Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2020) 28: 3335 – 3351
© TÜBİTAK
doi:10.3906/elk-2005-49

Quantum key distribution over free space optic (FSO) channel using higher order Gaussian beam spatial modes

Muhammad KAMRAN[1], **Muhammad Mubashir KHAN**[1,*], **Tahir MALIK**[2], **Asad ARFEEN**[3]

[1]Department of Computer Science and Information Technology, Faculty of Information Sciences & Humanities, NED University of Engineering and Technology, Karachi, Pakistan

[2]Department of Electronic Engineering, Faculty of Engineering, NED University of Engineering and Technology, Karachi, Pakistan

[3]National Center for Cyber Security, NED University of Engineering and Technology, Karachi, Pakistan

Received: 06.05.2020 • **Accepted/Published Online:** 29.07.2020 • **Final Version:** 30.11.2020

Abstract: Quantum key distribution (QKD) has emerged as a secure solution of secret key distribution utilizing the well established theories of modern physics. Since its introduction in 1984, many interesting and innovative ideas have been proposed for QKD in order to improve the security and efficiency of the scheme keeping in view of its applications and practical implementation. High error rate QKD scheme for long distance communication – the so-called KMB09 protocol – is one such scheme which was designed to achieve longer communication distance in QKD, without compromising its security, by allowing the utilisation of higher dimensional photon states which is not possible with standard BB84 scheme. However the practical implementation of KMB09 protocol has not been presented yet because of its unique design. In this paper, we propose a framework for the practical implementation of QKD system that runs KMB09 protocol in two or more dimensions of photon states. We present the KMB09 based QKD system design and its simulation for practical implementation based on the encoding of secret bits in higher order Gaussian beam spatial modes. The proposed framework is specifically evaluated in terms of efficiency or success rate with two and four dimensions of photon states. We find that the simulation results of the proposed framework are inline with the numerical and analytical results of the same QKD model presented earlier.

Key words: Network security, quantum key distribution, opto-electronics

1. Introduction

Ever since the introduction of the computer 'bit', one of the most revolutionary developments in communication technology is the quantum bits or Qubits based communication. This field has been classified as quantum technology and includes, but is not limited to, quantum computation and quantum information. The applications of such technology towards cybersecurity are immense and its impact on how we view cyber security will stay for a long time [1]. Most notably is the development of fast processing quantum computers and highly secure communication with quantum cryptography or quantum key distribution (QKD) [2]. QKD comprises of cryptographic protocols using various photonic properties at the physical layer. Systems employing QKD enabled sharing of secret cryptographic keys with unconditional security due to Heisenberg's uncertainty principle and quantum no-cloning theorem [3]. QKD shows better security compared to conventional classical techniques that are mostly based on computational security [4–7]. It is believed that conventional security techniques

[*] Correspondence: mmkhan@cloud.neduet.edu.pk

will remain no longer secure in the presence of a full-fledged quantum computer. Hence, cryptosystems with enhanced and optimized quantum features are required to fulfil the long-term requirements of communication security in cyberspace.

Over the years numerous QKD system designs have been proposed and successfully implemented [8–10]. However, new developments in optoelectronic devices such as lasers, SLM, DMD, and superconducting nanowires, single-photon detectors, etc. [11–14] contribute towards the innovative development in QKD systems. Today's QKD protocols and systems utilize various degrees of freedom in photons i.e. polarization basis and orbital angular momentum [15, 16]. In addition, holographic principles are used to facilitate the control of structured light [11, 17] in the form of computer-generated holography (CGH). This also finds extensive use in applications such as computer aided design, gaming, holographic video, automotive and communication. As the requirement of secure channels for information transfer is increasing with expanding consumer needs, current proposed QKD systems need to be assessed thoroughly. The provision of innovation in its design and integration with emerging innovative technologies needs to be addressed.

In this paper, we present the framework for practical implementation of QKD system based on the KMB09 protocol. To the best of knowledge the KMB09 protocol has not been practically implemented yet and the benefits of utilising this protocol in a practical QKD system are still awaited. The main contribution of our work is to present the practical approach to utilise KMB09 protocol for secure communication. KMB09 protocol allows to utilise higher dimensional photon states [18]. The simulation is performed with two and four dimensional photon states. The simulation results are used to determine QKD protocol efficiency. The states of simulation setup are generated using spatial modes of Hermite–Gaussian and Laguerre–Gaussian beams, and also their superposition modes [19]. The rest of this paper is organized as follows. Section 2 presents the related work done towards the practical implementation of QKD systems. Section 3 explains the standard QKD process with explanation of KMB09 protocol. Section 4 explains the details of holistic simulation setup. Section 5 presents and discusses the simulation results obtained with two and four dimension cases of KMB09 protocol. Finally, we present the conclusion and highlights of future work.

2. Literature review

Over the past two decades there has been extensive research conducted on QKD systems utilizing various photonic properties and various QKD protocols such as BB84, two-state and EPR (Einstein, Podolsky and Rosen) [20–23]. The first known reference architecture for practical QKD system was published by Mailloux et al. in 2015 which they called qkd'x [24]. Their work supported the development and performance analysis of a practical QKD system. They used a qkd'x framework to model polarization based prepare-and-measure BB84 QKD system. They also provided a brief listing of qkd'x modelled optical component library that helped other researchers in understanding and investigating other QKD architectures along with their security and performance analysis. The computer modelling of opto-electronic systems was carried out by Engle et al. in 2015 [25] in the context of QKD system architecture. Their study involved three main systems which are prepare-and-measure BB84 QKD system, decoy state enabled QKD system and measure-device-independent QKD system.

Archana and Krithika presented the simulation of BB84 QKD protocol in [26]. Their work presented detailed QKD system simulations but did not consider practical eavesdropping attacks. In [27] Hussain et al. presented the numerical modelling of the QKD system which made use of higher dimension KMB09 protocol. Their work mainly focuses on the aspect of utilising higher dimension quantum states in QKD simulation using a numerical approach but lacked the practical considerations of the QKD system. Shall et al. presented the mathematical model of the QKD system using BB84 prepare-and-measure protocol [28]. Their simulator closely depicts the results and behavior of a QKD system using nonideal conditions. However it lacked comparison with newer QKD protocols.

The QKD system based on higher dimensional quantum states via orbital angular momentum (OAM) and angular position (ANG) was initially reported by Mirhosseini et al. in [16]. For the generation of OAM and ANG modes at faster rate, they make use of DMD at a rate of 4 KHz. They also integrate mode separator with efficiency of 93%. They tried to encode OAM and ANG bases using a seven-dimensional alphabet and achieve channel width of 2.05 bits per shift photons. Wang et al. proposed a high dimensional QKD system using semi mutually unbiased bases (MUBs) of photon's orbital angular momentum [29]. Their experimental setup also shows high key generation rate as compared to previous setups by focusing antinoise ability under atmospheric turbulence with high efficiency QKD system based on the clever utilisation of Hermite and Laguerre Gaussian modes.

