International Journal of Information & Network Security (IJINS)
Vol.2, No.4, August 2013, pp. 311~321
ISSN: 2089-3299

A Theoretical Model of Multi-user QKD Network as the Extension of E91 Protocol

Vikas Jha*, Pankaj Srivastava*
* Quantum Computing and Information Group, ABV-Indian Institute of Information Technology and Management Gwalior, M.P. 474015, India

Article Info

Article history:

Received Apr 29th, 2013
Revised Jun 5th, 2013
Accepted Jul 26th, 2013

Keyword:

Entanglement
Quantum Cryptography
Quantum key distribution
Hadamard transform

ABSTRACT

A theoretical model is represented by us towards the scope of developing a Quantum key distribution network. There is always a requirement of secured and confidential information processing so that the authentic and legitimate information one can get each time. Hence the quest for obtaining a perfect cypher continues. Considering the recent development in cryptography it was found that quantum mechanics exhibiting more solidarity when applied to cryptography and that generated a new dimension of secured information processing known as Quantum Cryptography. We propose a theoretical model of a network that will be used for quantum key distribution among $n \times n$ users of the network as the extension of two-party E91 protocol for multiple users simultaneously. Applying the concept of parallel Hadamard transform with optical fiber channels gives us the platform of WDM multiplexing and de-multiplexing through the network.

Corresponding Author:

Vikas Jha,
Quantum Computing and Information Group,
ABV-Indian Institute of Information Technology and Management Gwalior
Morena Link Road, Gwalior, Madhya Pradesh, 474015, India
Email: vikas.jnct@gmail.com

1. INTRODUCTION

Quantum communication is thought to be the future of communication engineering. Quantum cryptography [1, 2] started gaining popularity since the proposal of a two party key sharing protocol based on conjugate observables by Charles H. Bennett, of the IBM T. J. Watson Research Center and Gilles Brassard of the Université de Montréal in the year 1984 popularly known as the BB84 protocol [1]. BB84 represents how the polarization of photons one of its physical property and its analysis by the polarization analyzer during detection helps processing of a secret bit streams. Prior to this in the early 1970s, the concept of quantum conjugate coding was introduced by Stephen Wiesner [3], at Columbia University in New York. Stephen showed how linear and circular polarisation of photon can help in decoding of information. However in the year 1991 Artur Ekert [6, 7] proposed a quantum key distribution model based on entanglement of photons. They proposed that the property of entanglement can enhance the feature of quantum cryptography so that it gives the freedom of the selection of a source of photon entanglement in terms of reliablity. The same cryptography key sharing can happen if the Eve handles or control the source of photon entanglement. Each time the source generates two photons having polarisation entanglement, one of them is send to Alice and other one to Bob. And the separate and independent polarization measurement by both of the detectors will result into a key if the direction of polarization measurement is compatible at both locations. There was yet another protocol by C. H. Bennett which was discussed in the year 1992, famous as B92 protocol [2]. This was based on phase analysis of the photon. Until now there are many specification protocols developed but the world is waiting for a still to come milestone in this domain that will support a huge load of communication traffic which is increasing day by day in ordinary life. It is worth to say quantum cryptography is a better commercial alternative to more conventional present day technology of classical

