SAND2010-4957P

The Center for Cyber Defenders

Expanding Computer Security Knowledge

Quantum Error Correction

Kristin Cordwell, Princeton University; Sara Kimberly, Texas Tech University;
Susan Wade, Iowa State University
Project Mentors: Uzoma Onunkwo and Anand Ganti, 9336

Overview and Motivation:

- Unlike classical computing that is either in '0' or '1' state (bit), quantum computing allows for being in multiple states at the same time (superposition)
- Quantum computing promises efficient solution to "difficult" problems that has no classically efficient counterpart today (number factorization)
- Classical bits (0,1) replaced by Quantum bits or "qubits". Single qubits are represented as 2-element column vector, for example:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- Quantum computation are realized through "gate" operations. Similar to classical computing with such gates as AND, OR, NOT etc.
- The other types of quantum operation are the Preparation of qubits, and Measurement

Specific Technical Challenges:

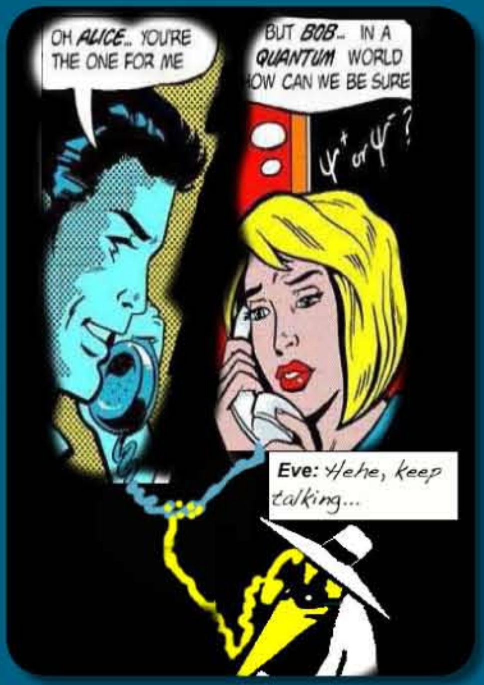
- *No cloning principle:* It is impossible to make a copy of unknown quantum state (qubits)
- Observing a qubit by measurement "alters" the qubit; measurement is an irreversible process
- Qubits in superposition of states have associated probability (not certainty) of yielding certain measurement outcomes
- Quantum computing are intrinsically prone to errors. Unlike classical computing with only two bits, there are infinite number of realizable qubits
- Scheduling of Quantum Operations (slide 10) - Hardware constraints must be considered in scheduling quantum computation for real systems since scheduling has significant impact on the ability to be fault-tolerant and the computation time.

Goals:

- Improve on threshold search confidence that currently uses Monte-Carlo simulation
- Provide faster simulation with tight lower bounds on threshold values

Impact and Benefits:

- Cryptographic revolution
- Instantaneous computation
- Exponentially less communication between computers to solve certain problems
- Quantum Teleportation
- Become leaders in the development of a fast-growing research area: quantum information science
- Demonstrate the realms of feasible fault-tolerant quantum computation
- Guide engineers and scientists in the design and development stages of realizing fault-tolerant quantum circuits



Algorithms and Applications:

