5:15 PM Tuesday, July 22 in Oxford

Commuting Ramanujan Graphs and the Random Self-reducibility of Isogeny Problems

David Jao

University of Waterloo, Canada

Recent attacks on SIDH have led to increased scrutiny of hardness assumptions for isogeny based cryptosystems, especially in the case of SIDH variants which mask some of the information disclosed by the original. One such piece of information which is potentially public in SIDH variants is the endomorphism ring of the domain of the secret isogeny. A possible way to mask this information is to use a random starting elliptic curve instead of a fixed one. This approach raises the question of whether doing so generates a new vulnerability, that is, whether the hardness assumptions corresponding to these new SIDH variants are randomly self-reducible.In this paper, we study families of Ramanujan graphs whose adjacency matrices commute. We use results on these families of commuting matrices to prove the random self-reducibility of the hardness assumptions underlying the FESTA scheme, as well as for some SIDH-based proof of knowledge schemes.

In Special Session 55 on Post-Quantum Cryptography at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS55-T02