System for Transmitting Quantum-Random-Generated Data via Light

FIELD OF THE INVENTION

The present invention relates generally to the transmission of quantum entropy via a detachable light transmitting device to allow for the transmission of two or more random binary digits. More specifically, the present invention discloses wireless systems that allow the transmission, via a detachable light transmitting device, of true random numbers generated from a hardware random number generator.

BACKGROUND OF THE INVENTION

In computing, entropy refers to the randomness of data collected from hardware sources in a computing system which can be used in applications that require the use of random data. For example, a hardware random number generator, true random number generator, non-deterministic random bit generator, or physical random number generator utilizes entropy to generate random numbers that are non-deterministic and non-probabilistic. A hardware random number generator is expected to output near-perfect random numbers, which can be referred to as using "full entropy.” On the other hand, a Pseudorandom Number Generator (PRNG) is a deterministic random bit generator that utilizes a deterministic algorithm and non-physical nondeterministic random bit generators that do not include hardware dedicated to generation of entropy. Conventional cryptography may generate a cryptographic seed-key based on numbers generated by a pseudorandom number generator. However, numbers generated by a pseudorandom number generator may eventually repeat. Once repetition occurs, a party monitoring communication may exploit the repetition to decipher the cryptographic key and decrypt encrypted communications.

Other communication technologies have been developed to minimize the risk of exploits due to vulnerabilities in data encryption using PRNGs. Light Fidelity (Li-Fi) is a technology that can be used to transmit information wirelessly through light. Li-Fi transmits bits of information by rapidly starting and stopping light signals in a manner that is imperceptible to human eyes. Li-Fi transmits at the speed of light in a manner like fiber optic cable. In general, Li-Fi works by switching the power current of the light source "Off" (0) and "On" (1) at a very high speed. Although Li-Fi light sources are kept on while transmitting data, these Li-Fi light sources can be dimmed below human visibility while still emitting enough light to carry data. In addition, the light waves cannot penetrate walls, which translates to a much shorter range, and a lower hacking potential. A direct line of sight is not necessary for Li-Fi to transmit a signal as the light can be reflected off surrounding surfaces. Further, Li-Fi can transmit data via visible or infrared light waves.

SUMMARY OF THE INVENTION

The present invention provides novel and unique means that facilitate the transmission of encrypted data using Light Fidelity (Li-Fi) and quantum-based cryptography. A method of the present invention utilizes a first computing device that generates quantum seed-key encrypted data, which may include two or more binary digits. The quantum seed-key encrypted data is relayed to at least one light transmitting device which transmits the data, via Li-Fi, to at least one optical receiver. The at least one optical receiver can be integrated into various computing devices or can be provided as an accessory that can be connected to the desired computing device. Further, the cryptographic seed-key generated can be based on quantum shot noise and can further include information regarding at least one key to be inserted into WPA, WEP, AES, or other standard encryption schemes.

Furthermore, the first computing device is preferably designed to generate non-deterministic, non-probabilistic data. The first computing device can include a true random number generator device to generate random numbers based on quantum shot noise. The first computing device accesses data and a seed-key including random numbers generated by the random number generator. Further, the first computing device can access information regarding at least one key to be inserted into the standard encryption used in the information data stream.

Furthermore, the present invention can include a cryptographic key with an entanglement key based on the information regarding authorization to view the data. The first computing device is further configured to encrypt the cryptographic key using one or more keys related to an enterprise to produce an encrypted cryptographic key and encrypt the data for transmission using the cryptographic key to produce encrypted data for transmission. The first computing device is arranged to relay the encrypted cryptographic key and the encrypted data for transmission to the at least one light transmitting device that is configured to transmit, via light, to the at least one light receiving device arranged to provide the encrypted cryptographic key and the encrypted data to a respective physically connected second computing device for decrypting.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an illustration of the present invention showing quantum encrypted data being wirelessly transmitted to a computing device via Li-Fi.

FIG. **2** is an illustration of the present invention showing a plurality of light sources being wirelessly controlled from a single switch.

FIG. **3** is a schematic view of the present invention.

FIG. **4** is a schematic view of the present invention, wherein the present invention is shown interfacing with a secondary computing device.