cryptography. Many researchers and industrialists are involving in the development of various Quantum Key Distribution (QKD) plug and play setup. Implementations are being done for desirable channel length by considering the most suitable and mature process of communication of present era, the photonic communication through optical fiber channel. It was found that photonic communication is the best choice for Quantum Cryptography and Quantum information processing. We are proposing a new approach in this paper for the establishment of a Quantum multi-user key distribution network a backbone network for secured multi-user QKD using the concept of entanglement of photons, and based on E91 model [6, 7]. Entanglement gives a superposition state to a photon pair known as EPR state and the theory that entanglement did not hide local variables is famous as EPR paradox by Einstien, Podolsky and Rosen in the year 1935 [4]. Core concept of our network is the transmission of entangled photons at different wavelength by WDM multiplexing. Fixing of the wavelength will give the network a wavelength based addressability, however the purpose of this network is to share N number of keys through the network and distributed among N-users at the opposite end. This needs N-entangled photons to be transmitted through the channel at a time by wavelength division multiplexing them. Quantum Entanglement [18] is a part of Quantum mechanics that tells us about certain parameter based mutual correlation among two particles which are generated and then separated. With photon entanglement, a pair of photon is generated having correlation in either temporal or spectral distribution of photon wave-function [8, 11, and 13]. There is very interesting theory behind quantum entanglement considering a paper published in the year 1935 [4] about quantum mechanical distribution of real world objective that quantum mechanics was insufficient to explain objective reality and it was concluded that quantum hides some local variables. John S. Bell carried further the EPR theory about local hidden variables originally published in the journal Physics in 1964 [5]. Whereas above discussion made by Einstein, Podolsky and Rosen famous as EPR paradox was later justified that quantum mechanical distribution did not hide any local realistic variable.

The EPR analysis of quantum mechanics is famous as EPR paradox and it is related with entanglement of photon. Therefore entanglement opposes the foundations of classical realm and proposes that particles quantum property is related to another particles in such a way that a change or measurement made to it changes the property of others practically separated. Whereas to objectify entangled particle one has to perform measurement with true basis of correlation or degree of freedom and thus measuring one particle's information the objective realm of other particle can be obtained. If Eve is performing such an activity then quantum bit error ratio (QBER) is supposed to increase and the presence of Eve can be detected by further calculating QBER. To generate entangled photon pair the most common and matured technique used is Parametric down conversion also called as PDC [8, 11, 13, 14], which uses a Laser source and a non linear crystal. Thus interaction of photons at higher frequency is pumped towards a crystal with non-linearity function (χ^2). When light is propagated towards an optically non-linear crystal its non-linearity gives correlations in certain degree of freedom and generates a photon pair as idler and signal photons, these photons are entangled due to Energy and Momentum conservation principle. Photon pair generated by this technique has entanglement in different degrees of freedom such as position-momentum or time-energy entanglement. Optical fiber communication [17] was found more efficient if wavelength of photon is kept around 1550 nm so that losses are minimum or negligible.

2. DEVICE REQUIREMENT

2.1. Source of entanglement

Generating a high frequency photon from laser at pump frequency ω_p and then it is made to pass through a non-linear optical crystal. The crystal behaves as a source of polarization entanglement that generates a pair of entangled photons at low frequencies respectively ω_i and ω_s so that one of the photons will be detected by user A and other by user B. The polarization entangled photons are generated from a type-II BBO crystal [8, 11] which uses the concept of spontaneous parametric down conversion (SPDC). The network we are discussing requires a central system consisting of n set of lasers and crystal so that each time n pairs of entangled photons at respective frequencies can be generated for further transmission from the optical fiber channel.

2.2. Wavelength Selective Filtering

The transmission of photons is done by dense wavelength division multiplexing. Thus it is required that different entangled photons are at different frequencies which are capable to identify according to the users. The approach is that each pair of users to which a key is to be shared will only receive the pair of entangled photons and further detect them.

2.3. Parallel Hadamard gates

A Hadamard gate behaves like an operator to qubits so that, if qubit 0, $|0>$ is applied to a Hadamard gate it will transform into the qubit state as given by the following equation,

$$H|0> = \frac{(|0> + |1>)}{\sqrt{2}} \quad (1)$$

However qubit 1, $|1>$ is transformed as shown in Eq. (2) given below, when applied to a Hadamard gate.

$$H|1> = \frac{(|0> - |1>)}{\sqrt{2}} \quad (2)$$

A Hadamard transform in the matrix form is shown in the equation below,

$$[H] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (3)$$

Parallel Hadamard gates plays interesting role in Quantum algorithms. We can obtain a Hadamard transform from n-Hadamard gates in parallel acting on n parallel qubits. Using of parallel Hadamard gates helps in order to get a wavelength division multiplexed wavepacket comprising of different signal photons at different wavelength. The wavepacket will exactly represent a large hilbert space tensor product of individual signal photons. Thus using of parallel Hadamard gates gives us a sense of wavelength division multiplexing.

