
- Provably secure symmetric primitives
- Tightness of security reductions
- Provable security in post-quantum cryptography
- Privacy and anonymity technologies
- Cryptographic protocol verifier
- Theory and practice of game-hopping proof techniques
- Secure hash functions
- Provable security in the real-world security systems
- Secure key management
- Refinement of proof techniques
- Provably Secure cryptographic protocols and applications
- Security notions, approaches and paradigms
- Steganography
- Lightweight cryptography
- Lattice-based 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:

Selected papers from ProvSec2018 will be published by IEICE Transactions on Information and Systems - Special Section on Security, Privacy, Anonymity and Trust in Cyberspace Computing and Communications (pending acceptance of the proposal).

Important Dates:
Paper submission deadline: 17 June 2018 (UTC 24:00)
Notification of acceptance: 3 August 2018
Camera ready deadline: 17 August 2018
Conference date: 25 - 28 October 2018

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=provsec2018.

Please send any enquiry to: provesec2018@gmail.com

Keynote Speakers:
TBA

Conference Venue:
TBA

General Co-Chairs:

Ilsun You	Soonchunhayng University, Korea

Program Co-Chairs:

Willy Susilo	University of Wollongong, Australia
Joonsang Baek	University of Wollongong, Australia

Publication Co-Chairs:

Jongkil Kim	University of Wollongong, Australia

Registration Co-Chairs:
TBA

Program Committee:

Elena Andreeva	K.U. Leuven, Belgium
Man Ho Au	The Hong Kong Polytechnic University, Hong Kong
Aniello Castiglione	University of Salerno, Italy
Jie Chen	East China Normal University, China
Liqun Chen	University of Surrey, UK

Xiaofeng Chen	Xidian University, China
Raymond Choo	The University of Texas at San Antonio, USA
Cheng-Kang Chu	Huawei, Singapore
Bernardo David	The University of Tokyo, Japan
Jean Paul Degabriele	TU Darmstadt, Germany
Robert Deng	Singapore Management University, Singapore
Keita Emura	NICT, Japan
Ryo Kikuchi	NTT, Japan
Jinguang Han	University of Surrey, UK
Jongkil Kim	University of Wollongong, Australia
Hyung Tae Lee	Chonbuk National University, South Korea
Jooyong Lee	KAIST, South Korea
Joseph Liu	Monash University, Australia
Bernardo Magri	Friedrich-Alexander-University, Germany
Barbara Masucci	University of Salerno, Italy
Bart Mennink	Radboud University, Netherlands
Chris Mitchell	Royal Holloway, University of London, UK
Khoa Nguyen	Nanyang Technological University, Singapore
Abderrahmane Nitaj	Université de caen, France
Josef Pieprzyk	CSIRO, Australia
Kouichi Sakurai	Kyushu University, Japan
Reza Reyhanitabar	KU Leuven, Belgium
Rainer Steinwandt	Florida Atlantic University, USA
Chunhua Su	Univeristy of Aizu, Japan
Katsuyuki Takashima	Mitsubishi Electric, Japan
Atsushi Takayasu	The University of Tokyo, Japan
Qiang Tang	New Jersey Institute of Technology, USA
Dongvu Tonien	University of Wollongong, Australia
Damien Vergnaud	ENS, France
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	The University of Hong Kong, Hong Kong
Yong Yu	Shaanxi Normal University, China
Tsz Hon Yuen	Huawei, Singapore
Aaram Yun	UNIST, South Korea
Rui Zhang	Chinese Academy of Sciences, China