



QUANTUM CRYPTOGRAPHY

*science
for the 21st
Century*

will involve more advances in quantum cryptography

Secrets, either creating them or protecting them, have always been a part of Los Alamos. Today, with advanced electronic communications and eavesdropping technologies the need to protect personal, financial, or national security information as it is transferred from place to place is even greater. As Los Alamos looks to the next millennium, researchers are exploring ways to use quantum cryptography to encrypt and transmit both classified and unclassified information. Quantum cryptography takes advantage of quantum physics theory to create what many believe are unbreakable codes.

Quantum theory explores interactions between electromagnetic radiation and matter. It differs from classical physics theory in that energy at the subatomic level is neither radiated nor absorbed continuously, but moves sporadically in multiples of discrete, indivisible units called quanta. These quanta, typically in the form of photons, units of light, are used in quantum cryptography in place of the ones and zeroes that make up binary number sequences in digital communications.

Los Alamos quantum cryptography uses photons randomly polarized to states representing ones and zeroes. Polarization refers to the direction of oscillation for the electromagnetic wave of a photon. These polarized photons are transmitted between sender and receiver to create a random string of numbers known only to the sender and receiver. This string of numbers becomes a quantum cryptographic key that locks or unlocks the encrypted messages that are sent via normal communication channels. Because the photons cannot be intercepted without tipping off the receiver, the quantum cryptographic key is secure and the data is secure.

In 1999, researchers at Los Alamos set a record when they sent a quantum key through a 31-mile-long optical fiber. While this distance is far enough to create networks connecting closely spaced government offices or local branches of a bank, at greater distances the signal loss in optical fiber increases until the photons are absorbed. For longer distances, Los Alamos researchers developed free-space quantum cryptography which allows codes to be sent through the air. Researchers have already sent free-space code transmissions over a distance of half a kilometer. This distance horizontally is roughly equivalent to the amount of atmospheric interference encountered between the Earth's surface and a satellite.

The challenge remains to develop the free-space technology for global communications networks by creating better ways to send quantum-encrypted information from the ground to satellites and around the globe. Los Alamos researchers are working on ways to fire the individual photons used to build the quantum cryptographic key through the atmosphere and hit a satellite circling the Earth.

From bank networks to satellite communications, research at Los Alamos in quantum cryptography will create very secure encryption technologies that have the potential to make many forms of electronic communications more secure.

CONTACT: Todd Hanson at tahanson@lanl.gov or (505) 665-2085. For more "Science for the 21st Century," go to <http://www.lanl.gov/orgs/pa/science21> on the World Wide Web.