2.4. Setting of Communication Channel length

Optical communication using optical fiber is the mature method of signal transmission used in present communication technology. There are few limitations of entanglement; one of them is that the correlation does not hold for longer distances of fiber length [8]. Therefore a broad area research is being done to increase this length of fiber channel for proper and secured transmission of entangled photons such that the correlations among photons do hold for a longer distance. Going through numerous papers it was found that setting of proper channel length to provide good key rate with optimized QBER is a challenge to quantum communication. A number of implementations in the field of QKD have been done for certain range of optical fiber by using BB84 or B92 protocols. But increasing of the channel length for entangled photon transmission is that specific area where maximum stress is given these days. One method to increase the channel length may be using of quantum repeaters so that the same sequence of photons at particular wavelength with correlation will be regenerated before that photon losses its entanglement degree of freedom. Some specific kind of material is also being prepared for manufacturing optical fiber so that no loss in entanglement will happen with transmission of photons; optical solitan is one such material. Solitan gives a compromising nonlinearity to the waves so that no dispersion happens in the wavelength of multiplexed optical signal.

2.5. APD Detectors

For developing such a network there is a requirement of a high performance single photon detector at A as well as B user's location. The detector is supposed to be useful to identify good spectral range, the dead time, rate of dark count, jitter during continuous photon receiving, with good detection efficiency, and its ability of resolving photon number. On the basis of above stated parameters a good working detector can be devised and utilized for designing of such a Quantum network. In previous years there was lots of photon detectors designed by using photomultipliers tubes but semiconductor APDs have replaced them in present era of technology. Using of (Si-SPAD) Silicon single-photon avalanche photodiodes [19] is now a popular tool for using them as detectors in laboratory quantum optics experiments as well as the free space QKD systems.

2.6. Photon polarization analysis

During the detection of respective photons of the entangled photon pair at A and B locations proper photon polarization analysis of received photon is to be carried out. According to the E91 or Ekert protocol [6, 7] users A and B perform their separate basis analysis and measurement in a manner so that if basis of

user B matches with that of user A then both of them will have exactly the same information bit but if no basis matching there will be no sharing of information and that detected photon is liable to be discarded. Thus we need different polarization analyzer attached with respective APD detectors [19] which will be used to analyse the polarization of photon wave.

2.7. Public Channel Communication

After successive entangled photon distribution and detection between A and B, user A should know the basis of measurement used by B and therefore both of them communicate through a public channel so that A will listen to the B all of the measurement basis used by him in sequence. A listen to them and matches with measurement basis of his own. Therefore it is the measurement basis announced by B via public channel after the measurement of photon which will help knowing of shared quantum bit stream between them. Eve can't predict the actual information shared and thus key will remain intact and secret.

2.8. Error Detection and Correction

Key rate is estimated with the final process of network communication i.e. the error detection and error correction methodology. Users A and B have to use error correction and error detection process in order to insure that both of them have identical key. Basic approach to achieve this is from the classical bit correction approach. They can perform a parity checking matrix. Using of Shannons minimum function [15] to obtain the minimum amount of information needed to correct two identical strings of bits. However we are referencing here the approach of Brassard and Salvails Cascade algorithm for error correction used in QKD experiment by Catherine Holloway [14]. In the cascade approach several rounds of parity checking is done and then a binary search is used to determine the source of error.

