I J C T A, 9(4), 2016, pp. 2005-2013
© International Science Press

Embedded System Based Quantum Encryption and Decryption Model Using Polarization

B. Raja[1], **M. Anand**[2] **and S. Ravi**[3]

ABSTRACT

In this paper, embedded system besed quantum encryption and deccryption using polarization is proposed. The information data and encryption code is fed into quantum encryption where the data has been encrypted and then passed to LED polarized in that the data is converted as photons and passed to the transmitter. At the receiver end, LDR will be used as a detector for reproduction of electrical signal from light energy. LDR output has to be decrypted using quantum decrypting code and got the original message receiver side. In proposed system, the polarization state of a photon carries quantum encryption key (private key of user). In proposed system, property of photons is used to error detection.

Keywords: Quantum encryption, polarization, embedded system, LED and LDR.

1. INTRODUCTION

In qunatun key distribution, individula photons are used for the secure transmission between transmitter and receiver. Quantum encrytion is an active research area. If photon travels in free space its polarization state does not change, if air turbulence is negligible. However, if a photon travels in an optical fiber its polarization state is subjected to changes. In this paper, quantum encryption and decryption is achieved by exploiting the properties of quantum objects such as photons.

2. RELATED WORK

A. V. Gleim et al., (2016) quantum key distribution system based on the subcarrier wave modulation method has been demonstrated. A passive unidirectional scheme used to compensate for the polarization dependence of the phase modulators in the receiver module, which resulted in a high visibility of 98.8%. The system is fully insensitive to polarization fluctuations and robust to environmental changes, making the approach promising for use in optical telecommunication networks. Secure key rate and transmission distance achieved by implementing the decoy states protocol or by optimizing the mean photon number used in line with experimental parameters.

Jindong Wang et al., (2016) demonstrated a one-way polarization encoding quantum key distribution (QKD) system. This approach can automatically compensate for birefringence and phase drift. This is achieved by constructing intrinsically stable polarization-modulated units (PMUs) to perform the encoding and decoding, which can be used with four-state protocol, six-state protocol, and the measurement-device independent (MDI) scheme.

Feihu Xu et al., (2013) presented a feasible method for quantum key distribution (QKD) both ultra-long-distance and immune to all attacks in the detection system. This measurement-device-independent

[1] Research scholar, ECE Department, Dr. M.G.R. Educational and Research Institute, *Email: Chennaiamutha.raja77@gmail.com*

[2] Professor, ECE Department, Dr. M.G.R. Educational and Research Institute, Chennai, *Email: harshni.anand@gmail.com*

[3] Professor Head, ECE Department, Dr. M.G.R. Educational and Research Institute, Chennai, *Email: ravi_mls@yahoo.com*

QKD (MDI-QKD) is with entangled photon sources in the middle. By proposing a model and simulating a QKD experiment, that MDI-QKD with one entangled photon source can tolerate 77dB loss (367km standard fiber) in the asymptotic limit and 60dB loss (286km standard fiber) in the finite-key case with state-of-the-art detectors.

LIU Xiao-Bao et al., (2008) introduced an intrinsically stable quantum key distribution system (QKD) with six polarization states encoded by phase modulation. Six state QKD is proven to bear higher security than a four state QKD system. As a result, proposed QKD system with six polarization states encoded by phase modulation is worth of application in polarization-code QKD.

3. PROPOSED SYSTEM

LED sources are randomly polarized. In the proposed system, two types of polarization (set 0 and set 1) with two different symbol set used respectively as plus, Y, cross and square. The oscillating angle or plane of light from each point on the light source is time varying. Taken as a time average, therefore, randomly polarized light sources continuously output multiple angles of polarization.Polarizers absorb incident light oscillating in all but one plane, its polarization axis, yielding linear polarization. Light that passes through two polarizers with orthogonal polarizing axes. Quantum encryption is done for secure data communication. The relationship between input/output voltage and state is shown in below table 1.

