MARTIN ROETTELER, NEC Laboratories America, Inc.

*On the Power of Random Bases in Fourier Sampling: Hidden Subgroup Problem in the Heisenberg Group*

The hidden subgroup problem (HSP) provides a unified framework to study problems of group-theoretical nature in quantum computing such as order finding and the discrete logarithm problem. While it is known that Fourier sampling provides an efficient solution in the abelian case, not much is known for general non-abelian groups. Recently, some authors raised the question as to whether post-processing the Fourier spectrum by measuring in a random orthonormal basis helps for solving the HSP. Several negative results on the shortcomings of this random strong method are known. In this talk I will show that the random strong method can be quite powerful under certain conditions on the group $G$. In particular the HSP for finite Heisenberg groups can be solved using polynomially many random strong Fourier samplings followed by a possibly exponential classical post-processing without further queries.

Joint work with Jaikumar Radhakrishnan and Pranab Sen.