Iraqi Journal of Information and Communications Technology(IJICT)
Vol. 6, Issue 1, April 2023
www.ijict.edu.iq
ISSN:2222-758X
e-ISSN: 2789-7362

EXPERIMENTAL REALIZATION OF QUANTUM CRYPTOGRAPHY BY ARDUINO

Harith A. Qaisi [1], **M. F. Al-Gailani** [2]
[1,2] College of Information Engineering, Al-Nahrain University, Baghdad, Iraq
harith.ahmed@coie-nahrain.edu.iq [1], m.falih@nahrainuniv.edu.iq [2]
Corresponding Author: M. F. Al-Gailani
Received:26/12/2021; Revised: 11/02/2022; Accepted:22/02/2022
DOI:10.31987/ijict.6.1.204

***Abstract*- This paper is concerned with the experimental realization of an Arduino-based quantum cryptography system, in which a setup of five laser diodes is constructed in the transmitter that randomly emits photons to encode information consisting of a sequence of "0" and "1" bits. The receiver contains five photoresistor sensors that detect the presence or absence of light as well as determine the intensity of the light. Laser light is used to securely transmit data, such as text or numbers, in this technology.**

keywords: **Arduino, Photoresistor, Laser Diodes, Quantum Cryptography**

I. INTRODUCTION

Quantum cryptography uses quantum physics to provide information security [1]. Two phases are usually included in secure communication between two parties. To begin, a key is shared between them. Second, the key is used to encrypt messages between parties. Classical cryptography relies on either "safely" distributed symmetric keys (e.g. via smart cards) or computational complexity (e.g. factorization), and trusting the courier is required, or it can be undermined by greater computer power or quantum techniques. However, quantum cryptography addresses these flaws by providing a framework based on quantum physics for determining if a potential adversary has gathered enough information to threaten the secrecy of distributed keys. In 1984, Bennett and Brassard devised a method for safely distributing symmetric keys between two parties [2]. The security is based on the no-cloning theorem, which states that an eavesdropper cannot duplicate an arbitrary unknown quantum state.

This paper aims to illustrate the implementation of quantum cryptography by Arduino. The data is communicated between two computers using laser light, which is a form of quantum cryptography based on photons. On the transmitter side, a setup of five randomly operating laser diodes was developed to emit photons. At the receiver side, five light-dependent resistors (LDR), photoresistors, are configured as an array of these photoresisistors [3].

II. RELATED WORK

Recently, quantum cryptography has been developed as a new technique for protecting sensitive data throughout the transmission process in a new networking environment. Several academics have collaborated in developing secure file communication based on various simulation criteria. Ryabtsev et al., in 2017 [4]The dependence of the rate of quantum key distribution on the average number of photons in a laser pulse is studied experimentally and theoretically, and the results are reported. Using atmospheric and fiber optic experimental setups, the experimental data for a quantum key distribution based on the BB84 protocol were collected. Singamaneni et al., in 2018 [5] Quantum cryptography takes advantage of

ISSN:2222-758X
e-ISSN: 2789-7362

photon polarization to provide the highest level of security assurance. The distribution of a quantum cryptographic key requires sharing the key with photons and their polarization property, resulting in a secure key that notifies the user of eavesdropping attempts. The implementation of a quantum key distribution mechanism is very difficult and expensive. The experimental setup for this article is suitable for photon streams. The laser light generates a stream of the photon, which is then polarized by a stepper motor controlled by the Arduino. The light is transmitted from the transmitter to the receiver via an optical fiber line.