A QKD system with biased basis using decoy states in term of practical implementation has been deeply discussed and reported by Mao et al. in [30]. According to their scheme, the signal pulse must be prepared in X and Z basis, but the weak decoy state must be prepared in only X basis in contrast to standard decoy-state method with biased basis. Based upon their scheme they presented numerical modelling in combination with the weak coherent source in many flavors e.g. statistical variations and full parameter boundary testing. Results have opened several paths of technical research in the area of QKD. The scheme also provides speedy key generation process and greater transmission efficiency in comparison with biased basis and three-intensity decoy state generator. Performance efficiency is also increased using full parameter optimization.

3. QKD protocols

QKD involves the encoding of digital information into quantum states in contrast to classical communication in which digital bits are encoded into electrical signals. Normally, various photonic properties play pivotal role in the generation of quantum states. Researchers have developed several protocols to exploit these properties to get the secured transfer of information. These may be divided into two broad categories: (1) Prepare-and-measure based protocols and (2) Entanglement based protocols. Here we focus on prepare-and-measure QKD that is relatively easier to implement with conventional BB84 protocol but there challenges associate with the implementation of KMB09 protocol because of freedom of increasing the dimensions of photon states to achieve long distance QKD communication.

3.1. The basic QKD protocol

The well-known BB84 protocol developed in 1984 by Bennett and Brassard is considered to be the standard and most basic QKD protocol that comes under the category of prepare-and-measure based protocols [31]. The BB84 protocol, named after its cofounders and the year of invention, makes use of photon's polarization states for information encoding by selecting any two sets of nonorthogonal mutually unbiased bases (MUBs). MUBs in the Hilbert space are the bases which consists set of orthonormal states and their inner product magnitude square (one state from each basis) is equal to the inverse of the dimension [32]. The protocol is no doubt the most famous and the most noticeable among all QKD protocols. The security proof of this protocol against arbitrary eavesdropping strategies was first proved by Mayers [33], and a simple proof was later shown by Shor and Preskill [20].

Generally, in BB84 QKD protocol, two bases each having two-dimensional states are used for encoding classical bits. The rectilinear basis $\oplus$ at, for example, 0° degree and +90° polarisation of photon states represented via intuitive symbols $|0\rangle$ and $|1\rangle$ while the diagonal basis $\otimes$ which consists of +45° and +135° polarisation of photon states represented as $|+\rangle$ and $|-\rangle$ respectively [34]. Hence, there are two sets of states each belonging to respective mutually unbiased basis

$$\oplus = \{\, |0\rangle \,, |1\rangle \,\} \quad \textit{and} \quad \otimes = \{\, |-\rangle \,, |+\rangle \,\} \tag{1}$$

where

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} = Q_{00}, \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix} = Q_{01} \quad \textit{and} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = Q_{10}, \quad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = Q_{11}$$

According to standard BB84 protocol, the relationship between the digital information bits and their respective quantum states are described in Table 1. The overall QKD protocol consists of two main phases in which the first one facilitates the exchange of qubits through a quantum communication channel and the second one facilitates classical communication for the accomplishment of final shared key [35, 36].

Table 1. Encoding scheme of the basic BB84 protocol.

Bits	Basis	
	$\oplus$	$\otimes$
0	Q_{00}	Q_{10}
1	Q_{01}	Q_{11}

Phase 1: Quantum transmission (over quantum channel)

1. Alice and Bob agree on sending and receiving the encoded photon states Q_{ij} belonging to the set of mutually unbiased bases M $\in \{\oplus, \otimes\}$. The selection of states is performed from a set of randomly selected bits D $\in \{0,1\}^n$ according to Table 1.

2. Let Q_{ij} be a quantum state of photon prepared and transmitted by Alice to Bob for each randomly selected bit according to Table 1. This communication of qubits is accomplished using quantum channel.

3. By randomly selecting the bases $\oplus$ or $\otimes$, Bob measures every transmitted qubit on reception and records his measured qubit D_{ij}.

4. Before finalising the shared key bits Bob waits for the public discussion over the classical channel.

Phase 2: Public discussion (over classical channel)

1. For each qubit Q_{ij} prepared and sent by Alice and measured by Bob as D_{ij}:

   (a) Bob publicly announces his measurement basis $M_i \in$ M which he used to measure each of the incoming qubits D_{ij}.

(b) Alice, in response, publicly tells Bob to discard all those cases in which she finds a basis mismatch of prepared and measured qubits. Hence, both parties discard all such cases and consider the remaining bits as the shared key.

2. Alice selects arbitrary subset of the remaining shared bits and compare them publicly with Bob on classical channel.

3. If the difference of bits is found near 25%, they consider it as the error due to possible intercept and resend attempt by the eavesdropper and resume the protocol by discarding all the shared bits. Otherwise, they proceed to use the shared secret key by applying necessary classical algorithms for error correction and privacy amplification.

3.2. The KMB09 protocol

The KMB09 protocol named after its inventors Khan, Murphy and Beige is famous because of its ability to run with higher dimensional photon states [18]. By design it is better than standard BB84 protocol in term of variety of higher error rates due to eavesdropping. In addition to conventional quantum bit error rate (QBER), it allows to calculate the eavesdropping error rate in terms of the index transmission of photon states i.e. the index transmission error rate (ITER). However, this important advantage is achieved at the cost of lower efficiency than standard BB84 protocol. Brierley [37] explains the utilization of bases with higher dimensional photon states in KMB09 protocol in order to further improve the eavesdropping error rate. In KMB09 protocol, Alice and Bob use two bases $\boldsymbol{\tau}$ and $\boldsymbol{\upsilon}$, as explained in [38], which can be written as:

$$\boldsymbol{\tau} \in \left\{ |\boldsymbol{\tau}_b\rangle : b = 1, 2, ..., N \right\} \quad \textit{and} \quad \boldsymbol{\upsilon} \in \left\{ |\boldsymbol{\upsilon}_b\rangle : b = 1, 2, ..., N \right\} \tag{2}$$

Although the protocol is extendable to N dimensions for which the encoding bits explained in Table 2. For concrete bases examples in $N = 2$ dimensions, the KMb09 protocol uses same bases set as BB84, refer to Eq (1). For $N = 4$ dimensions, we may have following bases set of two MUBs as also defined in [18]:

$$\boldsymbol{\tau} = \left\{ |\boldsymbol{\tau}_1\rangle, |\boldsymbol{\tau}_2\rangle, |\boldsymbol{\tau}_3\rangle, |\boldsymbol{\tau}_4\rangle \right\} \quad \textit{and} \quad \boldsymbol{\upsilon} = \left\{ |\boldsymbol{\upsilon}_1\rangle, |\boldsymbol{\upsilon}_2\rangle, |\boldsymbol{\upsilon}_3\rangle, |\boldsymbol{\upsilon}_4\rangle \right\} \tag{3}$$

where

$$|\boldsymbol{\tau}_1\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |\boldsymbol{\tau}_2\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \quad |\boldsymbol{\tau}_3\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad |\boldsymbol{\tau}_4\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \quad \textit{and}$$

$$|\boldsymbol{\upsilon}_1\rangle = \frac{1}{2}\begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}, \quad |\boldsymbol{\upsilon}_2\rangle = \frac{1}{2}\begin{pmatrix}-1\\1\\1\\-1\end{pmatrix}, \quad |\boldsymbol{\upsilon}_3\rangle = \frac{1}{2}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \quad |\boldsymbol{\upsilon}_4\rangle = \frac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$$

Again the complete protocol runs in the following two phases as BB84 protocol:

Phase 1: Quantum transmission (over quantum channel)

1. First, Alice generates a photon state to transmit to Bob by randomly selecting from $|\boldsymbol{\tau}_b\rangle$ and $|\boldsymbol{\upsilon}_b\rangle$ states.

