IAA-04-IAA.1.1.1.10

QUANTUM OPTICAL CRYPTOGRAPHY AND SETI

Walter Simmons

Department of Physics and Astronomy, University of Hawaii, Honolulu, HI 96822 USA
Phone: +1 808 956 2969; Email: WAS@Phys.hawaii.edu

Motivated by security concerns, advanced civilizations may turn to quantum cryptography for optical data links over interstellar distances, thus avoiding leakage radiation might otherwise attract unwelcome hostile attention. Such applications require techniques that go beyond most cryptographic systems in use today, for at least two reasons. First, is the fact that it is the very existence of the transmission, which must be concealed, not just the content of the messages. Second, transmissions may go on for long periods, thus giving an eavesdropper an enormous amount of data from which to extract a hint of signal.

My colleagues and I have reformulated the theory of direction-finding (of electromagnetic radiation in free space) upon a quantum mechanical basis. We have developed several model quantum communication systems which are highly resistant to direction finding, (i.e. to triangulation, for point sources), in noisy environments.

A traditional cryptographic technique turns a message into a pseudo-random stream of bits, which can be deciphered only if one has the key. A potential weakness in high volume communication situations is that an eavesdropper, with enough data and enough computing power, may guess the key. Moreover, the transmission of the message, itself, even if not deciphered, discloses the location of the transmitter. Quantum cryptography operates at a deeper and more secure level. In quantum optical cryptography, the bits are represented by quantum correlations between two separate beams of light. The light in each beam contains no bits, or physical structures that represent bits. No amount of analysis of one beam will disclose bits that are simply not there. It is only when the two beams are combined, that the bits come into existence. The essence of quantum mechanical direction cryptography is to make it impossible to both read the bits and to discern the direction from which they came. Two features of quantum states of light that make this possible are (1) the impossibility of copying the states, and (2) the fragility under measurement. Because of these properties, it is not generally possible to triangulate a signal.

An advanced civilization may communicate internally using the methods, which we shall describe, or they may broadcast beacons, which are difficult or impossible to locate from the signal alone.