CALL FOR PAPERS

Special issue on

Advances of Provable Security Techniques

Journal of Universal Computer Science

Background

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 are 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 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.

Topics

Topics of interest include but are not limited to those listed below.

- Tight security reduction techniques
- Formal methods in provable security
- Applied cryptography protocols with provable security
- Anonymity
- Digital signature
- Public key encryption
- Data integrity
- Authentication and access control
- Lightweight secure protocols
- Privacy enhanced technology
- Design and analysis of cryptographic protocols

Important Dates

Submission Due	March 28, 2018
1stRound Notification	July 1, 2018
Revision	September 1, 2018
Final Notification	December 1, 2018

Guest Editors

Prof. Yong Yu, E-mail: yuyong@snnu.edu.cn
School of Computer Science, Shaanxi Normal University, China.
Prof. Yi Mu, Email: ymu@uow.edu.au
School of Computing and Information Technology, University of Wollongong, Australia.

Submission

Only high quality original papers will be selected after reviewing process. Authors should submit their papers via e-mail to yuyong@snnu.edu.cn. The subject of the e-mail should be [JUCS-ProvSec SI]. Submissions will be reviewed by at least 3 reviewers following a blind review process. All submission must be written in English and follow the JUCS's special issues guidelines:

http://www.jucs.org/ujs/jucs/info/submissions/style_guide.html.

The length of the manuscript may not exceed 20 pages.