Call for Papers

The 21st International ISC Conference on Information Security and Cryptology (ISCISC 2024)

October 16-17, 2024, Tarbiat Modares University, Tehran, Iran
https://iscisc2024.modares.ac.ir/en

For the past two decades, the International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC) has served as the flagship event in the field of information security and cryptology in Iran. Now, we are pleased to announce the **21st International ISC Conference on Information Security and Cryptology (ISCISC 2024)**, organized by **Tarbiat Modares University, Tehran, Iran**, in collaboration with the **Iranian Society of Cryptology (ISC)**. The conference will take place on **October 16-17, 2024**.

ISCISC 2024 aims to bring together researchers, engineers, and practitioners who share a keen interest in various aspects of information security and cryptology. Our goal is to provide a dynamic forum where academicians, engineers, specialists, and students from around the world can convene to discuss the latest developments in theory and practice across diverse areas of information security. The conference will foster collaboration, knowledge exchange, and innovation.

We invite researchers, developers, and practitioners to submit their original papers and propose workshops on emerging topics related to cryptology and information security. Industrial exhibitions will run alongside the main conference, providing additional opportunities for engagement. Notably, keynote and plenary talks, as well as panel discussions, will enrich the conference experience.

Important Dates

- Paper submission: **June 15, 2024**
- Workshop proposals: **June 15, 2024**
- Decision Notification: **August 14, 2024**
- Conference : **October 16-17, 2024**

Topics of interest

The topics of interest include, but are not limited to:

- **Foundations of cryptology**
  - Symmetric cryptographic algorithms
  - Asymmetric and cryptographic algorithms and digital signatures
  - Hash functions
  - Information-theoretic security
  - New methods in cryptography (functional cryptography, homomorphic cryptography, ...)
- **Implementation of cryptographic algorithms and related attacks**
  - Software and hardware implementation of cryptographic algorithms
  - Side channel attacks and countermeasures
  - Embedded cryptographic systems
  - Hardware tampering and countermeasures
  - Cryptographic hardware accelerators
  - Verification and fault detection of implementations
- **Network security**
  - Wireless and mobile network security
  - Security of network infrastructures
  - Security of network protocols and layers
  - Intrusion detection and prevention systems
  - Security of critical infrastructures
- **Cryptography and security models and protocols**
  - Authentication and identification protocols
  - Anonymity, privacy, and trust management
  - Cryptanalysis of security protocols
  - Trust and security models
  - Formal methods in information security
  - Secure Multiparty Computation
- **Security of computation**
  - Security in computer architecture
  - Operating system security
  - Database security
  - Analysis of security and vulnerability of software and application programs
  - Malware Analysis
  - Security and privacy in mobile devices and applications
  - Access control
- **Security and privacy management**
  - Social engineering in security
  - Information security management system (ISMS)
  - Risk Management
  - Information security training
  - E-business and e-service security
  - E-health security
  - E-banking security
  - E-learning security
  - Privacy-Enhancing Technologies

- **Information hiding**
    - New algorithms in steganography and watermarking
    - Steganalysis
    - Applications of Information hiding
- **Digital forensics**
    - Digital forensics methods and tools
    - Database and network forensics
    - Mobile device forensics
    - Fraud detection
- **Recent topics in cryptography and security**
    - Quantum cryptography
    - Post-quantum cryptography
    - Artificial Intelligence (AI) Security
    - Blockchain technology and cryptocurrency
    - Internet of Things (IoT), big data and cloud security
    - Cyber-physical systems security
    - Soft security

Submission Guidelines

- **Paper Submission:** All submissions must be made through EDAS submission system at https://edas.info/N31896. Please select our conference as your submission outlet.
- **Presentation Requirement:** For each accepted paper, at least one author must register for the conference and ensure in-person presentation. Non-local researchers have the option to present their papers online.
- **Publication:** Accepted papers will be featured in a special issue of the ISeCure journal, which is indexed in WoS-JCR, SCImago-SJR, and Scopus, among other reputable indexing services.
- **Quality Assurance:** Each paper submitted for evaluation will undergo rigorous review by three experts in the field.

Manuscript Details

- Submitted papers should not significantly overlap with previously published or accepted works.
- Manuscripts must be in PDF format, adhering to the ISeCure template: https://www.isecure-journal.com/journal/authors.note
- The maximum length for submissions is **8 pages**, with an acceptable extension to **11 pages** (subject to an extra-page fee).

We eagerly anticipate your valuable contributions to ISCISC 2024!

More Information

- Visit the conference website for further details: https://iscisc2024.modares.ac.ir
- Fax: +98 (21) 82884325
- Email: iscisc2024@isc.org.ir, iscisc2024@modares.ac.ir
- Skype: https://join.skype.com/invite/DMa4cyrvhj59