JST-DST アジア学術セミナー受講者公募

INDO-JAPAN JOINT WORKSHOP&EXPOSITORY TUTORIAL SESSION　in　QUANTUM COMPUTATION AND QUANTUM INFORMATION

下記で開催するセミナー（ワークショップとチュートリアル講義）に参加する若手研究者を募集します。

１）日時：チュートリアル講義(令和2年1月2日~1月5日)、ワークショップ(令和2年1月6日~8日)　1月1日は移動日＆レセプション
２）場所：インド　Indian Statistical Institute, Kolkata
３）開催責任者：Bimal Roy(ISI Kolkata)、小谷元子(東北大学)
４）プログラム：別紙
５）対象：博士後期課程学生もしくは若手研究者(特に定義しない)　5名~10名
６）支給：旅費、滞在費を支給
７）締め切り：令和1年11月8日(金)
８）応募書類：履歴書、業績、志望動機（A4　1枚以内)、学生の場合は指導教員の許可書（様式自由、簡単なものでよい）
９）提出先：sec_kotanilab@grp.tohoku.ac.jp

セミナー主旨

Today's computer, both in theory and practice are based on classical physics. They are limited by locality and by the classical fact that systems can be in only one state at the time. However, modern quantum physics tells us that the world behaves quite differently. A quantum system can be in a superposition of many different states at the same time, and can exhibit interference effects during the course of its evolution. Moreover, spatially separated quantum systems may be entangled with each other and operations may have "non-local" effects because of this. Quantum computation is the field that investigates the computational power and other properties of computers based on quantum-mechanical principles with the apprehension that they might be able to solve some complex problems more quickly. With initial formalisation of a quantum computer by Yuri Manin, Richard Feynman, and Paul Benioff, complexity theory by Sanjeev Arora, it started gaining momentum after the development of Deutsch and Jozsa algorithm, providing exponential speedup over best known classical algorithm for the same problem. However, interest in the field increased

tremendously after Peter Shor's very surprising discovery of efficient quantum algorithms for the problems of integer factorization and discrete logarithms. Since most of current classical cryptography is based on the assumption that these two problems are computationally hard, the ability to actually build and use a quantum computer would allow us to break most current classical cryptographic systems, notably the RSA system. At the same time a quantum primitives of cryptography was also proposed by Bennett and Brassard.

To what extent will quantum computers ever be built? At this point in time, it is just too early to tell. The first small 2-qubit quantum computer was built in 1997 and in 2001 a 5-qubit quantum computer was used to successfully factor the number 15. Since then, experimental progress on a number of different technologies has been steady but slow. Currently, the largest quantum computers have a few dozen qubits. The practical problems facing physical realizations of quantum computers seem formidable. The problems of noise and decoherence have to some extent been solved in theory by the discovery of quantum error-correcting codes and fault-tolerant computing but these problems are by no means solved in practice. Moreover, while the difficulties facing the implementation of a full quantum computer may seem daunting, more limited applications involving quantum communication have already been implemented with some success, for example teleportation.