I4CS 2022

International Conference on Cryptography, Codes, and Cyber Security

October 26–28, 2022 • Casablanca, Morocco

Program chairs
  Abderrahmane Nitaj, *Caen, France*
  Karim Zkik, *ESAIP Angers, France*

General chair
  Khadija Bouzkoura, *Casablanca, Morocco*

Program committee
  EL Bachir Ameur, *Kenitra, Morocco*
  Muhammad Rezal Ariffin, *UPM, Malaysia*
  François Arnault, *Limoges, France*
  Ahmed Asimi, *Agadir, Morocco*
  Ezedin Barka, *College of Inf.Tech. UAE*
  Daniele Bartoli, *DPerugia, Italy*
  Lejla Batina, *Radboud University, NL*
  Thierry Berger, *Limoges, France*
  Lilya Budaghyan, *Bergen, Norway*
  Florian Caullery, *Qualcomm*
  Pierre-Louis Cayrel, *Saint Etienne, France*
  Joan Daemen, *Nijmegen, NL*
  Luca De Feo, *IBM, Zürich, Switzerland*
  Pierre Dusart, *Limoges, France*
  Nadia El Mrabet, *EMSE, France*
  Philippe Gaborit, *Limoges, France*
  Elisa Gorla, *Neuchatel, Switzerland*
  Marcus Greferath, *U.C. Dublin, Ireland*
  Kenza Guenda, *Algiers, Algeria*
  Cheikh T. Gueye, *Dakar, Senegal*
  Sylvain Guilley, *Telecom Paris, France*
  Tor Helleseth, *Bergen, Norway*
  Delaram Kahrobaei, *New-York, USA*
  Juliane Krämer, *TU Darmstadt, Germany*
  Fabien Laguillaumie, *Lyon I, France*
  Petr Lisonek, *Simon Fraser, Canada*
  Sihem Mesnager, *Paris VIII, France*
  Abderrahmane Nitaj, *Caen, France*
  Gizlane Orhanou, *Rabat, Morocco*
  Ferruh Özbudak, *Ankara, Turkey*
  Massimiliano Sala, *Trento, Italy*
  Palash Sarkar, *Indian S.I. Kolkata, India*
  Amr M. Youssef, *Concordia, Canada*

Important dates

  Submission deadline: **July 15, 2022.**
  Notification: August 30, 2022.
  Camera-ready version: September 10, 2022.
  Conference dates: October 26-28, 2022.

The first International Conference on Cryptography, Codes and Cyber Security (I4CS) is an international conference on the theory and applications of cryptology, coding theory, and cyber security. I4CS 2022 will be held as a physical and a virtual event in Casablanca, Morocco, from July 14 to July 16, 2022. The conference is organized by Hassan II University in Casablanca in cooperation with the International Association for Cryptologic Research (IACR). The aim of I4CS 2022 is to provide an international forum for practitioners and researchers from industry, academia, and government worldwide for a wide-ranging discussion of all forms of cryptography, coding theory, cyber security, and their applications.

Original research papers are welcomed on any cryptography, codes, and cyber security topics, including but not limited to:

– Secret-key cryptography (block ciphers, stream ciphers, hash functions)
– Public-key cryptography (protocols, digital signatures, encryption)
– Security proofs
– Design of cryptographic schemes
– Cryptanalysis
– Anonymity (electronic commerce and payment, electronic voting)
– Information theory
– Multi-party computation
– Post quantum cryptography
– Lightweight Cryptography
– Elliptic curves, Lattices, Lattice-based cryptography, Code-based cryptography
– Cryptography for Blockchain
– Efficient implementations
– Cyber security
– Privacy
– Boolean functions for coding theory and symmetric cryptography
– Coding theory (Algebraic Coding Theory, Combinatorial Coding Theory, Quantum Codes, Decoding algorithms, etc.)
– Coding for Communications (Convolutional and Turbo Codes, LDPC Codes, Polar Codes, Rank Modulation Codes, Reed-Solomon and MDS codes, etc.)
– Discrete mathematics and algorithmic tools in all these areas
– Private Information Retrieval

Proceedings

The proceedings will be published in the Springer Communications in Computer and Information Science (CCIS) series. Accepted papers should follow the CCIS default author instructions http://www.springer.com/series/7899

Instructions for authors

Authors are invited to submit papers (PDF format) with novel contributions electronically. Submitted papers must be original, unpublished, *anonymous*, and not submitted to journals or other conferences/workshops that have proceedings. Submissions must be written in English and should be at most 20 pages in total, including bibliography and appendices. All submissions will be blind-refereed. Authors of accepted papers must guarantee that they will be presented at the conference and make a full version of their paper available online.

Authors should consult Springer's authors' guidelines and use their proceedings templates for LaTeX for the preparation of their papers. Springer encourages authors to include their ORCIDs in their papers. In addition, the corresponding author of each paper, acting on behalf of all of the authors of that paper, must complete and sign a Consent-to-Publish form.

For submission please use Easychair at

  https://easychair.org/account/signin?l=6kzDVKfXy05jl7BM7OLUOW

Further information and instructions can be found at:

  http://i4cs22.univh2c.ma