2. Bob measures the incoming photon states from Alice by randomly switching between two bases $\boldsymbol{\tau}$ and $\boldsymbol{\upsilon}$ and records his measurement outcome.
3. Before finalising the shared key bits Alice and Bob wait for the public discussion over the classical channel.

Phase 2: Public discussion (over classical channel)

1. After the transmission and measurement of all photon states Alice reveals the index of each of the photon states she sent to Bob on a public channel.
2. Bob matches the indices revealed by Alice with the corresponding indices of his computed states and publicly reveals all those cases in which an index mismatch is found.
3. Both Alice and Bob interpret their results according to Table 2 and discard all those cases in which they do not find any shared key bit.
4. Alice and Bob perform calculation of errors in key transmission to disclose any possible attempt of eavesdropping.
5. After finding no evidence of eavesdropping they apply classical processes of error-correction and privacy amplification.

Table 2. KMB09 protocol encoding scheme.

Index by Alice	Measurement by Bob (bits)											
	$\vert\boldsymbol{\tau}_1\rangle$	$\vert\boldsymbol{\tau}_2\rangle$	$\vert\boldsymbol{\tau}_3\rangle$	$\vert\boldsymbol{\tau}_4\rangle$	...	$\vert\boldsymbol{\tau}_N\rangle$	$\vert\boldsymbol{\upsilon}_1\rangle$	$\vert\boldsymbol{\upsilon}_2\rangle$	$\vert\boldsymbol{\upsilon}_3\rangle$	$\vert\boldsymbol{\upsilon}_4\rangle$	...	$\vert\boldsymbol{\upsilon}_N\rangle$
1	×	1	1	1	...	1	×	0	0	0	...	0
2	1	×	1	1	...	1	0	×	0	0	...	0
3	1	1	×	1	...	1	0	0	×	0	...	0
4	1	1	1	×	...	1	0	0	0	×	...	0
...	...	...	...	...	...	...	...	...	...	...	...	...
$\boldsymbol{N}$	1	1	1	1	...	×	0	0	0	0	...	×

KMB09 is a unique QKD protocol that exhibits two different types of errors that may provide a signature for the possible eavesdropping attempt of an attacker. Its another important feature is that it allows to switch the dimensions of photon states to any higher level in order to achieve improved security. To the best of our knowledge until now there has been no known attempt towards the practical implementation of KMB09 protocol. In the next section, we present the design of our practical KMB09 QKD setup with its simulation details. Our simulation of the practical system has been test for desired efficiency of KMB09 protocol for the case of $N = 2$ and $N = 4$ dimensions. We believe that this simulation will help in the detailed analysis of the KMB09 protocol.

4. Simulation setup

Similar to any communication system, the overall model of QKD system consists of two communicating parties Alice and Bob as shown in Figure 1. Alice and Bob use two channels, the first being the classical channel consisting of digital bits $(0, 1)$ and the second being the quantum channel which is used for the transportation of qubits in the form of polarized photon states or any other degree of freedom to exchange secret key information between Alice and Bob. The quantum unit on both sides of the system handles the quantum states generation, detection and their interpretation in terms of secret keys. The network unit establishes digital communication between both the systems at a higher network layer. The processor unit supervises overall activity and ensures that the overall communication process is completed successfully with high efficiency.

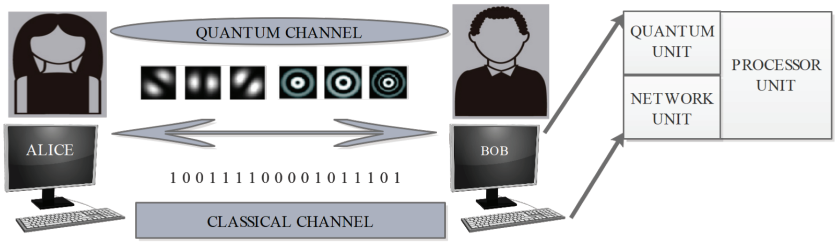

Figure 1. QKD basic system.

The quantum unit on both sides of the QKD system generates and controls the real time qubits by using computer generated binary holograms (CGBH) that is utilized by a type of SLM known as digital micromirror device (DMD). The optical engine (consisting of beam expander, mode cleaners, beam splitters etc.) within the quantum unit, also helps in the generation and propagation of Hermite–Gaussian and Laguerre–Gaussian beam spatial modes. For comparison of our system wide simulation results with those obtained analytically and numerically of the KMB09 protocol [18] we restrict our simulation to the cases of $N = 2$ and $N = 4$ dimensions. This includes designing the quantum unit, as shown in Figure 2 and a a detailed block level design as shown in Figure 3. The Laser is the basic constituent of all QKD systems for photonic communication. The different chemical and electrical properties of laser decides the propagation of photonic beam. For our simulation setup the laser has a polarized spectrum with a wavelength of 632 nm and having mode structure TEM_{00} greater than 95%. A TEM_{00} mode structure means that it follows the basic Gaussian beam having complex amplitude with phase angle in free space due to paraxial approximation as shown below [39]:

$$\boldsymbol{E}(r,z) = \boldsymbol{E}_0 \frac{W_0}{W(z)} exp\left\{ -\frac{r^2}{W(z)^2} \right\} exp\left[\iota \left\{ Kz - arctan\frac{z}{z_R} + \frac{Kr^2}{2R(z)} \right\} \right] \tag{4}$$

where $\boldsymbol{E_0}$ = Peak amplitude, z = Direction of propagation, $W(z)$ = Beam waist, K = Wavenumber $(2\pi/\lambda)$, λ = Wavelength, z_R = Rayleigh length and $R(z)$ = Radius of curvature.

The next component is the attenuator which decreases the laser power to modify the light beam in a controlled manner. The effect of reducing the laser pulse power leads to the creation of weak coherent pulses that contains minimal mean photon number (MPN) per pulse. For our simulation setup we choose a value of MPN to be 0.6 per pulse. This value has been shown to be experimentally valid as in [40]. The other notable component is the Galilean beam expanders utilized for the expansion of laser beam width with respect to the incident area of the SLM.

