ICISC 2022

Call for Papers

The 25th Annual International Conference on Information Security and Cryptology

November 30 ~ December 2, 2022, Seoul, Korea

http://www.icisc.org/

General Chairs: Hyojin Choi (NSR, Korea), Okyeon Yi (Kookmin University, Korea)

Organizing Committee Chairs:

ChangHoon Lee (Seoul National University of Science and Technology, Korea), HeeSeok Kim (Korea University, Korea)

Programming Committee Chairs:

Seung-Hyun Seo (Hanyang University, Korea), HwaJeong Seo (Hansung University, Korea)

IMPORTANT DATES

Submission deadline	**September 2, 2022 18:00 KST (GMT + 9 hr)**
Acceptance notification	**November 11, 2022**
Camera-ready submission	**November 16, 2022**
Author registration deadline	**November 17, 2022**
Participant registration deadline	**November 21, 2022**
ICISC 2022 Conference	**November 30 ~ December 2, 2022**

OVERVIEW

Original research papers on all aspects of theory and applications of information security and cryptology are solicited for submission to ICISC 2022, the 25th Annual International Conference on Information Security and Cryptology which is sponsored by NSR(National Security Research Institute) and KIISC (Korean Institute of Information Security and Cryptology), Korea.

TOPICS of INTEREST INCLUDE, but are not limited to:

Cryptography Track

- Authentication and Authorization
- Biometrics
- Blockchain Security
- Block and Stream Ciphers
- Copyright Protection
- Cryptographic Protocols
- Cryptanalysis
- Digital Forensics
- Digital Signature
- Distributed Systems Security
- Efficient Cryptography Implementation
- Functional encryption
- Hash Function
- Homomorphic Encryption
- ID-based Cryptography
- Intrusion Detection and Prevention
- Information Hiding
- Key Management
- Post-quantum cryptography
- Privacy Enhancement
- Public Key Cryptography
- Side Channel Attacks and Countermeasures
- Secure Multiparty Computation
- Software Security
- Smart Device Security
- Zero-knowledge proofs

Security Track

- Analysis of network and security protocols
- Anonymity and censorship-resistant technologies
- Applications of cryptographic techniques
- Authentication and authorization
- Automated tools for source code/binary analysis
- Automobile security
- Botnet defense
- Critical infrastructure security
- Denial-of-service attacks and countermeasures
- Embedded systems security
- Exploit techniques and automation
- Hardware and physical security
- HCI security and privacy
- Malware analysis
- Mobile/wireless/cellular system security
- Network-based attacks
- Network infrastructure security
- Operating system security
- Practical cryptanalysis (hardware, DRM, etc.)
- Security policy
- Techniques for developing secure systems
- Trustworthy computing
- Trusted execution environments
- Unmanned System Security
- Vulnerability research
- Web Security

INSTRUCTIONS for AUTHORS

Submissions must not substantially duplicate work that any of the authors have published elsewhere or submitted in parallel to any other conference or workshop that has proceedings. The paper should start with a title, an abstract and keywords, but must be anonymous. The length of the submission should not exceed 20 pages in Springer's LNCS format, excluding the bibliography and clearly marked appendices. Since committee members are not required to read the appendices, the paper should be intelligible without them. All papers must be in PDF format. It is strongly recommended that submissions be processed using LaTeX2e according to the instruction at http://www.springer.de/comp/lncs/authors.html. Authors of accepted papers must guarantee that their paper will be presented at the conference.

CONFERENCE PROCEEDINGS

The proceedings will be published by Springer-Verlag in the Lecture Notes in Computer Science.