انجمن رمزایران
شاخه دانشجویی دانشگاه شهید بهشتی

Post-Quantum Cryptographic Engineering

Dr. Hassan Khodaiymehr

Assistant Professor; Department of Mathematics at Khajeh Nasir Toosi University of Technology

Abstract

In his seminal work, Wyner introduced the wiretap channel, a discrete memoryless channel where the sender Alice transmits confidential messages to a legitimate receiver Bob, in the presence of an eavesdropper Eve, who has only partial access to what Bob sees. Indeed, Eve's access is modeled as a separate channel with quality lower than the quality of the channel between Alice and Bob. Both reliable and confidential communication between Alice and Bob is shown to be achievable at the same time, by exploiting the physical difference between the channel to Bob and that to Eve, without the use of cryptographic means. We present an overview of code design for Gaussian wiretap channels and recent advances in the area of information security using algebraic number fields. This overview indicates the importance of modular lattices in information security and recently proposed methods for obtaining modular lattices using algebraic number fields.

Biography:

Hassan Khodaiemehr received the B. Sc. in pure mathematics in 2010, the B. A. Sc. in electrical engineering and the M. Sc. in pure mathematics in 2012, and the Ph.D. in mathematics in 2017 from Amirkabir University of Technology. From Oct. 2016 to Aug. 2017 he was a visitor in the School of Mathematics and Statistics at the University of Carleton, Ottawa. From Oct. 2017 to Feb. 2018 he was a postdoctoral fellow in the institute for research in fundamental sciences (IPM). His research interests include coding and information theory, digital and wireless communications, space-time coding, physical layer network coding and information security. Currently, he is an assistant professor in the computer science department of K.N. Toosi University of Technology and also a resident researcher in the school of mathematics of IPM.

Tue., November 4 (Aban 14, 1398),12:30-13:30, Conference Room of Cyber Space Center