2.9. Toolbox for Simulation

There are certain toolbox developed in various scripting languages and thus they can help in analyzing of the photonic quantum information transfer and related performance measurement that of a quantum environment and quantum computer. Quantum toolbox of implementations in Python (QuTiP) [16] is a newly developed toolbox for simulation in a quantum mechanical environment developed for scripting in python. Considering the experimental work done by Thomas Jennewein and Catherine Holloway [13] so that they give the successful experimental validation of entanglement distribution our entanglement distribution can also be optimized.

3. QUANTUM KEY DISTRIBUTION NETWORK

3.1. Proposed Network Layout

The proposed Quantum communication network has been shown in Fig (1). The QKD network will work according to step written in the methodology in subsection 3.2. We see that the architecture of the network is proposed to have distribution of quantum key among multiple users simultaneously. Users from A side can share their secret quantum key to any of the users from B side. The network is proposed for providing quantum cryptographic key distribution among total of $n \times n$ users. Dense wavelength division multiplexing is considered so that the photon wavelength will remain in the conventional or C-band.

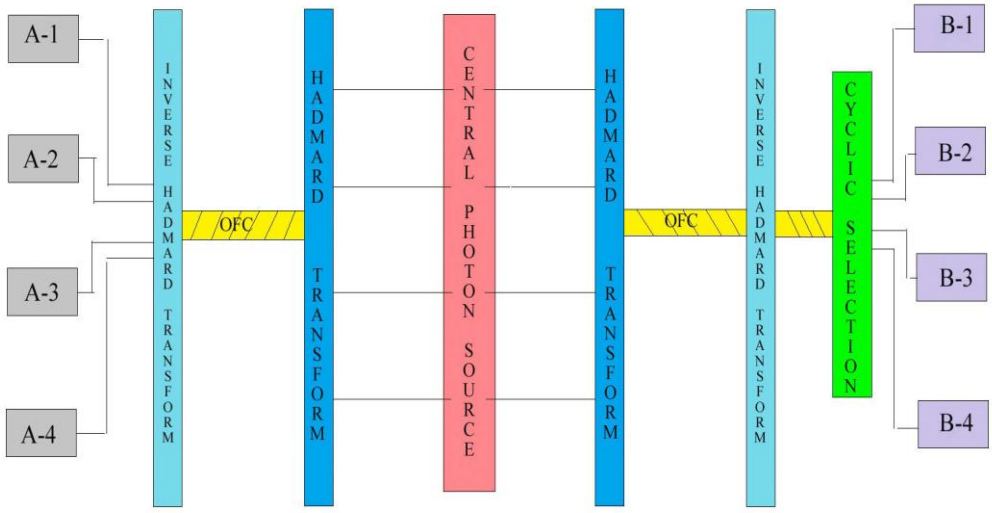

Figure 1: QKD network block diagram with 4x4 users respectively A-side and B-side.

As the diagram is shown in figure-(1), a central system for entangled photon generation is kept in the middle. There will be a secret key distribution between n-pair of users through the network. The network is secured enough in the case if Eve handles the central system since Eve herself don't know what is the key by transmitting the entangled photons.

1) Central source consists of n-set of non-linear crystals to generate n-pairs of photons at a time.
2) Four set of Hadmard transform system.
3) One cyclic photon distribution system. (Cyclic selection switching)
4) A total of n-pairs of single photon detectors and photon polarization analyzers.

3.2. Methodology

As the diagram is shown in figure-(1), a central system for entangled photon generation is kept in the middle. There will be a secret key distribution between n-pair of users through the network respectively the A-side users and the B-side users. The network is secured enough in the case if Eve handles the central system since Eve herself don't know what is the key by transmitting the entangled photons. Here the source of photon is kept central to the network so that it is in the midway between the path from A user to B user, similar to Ekert's E91 [6, 7] two party protocol. The schematic of a basic E91 protocol is shown in the figure-(2).