Table 1

Symbol set		*Output values (in volts)*	*Minimum*	*Maximum*
Zero	Plus	2.71, 2.72 ……….	2.70	3.2
	Y	2.75, 2.76, 2.77……..	2.75	3.3
One	Square	3.09, 3.1, 3.11……	3.09	3.41
	Cross	3.66, 3.67, 3.68, 3.69….	3.66	3.55

In receiver side of proposed embedded system, encryption and polarization are carried out. In receiver side of proposed embedded system, decryption and depolarization are carried out. Initially, data is encrypted into bits of 0s and 1s. Photons used for the conversation of encrypted data into a polarized light between the transmitter and the receiver. Photon in the polarized light is used to denote a single bit of data. In receiver side, bit value (0 or 1) is decrypted by states of the photon such as polarization or spin. By proposed method receiver send an encrypted data with photons to the receiver. The encryption and decryption are in the same arrangements that consist of two polarizing device such as LED and LDR. This process is shown in figure 1.

4. ERROR DETECTION

Error detection is also possible by proposed embedded system. In error detection, photon's state will be changed if any try to measure or to decrypt the data. This change confirms that the received polarized light will be changed. Both the sender and receiver detects that the message is interrupted.

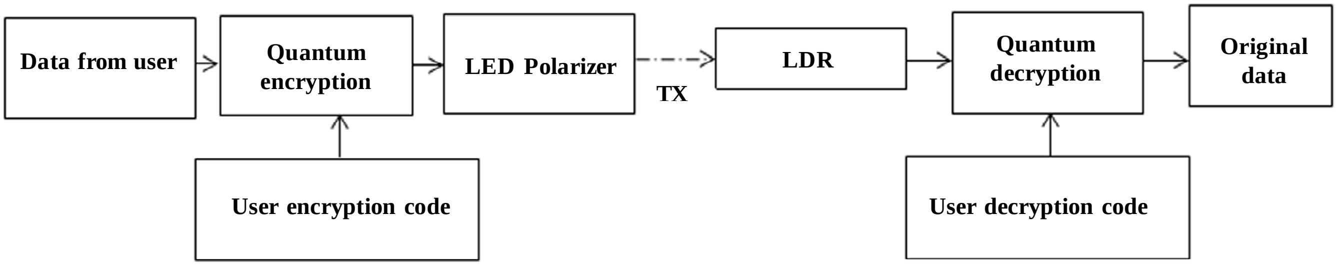


Figure 1: Block diagram of proposed system

4.1. Hardware setup

In hardware implementation, position of LED(Tx;) and LDR (Rx;)are shown in table 2 and table 3.

Table 2
Position of LED in hardware setup

LED_1	LED_2	LED_3
LED_4	LED_5	LED_6
LED_7	LED_8	LED_9

Table 3
Position of LDR in hardware setup

LDR_1	LDR_2	LDR_3
LDR_4	LDR_5	LDR_6
LDR_7	LDR_8	LDR_9

4.2. Pseudo code

Initiate serial port communication

```
Transmitter
execution calibration loop
select polarization set
enter the data
encrypted data
$x$ = length of data
encrypted data = symbol set
```

```
Receiver
Select polarization set
if (received data length = = $x$)
receiver char is calculated
decrypt data
```

```
Loop: calibration
minimum value of plus
maximum value of plus
minimum value of $Y$
maximum value of $Y$
minimum value of cross
maximum value of cross
minimum value of square
maximum value of square
```

4.3. Receiver code flow

The main menu of receiver consist four options namely set voltage range, symbol set, receive data and exit. The set voltage range is used for initial calibration. In calibration, minimum and maximum value of various symbol set is assigned. The symbol set is used for selecting polarization type (0 or 1). The receive data is used to initiate receiver. Exit is used to close the transmitter.

4.4. Transmitter code flow

The main menu of transmitter consist three options such as set symbol set, transmit data and exit. The symbol set is used for selecting polarization type (0 or 1). The transmit data is used to for transmit data by quantum cryptography. Exit is used to close the transmitter.