On the receiver side, a light-collecting photodiode is used[6]. Martelli et al., in 2019 The usage of a Faraday rotator variable over four states and a single SPAD (single-photon avalanche photodetector) is used to build the BB84 protocol for QKD at a low cost [7]. Salih et al. created and tested a true random TTL pulse generator for use in quantum key distribution systems. Cheap local-market components generate random TTL signals. TTL signals are generated by comparing the photon arrival times in two coincidence windows of a single-photon detector. The operation of the true random TTL pulse generator was tested using digital converters time, which gives correct photon time values. The recommended authentic random pulse TTL generator can be used in any quantum key distribution system to ensure that the transmitters do not operate erratically. Abbas & Abdullah, in 2021[8] Using Field Programmable Gate Arrays, this study proposes a new hardware implementation of the quantum key distributed cryptography protocol (FPGA). The software implementations of key distribution techniques are slow and inefficient in many security applications. A novel hardware architecture was developed to speed up the performance and flexibility of key distribution algorithms to tackle these challenges. Using a high-speed integrated circuit hardware description language (VHDL) (an efficient hardware architectural model for the quantum key distribution protocol) was constructed. This gadget is designed to distribute the secret key safely using any quantum key distribution methodology. The hardware was built and tested on a Spartan-3 FPGA board, yielding an 8 Mbps throughput and a 1.6 Mbps/slice efficiency.

From the literature above, it may be deduced that a variety of technologies could be utilized to implement quantum cryptography. Some of these studies have some limitations, such as equipment, devices, and cost. The proposed work varies from previous works in that it implements quantum cryptography by Arduino, sends data through laser light, provides secure transmission, and no one can listen to the information except the relevant receiver because it uses end-to-end encryption. This transmission process is characterized by a speed that varies from milliseconds to seconds.

III. IMPLEMENTATION TOOLS

A. Arduino Uno

The title "Uno" means "one" in Italian and was chosen to represent the upcoming release of the Arduino 1.0 platforms. Arduino "Uno" is a microcontroller. It consists of; 14 digital output ports, 6 analog inputs, a 16 MHz crystal oscillator, a USB connector, and an ICSP header. The Uno board does not have an FTDI USB serial driver chip, which limits their use and could be a big distinction. However, Arduino Uno has a USB-to-serial converter. Although a variety of USB Arduino boards are available, Uno is the only intended as a reference model for the Arduino platform

ISSN:2222-758X
e-ISSN: 2789-7362

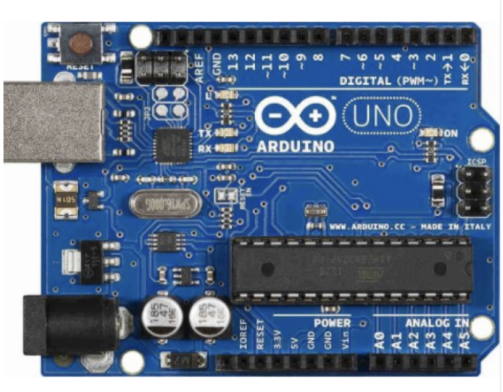

Figure 1: Arduino Uno board from (Sanni et al., 2019)

For safety purposes, a fuse is built into Arduino Uno board to protect the computer's motherboard from excessive electricity flowing via the USB port. If the current exceeds 500 mA, the fuse opens (closes) the connection. When the current returns to safe levels, the resettable fuse closes (turns on) the circuit.

TABLE I
Specifications of the Arduino Uno

Voltage	5 V
Clock speed	16MHZ
I/ O pins	14
Flash memory	32kB
SRAM	2 KB
EEPROM	1 KB

B. Laser Diodes

Lasers are devices that produce coherent light of certain wavelengths using stimulated emission of radiation. The term laser is an acronym for "light amplification by stimulated emission of radiation". As a result, several types of lasers can be generated using various procedures. These methods are Gas and chemical lasers, solid-state lasers, fiber lasers, free-electron lasers, and p-n junctions diode lasers. Diode lasers are semiconductor devices [10][11] that use p-n junctions of semiconductor diodes to generate coherent light. Because of their small size, low power consumption, and low cost of manufacture, diode lasers have become the most popular lasers in the world. The "threshold current," "slope efficiency," and "characteristic temperature" of diode lasers all have an impact on their performance. Lasers are extremely useful for long-distance communication due to the little divergence of their light compared to LED lights. Since the efficiency of the laser is strongly reliant on temperature, a diode laser used for extended periods of transmission of massive amounts of data must be extremely resistant to process-induced overheating. Telecommunication systems benefit from finding a laser with a low threshold current at high temperatures [12][13].

