The Math Colloquium
Department of Mathematics
San José State University

Wolfgang Polak

Factoring on a Quantum Computer

April 14, 2010, MH320

Abstract: All practical public-key encryption systems rely on the complexity of either factoring or discrete logarithms. Both problems can be solved efficiently on a quantum computer. Thus, once built, quantum computers can defeat most known digital security schemes.

This talk takes an axiomatic view of quantum mechanics to characterize quantum information, quantum state transformations and their use for computation. Peter Shor's polynomial-time factoring algorithm will be used to illustrate the unique features of quantum computation.

Background: First courses in linear algebra and abstract algebra.

About the speaker: Wolfgang Polak received his Ph.D. from Stanford in Computer Science and is working as an independent research consultant with expertise in programming language semantics, formal verification, program synthesis and machine learning. He has been dabbling in quantum computation for over 10 years and is currently finishing a textbook on the subject.

Snacks in MH331B at 2:30 pm
Talk starts at 3 pm

For more information, see our full schedule at:

`http://www.math.sjsu.edu/∼hsu/colloq/`