Talk Title: Cryptanalysis of some Lattice-based Assumptions

Venue: KD101

Time: 15:30-16:30 on 24/11/2023

Abstract:

Cryptography relies on the assumptions of computationally hard problems. The assumptions should be hard for security, offer functionalities for cryptographic applications, and be efficient to implement. Recently, lattice-based assumptions have emerged as a strong building block for post-quantum cryptography. This was also reflected in the NIST Post-Quantum Cryptography Standardization. In this talk, I will present recent cryptanalytic results on two lattice-based assumptions, namely the Finite Field Isomorpshim problem (PKC'18, JoMC'20), and the Partial Vandermonde Knapsack Problem (ACNS'14, DCC'15, ACISP'18, DCC'20, Eprint'20). These assumptions have been used extensively for various lattice-based constructions, including encryptions, fully homomorphic encryptions, signatures, signature aggregations, etc.

Bio:

Dipayan Das was a PostDoc at CISPA-Helmholtz Center for Information Security in the group of Antoine Joux. He has completed his Ph.D. from NIT Durgapur. During his Ph.D., he was a visiting student at Hong Kong Polytechnic University (hosted by Man Ho Au). He has completed his MSc and BSc in mathematics from NIT Durgapur and University of Calcutta, respectively. He was an intern in the summer cryptology internship conducted by the R.C.Bose Center for Cryptology and Security of the Indian Statistical Institute. He will start at NTT Japan as a researcher in December 2023.

Website: **https://sites.google.com/site/dasdipayan9038**