ISSN:2222-758X
e-ISSN: 2789-7362

C. *Photoresistors*

A photoresistor is defined as a "variable resistor whose resistance varies inversely with the intensity of the light." Willoughby Smith discovered the photoconductivity of selenium in 1873, which led to the creation of the photoresistor. The photoconductive devices were then manufactured in a variety of shapes and sizes. It is a photosensitive sensor that changes resistance based on how much light it is exposed to. It is used in optical systems. At lower light levels, the resistance is higher, while at higher light levels, the resistance is lower. It consists of an upper layer of photosensitive resistive material that encapsulates the photoresistor. Light-sensitive material with metal connectors at both ends. A semiconductor layer would be a good analogy for this component. Under this semi-insulated substrate, it is usually ceramic.

IV. EXPERIMENTAL IMPLEMENTATION

A. *Overview*

The software is designated to transmit information between sender and receiver using laser light. This information may be text or a number without any limit on the message length. Figure 2 depicts the major components of the proposed system.

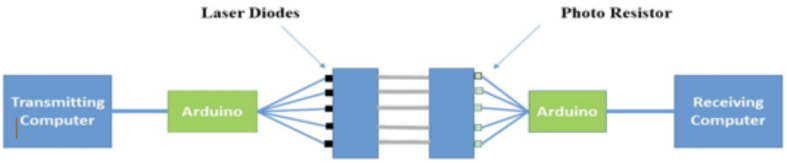

Figure 2: Block diagram of the proposed system

The suggested system includes two Arduino Unos, one on the transmitter side and the other on the receiver side, in addition to the laser diodes and photoresistors.

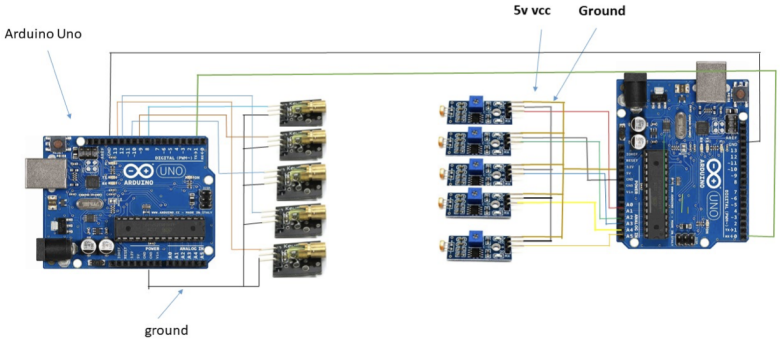

Figure 3: Circuit diagram of the proposed system

ISSN:2222-758X
e-ISSN: 2789-7362

B. Sender side

Five laser diodes are connected to the Arduino Uno chip on the sender side. Four of these lasers were used to transmit data, while the fifth was utilized as a buffer for additional data from the other four lasers. This effort helps improve the accuracy and speed with which information is transmitted. The five lasers are connected to pins $8, 9, 10$, 11, and 12 of the Arduino chips, as shown in Fig. 4. Data encryption of information consisting of 0's and 1's is achieved by using lasers that randomly produce photons on diagonal and rectilinear bases. This process is accomplished by end-to-end encryption.

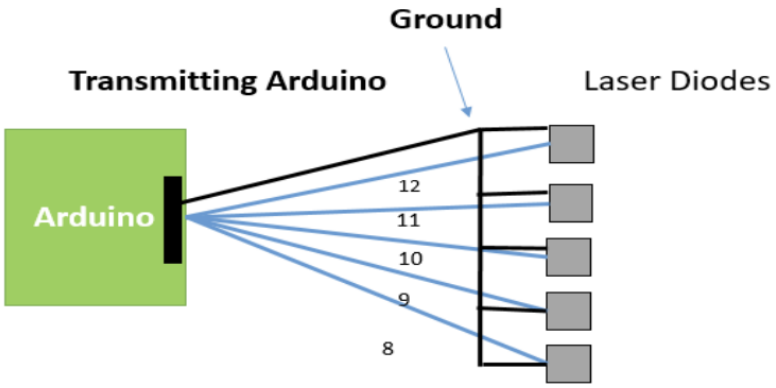

Figure 4: Block diagram of the transmitter side.