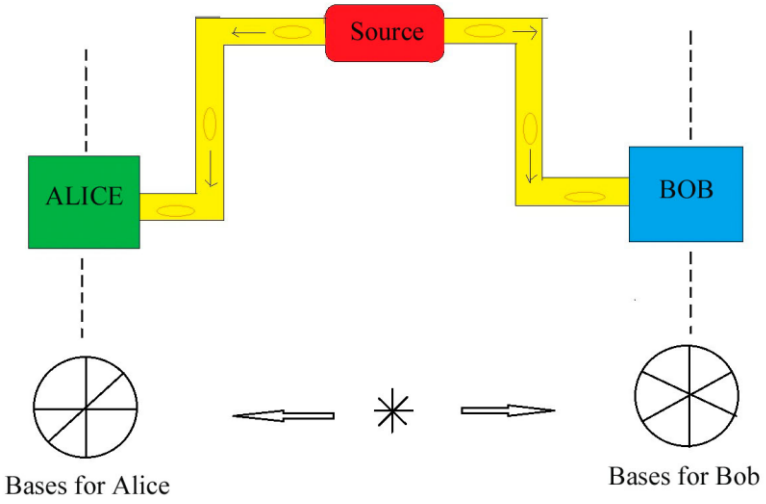

Figure 2: Basic diagrammatic representation of Ekert's E91 protocol

- Each time the entangled photon sorce will produce photons at fixed wavelengths, so that n-number of signal photons as well as n-idler photons will be generated.
- Let the idlers photons will be at fixed wavelengths λ_1, λ_2, λ_3, λ_4 and so on, fixed respectively for A-side users. So that,

$$\lambda_1 - \lambda_2 = \lambda_2 - \lambda_3 = \lambda_3 - \lambda_4 = \Delta\lambda$$

- However the signal photons having wavelength respectively λ_1', λ_2', λ_3', λ_4' are kept variable for B-side users.
- Photons generated at each time are polarization entangled photons with anticorrelation states given by,

$$|\Psi> = \frac{1}{\sqrt{2}}(|01> + |10>) \quad (4)$$

- We are considering here for illustration 4-pairs of users at the opposite end of the network, the A-side and the B-side users.
- Four signal photons and four idler photons are to be processed for a Hadmard transform to form a wave packet and transmitted through the optical fiber channel.
- Wave packets of signal and the idler photons are represented as given in eqn (6); such that signal photon wave packet is represented by $|\Phi_s>$ and idler is by $|\Phi_i>$.

- Doing again Hadmard transform near the receiving station will result into the prior (original) entangled photon state.
- Photons wavelength is kept fixed for A-side users whereas it is kept variable for the B-side users.
- A cyclic selection switching is used at the B-side users receiving station for distribution of photons at respective wavelength in a cyclic manner.
- Based on cyclic switching we have entangled photon pair distribution between any two users at the opposite ends.
- According to the distribution of photons we can have a number of passes so that in each pass two of the opposite end users are connected.