5. IMPLEMENTED HARDWARE

5.1. Simulation setup

UART setup is required for interacting with the receiver, transmitter and Hyper terminal. USB address (for both Transmitter& Receiver) is found by using dmesg in the terminal window. Connect the Circuit as per the connection diagram as shown in figure 2. Change corresponding USB address in minicom-s. To communicate on serial port in Linux, minicom is used. Minicom is a text-based serial port communications program. It is used to talk to external RS-232 devices such as mobile phones, routers, and serial console ports.

5.2. Receiver

Initially, calibration is done for corresponding polarization set. Receiver mode is enabled.The data received as output voltage ranges.

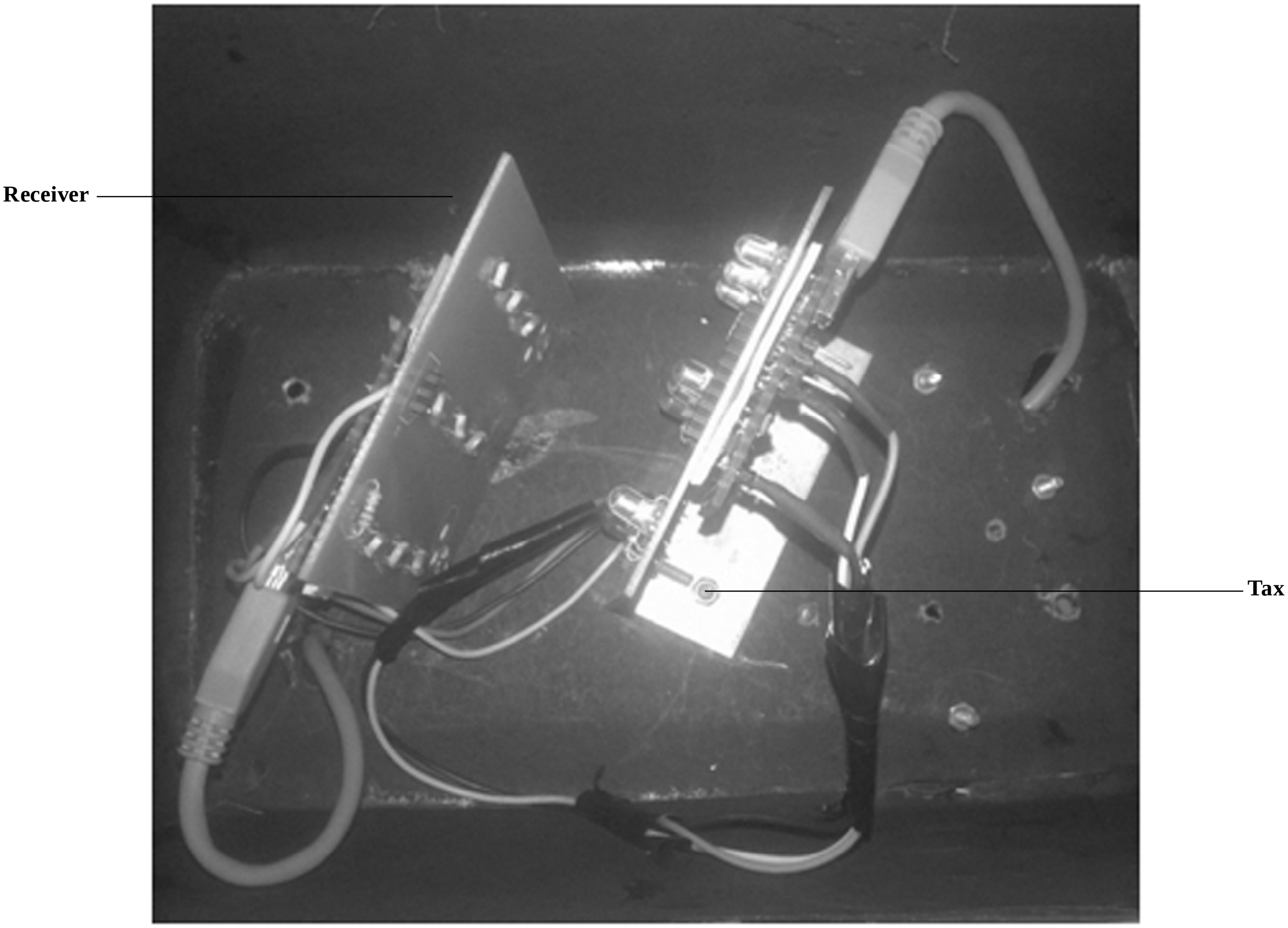


Figure 2: Implemented hardware

5.3. Transmitter

Polarization set is selected. The data for transmission is entered. The encryption of data by qunatum cryptography. Encrypted data is sent to the receiver.

Case 1: Set 0 and d = 1/X.

The calibration values and output voltage for case1 are shown in table 4 and table 5.

Table 4
Calibration values

Symbol set		*Minimum*	*Maximum*
One	Cross	3.33	3.41
	Square	3.66	3.69

Table 5
Output voltage

Output voltage	*Symbol set*
3.38	Cross
3.38	Cross
3.38	Cross
3.67	Square
3.38	Cross
3.67	Square
3.67	Square
3.38	Cross

Case 2: Set 1 and d = 1/X

The calibration values and output voltage for case2 are shown in table 6 and table 7.

