**Speaker:** Rajendra Kumar, a postdoc at NUS and our alumnus.

**Time and Date:** 4-5 PM, 20th April (Wednesday)

Venue: KD 103

**Title:** Are Lattice problems really that hard?

**Abstract:**

Lattice-based cryptographic schemes have generated much interest in recent years. Their security relies on the computational hardness of computational problems over geometric objects called lattices. These schemes have been used to build advanced cryptographic primitives such as fully homomorphic encryption, and they are believed to be resistant to quantum attacks. Given the recent advancement in quantum technologies, many institutes such as the National Institute of Standards and Technology (NIST) and European Telecommunications Standards Institute (ETSI) have initiated a process for standardization and deployment of lattice-based schemes widely over the next few years.

The security of these schemes crucially relies on the assumption that the best-known algorithms for the corresponding lattice problems cannot be improved. In this talk, I will describe the state of the art of this assumption. More specifically, I will talk about the fine-grained the hardness of the lattice problems in different p-norms. I will also talk about our recent work that shows that it is impossible to get any fine-grained hardness for the lattice problems in the euclidean norm, under a complexity-theoretic assumption.