Title: Lattices in Cryptography, Past, Present, and Future

Speaker: Dr. Angshuman Karmakar, Katholieke Universiteit Leuven, Belgium

Date and Time: 4th January 2022 (Tuesday), 3:30 PM

Venue: Zoom

Abstract:

The use of hard lattice-based problems for cryptographic constructions is not new. Recently the interests have received a fresh impetus due to the use of lattices in the construction of post-quantum cryptography and fully homomorphic encryption. This talk will cover the design and implementation details of the state-of-the-art lattice-based key-encapsulation mechanism Saber which is one of the four finalist candidates in the ongoing National Institute of Standards and Technology's post-quantum cryptography standardization procedure. This talk will also discuss the future challenges of post-quantum cryptography beyond the standardization procedure. Finally, it will briefly introduce functional encryption which is a new paradigm of computation on encrypted data, and its applications.

Speaker bio:

Angshuman Karmakar received the BE degree in computer science and engineering from Jadavpur University, Kolkata, and the MTech degree in computer science and engineering from the Indian Institute of Technology, Kharagpur. He received his doctorate from Katholieke Universiteit Leuven, Belgium for his dissertation titled "Design and implementation aspects of post-quantum cryptography". He is one of the primary designers of the post-quantum Saber key-encapsulation mechanism scheme which is one of the finalists in the National Institute of Standards and Technology's post-quantum standardization procedure. He is currently an FWO post-doctoral fellow in the COSIC research group of KU Leuven. Earlier, he worked as an engineer in Citrix R&D India Ltd, Bangalore, and as a research intern at Microsoft Research, Redmond, USA. His research interest spans different aspects of lattice-based post-quantum cryptography and computation on encrypted data.