



# ICISC 2023

## Call for Papers



*The 26th Annual International Conference on Information Security and Cryptology*

*November 29 ~ December 1, 2023, Seoul, Korea*

<http://www.icisc.org/>

**General Chair:** Yoojae Won (Chungnam National University, Korea)

**Organizing Committee Chairs:**

Young-Ho Park (Sejong Cyber University, Korea), Junbeom Hur (Korea University, Korea)

**Programming Committee Chairs:**

HwaJeong Seo (Hansung University, Korea), Suhri Kim (Sungshin Women's University, Korea)

### IMPORTANT DATES

Submission deadline	<b>September 15, 2023 18:00 KST (GMT + 9 hr)</b> → <b>October 6, 2023 18:00 KST (GMT + 9 hr)</b>
Acceptance notification	<b>November 10, 2023</b>
Camera-ready submission	<b>November 15, 2023</b>
Author registration deadline	<b>November 17, 2023</b>
Participant registration deadline	<b>November 21, 2023</b>
ICISC 2023 Conference	<b>November 29 ~ December 1, 2023</b>

### OVERVIEW

Original research papers on all aspects of theory and applications of information security and cryptology are solicited for submission to ICISC 2023, the 26th Annual International Conference on Information Security and Cryptology which is sponsored by 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

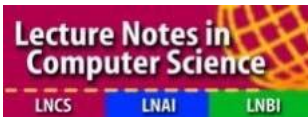
#### Security Track

- 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.

---