The SLM is the most important component of the currently designed QKD system [12, 41]. It is used for amplitude, phase or polarization modulation of light waves of the Gaussian laser beam to produce other modes of interest such as a Hermite–Gaussian (HG) and Laguerre–Gaussian (LG) beam spatial modes. SLM devices are divided into two categories namely the transmissive type and the reflective type [42]. Transmissive type

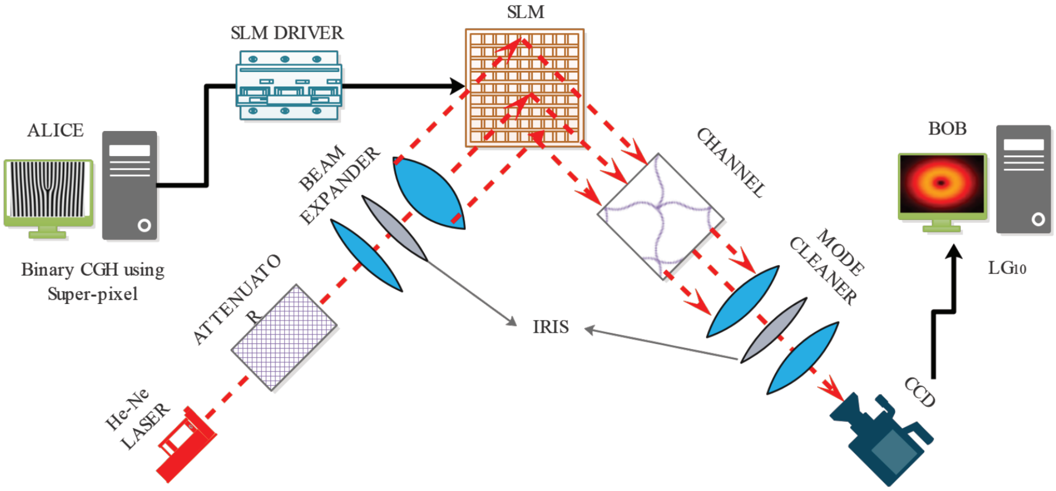

Figure 2. Quantum states generation and detection in two-dimensional KMB09 QKD system.

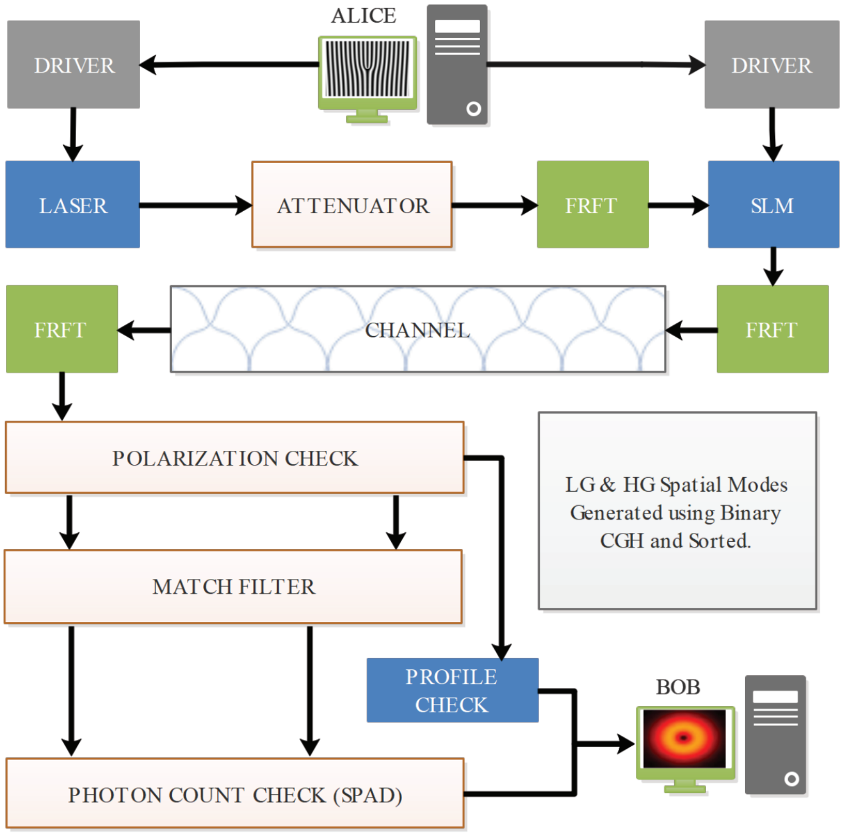

Figure 3. QKD system block diagram.

are made of liquid crystal material which are translucent [43] and the reflective type are made of liquid crystal microdisplays (LCOS) or small micromirrors (usually referred to as DMD) [44]. DMD contains row and column combination of many micro mirrors that are switched on and off by digital signals through a computer. This allows us to reflect the the incident light beam by ±12 degrees. The DMD pattern is controlled by dedicated computer software that has already processed the required binary hologram in the form of matrices essential for the generation of HG and LG beam spatial modes. Our simulation setup comprises of a DMD contains an array of 1024 × 768 micrometer sized mirrors with total active screen area of 14 × 10 mm and having 13.68 µm micromirror pitch.

For Cartesian coordinates, the amplitude and the phase angle terms of the Gaussian function Eq. (4) with respect to Hermite polynomial [45] is given as follows:

$$\boldsymbol{A}_{HG}(x,y,z) = \frac{1}{\omega(z)}\sqrt{\frac{2^{(1-n-m)}}{\pi n!m!}}\boldsymbol{H}_n\left\{\frac{\sqrt{x}}{\omega(z)}\right\}\boldsymbol{H}_m\left\{\frac{\sqrt{y}}{\omega(z)}\right\}exp\left[\left\{-\frac{\rho}{\omega(z)}\right\}^2\right] \tag{5}$$

and

$$\boldsymbol{\Phi}_{HG}(x,y,z) = exp[\iota(n+m+1)\xi(z)]exp\left[-\frac{\iota K\rho^2}{2R}\right]exp[-\iota Kz] \tag{6}$$

where n and m are positive integers.

Similarly for cylindrical coordinates, the amplitude and the phase angle terms of the Gaussian function Eq. (4) with respect to Laguerre polynomial [45] is given as follows:

$$\boldsymbol{A}_{LG} = \frac{\omega_0}{\omega(z)}\sqrt{\frac{2p!}{\pi(|\ell|+p)!}}\left(\frac{\sqrt{2}\rho}{\omega(z)}\right)^{|\ell|}\boldsymbol{L}_p^{|\ell|}\left[\left\{2\frac{\rho}{\omega(z)}\right\}^2\right]exp\left[\left\{-\frac{\rho}{\omega(z)}\right\}^2\right] \tag{7}$$

and

$$\boldsymbol{\Phi}_{LG} = exp[\iota(2p+|\ell|+1)\xi(z)]exp\left[-\frac{\iota K\rho^2}{2R}\right]exp[-\iota\ell\varphi] \tag{8}$$

where, $\ell(\mathbb{Z})$ denotes azimuthal index number and , $p(\mathbb{N})$ denotes radial index number.

The LG beam spatial modes have some important characteristic that are useful for the whole process of QKD system or quantum state tomography (QST). Compared to standard form i.e. LG_{00}, the higher order spatial LG modes have an extra rotating phase factor $\mathrm{e}^{\iota\ell\theta}$ concentric at origin [46]. This revolving phase term creates continuous visible radial component and its beam has what we call OAM around the axis. Each photon acquires OAM which is equal to the ℓ (OAM quantum number in $\hbar$ units). It is this special characteristic of OAM which makes the ℓ an essential quantum digit for the encoding of secret key over radial index number p [41].