FIG. **5** is a schematic view of the present invention, wherein the present invention is shown interfacing with an Internet provider feed to enable the wireless connectivity of computing devices in a location via Li-Fi.

FIG. **6** is a flowchart showing an exemplary method of connecting to the system of the present invention from a computing device.

DETAIL DESCRIPTIONS OF THE INVENTION

All illustrations of the drawings are for the purpose of describing selected versions of the present invention and are not intended to limit the scope of the present invention.

The present invention provides a novel means for transmitting quantum-random-generated data via light. As can be seen in FIG. **1** through **6**, the present invention utilizes Light Fidelity (Li-Fi) and quantum-based cryptography to convert a light source into a quantum entropy source. The present invention can generate an endless stream of quantum random numbers that are used to fuel software applications, act as independent encryption devices, and/or create un-hackable passwords. The greater the number of light sources connected to the network, the stronger the quantum entropy (randomness) in the system. In the preferred embodiment, the present invention comprises at least one light source, a Quantum Random Number Generator (QRNG), and at least one transmitter. The at least one light source serves to facilitate the transmission of data via light. Li-Fi is the preferred means to transport the data generated by the system. However, in other embodiments, other light-enabled wireless communication technologies can be implemented into the system. The QRNG serves to randomly generate a plurality of quantum bits (qubits) for the safe transmission of data. Further, the plurality of qubits generated by the QRNG can include, but is not limited to, at least three qubit values. The at least one transmitter enables the transmission of the plurality of qubits to at least one optical receiver using light from the at least one light source as a carrier. The at least one optical receiver is preferably configured to establish encryption and decryption keys based on the received plurality of qubits.

Conventional encryption resets after a specific number of characters or bits. On the other hand, the present invention generates a quantum stream that can run endlessly without restarting. As can be seen in FIG. **1** through **6**, the present invention can be provided in an enclosure that can be attached to the at least one light source or be part of the at least one light source structure. The QRNG and the at least one light source are preferably electronically connected to the at least one transmitter in such a way that the random data generated by the QRNG is relayed to the at least one transmitter for wireless transmission to the target at least one receiver using the at least one light source. Further, the QRNG and the at least one transmitter can utilize the power from the at least one light source for operational purposes. So, the QRNG and the at least one transmitter can be electrically to the power source of the at least one light source. Further, the QRNG and the at least one transmitter can be mounted within the enclosure to protect the electronics from the surroundings. In other embodiments, the present invention can provide a separate power source to operate independent from external systems.

As previously discussed, the present invention allows for the transmission of quantum encrypted via the light emitted by the at least one light source. As can be seen in FIG. **1** through **6**, the present invention can further comprise at least one encoder to convert the plurality of qubits having the respective qubit values to the appropriate format for transmission. The at least one encoder can be integrated into the at least one transmitter or provided as a separate component that is electronically connected to the at least one transmitter and the QRNG. In addition, the present invention may further comprise at least one modulator to further facilitate the wireless transmission of the quantum encrypted data. The at least one modulator is preferably a chip-based optical modulator to modulate the randomly generated plurality of qubits and the corresponding values. The modulation of the plurality of qubits allows for the transmission of data using the at least one light source as a series of light flickers that are imperceptible to human eyes. Like the at least one encoder, the at least one modulator can be integrated into the at least one transmitter or provided as a separate component that is electronically connected to the at least one transmitter and the QRNG. Furthermore, the at least one transmitter can be configured to interface with external computing devices. For example, the at least one transmitter can be designed to interface with an Arduino computing device. In other embodiments, different components can be integrated to further facilitate the wireless transmission of quantum encrypted data using Li-Fi.

In the preferred embodiment, the present invention can support modulation rates in the range of 38400 to 115200 bits per second. The system can also support Universal Asynchronous Receiver-Transmitter (UART) communication and can wirelessly transmit data from a height range of 6 to 15 feet. Furthermore, the present invention can accommodate the transmission of quantum encrypted data in binary or hexadecimal. This allows the present invention to be applied to different applications. For example, the present invention can be utilized for security applications, in Electromagnetic Interference (EMI) sensitive environments, Augmented Reality (AR) applications, localized advertising, underwater communication, safety environments, intelligent transportation systems, indoor navigation, dense urban environments, etc. Further, dense urban environments by nature tend to have complete artificial lighting coverage. This lighting infrastructure can provide always available high data rate access for users moving through that environment.

