WELCOME TO ISCwsISC 2023

Third ISC Winter School on Information Security and Cryptology
February 2023 (Virtual Event)

Iranian Society of Cryptology (ISC)

- Iranian Society of Cryptology (ISC) is a non-profit organization devoted to promoting the science of cryptology.

Iranian Society of Cryptology (ISC)

- Iranian Society of Cryptology (ISC) is a non-profit organization devoted to promoting the science of cryptology.
- The ISC International Journal of Information Security (ISeCure) is a peer reviewed scholarly publication by Iranian Society of Cryptology.

Iranian Society of Cryptology (ISC)

- Iranian Society of Cryptology (ISC) is a non-profit organization devoted to promoting the science of cryptology.
- The ISC International Journal of Information Security (ISeCure) is a peer reviewed scholarly publication by Iranian Society of Cryptology.
  - It is published since 2009.

Iranian Society of Cryptology (ISC)

- Iranian Society of Cryptology (ISC) is a non-profit organization devoted to promoting the science of cryptology.
- The ISC International Journal of Information Security (ISeCure) is a peer reviewed scholarly publication by Iranian Society of Cryptology.
  - It is published since 2009.
  - Articles published in ISeCure Journal are indexed in the Emerging Sources Citation Index (ESCI) database of **Web of Science/ISI** and **Scopus**.

Iranian Society of Cryptology (ISC)

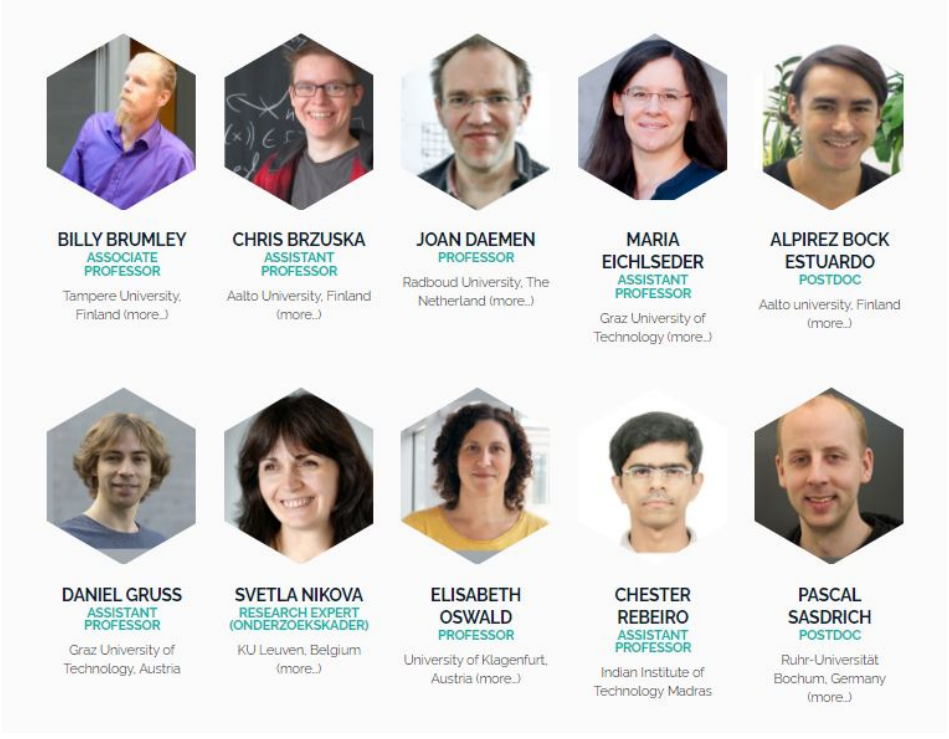
- Iranian Society of Cryptology (ISC) is a non-profit organization devoted to promoting the science of cryptology.
- The ISC International Journal of Information Security (ISeCure) is a peer reviewed scholarly publication by Iranian Society of Cryptology.
  - It is published since 2009.
  - Articles published in ISeCure Journal are indexed in the Emerging Sources Citation Index (ESCI) database of **Web of Science/ISI** and **Scopus**.
  - https://www.isecure-journal.com/

ISCISC2023

- 20th International ISC Conference on Information Security and Cryptology (ISCISC2023) will be held in Tehran on August 30-31, 2023.
  - Submission Deadline: June 6, 2023
  - Notification: August 7, 2023
- https://iscisc2023.conf.irost.ir/en/
- All accepted papers will be published in **ISeCure journal**.
- If you are not able to attend in the conference, you can present your paper online.

