# Information protection by quantum encryption

Auto-disconnect does not allow data flow to continue circulating and alarming to network administrators whenever any intrusion is detected, even if it is simply a wiretapping, computer network due to Harvard University, Boston University and BBN Technologies research and development really promise the future of a super-secure network.

**Automatic shutdown does not allow data flow to continue circulating and alarming to network administrators whenever any intrusion is detected, even if it is simply "eavesdropping", network machine researched and developed by Harvard University, Boston University and BBN Technologies really promises the future of a super-secure network.**

Picture 1 of Information protection by quantum encryption

This project has the closest approach to the concept ***of real quantum coding system*** , using photon photons to lock and unlock the flow of information, instead of using the key with a random number sequence as shown. now on. Using light quantum technology, scientists can exchange data, email and visit other websites leisurely because their data is strictly protected.

Although the team is still exploring and studying the practical applications of super-security networks, one day, it will be able to replace the coding system currently used in most Internet security, shelter information activities of important government and financial agencies."It's really the technology of the future."- Harvard University scientist John M.Myers said - "Just like lasers and transistors, this technology will be widely applied even though people didn't even think it was feasible or used for it". .

**Quantum coding principle**

**Picture 2 of Information protection by quantum encryption**

Based on a physics principle, even photons used in quantum coding can cause subatomic particles to change and destroy the key code.

The root foundation of quantum coding comes from the "disposable code" system that spies often use during World War II.These are identical random number pages, each containing a different decryption and encryption key.Confidential information will only be clarified when the recipient has the same digital page as the sender.Similarly, on a quantum network, a laser will separate individual photons, sending them to a device named modulator.The modulator will "pump" them to other network nodes located on fiber optic cables.These photons are encoded when the modulator sends them at different distances and distances: a long distance represents one bit of information, a short distance refers to another bit of information.

At the receiving end, another device will receive photons and determine how they are modulated.If the information sequence corresponds to the original string sent, the key to the code will be saved and used to decrypt the data through conventional means such as the Internet.Any invasion or interference, even just "stealing" photons by sneaking a camera to read the code, will break the motion of the photon line, making the code impossible to use. use, and "ring the bell" to alert network administrators.

**What future for super-secure networks?**

Picture 3 of Information protection by quantum encryption

What future for real quantum coding?
This is not the first project to develop quantum coding. Previously, MagiQ Technologies once sold a similar system. Recently, a coalition group in Europe also conducted the first bank transfer transaction using quantum cryptography.

However, Boston and Boston's Boston Project, together with BBN, although only limited to these three locations, are still rated as the first Internet integration system that can run seamlessly among many other locations. each other and apart.

Every week, researchers meet at BBN.In the meeting room, a set of transmitters and receivers called "Alice and Bob" - took over two large tables, connected to each other through cables that fell down from the ceiling.They discussed the types of network worms, the problem of energy shortages and the process of developing new devices that complement the system.They even recruited a group of internal hackers who specialized in finding ways to invade the system.

Dr. Myer said this project involves a lot of central knowledge and doctrine of physics, but it is still too early to know exactly what its development direction is.It is possible that the super-security network will be put to commercial use, but right now, the cost and complexity of it will cause the user to limit the localization to customers "heavy bag. "Like big governments and corporations.

However, warnings by Carl J. Williams, a physicist at the National Institute of Standards and Technology, are also conducting independent research on high-speed quantum coding if scientists Only developing a personal quantum supercomputer, hackers will easily take advantage of it to break existing coding standards.

In theory, quantum computers can also become as popular as today's desktop computers.Moreover, there are no technical barriers to the widespread use of quantum encryption technology.For the scientific world, the problem is only "when" but not "if possible" anymore.

Quantum coding is based on a physical principle: subatomic particles can exist simultaneously in many different states before interacting with another. Therefore, even photons used in quantum coding can cause them to change and destroy the key code.