Optics and Laser Technology 101 (2018) 312–318

Contents lists available at ScienceDirect

Optics and Laser Technology

journal homepage: www.elsevier.com/locate/optlastec

Full length article

Development of authentication code for multi-access optical code division multiplexing based quantum key distribution

Ambali Taiwo [a,*], Ghusoon Alnassar [a], M.H. Abu Bakar [a], M.F. Abdul Khir [b], Mohd Adzir Mahdi [a], M. Mokhtar [a]

[a] *Computer and Communication Sys. Engineering/Center of Excellence for Wireless and Photonic Network (WiPNET), Faculty of Engineering, University Putra Malaysia, Malaysia*
[b] *Information Security and Assurance Programme, Faculty of Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai 71800 Nilai, Negeri Sembilan, Malaysia*

ARTICLE INFO

Article history:
Received 11 January 2017
Received in revised form 4 October 2017
Accepted 20 November 2017

Keywords:
Authentications
Key distribution
Information security
Quantum communication
Cryptography

ABSTRACT

One-weight authentication code for multi-user quantum key distribution (QKD) is proposed. The code is developed for Optical Code Division Multiplexing (OCDMA) based QKD network. A unique address assigned to individual user, coupled with degrading probability of predicting the source of the qubit transmitted in the channel offer excellent secure mechanism against any form of channel attack on OCDMA based QKD network. Flexibility in design as well as ease of modifying the number of users are equally exceptional quality presented by the code in contrast to Optical Orthogonal Code (OOC) earlier implemented for the same purpose. The code was successfully applied to eight simultaneous users at effective key rate of 32 bps over 27 km transmission distance.

1. Introduction

Ever since its discovery three decades ago [1], quantum cryptography has maintained its exceptionality in providing anticipated secure mechanism between two communicating ends. Its security establishment has remained a promising solution to the challenges posed by the progress towards quantum computing, a rare opportunity that might be explored to mount attack on the existing security system that relied on mathematical complexity. Quantum cryptography often referred to as quantum key distribution (QKD) proffers its security measure by exchange of set of random bits between two users [2–4], which upon series of post-processing, are used in the generation of secured key for information exchange. Its security provision, guaranteed by fundamental law of physics [2,4–6] has remained unconditional in the presence of eavesdroppers.

Over the years, tremendous progress have been recorded in the area of the security enhancement against all emerging loopholes in various QKD protocols [4, 7–9] One of the most appealing among them is the decoy state system [2], which provides security against Photon Number Splitting (PNS) attack. This has been achieved through additional pulses that tends to raise an alarm whenever alteration is perceived in the intensity of the received pulses. This eventually lessens the impending challenges in practical QKD that are based on weak pulse laser source.

Subsequent works focused on the transmission distance and secured key rate. The first practical implementation of QKD was only achieved over 30 cm distance. The latest development have reported between tens and hundreds of kilometers [10,11 which have been achieved both theoretically and in practical. A number of works on the other hand, focus on improving the secret key rate while sacrificing the supported transmissions distance. A key rate of 1 Mb/s was recently reported in [12] over a distance of 20 km and 50 km [13] respectively. One specific thing about all the above-described works is that they are only addressing a point-to-point communication between two end users.

The latest trends in QKD development are unequivocally exploring the multi-user ability of the system. Imagine an establishment with several sections within a certain location. Each user requires a distinctive way of identification with minimal resources. Subcarrier QKD multiplexing was proposed in [14] and further developed in [15,16]. The technique, which saw bands of diverse frequency used in modulating the weak pulse laser, was subsequently experimented for two users in [17]. Its low key rate was due to complexity in the system design. Subsequent work include Orthogonal Frequency Division Multiplexing of QKD (OFDM-QKD) [18] proposed in 2015. The system recorded better performance only with activate decoding technique which subsequently add to the cost and complexity of the design. Previously in 2012, Razavi

* Corresponding author.
E-mail address: taiwoambaliyu@yahoo.com (A. Taiwo).

https://doi.org/10.1016/j.optlastec.2017.11.034
0030-3992/© 2017 Elsevier Ltd. All rights reserved.

proposed a thrilling multi-access QKD system based on OCDMA system [19]. The system was demonstrated with both passive and active decoders. The active system is a form of "listen-befor e-send" approach whereby both communicating ends pay attention to the channel to ensure it is unengaged before transmission. The work however made use of Optical Orthogonal Code (OOC), which has complexity in its derivation as well as longer code length, with heavy spectral dependency on the light source [20, 21].