ISC Winter School on Information Security and Cryptology

- First ISC Winter School in 2020: Symmetric Cryptography
- Second ISC Winter School in 2021: Secure Implementation



ISCWSISC 2023

- Three main topics:
  - ZK (Zero-Knowledge) Proofs
  - MPC (MultiParty Computation)
  - FHE (Fully-Homomorphic Encryption)

JENS GROTH
DIRECTOR OF RESEARCH IN FORMAL SECURITY AT DFINITY, SWITZERLAND

Title: Introduction to ZK and Foundations of NIZK Arguments

CARLA RAFOLS
RESEARCHER IN CRYPTOGRAPHY, UNIVERSITAT POMPEU FABRA, SPAIN

Title: On Updatable and Universal zk-SNARKs

CYPRIEN DE SAINT GUILHEM
POSTDOCTORAL RESEARCHER, KU LEUVEN, BELGIUM

Title: On the MPC-in-the-Head Paradigm and Limbo

EMMANUELA ORSINI
ASSISTANT PROFESSOR, BOCCONI UNIVERSITY, ITALY

Title: Introduction to MPC and SPDZ Protocol

MICHELE CIAMPI
CHANCELLOR'S FELLOW, UNIVERSITY OF EDINBURGH, UK

Title: On Round Optimal MPC protocols

AARUSHI GOEL
POST-DOCTORAL RESEARCHER AT NTT RESEARCH, USA

Title: Fluid MPC: MPC with Dynamic Participants

YOUNES TALIBI ALAOUI
RESEARCHER, KU LEUVEN, BELGIUM

Title: Financial Applications of MPC

HILDER V. L. PEREIRA
POSTDOCTORAL RESEARCHER AT COSIC, KU LEUVEN, BELGIUM

Title: Foundations of FHE

ILARIA CHILOTTI
DIRECTOR OF RESEARCH, ZAMA, FRANCE

Title: TFHE and Applications (more..)

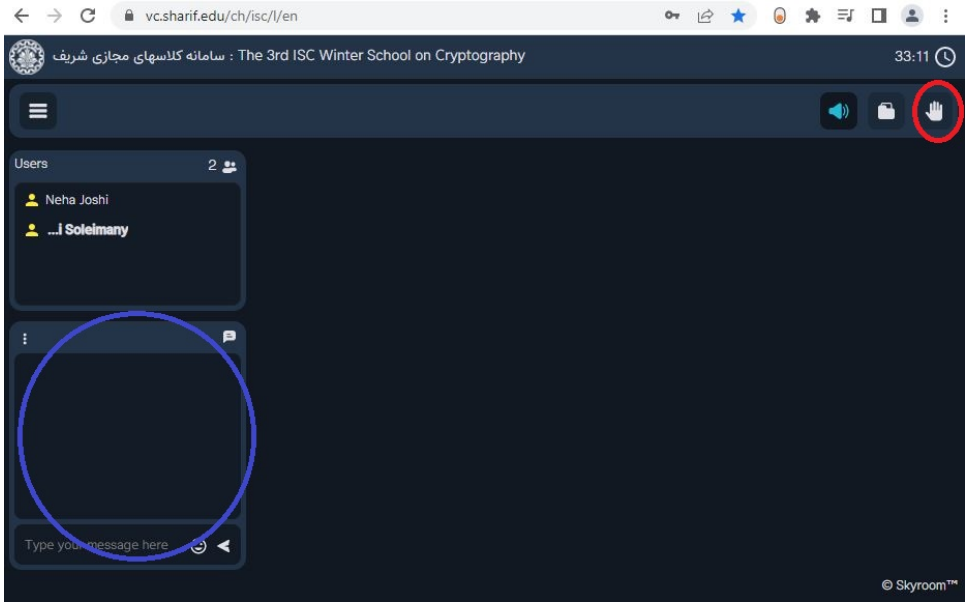
JEONGEUN PARK
POSTDOCTORAL RESEARCHER, KU LEUVEN, BELGIUM

Title: Applications of FHE (more..)

Pre-school Event

- ISC pre-school event that involves introduction lectures by experienced researchers was held between 1 February and 22 February 2023.
- 130 participants
- Slides are available in the website: http://iscwsisc2023.sbu.ac.ir/fa/
- Videos are available in ISC Aparat channel

Skyroom



- To raise your hand during a session, select Raise Hand from the top right.
- Chat Box located in bottom left, but please do not use it!
- Please join the event's Discord server by clicking on the link available in the website of school.
- By joining the server, you will be able to receive the latest announcements about the school, participate in debates and chats, and ask questions during the lectures.

More points

- Videos will be available in the ISC YouTube Aparat channel: IranCrypt.

More points

- Videos will be available in the ISC YouTube Aparat channel: IranCrypt.
- Slides will be added in the winter school website: http://iscwsisc2023.sbu.ac.ir/

More points

- Videos will be available in the ISC YouTube Aparat channel: IranCrypt.
- Slides will be added in the winter school website: http://iscwsisc2023.sbu.ac.ir/
- Feel free to contact us if you have any questions or problem (email address: iscwsisc2023@sbu.ac.ir)

Thank you very much and Enjoy ISCwsISC 2023!