

## IMS Public Lecture

# Are Quantum Computers The Next Generation Of Supercomputers?

**Speaker:** Professor Reinhard Werner  
*Technical University of Braunschweig, Germany*

**Date:** Wednesday, 27 August 2008

**Time:** 6:30pm - 7:30pm

**Venue:** LT31, Block S16, Science Drive 1  
National University of Singapore

FREE ADMISSION

## About the Speaker

Professor Reinhard Werner was educated in Germany and the USA, at the universities in Clausthal, Marburg, and Rochester NY. He received his PhD in Physics at Marburg (1982), and the habilitation in Theoretical Physics at Osnabrück (1987). After some years in Osnabrück, he became Professor of Mathematics at the Technical University of Braunschweig in 1997, and very recently he accepted an offer from the University of Hannover. Professor Werner's research interests are the conceptual and mathematical foundations of quantum theory, including quantum statistical mechanics. More recently, he has become interested in Quantum Information theory. He is well-known for his many original contributions, in particular to the theory of entangled states. He is presently participating in a Session as part of the IMS Program on Mathematical Horizons for Quantum Physics.



## Abstract

Quantum Computers are said to outperform all classical computers, even the classical computers of the future. In particular, the standard public key encryption methods, which rely on the difficulty of factoring large numbers, could be broken on a quantum computer. In this talk, we will see how to make sense of such wild claims, and which features of quantum mechanics, the theory of atomic scale systems, enable such feats. We will also describe the current state of quantum technology, which still lags far behind the dreams, but has made remarkable progress in recent years. Quantum simulators, i.e., especially designed quantum systems, which simulate the dynamics of other quantum systems too complex for classical numerical methods, are singled out as the most likely candidate for the first quantum computer beating classical computers at a practically relevant task.

Jointly Organized by



Institute for Mathematical Sciences  
National University of Singapore