Table 6
Calibration values

Symbol set		*Minimum*	*Maximum*
One	Cross	3.33	3.41
	Square	3.66	3.69

Table 7
Output voltage

Output voltage	*Symbol set*
3.38	Cross
3.38	Cross
3.38	Cross
3.67	Square
3.38	Cross
3.67	Square
3.67	Square
3.38	Cross

Case 3: Set 0 and d = 2/X

The calibration values and output voltage for case 3 are shown in table 8 and table 9.

Table 8
Calibration values

Symbol set		*Minimum*	*Maximum*
Zero	Plus	2.7	2.85
	Y	2.86	3.02

Table 9
Output voltage

Output voltage	*Symbol set*
2.78	Plus
2.78	Plus
2.78	Plus
3.0	Y
2.78	Plus
3.0	Y
3.02	Y
2.78	Plus

Case 4: Set 1 and d = 2/X

The calibration values and output voltage for case 4 are shown in table 10 and table 11.

Table 10
Calibration values

Symbol set		*Minimum*	*Maximum*
One	Cross	3.09	3.16
	Square	3.4	3.45

Table 11
Output voltage

Output voltage	*Symbol set*
3.09	Cross
3.1	Cross
3.1	Cross
3.43	Square
3.1	Cross
3.44	Square
3.42	Square
3.1	Cross

Case 5: Set 0 and d = X

The calibration values and output voltage for case 5 are shown in table 12 and table 13.

Table 12
Calibration values

Symbol set		*Minimum*	*Maximum*
Zero	Plus	2.94	3.0
	Y	2.75	2.83

Table 13
Output voltage

Output voltage	*Symbol set*
2.95	Plus
2.95	Plus
2.96	Plus
2.77	Y
2.95	Plus
2.77	Y
2.77	Y
2.95	Plus

Case 6: Set 1 and d =X

The calibration values and output voltage for case 5 are shown in table 14 and table 15.

