



WINNER

2001 R&D 100 Awards Winner **Free-Space Quantum Cryptography**

Features

Secrets—diplomatic, military, and, increasingly, business secrets—must be exchanged secretly. To help with this important task, we have developed Free-Space Quantum Cryptography, a new system for distributing the random-number cryptographic "keys" used to encode and decode information. Users generate and share a key by sending and receiving single photons through open air or space over an insecure, high-speed laser communication channel. Each key permits secure exchanges on the same laser communication channel or over an insecure phone line, Internet connection, or radio link. The laws of quantum physics and information theory ensure that the keys will never succumb to computer attack and that attempts to steal or copy a key can be detected and foiled. For distances under 10 kilometers, key distribution takes less than a second.

Applications

Free-Space Quantum Cryptography provides secure communications

- in metropolitan areas—between banks, corporate offices, or off-site stock-trading centers and central stock exchanges;
- on the battlefield—between ground bases or land-, sea-, air-, or spacecraft; or
- between any two points on Earth, by using an intermediary satellite.

Benefits

- Enables secure day or night communications between any two users that can see each other or an intermediary station—in nearly any kind of weather.
- Thwarts any computer attack that can be launched now—or in the future!—unlike the systems now used for Internet transactions.
- Detects eavesdropping and continues secure transmissions despite it, thereby discouraging perpetrators.
- Permits absolutely secure domestic and international electronic fund transfers—now amounting to over \$2 trillion per day worldwide.
- Gives remote users secure access to broadband Internet nodes.