As previously discussed, the present invention can include at least one optical receiver that can capture the wirelessly transmitted data generated by the system via the light emitted by the at least one light source. As can be seen in FIG. **1** through **6**, the at least one optical receiver is preferably a portable accessory that can be plugged into the desired computing device in order to receive the transmitted quantum encrypted data. For example, the at least one optical receiver can be provided as a Universal Serial Bus (USB) compatible device that can be plugged into a USB port of a portable computer, such as a laptop. In order for the at least one optical receiver to process the plurality of qubits with respective qubit values encoded in light from the at least one light source, the at least one optical receiver may comprise at least one demodulator, at least one decoder, and at least one key generator. The at least one demodulator is designed to demodulate the light signals from the at least one light source to recover encoded qubits. The at least one decoder helps recover the captured qubits to produce the respective qubit values. Further, the at least one optical receiver may include a key generator to generate encryption/decryption keys based on the produced respective qubit values. In addition, the generated encryption/decryption keys for encryption and decryption of data is provided only while light including the qubits is being received by the optical receiver.

In some embodiments, the generated encryption/decryption keys can be valid only during a predefined time interval. This increases the protection of the transmitted data from the at least one transmitter to the at least one optical receiver via the light emitted by the at least one light source. Furthermore, the generated encryption/decryption keys can be valid only during a specified time interval, the specified time interval being encoded in the received light as a second plurality of qubits having respective qubit values. In other embodiments, different security protocols can be implemented to prevent unauthorized access to the transmitted data from the at least one light source.

In some embodiments, the present invention can be implemented to enable the wireless transmission of quantum encrypted data via Li-Fi to target computing devices in a facility. For example, the present invention can enable computing devices in a residential or commercial facility to connect to the Internet using the system of the present invention. In this embodiment, several light sources are installed throughout the facility in target areas where the computing devices are utilized. As can be seen in FIG. **1** through **6**, the several light sources can be wirelessly controlled from at least one switch to enable authorized users to monitor the usage of the present invention. Further, the several light sources can be designed to emit light in different wavelengths so that the light sources can emit visible light to illuminate the target area or emit light invisible to the human eye (e.g., infrared light) to wirelessly transmit the quantum encrypted data. Further, the system of the present invention can be directly connected to the Internet service provider's utilities. For example, at least one demodulator can be connected to the Internet feed line to convert the data that is relayed to a controller. The controller is connected to the QRNG to quantum encrypt the data that is relayed to the transmitter of each light source installed in the building. Further, the controller and the QRNG can be connected to the facility's power supply. A switch control can be further provided to directly control the operation of the controller and/or the QRNG. Further, one or more switches can be installed throughout the building to enable users to control the light source emitted from the desired light sources as well as to activate/deactivate the transmission of the quantum encrypted data through the desired light sources. In other embodiments, the system of the present invention can be modified to specific applications that need different data transmission requirements.

In some embodiments, the present invention can further provide a software application to enable users to interact with the system of the present invention via the desired computing device. For example, the software application can be provided as a computer application that can be installed on a portable computer or desktop computer that needs to be connected to the Internet using the system of the present invention. As can be seen in FIG. **6**, once the necessary light sources are installed in the target locations, the user can connect the at least one optical receiver to the computing device. Using the User Interface (UI) of the computing device, the user can proceed to sign in or create an account that enables the user to access the system of the present invention. Afterwards, the user can select the port connected to the at least one optical receiver so that the user can connect to the near light source (Li-Fi source) with the at least one optical receiver. Once connected, the user can obtain the necessary quantum keys to access the quantum encrypted data transmitted from the Li-Fi source to the at least one optical receiver. Then, the user can test the connection by partially blocking the light source. In other embodiments, different systems can be provided to help users connect to the system of the present invention according to the application's security requirements.

Although the invention has been explained in relation to its preferred embodiment, it is to be understood that many other possible modifications and variations can be made without departing from the spirit and scope of the invention.