RJPHY Research Journal of Physics

OPEN ACCESS

News & Comments

Quantum Cryptography: A basic Undergraduate Experiment and Simulation

Harpreet Singh

Nowadays, private communication is extremely important, which is driving up the demand for creating secure message delivery techniques. At the heart of cryptography is secret key encryption, which enables secure message exchange across a public channel in the presence of a possible adversary. Its protocols display anonymous messages that can only be read by the sender and recipient, guaranteeing that an encrypted message sent via a public channel is unreadable by outsiders. Prior to the advent of the digital age the main goal of cryptography was to transform messages into unreadable forms that could not be read by interceptors. These days, the field has extended to include secure computing, integrity checking, and identity authentication in addition to military and communication secrecy. A fundamental tenet of quantum physics stipulates that a photon's state must change when it is measured. It is impossible to copy an information bit carried by a single photon in a particular state without changing its state. Quantum key distribution (QKD), which uses quantum communication to create a shared key between two users without letting a third party learn anything about it, is this type of quantum cryptography. The one-time pad is a classical encryption scheme that, in theory, is 100 percent secure and that uses quantum mechanics to help it achieve its requirements. The eavesdropper needs the key to decode the communication if the encrypted message is intercepted; else, the random sequence cannot be interpreted. Since the experimental system's light source is a pulsed laser rather than a single photon source, interception cannot be completely prevented. The system's collimated laser diode module is a Thorlabs CPS635R type with a 635 nm, 1.2 mW, Gaussian profile beam. A Python script was created for the simulation of the BB84 protocol using modules like NumPy, endecrypt, and more to compare the experimental findings with the theory. The implementation of a cryptographic protocol using elements of quantum mechanics is known as quantum key distribution. It allows two parties to generate a secret shared key that is only known to them and can be used to encrypt and decrypt messages. For more information on the general functions of the simulation and the code, see Appendix A. People can find the complete script on GitHub under available materials. When an eavesdropper is present, the code executes a sequence to determine whether Eve is eavesdropping using bits that are selected at random, if the bases selected by the corresponding units are different. For the investigation of each sequence's complexity, the average simulation running time was determined for ten different executions and recorded.

Source: Physics

KEYWORDS

Quantum, key, distribution, cryptography