C. End to end encryption

The main advantage of end-to-end encryption is to protect the data from being intercepted by anyone other than the intended recipient. End-to-end encryption ensures that the communications channel remains private. Making an impenetrable chest is tough in the physical world, but it was much easier in the information world. Experts are constantly working to develop new encryption methods and improve the security of the existing ones. Another advantage is that end-to-end encrypted transmissions can only be decrypted by the intended recipient; the message cannot be altered. This ensures that people's conversation is not disturbed. If the communication is decrypted, the matching message can be confirmed and transmitted, ensuring that it has not been tampered with in any manner. Hybrid encryption can be employed to efficiently encrypt the message. Thus, the message is encrypted using a symmetric key algorithm, such as AES. Then the receiver's public key is used to encrypt the AES key used. After that, the encrypted message will be received as well as the encrypted AES key. Then the recipient uses the private key to decrypt the AES key and then uses the received AES key to decrypt the message.

D. Receiver side

Five photoresistor sensors on the receiver side are used to convey the presence or absence of light or to quantify the intensity of light. In the dark, their resistance was rather high, sometimes reaching a million ohms, but when exposed to light, the resistance dropped considerably, sometimes to only a few ohms, depending on the strength of the light. LDRs

ISSN:2222-758X
e-ISSN: 2789-7362

are nonlinear devices with a sensitivity that varies with the wavelength of the light used. These sensors are linked to pins (8, 9, 10, 11, and 12) of the Arduino receiver chip as shown in the Fig. 5.

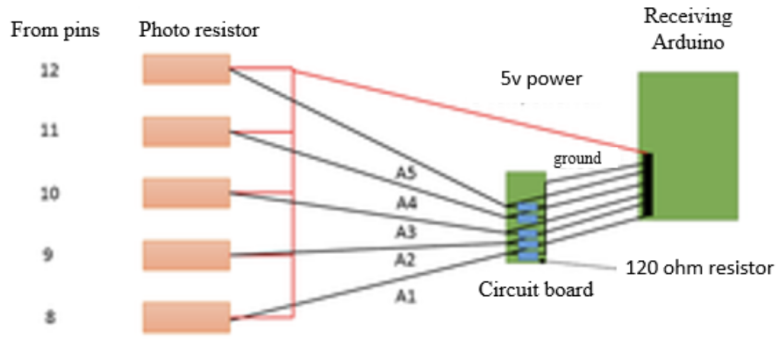

Figure 5: Block diagram of receiver side

The output of the LDR is connected to a circuit known as a voltage circuit divider, which is a simple circuit for decreasing voltage. It disperses the input voltage among the circuit's components. The finest example of a voltage divider was two resistors connected in series, with the input voltage applied across the resistor pair and the output voltage measured at a position in between. It was used to generate variants of voltage levels from a single voltage source while keeping all components in a series circuit at the same current. This point could pose a question, the "photoreresistor." was already a "resistor" and therefore would limit the circuit voltage. Why it is not possible to connect this with a pin and measure it? The simple answer was that the Arduino could easily measure voltage, but not resistance. Variable resistors have been used in the majority of sensors, including photoresistors, flex sensors, and thermistors. The Arduino and "most integrated circuits" feature a modest analog-to-digital converter (ADC) system, which makes it difficult to monitor resistance changes. This technology turns analog voltage changes into 1 s and 0s sequences that can be translated into an integer. Since the ADC is designed to read voltage changes, it is required to convert resistance changes into voltage changes to read the photoresistor values using the Arduino's analog readout (which uses the ADC). The easiest way to achieve this was by using a voltage divider. Since the sensor was a resistor, the voltage across it should vary. There were no other reference points besides Vcc (5V) and ground, thus, measuring voltage changes would be tricky. The photorexesistoris also has a maximum current rating; a series resistor will help limit the current flow under intense light. As shown in Fig. 6.