4.1. N = 2 dimensions

For a two-dimensional state space the corresponding LG spatial modes have $\ell \in \{+1,-1\}$ and $p = 0$. From the above explanation, we now have the essential standard basis $|R\rangle$ which refers to $|0\rangle$ or $\ell = 1$, and $|L\rangle$ which refers to $|1\rangle$ or $\ell = -1$ as shown in Figure 4. This standard additional MUB is required for the measurement of a two dimensional QKD system [41, 47]. The superposition of these LG spatial modes will create further two MUBs [40]. Rectilinear basis comprises of $|V\rangle$ and $|H\rangle$ from $|\pm\rangle = |0\rangle \pm |1\rangle$. Diagonal basis comprises of $|D\rangle$

and $|A\rangle$ from $|\pm\iota\rangle = |0\rangle \pm \iota\,|1\rangle$. Finally, we have successfully compiled total of three MUBs with the help of following relations:

$$\begin{pmatrix}|R\rangle\\|L\rangle\end{pmatrix} \quad\Longrightarrow\quad |\boldsymbol{\tau}\rangle = \begin{pmatrix}|R\rangle+|L\rangle\\|R\rangle-|L\rangle\end{pmatrix} \quad \mathit{and} \quad |\boldsymbol{\upsilon}\rangle = \begin{pmatrix}|R\rangle+\iota\,|L\rangle\\|R\rangle-\iota\,|L\rangle\end{pmatrix}: \tag{9}$$

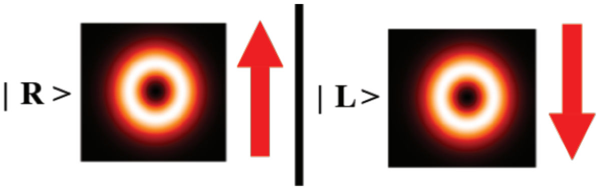

Figure 4. 2-dimensional standard basis analogy.

4.2. N = 4 dimensions

For a four-dimensional state space the corresponding LG spatial modes have $\ell \in \{+1,-1,+3,-3\}$ and again $p = 0$. As discussed in Section 4.1, we must need essential standard basis which refers to $|R_1\rangle$ or $\ell = +1$, $|L_1\rangle$ or $\ell = -1$, $|R_2\rangle$ or $\ell = +3$ and $|L_2\rangle$ or $\ell = -3$ for the measurement purpose as shown in Figure 5. The superposition of these LG spatial modes will further create other two MUBs required for the QKD process [40, 48]. Finally, we have successfully compiled all three MUBs as follows, which are required for our simulation setup to execute the KMB09 protocol using higher order LG and HG spatial modes.

$$\begin{pmatrix}|R_1\rangle\\|L_1\rangle\\|R_2\rangle\\|L_2\rangle\end{pmatrix} \quad\Longrightarrow\quad |\boldsymbol{\tau}\rangle = \begin{pmatrix}|R_1\rangle+|L_1\rangle\\|R_1\rangle-|L_1\rangle\\|R_2\rangle+|L_2\rangle\\|R_2\rangle-|L_2\rangle\end{pmatrix} \quad \mathit{and} \quad |\boldsymbol{\upsilon}\rangle = \begin{pmatrix}|R_1\rangle+\iota\,|L_1\rangle\\|R_1\rangle-\iota\,|L_1\rangle\\|R_2\rangle+\iota\,|L_2\rangle\\|R_2\rangle-\iota\,|L_2\rangle\end{pmatrix}: \tag{10}$$

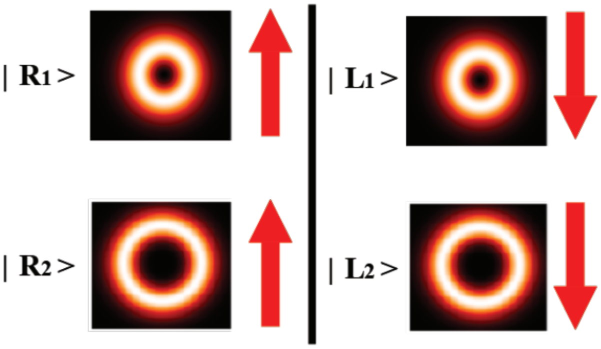

Figure 5. 4-dimensional standard basis analogy.

In either case of HG or LG spacial modes, the required holograms matrices equations, which are encoded on the DMD, will be similar in nature except for their specific amplitude and phase terms [45] i.e.

$$\boldsymbol{\Phi}_{SLM} = \boldsymbol{f}_{A\Phi}\Big[\boldsymbol{\Phi}_{HG/LG} + G_x X + G_y Y\Big] \tag{11}$$

where $\boldsymbol{f}_{A\Phi}$ is the amplitude phase function can be found easily by numerical evaluation from the following relation:

$$\boldsymbol{J}_1 \quad \left[\boldsymbol{f}_{A\Phi}\right] = \boldsymbol{A}_{HG/LG} \tag{12}$$

where, $\boldsymbol{J}_1$ is the first order Bessel function and $\boldsymbol{A}_{HG/LG}$ is the amplitude found in the Eqs. (5 and 7).

As the holograms are developed according to the desired higher order Gaussian beam spatial modes, this pattern will be displayed on the DMD. This is achieved by using the special SLM driver board controlled separately by computer software control code. When the laser light beam is incident on the DMD surface area, the reflective mirrors of the DMD (based on desired hologram pattern) will produce various higher order spatial modes i.e. HG or LG. The mode cleaner module now selects the 1st order spatial mode and removes the other modes. As far as the experimental setup is concerned, the spatial modes wave-fronts can be monitored at the reception side, i.e. Bob, on a high definition CCD camera which is attached to a computer.

The detection or sorting process consists of a polarization check and matched filtering. The polarization check is carried out by an optical Mach–Zehnder interferometer (MZI). The MZI is used for variation checking in the relative phase shift measurement of the two beams generated from the same single source and propagating independently. Laser beams phase measurement are independently monitored in the polarization block and the same beam propagates further towards the matched filter in which a projective-based method is used [40]. In this method the laser beam coherent pulse containing photons is incident on a device that makes projection with respect to the OAM eigenstate before measurement. Once again the dynamically created CGBH of phase patterns are utilized for such purpose. The holograms are displayed on the transmissive type SLM coupled with single-mode fiber (SM Fiber). If the incoming photon state is conjugate with respect to the phase hologram of SLM, then the nonzero value of ℓ will be converted into standard Gaussian TEM_{00} like mode and impacts on the SM fiber along the axis of the fiber and hence increments the photon count. Alternatively, other modes will be nullified and no photons detected or sorted [40, 49]. The SM fiber paths are then merged optically and then both of the outputs are directed towards single-photon counting block or single photon avalanche diode (SPAD) as shown in Figure 3.

4.3. Simulation details

The firmware was developed for the simulation of KMB09 QKD protocol using Python language version 3.7 (64 bit) over Visual Studio platform (2019). The main open source libraries which were used in support of the simulation are matplotlib, slm-essentials, skimage, csv, PIL an CV2. Mainly there are two core processes: (1) Random generation of quantum states and (2) Detection of the quantum states using match filter logic. All SLM parameters are set as already explained in the simulation setup section. The fundamental steps required to carry out the complete simulation process is as follows:

1. First, all the SLM (DMD) parameters are initialized and a blank array of SLM screen size is created.

2. With the help of our customised slm-essentials library the above generated blank arrays is processed that results in creating the quantum states amplitude matrices. This also generates the holograms required practically to drive the SLM for the generation of specified higher order Gaussian beam spatial mode, i.e HG and LG modes.