Table 14
Calibration values

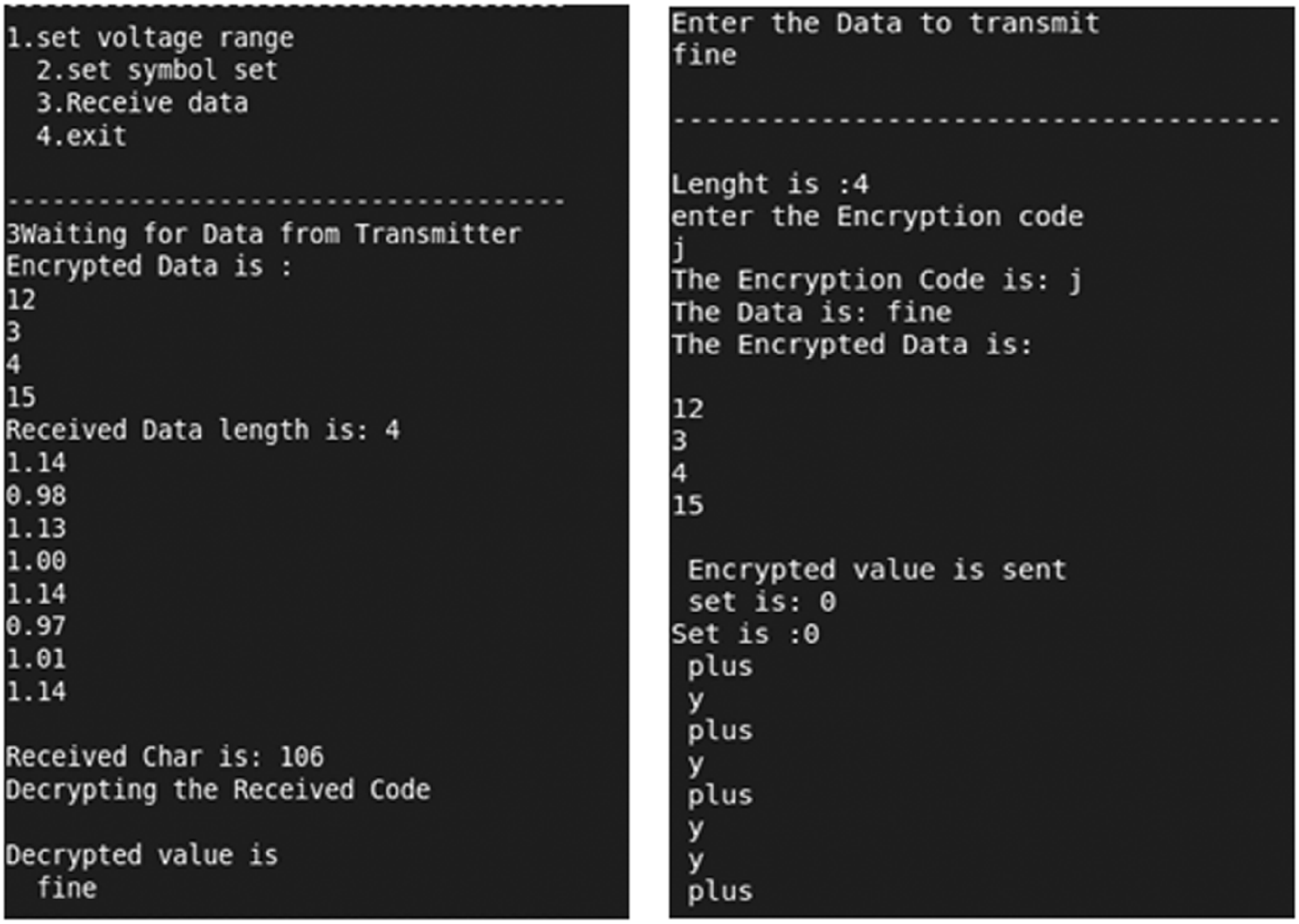
Symbol set		*Minimum*	*Maximum*
One	Cross	3.23	3.26
	Square	3.48	3.55

Table 15
Output voltage

Output voltage	*Symbol set*
3.24	Cross
3.25	Cross
3.25	Cross
3.55	Square
3.24	Cross
3.54	Square
3.54	Square
3.24	Cross

