

Quantum Information Science

Gerald Gilbert, PhD

732-935-5595 • ggilbert@mitre.org

MITRE Sponsored Research

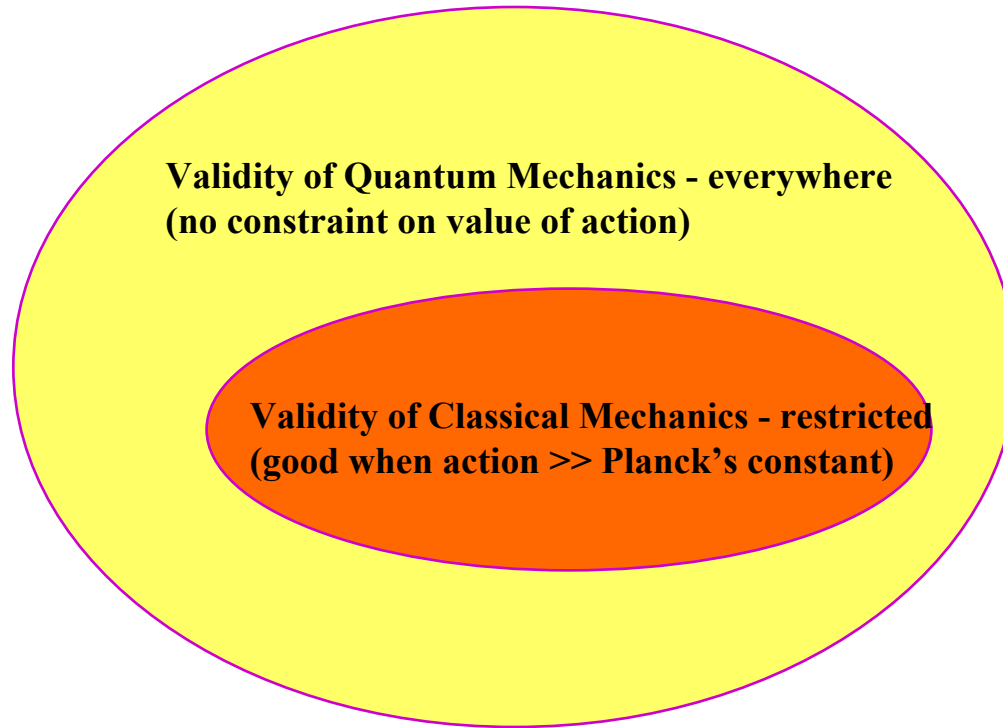
The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue to the left of the text.

MITRE
Technology
Program

Problem

- **Current cryptographic systems are only *provisionally* secret - improvements in computers and/or algorithms will break them.**
- **Quantum computers can solve problems that are effectively impossible to solve with classical computers.**
- **What is the fastest data transfer rate possible for a quantum cryptographic system? Can we design and build a system to achieve this?**
- **Can we discover new quantum computing algorithms?**

Background



Quantum Information Science exploits unique features of quantum mechanics to obtain results difficult or impossible to achieve with classical mechanical systems.

Objective

- In quantum cryptography our objective is to design, build and demonstrate the fastest working quantum cryptography system possible.
- In quantum computing our objective is to develop new quantum computational algorithms.
- This year we are extending the quantum cryptography system built last year to include multiplexing of data and free-space operation, and outside of the lab we are establishing further theoretical results leading to highest possible throughput rates.

Activities

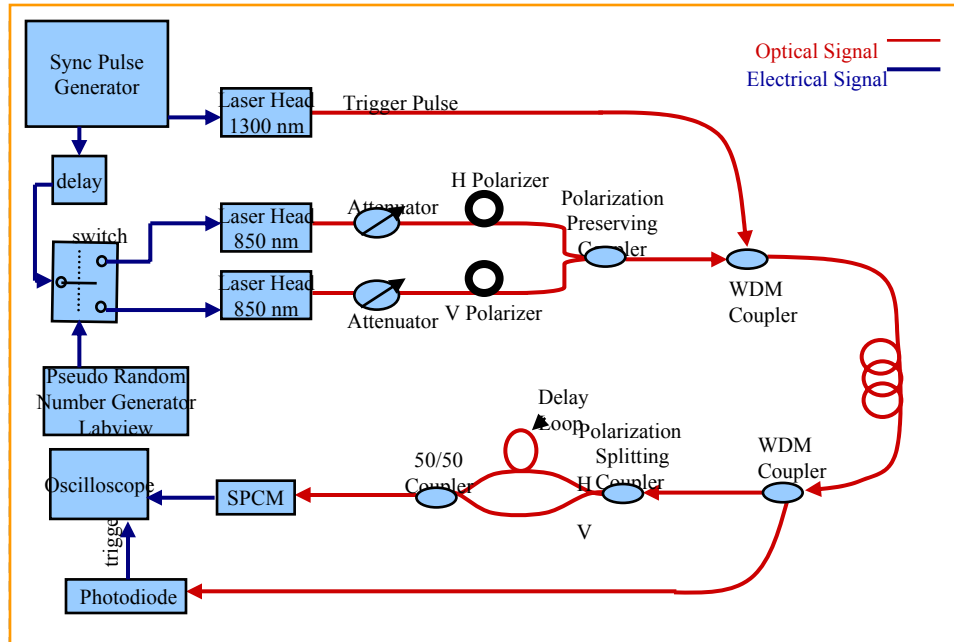
- **Laboratory demonstration of quantum key distribution with multiplexed transmission streams to increase throughput**
- **Comprehensive mathematical analyses leading to the quantification of entanglement in systems composed of many quantum bits. This will allow the construction of new quantum computing algorithms.**
- **Mathematically rigorous analytical studies of effective secrecy capacity and rate of fast quantum cryptographic systems**
- **Refinement of engineering design of ultrafast photon detection apparatus**

Highlight

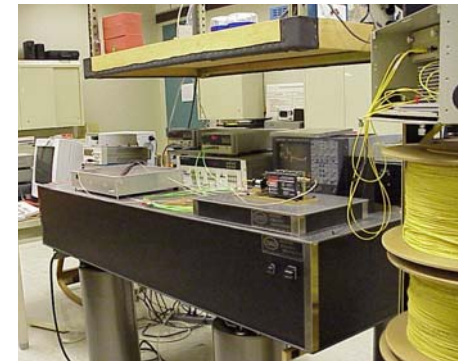
- 1) Alice sends: | | / - - \ - | - /
- 2) Bob sets: x + + x x x + x + +
- 3) Bob receives: / | - \ / \ - / - |
- 4) Bob tells Alice (publicly) what his settings were
- 5) Alice tells Bob (publicly) which settings were correct: 2,6,7,9
- 6) Alice and Bob keep those states correctly measured:
* | * * * \ - * - *
- 7) Using { | , \ } = 0 and { - , / } = 1 yields:
0 0 1 1 : the shared random key

A quantum cryptographic protocol (BB84) that allows undecipherable communications

Demonstration



QKD System Implementation



MITRE Quantum Cryptography Lab

Impacts

- **This work places MITRE at the very frontier of research worldwide.**
- **It will allow undecipherable communications at the fastest possible rate.**
- **It will find utility in national technical means applications.**
- **Intelligence community interest has been generated in the project.**
- **MITRE is now recognized as a leading player in this high-visibility research area.**

Future Plans

Quantum Cryptography SATCOM Networks

