

Quantum Cryptography - Modeling Completely Secure Key Exchange

Karl Heimbuck

Dr. Eric Moorhouse

Department of Mathematics

Wyoming EPSCoR

Quantum Physics

- Thomas Young - 1799
- Single emitted photon results in alternating pattern of light and dark spots
- Superposition
- Many-worlds interpretation


QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

Quantum Computers

- David Deutsch - 1985
- Operates in two states
- Spinning particles represent 1's and 0's
 - Particle represents 1 and 0 because of being in a superposition of states
- 250 particles would represent 10^{75} combinations (more atom than in the universe) or, in other words, calculations per second

Quantum Cryptography

- Alice sends a series of randomly polarized photons
 - Rectilinear Scheme X
 - $/ = 1, \backslash = 0$
 - Diagonal Scheme +
 - $| = 1, - = 0$
- Bob chooses randomly between the two schemes to read the photons

- 
- Alice and Bob call each other and find out when they used the same schemes during the transmission
 - They disregard any time they used separate keys
 - Key for a one-time pad

What about Eve?

- Quantum cryptography allows for completely secure key exchange
- Eve cannot intercept the key due to the laws of quantum physics
- Eve's presence on the line can be detected

The Model

- Created a program to simulate the transmission and call between Alice and Bob to find a key
 - 1) Choose Alice's binary sequence
 - 2) Choose Alice's schemes
 - 3) Choose Bob's schemes
 - 4) Simulate phone call and find a key

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

The End

- Thank you to Dr. Moorhouse and EPSCoR