3. The randomly generated quantum states amplitude matrices are separately stored for the transmission process.

4. Once the transmission process starts, the detection logic is applied on one state at a time with the help of matched filter mechanism. This is accomplished using open source skimage library, which is famous for structural similarity index measure (SSIM). The incoming quantum state's amplitude matrix is multiplied by the conjugate phase matrix of hologram of specified standard basis Gaussian state. The resulting plot is then compared with the standard TEM_{00} mode using skimage metrics.

5. The SSIM value decides the increment or decrements of photon counts of corresponding higher order Gaussian state.

6. At the end of simulation process and according to KMB09 protocol flow, the efficiency $\boldsymbol{\eta}$ is calculated using simply the division of the total number of the correct outcomes and the total number of quantum states generated at transmission sides.

7. While simulating the KMB09 protocol in both the mentioned dimensions, all above steps are followed with only change in dimension variables (which shows change in standard basis and corresponding measurement basis only).

5. Results

In this section we present and compare system efficiency $\boldsymbol{\eta}$ results of KMB09 protocol in two and four dimensional state. $\boldsymbol{\eta}$ is a universally accepted system metric for a QKD system [18, 50, 51] and is given by Eq. (13). The KMB09 protocol analytical and numerical results [18] are compared to our system results obtained after KMB09 protocol simulation. The simulation setup was carried out as discussed in Section 4.3.

$$\boldsymbol{\eta}_A = \frac{\boldsymbol{N-1}}{\boldsymbol{2N}} \tag{13}$$

where $\boldsymbol{\eta}_A$ = Analytical efficiency and $\boldsymbol{N}$ = Number of dimension.

The design of the proposed setup is such that the system first generates the CGBH as shown in Figure 6 for all the 3 MUBs, according to the DMD specified resolution in terms of pixels ratio i.e. 1024 × 768. This starts the QKD process according to the KMB09 protocol. Number of iterations occur several times and the system's efficiency $\boldsymbol{\eta}_S$ is noted against each iteration $\boldsymbol{i}$. The results are shown in Figure 7 wherein the y-axis denotes the efficiency $\boldsymbol{\eta}_S$ and the x-axis denotes the number of iterations performed on the simulated QKD system. From Figure 7 we observe that as we increase the number of iterations in our system, the value of $\boldsymbol{\eta}_S$ converges to a mean of 0.25 in case of two dimension and 0.3683 in case of four dimension.

The effect of number of iterations i.e. $i = \{50, 100, 150, 200, 250\}$ on the accuracy of average system efficiency $\boldsymbol{\eta}_S$ has also been explored and the results given in Figure 8. The figure has $\boldsymbol{\eta}_S$ of the simulated system on the y-axis and the number of iterations $\boldsymbol{i}$ on the x-axis. We observe from Figure 8 that average value of $\boldsymbol{\eta}_S$ for KMB09 approaches $\boldsymbol{\eta}_A$ in both cases i.e. for two dimension it has a value of 0.25 and for four dimension it has a value of 0.3683.

$$\boldsymbol{Error} \quad \% = \left| \frac{\boldsymbol{\eta}_S - \boldsymbol{\eta}_A}{\boldsymbol{\eta}_A} \right| \times \mathbf{100} \tag{14}$$

Finally Figure 9 depicts the % error between the $\boldsymbol{\eta}_S$ and $\boldsymbol{\eta}_A$ obtained at selected number of iterations i.e. $\boldsymbol{i}$ = {50, 100, 150, 200, 250}. Eq. (14) is used to compute the % error of the simulated and analytical

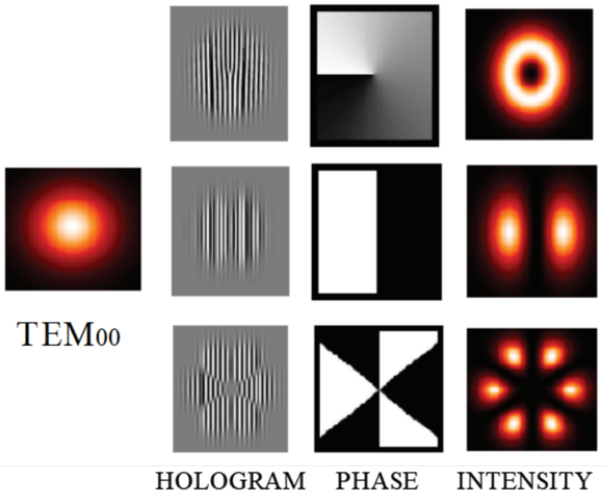

Figure 6. Wavefront results obtained from Gaussian standard mode through desired hologram patterns.

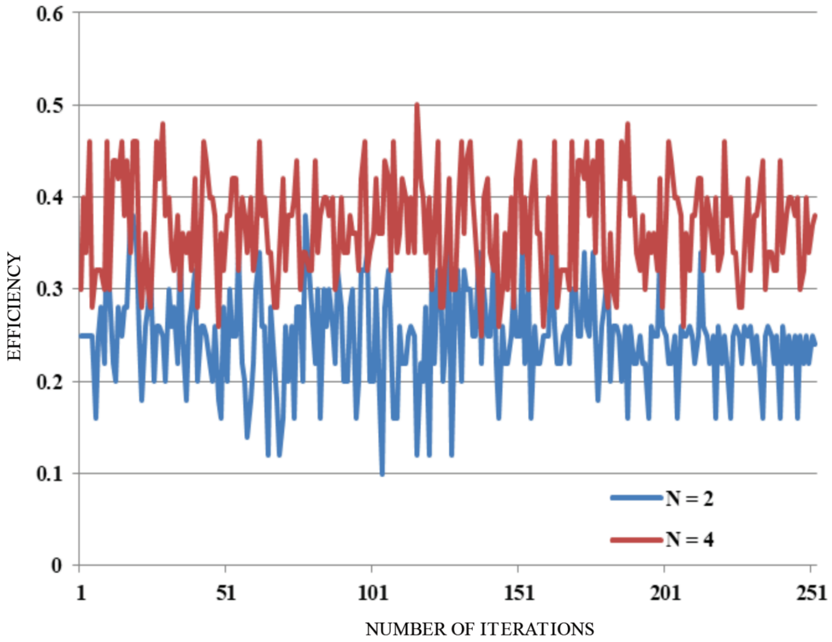

Figure 7. Efficiency of KMB09 protocol in 2 and 4 dimensions as a result of proposed system simulation.

efficiency for $n = 2$ and 4 dimensions. For the two dimension case we observe that the % error is maximum for 50 iterations and reaches a minimum value of approximately 1.25% when the number of iterations are 250. However, we observe some variation in values between 50 and 250 iterations which subsequently settles to a stable value at 250 iterations. However for the four dimensional case, we observe from Figure 9 that the simulation setup provides a stable value of 1.8% for % error at 250 iterations. The variation in the value for this case is minimal when compared to the two dimensional case.