6. RESULTS

Distance between transmitter and receiver is considering as X. The proposed system is tested for transmit data “fine” with encryption code “h” and the result is shown in figure 3.



```
-------------------------------------
1.set voltage range
  2.set symbol set
  3.Receive data
  4.exit

-------------------------------------
3Waiting for Data from Transmitter
Encrypted Data is :
12
3
4
15
Received Data length is: 4
1.14
0.98
1.13
1.00
1.14
0.97
1.01
1.14

Received Char is: 106
Decrypting the Received Code

Decrypted value is
  fine
```

```
Enter the Data to transmit
fine

-------------------------------------

Lenght is :4
enter the Encryption code
j
The Encryption Code is: j
The Data is: fine
The Encrypted Data is:

12
3
4
15

 Encrypted value is sent
 set is: 0
Set is :0
 plus
 y
 plus
 y
 plus
 y
 y
 plus
```

Receiver **Transmitter**

Figure: 3 Screen shot

7. CONCLUSION

Proposed polarization based encryption and decryption is more secure communication in free space. In this paper embedded system based quantum encryption and decryption using polarization is demonstrated. Implemented hardware analyzed for three different transmission length (1/X, 2/X and 3). The proposed system achieves long distance and free space secure communication. In proposed system, without any quantum repeaters transmission is possible.

REFERENCES

[1] A. V. Gleim, V. I. Egorov, Yu. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov and G. S. Buller, "Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference", OPTICS EXPRESS, Vol. 24, No. 3, Feb. 2016.

[2] Jindong Wang, Xiaojuan Qin, Yinzhu Jiang, Xiaojing Wang, Liwei Chen, Feng Zhao, Zhengjun Wei, and Zhiming Zhang, "Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units", OPTICS EXPRESS 8302, Vol. 24, No. 8, Apr. 2016.

[3] F. Xu, B. Qi, Z. Liao, and H.-K. Lo, "Long distance measurement-device-independent quantum key distribution with entangled photon sources," Appl. Phys. Lett. 103(6), 061101 (2013).

[4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. 68(21), 3121-3124 (1992).

[5] J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng, "Stable quantum key distribution with active polarization control based on time-division multiplexing," New J. Phys. 11(6), 065004 (2009).

[6] Y. S. Kim, Y. C. Jeong, and Y. H. Kim, "Implementation of polarization-coded free-space BB84 quantum key distribution," Laser Phys. 18(6), 810-814 (2008).

[7] H. Q. Ma, J. L. Zhao, and L. A. Wu, "Quantum key distribution based on phase encoding and polarization measurement," Opt. Lett. 32(6), 698-700 (2007).

[8] X. B. Liu, C. H. Liao, Z. L. Tang, J. D. Wang, and S. H. Liu, "Quantum key distribution system with six polarization states encoded by phase modulation," Chin. Phys. Lett. 25(11), 3856-3859 (2008).

[9] Xiao Tang, Lijun Ma, Alan Mink, Anastase Nakassis, Barry Hershman, Joshua Bienfang, Ronald F. Boisvert, Charles Clark and Carl Williams, "High Speed Fiber-Based Quantum Key Distribution using Polarization Encoding", *Proc. SPIE* 5893, Quantum Communications and Quantum Imaging III, 58931A (August 25, 2005); doi:10.1117/12.614598

[10] N. Sasirekha and M. Hemalatha, "Quantum Cryptography using Quantum Key Distribution and its Applications", International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249-8958, Volume-3, Issue-4, April 2014.

[11] Anton Zeilinger, "Long-Distance Quantum Cryptography with Entangled Photons ", *Proc*. *SPIE*6780, Quantum Communications Realized, 67800B (September 10, 2007); doi:10.1117/12.740268; http://dx.doi.org/10.1117/12.740268

[12] Daphna G. Enzer, Phillip G. Hadley, Richard J. Hughes, Charles G. Peterson and Paul G. Kwiat," Entangled-photon six-state quantum cryptography", New Journal of Physics 4 (2002) 45.1-45.8