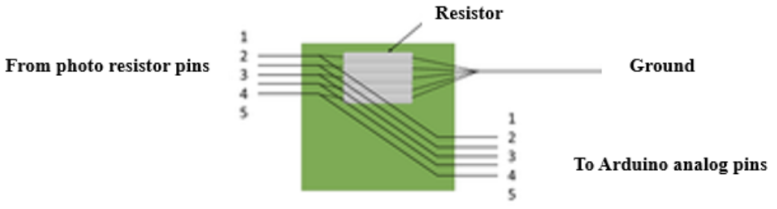

Figure 6: The voltage circuit divider

ISSN:2222-758X
e-ISSN: 2789-7362

V. RESULTS OF IMPLEMENTATION

Before running the system, it should be tested. First, the transmitter is connected to the COM3 port, which is a communications channel on the computer that allows data to be transmitted from linked hardware devices to the processor. Then the Arduino program is launched and a serial monitor is selected to check the connectivity if it is ready to start as shown in Fig. 7. After checking the system, it starts sending information from the transmitter to the receiver. This information may be text or numbers and is not sensitive to lowercase or uppercase. When begin sending information by flashing the laser light to the photoresistor in the receiver, the receiver decrypts it and shows it. The time to transmit information is less than a second and may increase depending on the size of the message. Figure 8 shows how sentences can be sent and received through the software, and the time is about 47 msec with a bit rate of 9.6 kbps.

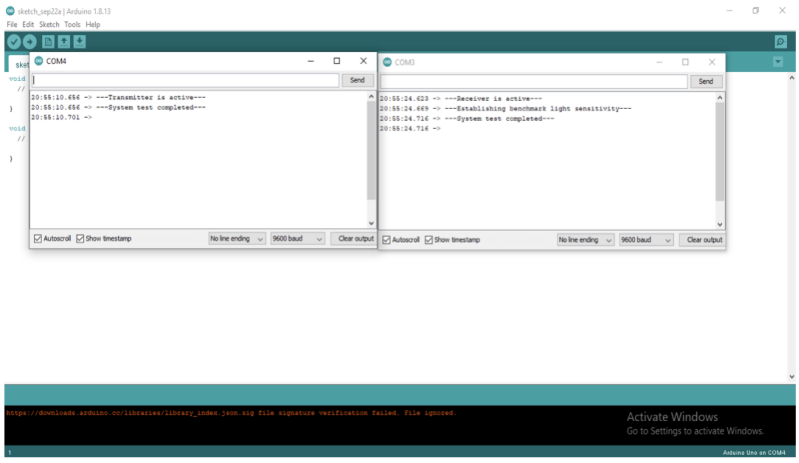

Figure 7: Screenshot of the software implementation

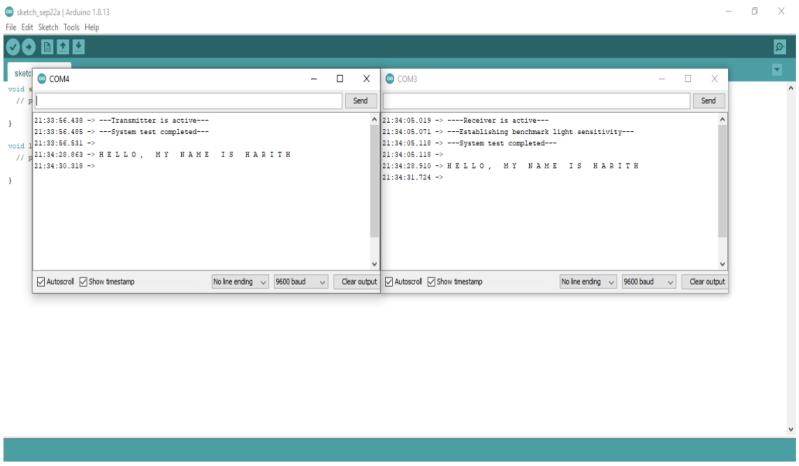

Figure 8: Screenshot of sending and receiving process implementation

VI. Conclusion

Quantum cryptography is the most advanced quantum technology accessible today. It is the first fundamental quantum notion that conveys the transition from theory to practice. In this paper, a quantum cipher was constructed using an Arduino. The proposed system consists of two Arduino Uno chips, five laser diodes, and five photoresistors. Laser light is used to transmit information such as text or numbers in a secure manner. In short, practical use of quantum cryptography has been proposed, which was previously difficult to implement. In addition, information was transmitted at a rate ranging from fractions of a second to seconds depending on the size of the message, which is considered a practical rate.