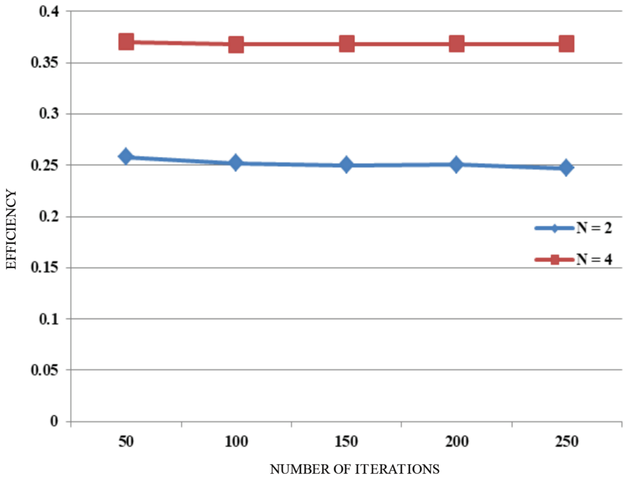

Figure 8. Effect of number of iterations on the average efficiency of KMB09 simulated system.

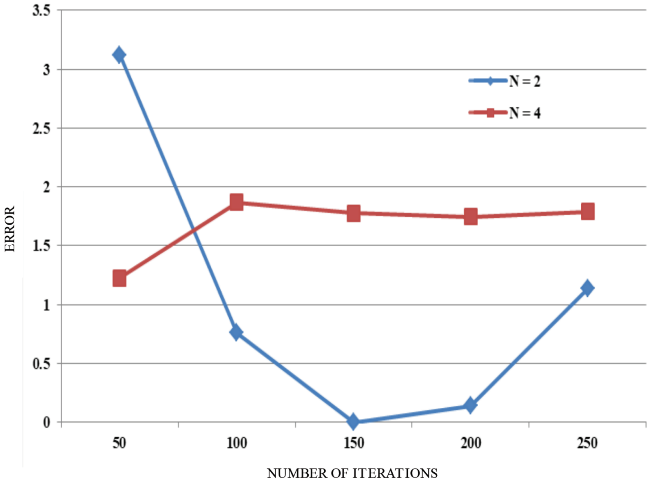

Figure 9. % Error in average efficiency of KMB09 protocol (analytical and simulated) for N = 2 and N = 4 cases.

6. Conclusion

Higher dimensional quantum key distribution protocols have many advantages over other conventional protocols but their system simulation and implementation is very challenging. KMB09 is one such protocol whose two-dimensional and four-dimensional versions are simulated between end to end users via the proposed QKD system simulation setup. To compare the accuracy of the simulated system we use efficiency η as the QKD system performance metric and compare it with the numerical and analytical efficiencies of the KMB09 QKD protocol in both cases. From the obtained results, we see that the system efficiency for both methods converges to a value of 0.25 in the case of two dimensions and 0.3683 in the case of four dimensions . This shows that the accuracy of our simulated QKD system is inline with that of the analytical model. In the future, work we aim to evaluate the proposed QKD setup for error rate due to eavesdropping as a result of intercept-and-resend attack.

Acknowledgments

We acknowledge funding from Higher Education Commission, Pakistan under the Quantum Technology Research Lab of National Center for Cyber Security (NCCS) at NED University of Engineering and Technology. Special thanks to Prof. Andrew Forbes, Distinguished Professor of Physics, University of the Witwatersrand, South Africa, whose detailed work ”How to Shape Light with Spatial Light Modulators” helped us in better understanding SLM and its applications. Thanks to Mr. Safdar Hussain for his valuable comments and discussion during this research.

References

[1] Mosca M. Cybersecurity in an era with quantum computers: will we be ready? IEEE Security & Privacy 2018; 16 (5): 38-41. doi: 10.1109/MSP.2018.3761723

[2] Zhou T, Shen J, Li X, Wang C, Shen J. Quantum cryptography for the future internet and the security analysis. Security and Communication Networks 2018; 1: 1-20.

[3] Peres A. Quantum Theory: Concepts and Methods. USA: Springer Science & Business Media, 2006. doi: 10.1007/0-306-47120-5

[4] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 1978; 21 (2): 120-6. doi: 10.1145/359340.359342

[5] Shen J, Zhou T, Chen X, Li J, Susilo W. Anonymous and traceable group data sharing in cloud computing. IEEE Transactions on Information Forensics and Security 2017; 13 (4): 912-25. doi: 10.1109/TIFS.2017.2774439

[6] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 1985; 31 (4): 469-72. doi: 10.1109/TIT.1985.1057074

[7] Tseng YM. An efficient two-party identity-based key exchange protocol. Informatica 2007; 18 (1): 125-36. doi: 10.15388/Informatica.2007.168

[8] Tang X, Ma L, Mink A, Chang T, Xu H et al. High-speed quantum key distribution systems for optical ber networks in campus and metro areas. In: Quantum Communications and Quantum Imaging VI. International Society for Optics and Photonics; New York, NY, USA; 2008. pp. 70920I. doi: 10.1117/12.793852

[9] Wang Q, Wang XB. Simulating of The Measurement-Device Independent Quantum Key Distribution With Phase Randomized General Sources. USA: Nature, 2014. doi: 10.1038/srep04612

[10] Rosenberg D, Peterson CG, Harrington JW, Rice PR, Dallmann N et al. Practical long-distance quantum key distribution system using decoy levels. New Journal of Physics 2009; 11 (4): 045009. doi: 10.1088/1367-2630/11/4/045009

[11] Hariharan P, Hariharan P. Optical Holography: Principles, Techniques and Applications. Division of Applied Physics. CSIRO. Canberra, ACT, Australia: Cambridge University Press, 1996. doi: 10.1017/CBO9781139174039

[12] Gruneisen MT, Miller WA, Dymale RC, Sweiti AM. Holographic generation of complex fields with spatial light modulators: application to quantum key distribution. Applied Optics 2008; 47 (4): A32-A42. doi: 10.1364/AO.47.000A32

[13] Magaña-Loaiza OS, Mirhosseini M, Cross RM, Rafsanjani SM, Boyd RW. Hanbury Brown and Twiss interferometry with twisted light. Science Advances 2016; 2 (4): e1501143. doi: 10.1126/sciadv.1501143

[14] Islam NT, Lim CC, Cahall C, Kim J, Gauthier DJ. Provably secure and high-rate quantum key distribution with time-bin qudits. Science Advances 2017; 3 (11): e1701491. doi: 10.1126/sciadv.1701491

[15] Wang J, Qin X, Jiang Y, Wang X, Chen L et al. Experimental demonstration of polarization encoding quantum key distribution system based on intrinsically stable polarization-modulated units. Optics Express 2016; 24 (8): 8302-8309. doi: 10.1364/OE.24.008302

[16] Mirhosseini M, Magaña-Loaiza OS, O'Sullivan MN, Rodenburg B, Malik M et al. High-dimensional quantum cryptography with twisted light. New Journal of Physics 2015; 17 (3): 033033. doi: 10.1364/FIO.2014.FM4E.4

[17] Goodman JW, Lawrence RW. Digital image formation from electronically detected holograms. Applied Physics Letters 1967; 11 (3): 77-79. doi: 10.1063/1.1755043

[18] Khan MM, Murphy M, Beige A. High error-rate quantum key distribution for long-distance communication. New Journal of Physics 2009; 11 (6): 063043. doi: 10.1088/1367-2630/11/6/063043

