Bimonthly Talks

CYBER-PHYISICAL SYSTEMS
SOCIETY OF IRAN

Fall 2023

Monday
Aban. 29 (Nov 20)
18:30 - 20:00

SPEAKER: Dr. Shahriar Ebrahimi (IDEAS NCBR, Warsaw, Poland)

Zero-Knowledge Proofs

ABSTRACT: Zero-Knowledge Proofs are cryptographic protocols that allow one party (the prover) to prove their knowledge about a specific piece of information to another party (the verifier) without revealing the actual information. The main goal of Zero-Knowledge Proofs is to establish confidence in the validity of a statement or the authenticity of a transaction without the need for trust between entities. These proofs have applications in various domains such as privacy-preserving identity verification, secure transactions, data privacy preservation, multi-party computations (MPC), and more generally in transforming interactive protocols into non-interactive versions.

BIOGRAPHY OF THE SPEAKER: Dr. Ebrahimi is a computer engineer and researcher currently working as a Postdoctoral Researcher at IDEAS NCBR in Warsaw, Poland. He earned his Ph.D. in Computer Engineering from Sharif University of Technology. He previously had the opportunity to lead blockchain projects at Nobitex Crypto-Exchange. His current research interests include Zero-Knowledge Proofs (ZKP), Verifiable Computation (VC), Multi-Party Computation (MPC), Privacy-Preserving Machine-Learning (PPML), Blockchain technology, Modern/Post-Quantum Cryptosystems

Cyber-Physical
Systems Society of Iran

Tel: (+98) 21 - 28421938
Email: info@cpssi.ir
Website: www.cpssi.ir

Scan the QR Code to Join the Session