Funding

None

ACKNOLEDGEMENT

The author would like to thank the reviewers for their valuable contribution in the publication of this paper.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

References

[1] Abbas, Y. A., & Abdullah, A. A. (2021). Efficient hardware implementation for quantum key distribution protocol using fpga. IOP Conference Series: Materials Science and Engineering, 1076(1), 12043.
[2] Agrawal, G. P., & Dutta, N. K. (1993). Infrared and visible semiconductor lasers. In Semiconductor Lasers (pp. 547-582). Springer.
[3] Bennett, C. H., & Brassard, G. (2014). Quantum Cryptography: Public Key Distribution and Con Tos5.
[4] DeVore, S., & Singh, C. (2020). Interactive learning tutorial on quantum key distribution. Physical Review Physics Education Research, 16(1), 10126.
[5] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum Cryptography, Reviews of modern physics. Vol74 (1), 145. quantum-well laser diode with a high characteristic temperature over 200 K. Japanese Journal of Applied Physics, 39(2A), L86.
[6] Kitatani, T., Nakahara, K., Kondow, M., Uomi, K., & Tanaka, T. (2000). A 1.3-ÎŒm GaInNAs/GaAs singlequantum-well laser diode with a high characteristic temperature over 200 K. Japanese Journal of Applied Physics, 39(2A), L86.
[7] Liu, G., Stintz, A., Li, H., Malloy, K. J., & Lester, L. F. (1999). Extremely low room-temperature threshold current density diode lasers using InAs dots in In/sub0.15/Ga/sub0.85/As quantum well. Electronics Letters, 35(14), 1163-1165.
[8] Martelli, P., Brunero, M., Fasiello, A., Rossi, F., Tosi, A., & Martinelli, M. (2019). Single-SPAD implementation of quantum key distribution. 21st International Conference on Transparent Optical Networks, ICTON 2019, 2019, 1-3.
[9] Rammohan, A., & Kumar, C. R. (2017). Performance analysis of photoresistor and phototransistor for automotive's halogen and xenon bulbs light output. IOP Conference Series: Materials Science and Engineering, 263(6), 62056.
[10] Ricketti, B. (2015). Diode Laser Characteristics. Heriot-Watt University.
[11] Ryabtsey, I. I., Tretyakov, D. B., Kolyako, A. V, Pleshkov, A. S., Entin, V. M., & Neizyestny, I. G. (2017). Experimental quantum cryptography with single photons. Bulletin of the Russian Academy of Sciences: Physics, 81(12), 1493-1496.
[12] Salih, S. M., Tawfeeq, S. K., & Khaleel, A. I. (2019). Generation of True Random TTL Signals for Quantum Key-Distribution Systems Based on True Random Binary Sequences. Iraqi Journal of Laser, $18(1), 31 - 42$.
[13] Sanni, S. O., Olusuyyi, K. O., & Mahmud, I. (2019). Design and Implementation of Home Appliance Energy Monitoring Device. International Journal of Electrical, Energy and Power System Engineering, 2(2), 1-6.
[14] Singamaneni, K. K., Naidu, P. S., & Kumar, P. V. S. (2018). Efficient quantum cryptography technique for key distribution. Journal Europeen Des Systemes Automatises, 51(4-6), 283.
[15] Zhang, Q., Xu, F., Chen, Y.-A., Peng, C.-Z., & Pan, J.-W. (2018). Large scale quantum key distribution: challenges and solutions. Optics Express, 26(18), 24260-24273.

