Call for Papers

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

October 16 and 17, 2024

Tarbiat Modares University, Tehran, Iran

https://iscisc2024.modares.ac.ir/en

For the past two decades, the International Iranian Society of Cryptology (ISC) Conference on Information Security and Cryptology (ISCISC) has been the flagship event in the field of information security and cryptology in Iran. We are pleased to announce the **21st International ISC Conference on Information Security and Cryptology (ISCISC 2024)**, organized by **Tarbiat Modares University, Tehran, Iran**, and in collaboration with the **Iranian Society of Cryptology**. The conference will take place on **October 16 and 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, specialists, and students from all 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. Keynote and plenary speeches, as well as panel discussions, will enrich the conference experience.

Important Dates

- Paper Submission Due: **June 29, 2024** (extended)
- Workshop Proposals Due: **June 29, 2024** (extended)
- Notification of Acceptance: **August 14, 2024** (extended)
- Conference Date: **October 16 and 17, 2024**

Topics of Interest

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

- **Foundations of cryptology and cryptanalysis**
  - Symmetric cryptographic algorithms
  - Asymmetric cryptographic algorithms and digital signatures
  - Hash functions
  - Information-theoretic security
  - Advanced topics 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
  - Cryptographic implementation analysis
- **Security protocols**
  - Authentication and identification protocols
  - Zero-knowledge protocols and proofs
  - Secure multiparty computation
  - Designing new security protocols
  - Cryptanalysis of security protocols
  - Attacks against security protocols
  - Formal verification of security protocols
- **Security methods and models**
  - Access control and authorization
  - Anonymity, privacy, and trust management
  - Security and privacy policies and metrics
  - Threat modeling and analysis
  - Formal methods and models
- **Network security**
  - Mobile and wireless network security
  - Network infrastructure security
  - Network intrusion detection and prevention
  - Denial-of-service attacks and countermeasures
  - Security analysis of network protocols
- **Security of computation**
  - Hardware security
  - Operating system security
  - Database security
  - Web security
  - Mobile application security
  - Fuzzing and vulnerability discovery
  - Malware Analysis

- **Security and privacy management**
  - Information security management system
  - Security architectures
  - Risk management
  - E-business and e-banking security
  - E-health security
  - E-learning security
  - Privacy-enhancing technologies
- **Information hiding**
  - Steganography and watermarking
  - Steganalysis
  - Applications of information hiding
- **Digital forensics**
  - Digital forensics techniques and tools
  - Database and network forensics
  - Mobile device forensics
  - Cybercrime forensics
- **Recent topics in cryptography and cybersecurity**
  - Quantum and post-quantum cryptography
  - Blockchain technology and cryptocurrencies
  - Internet of Things (IoT), big data and cloud security
  - Cyber-physical systems security
  - Artificial Intelligence (AI) security and privacy
  - Adversarial machine learning
  - Security of social networks, metaverse, and augmented reality-based systems

Submission Guidelines

- **Paper Submission:** All submissions must be made through the 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 an in-person presentation. Non-local authors will 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**. Additional pages (up to **11 pages**) are 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