Reconfigurable free-space quantum cryptography system

Duke File (IDF) Number

IDF #:T-004964

Meet the Inventors

Gauthier, Daniel
Kwiat, Paul

Contact For More Info

Dardani, Dan
919 684 3311
daniel.dardani@duke.edu

Department

Physics

Background

Wireless transmission of many types of sensitive data to be transmitted wirelessly creates a problem of security with respect to access to that information. This is particularly important when the transmitted data includes HIPAA-protected medical data, bank data, military drone technology and military data. As an example of compromised security, Predator military drones have reportedly been hacked. The creation of unbreakable encryption technology is thus vital to protect sensitive data.

Quantum cryptography has been determined to be an unbreakable encryption technology, when properly implemented. Quantum cryptography has thus far seen a number of demonstrations, either using a fiber optic channel. or using a free-space optical channel. Unfornately, the drawback is that the sending and receiving nodes are fixed, and generally not particularly portable. This is fine if there are already optical fibers in place, but in many cases that would not be the situation.

Hence, all secure communications links that have been demonstrated have required that either a free-space link or a fiber link exist either between two nodes or between both of the nodes and a common relay. Methods for overcoming that limitation would be of great value.

Technology

A new invention directed toward solving the problem of creating an unbreakable encryption technology where the spatial relationship between two or more parties is reconfigurable. It is a system, and methods, for transmitting quantum states between a first node and a second node, or among more than two nodes. Each node is characterized by an instantaneous spatial position, and the instantaneous spatial position of the second node is repositionable within a frame of reference associated with the first node. A hovering drone is adapted either for running a quantum key transmission protocol in secure communication with the first node, and/or for running a quantum key reception protocol in secure communication with the second node. Either drone may serve as a relay of optical data between a base station and another drone. Secure communication among more than two nodes may be reconfigured. This technology may enable quantum cryptographic links to be readily established, e.g., on the battlefield, between branches of a bank, between two drones, or even between residential users and a central communication hub.