Applied Cryptography in Computer and Communications

In this Thematic Series, we solicit original contributions on the area of applied cryptography in computer and communication systems. We encourage submissions on all technical aspects of applied cryptography, including symmetric cryptography, public-key cryptography, cryptographic protocols, cryptographic implementations, cryptographic standards and practices. We also encourage submissions on using cryptography to solve real-world problems in Internet of things, cyber-physical systems, edge computing, cloud computing, data science, information-centric networking, etc. We are especially in favor of those papers that are making real progress in cryptographic practice.

Topics include but are not limited to:

- Symmetric cryptographic primitives
- Public key cryptography
- Lightweight cryptography
- Post-quantum cryptography
- Cryptanalysis
- Searchable encryption
- Authentication and identification protocols
- Cryptographic privacy protection techniques
- Blockchain cryptographic primitives
- Cryptographic protocol implementation
- Cryptographic standards and legal regulations
- Side channels and preventions
- Cryptographic key attacks and defense
- Cryptographic hardware
- Applied cryptography in IoTs/CPS
- Applied cryptography in edge computing
- Applied cryptography in cloud computing
- Applied cryptography in information-centric networking
- Applied cryptography in software-defined networking
- Applied cryptography in big data and artificial intelligence

Key Dates

- Paper submission: August 1, 2021
- 1st round notification: October 1, 2021
- Revision due: November 1, 2021
- Final notification: December 1, 2021

Guest Editors

Bo Chen, Michigan Technological University, USA, bchen@mtu.edu
Xinyi Huang, Fujian Normal University, China, xyhuang@fjnu.edu.cn
Miroslaw Kutylowski, Wroclaw University of Science and Technology, Poland,
Submission Instructions
Prospective authors are invited to prepare and submit manuscripts following the instructions at: https://cybersecurity.springeropen.com/submission-guidelines; the complete manuscript should be submitted through: https://www.editorialmanager.com/cyse/default.aspx.

To ensure that you submit to the correct thematic series please select the appropriate thematic series 'Applied Cryptography in Computer and Communications' in the 'Additional Information'. In addition, indicate within your cover letter that you wish your manuscript to be considered as part of the thematic series on Applied Cryptography in Computer and Communications.