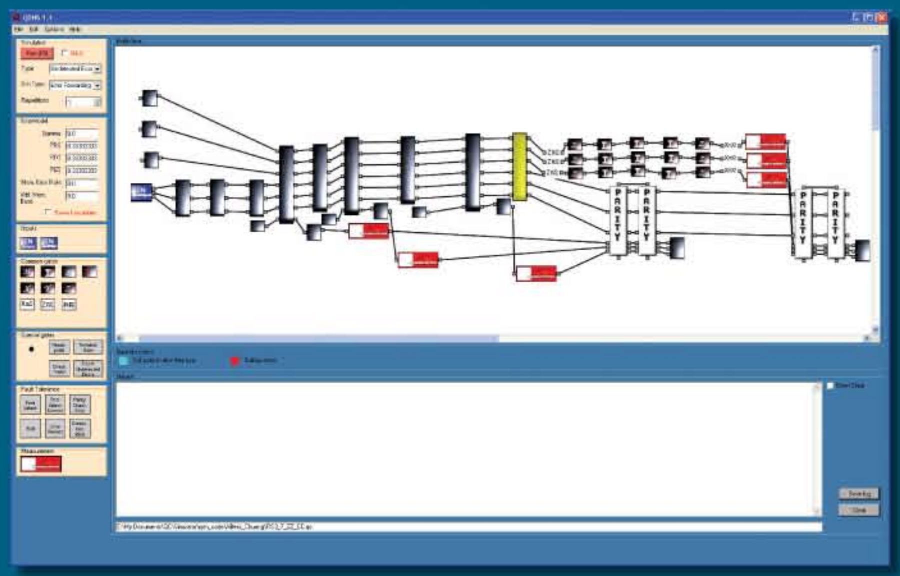
- Efficient factorization (Shor's Algorithm) which breaks prime number factorization-based encryption (e.g. RSA)
- Secure communication with Quantum Key Distribution which prevents eavesdroppers from intercepting private messages
- Polynomial time (efficient) solution to Pell's equation (x^2-dy^2=1) based on Hallgren's algorithm allows rational number representation of irrational square-roots

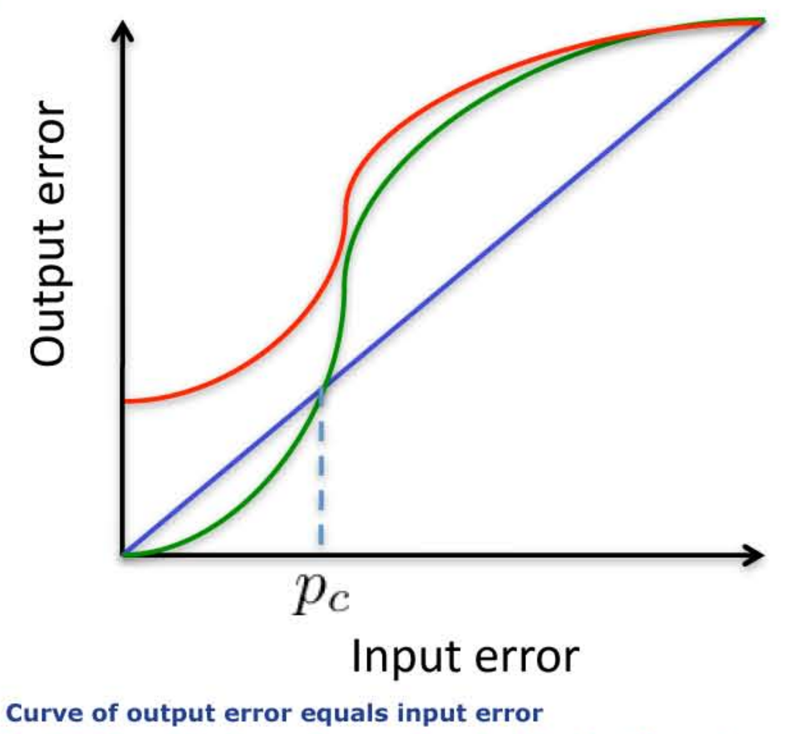
Example: set d=2, to obtain the fourth solution of (x,y) = (577,408)
$\sqrt{2}$ = 1.4142135… ≈ 577/408 = 1.4142156

No efficient classical solution is known to exist today

Simulation of Quantum Protocols:

Fault-tolerant protocols simulated for threshold search. Source code is written in MPI/C# and simulated efficiently (Gottesman-Knill theorem)





Curve of output error equals input error

Fault-tolerant scheme has no threshold under the noise model

Fault-tolerant scheme has a threshold (p_c) below which we can do arbitrarily long computation asymptotically error-free

Current Work:

- Verification of quantum gate schedules
- Exploring the implementation and underlying mathematical concepts of quantum error correction
- Comparing quantum accuracy thresholds using Monte Carlo and Counting Algorithms