This work proposed a new code, which is suitable for multiplexed QKD system. As established in [19] that a single weight code has proximity in performance to time division based system than multi-weight code, the proposed code is also a single-weight code which at the same time, is secured against channel attack. One other unique characteristics of the code is that it could equally be used as time-dependent code with all users sharing the same frequency spectrum at distinctive time interval.

The paper is organized as follows; Section 1 contains the introductory part while Section 2 vividly describes the proposed code derivation. The system setup will be addressed in Sections 3 and 4 will explain the mathematical derivation of the system. The results will be discussed in section 5 and the concluding part will be addressed in Section 6.

2. Proposed code design

The code begins with the formation of a matrix with a logical pattern of binary digit "1" and "0" denoting presence and absence of a certain pulse. The bits are arranged in 3 × 2 matrix with the first two bits position of the first row and last two bits position of the second row occupied by bit "1" as shown in the matrix.

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

The bit pattern can then be increased by diagonal repetition of the matrices.

$$\begin{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} & & \\ & \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} & \\ & & \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \end{bmatrix}$$

The patterns are combined in a large matrix to form a single matrix with N column and M row. This ensures that the element are located along the major diagonal in the matrix.

$$\begin{bmatrix} 1 & 1 & 0 & & & & & & \\ 0 & 1 & 1 & & & & & & \\ & & & 1 & 1 & 0 & & & \\ & & & 0 & 1 & 1 & & & \\ & & & & & & 1 & 1 & 0 \\ & & & & & & 0 & 1 & 1 \end{bmatrix}$$

The emerging vacuum are subsequently filled with bit "0" to obtain a full pattern of binary sequence.

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

The patterns are then treated as sets of binary digit and subsequently converted to their respective decimal equivalents by adding their corresponding decimal values horizontally.

$$\left\{ \begin{bmatrix} 2^8 & \cdot\cdot & \cdot\cdot & \cdot\cdot & \cdot\cdot & \cdot & \cdot & \cdot & 2^0 \\ 256 & 128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{matrix} \mathit{Decimal} \\ \mathit{value}\ (x) \\ \rightarrow 384 \\ \rightarrow 192 \\ \rightarrow 48 \\ \rightarrow 24 \\ \rightarrow 6 \\ \rightarrow 3 \end{matrix} \right\}$$

The obtained decimal values {x = 384, 192, 48, 24, 6, and 3} are divided by the common factor "3" to form the new pattern {128, 64, 16, 8, 2, 1}. These are subsequently converted to their respective binary form to generate the usable code sequence.

$$\left\{ \begin{bmatrix} 2^8 & \cdot\cdot & \cdot\cdot & \cdot\cdot & \cdot\cdot & \cdot & \cdot & \cdot & 2^0 \\ 256 & 128 & 64 & 32 & 16 & 8 & 4 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{matrix} x/3 \\ \downarrow \\ \leftarrow 128 \\ \leftarrow 64 \\ \leftarrow 16 \\ \leftarrow 8 \\ \leftarrow 2 \\ \leftarrow 1 \end{matrix} \right\}$$

With each row as a unique address location, each user can uniquely communicate with their respective partners on the channel with no or minimal interference from the adjacent users. The chip locations are diverse wavelength corresponding to the column value as shown in the final derivation above. One other unique characteristic of the proposed code is occasional presence of "all zero" column. Unlike the conventional channel code for classical OCDMA system where overlapping of chips are used to determine the level of security, the level of ambiguity in predicting the exact spectrum being used by a certain users in the derived quantum code could as well serve as a source of security. Other benefits of the code is flexibility in modifying the required number of users to suit ones purpose.

Theoretically, the number of users can further be increased through the formation of matrix $C_{i,j}$ with the position of the bits corresponding to

$$C_{i,j} = \begin{bmatrix} C_{0,0} & \cdots & C_{0,n} \\ \vdots & \ddots & \vdots \\ C_{m,0} & \cdots & C_{m,n} \end{bmatrix}$$

For $i = 0, 1, 2, \ldots\ldots\ldots m$ and $j = 0, 1, 2, \ldots\ldots n$.

The positions of "1" in Table 1 are at row (i) and column (j) locations described as

$$C_{0,1} = C_{1,2} = C_{2,4} = C_{3,5} = C_{4,7} = C_{5,8} = 1$$

In order to derive the location mathematically, the following steps are followed.

Step 1: Count j from 0 and increase by 1 in each stage. j = 0, 1, 2, 3, 4 . . .

Step 2: To find column with all "0". All element of a column will be "0" if $j \bmod 3 = 0$.