[19] Peřinová V, Lukš A. Quantization of Hermite–Gaussian and Laguerre–Gaussian beams and their spatial transformations. Journal of Modern Optics 2006; 53 (5-6): 659-675. doi: 10.1080/09500340500254285

[20] Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters 2000; 85 (2): 441. doi: 10.1103/PhysRevLett.85.441

[21] Kohnle A, Rizzoli A. Interactive simulations for quantum key distribution. European Journal of Physics 2017; 38 (3): 035403. doi: 10.1088/1361-6404/aa62c8

[22] Jakobi M, Simon C, Gisin N, Bancal JD, Branciard C et al. Practical private database queries based on a quantum-key-distribution protocol. Physical Review A 2011; 83 (2): 022301. doi: 10.1103/PhysRevA.83.022301

[23] Gao F, Qin S, Huang W, Wen Q. Quantum private query: a new kind of practical quantum cryptographic protocol. Science China Physics, Mechanics & Astronomy 2019; 62 (7): 70301. doi: 10.1007/s11433-018-9324-6

[24] Mailloux LO, Morris JD, Grimaila MR, Hodson DD, Jacques DR et al. A modeling framework for studying quantum key distribution system implementation nonidealities. IEEE Access 2015; 3: 110-130. doi: 10.1109/ACCESS.2015.2399101

[25] Engle RD, Hodson DD, Grimaila MR, Mailloux LO, McLaughlin CV et al. Modeling quantum optical components, pulses and fiber channels using omnet++. In: 2nd OMNeT++ Community Summit; IBM Research - Zurich; Zurich, Switzerland; 2015. pp. 1-20.

[26] Archana B, Krithika S. Implementation of BB84 quantum key distribution using OptSim. In: IEEE 2015 2nd International Conference on Electronics and Communication Systems (ICECS) - Karpagam College of Engineering; Coimbatore, Tamil Nadu, India; 2015. pp. 457-460. doi: 10.1109/ECS.2015.7124946

[27] Hussain SS, Khan MM, Baig MM, Wang G. Numerical modelling of quantum key distribution system for KMB09 protocol. International Journal of Computer Science and Information Security 2016; 14 (8): 140.

[28] Shall S, Monir MS, Rahman MS. Numerical modeling and simulation of quantum key distribution systems under non-ideal conditions. In: IEEE 2017 International Conference on Telecommunications and Photonics (ICTP) - Bangladesh University of Engineering and Technology (BUET); Bangladesh; 2017. pp. 38-42. doi: 10.1109/ICTP.2017.8285898

[29] Wang F, Zeng P, Wang X, Gao H, Li F et al. Towards practical high-speed high dimensional quantum key distribution using partial mutual unbiased basis of photon's orbital angular momentum. arXiv 2018; arXiv:1801.06582.

[30] Mao CC, Li J, Zhu JR, Zhang CM, Wang Q. An improved proposal on the practical quantum key distribution with biased basis. Quantum Information Processing 2017; 16 (10): 256. doi: 10.1007/s11128-017-1707-7

[31] Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theoretical Computer Science 2014; 560 (1): 7-11. doi.org/10.1016/j.tcs.2014.05.025

[32] Bengtsson I. Three ways to look at mutually unbiased bases. AIP Conference Proceedings American Institute of Physics 2007; 889 (1): 40-51. doi: 10.1063/1.2713445

[33] Mayers D. Unconditional security in quantum cryptography. Journal of the ACM 2001; 48 (3): 351-406. doi: 10.1145/382780.382781

[34] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information. Cambridge, UK: Cambridge University Press, 2002, pp. 558-559. doi: 10.1017/CBO9780511976667

[35] Elboukhari M, Azizi A, Azizi M. Implementation of secure key distribution based on quantum cryptography. In: IEEE 2009 International Conference on Multimedia Computing and Systems; Cancun, Mexico; 2009. pp. 361-365. doi: 10.1109/MMCS.2009.5256673

[36] Elboukhari M, Azizi M, Azizi A. Quantum key distribution protocols: a survey. International Journal of Universal Computer Science 2010; 1 (2): 1-20.

[37] Brierley S. Quantum key distribution highly sensitive to eavesdropping. arXiv 2009; arXiv:0910.2578.

[38] Khan MM, Xu J, Beige A. A detailed analysis of kmb09 qkd protocol. International Journal of Computer Science and Information Security 2017; 15 (1): 529.

[39] Paschotta R. Gaussian Beams. Encyclopedia of Laser Physics and Technology. USA: Springer, 2011

[40] Nicolas A, Veissier L, Giacobino E, Maxein D, Laurat J. Quantum state tomography of orbital angular momentum photonic qubits via a projection-based technique. New Journal of Physics 2015; 17 (3): 033037. doi: 10.1088/1367-2630/17/3/033037

[41] Mafu M, Dudley A, Goyal S, Giovannini D, McLaren M et al. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. Physical Review A 2013; 88 (3): 032305. doi: 10.1103/PhysRevA.88.032305

[42] Harriman J, Serati S, Stockley J. Comparison of transmissive and reflective spatial light modulators for optical manipulation applications. In: Proceeding of SPIE 5930, Optical Trapping and Optical Micromanipulation II; San Diego, CA, US; 2005. pp. 59302D. doi: 10.1117/12.619283

[43] Dorrah AH, Zamboni-Rached M, Mojahedi M. Experimental demonstration of tunable refractometer based on orbital angular momentum of longitudinally structured light. Light: Science & Applications 2018; 7 (1): 1-2. doi: 10.1038/s41377-018-0034-9

[44] Mirhosseini M, Magana-Loaiza OS, Chen C, Rodenburg B, Malik M et al. Rapid generation of light beams carrying orbital angular momentum. Optics Express 2013; 21 (25): 30196-203. doi: 10.1364/OE.21.030196

[45] Rosales-Guzmán C, Forbes A. How to Shape Light With Spatial Light Modulators. Bellingham, WA, USA: SPIE Press, 2017. doi: 10.1117/3.2281295

[46] Plick WN, Lapkiewicz R, Ramelow S, Zeilinger A. The forgotten quantum number: a short note on the radial modes of Laguerre-Gauss beams. arXiv 2013; arXiv:1306.6517.

[47] James DF, Kwiat PG, Munro WJ, White AG. Measurement of qubits. Physical Review A 2005; 64: 052312. doi: 10.1103/PhysRevA.64.052312

[48] Ding Y, Bacco D, Dalgaard K, Cai X, Zhou X et al. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. NPJ Quantum Information 2017; 3 (1): 1-7. doi: 10.1038/s41534-017-0026-2

[49] Forbes A, Nape I. Quantum mechanics with patterns of light: progress in high dimensional and multidimensional entanglement with structured light. AVS Quantum Science 2019; 1 (1): 011701. doi: 10.1116/1.5112027

[50] Fung CH, Tamaki K, Lo HK. Performance of two quantum-key-distribution protocols. Physical Review A 2006; 73 (1): 012337. doi: 10.1155/2018/8214619

[51] Wang J, Zhang Q, Tang CJ. Quantum key distribution protocols using entangled state. In: IEEE 2006 International Conference on Computational Intelligence and Security; Guangzhou, China; 2006. pp. 1355-1358.