Indian Statistical Institute

Applied Statistics Unit

SEMINAR NOTICE

Speaker: Sanjay Bhattacherjee, University of Kent, UK
Title: New lattice basis reduction algorithms - a greedy approach
Date: 29 August, 2023
Time: 16:15 PM
Venue: ASU Seminar Room
Online Platform: Google Meet (meet.google.com/qvx-dppe-sda)

Abstract: A lattice is the set of all discrete points attained as integer linear combinations of linearly independent vectors (its basis). There are infinitely many bases of a lattice. A reduction algorithm finds a basis of better quality - with shorter and more orthogonal vectors than the input basis. Lattice-based constructions arguably constitute the most promising direction in post-quantum cryptography (PQC). PQC systems run on classical computers, while they are believed to be resistant to both quantum and classical attacks. The security of lattice based PQC relies on the computational hardness of finding the shortest vector in a lattice, called the shortest vector problem or SVP. LLL was introduced in 1982 as the first lattice basis reduction algorithm that provides approximate SVP solutions, and is still widely used in practice. The BKZ basis reduction algorithm introduced in 1994, provides better quality output bases than LLL, at the cost of being slower. Since then, BKZ has emerged as the state-of-the-art in lattice basis reduction for cryptanalysis of PQC schemes. The FPLLL library provides the most efficient implementations of LLL and BKZ. This talk will describe a new framework of LLL-style algorithms that adopts a novel greedy approach. The algorithms have proofs of assured output quality and polynomial runtime where plausible. In experiments, the algorithms generally provide useful runtime efficiency versus output quality trade-offs. In some cases, they beat the FPLLL implementation of BKZ on both counts - they are faster and produce better quality bases as output. The draft of our first result titled "A greedy global framework for LLL" is available at: https://eprint.iacr.org/2023/261.

All are invited to attend.

Please write to SOMENATH DAS somenath1011@isical.ac.in in case you do not receive the invitation link 48 hours before the seminar time.