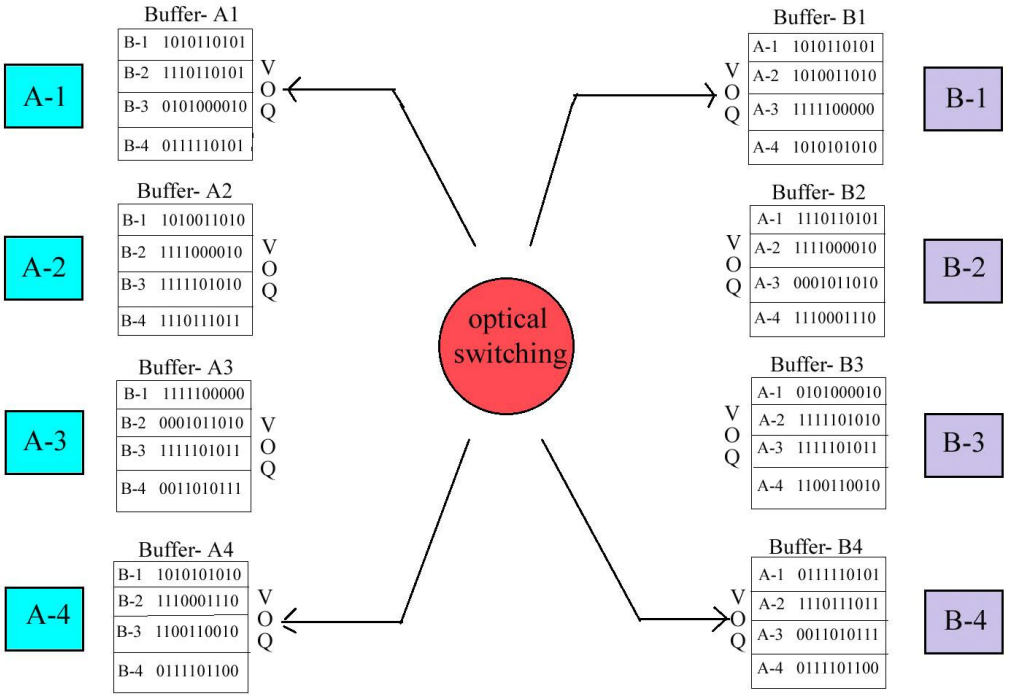

Figure-3: Sharing of key among A & B users in a 4 × 4 network

- After successful complition of total number of passes a classical communication channel is used so that various B-side users can share their base angles out of respective set of three coplanar angles to the A-side users.
- Now considering six basis coplanar angles so that 3 basis states for user-A and user- B each. Considering for A-side users the fixed angles are 0°, 45° and 90° whereas for B fixed basis angles are 45°, 90° and 135° both coplanar.
- These 6 basis states are categorized into the compatible and incompatible states. Such as (45°, 135°), (0°, 90°) of (A, B) are Rectilinear and Diagonal compatible states and measurement will result up spin/down spin $|\uparrow>$ or $|\downarrow>$.
- Based on above stated methodology the sharing of secret key among 4 × 4 users through the network keeping source at the middle is shown in the following diagram in figure-3.

Table-1: Cyclic switching between A & B users in different passes

	Pass-1	*Pass-2*	*Pass-3*	*Pass-4*	*Pass-5*
A-1	B-1	B-2	B-3	B-4	B-1
A-2	B-3	B-4	B-1	B-2	B-3
A-3	B-4	B-1	B-2	B-3	B-4
A-4	B-2	B-3	B-4	B-1	B-2

To distribute n bit secret key among 4×4 users with 100% photon detection efficiency in $4 \times n$ number of passes is required for the cyclic selection switch. However considering the E91 protocol we can have a total number of passes required with keeping 50% detection efficiency is $4 \times 2 \times n$. At each pass the photons received by the respective users are processed further for their polarization measurement and respective results are to be stored in seperate destined buffers.

4. MATHEMATICAL ANALYSIS

4.1. Measurements

There are two basic tests of quantum mechanics which are to be carried out for the generalization of the quantum states. These tests are listed below.

4.1.2 Violation of Bell states

John S. Bell great theoretical physist of the history in the year 1964 carried further the work done by EPR, Einstien, Podolosky and Rosen theory of local realism famous as EPR paradox and based on his thought experiment developed theories which is verified by local realism or objective reality i.e classical physics and violated by quantum mechanics. This experiment is experimentally testable in labs and almost used in all quantum mechanics based application. There are four different Bell states also called as the Bell's basis or EPR states. Given by,

$$|\beta_{00}> = \frac{1}{\sqrt{2}}(|00> + |11>) \quad (5)$$

$$|\beta_{01}> = \frac{1}{\sqrt{2}}(|01> + |10>) \quad (6)$$

$$|\beta_{10}> = \frac{1}{\sqrt{2}}(|00> - |11>) \quad (7)$$

$$|\beta_{11}> = \frac{1}{\sqrt{2}}(|01> - |10>) \quad (8)$$

We are using anti-correlation Bell states of photon. So that each of the idler and signal photon will be in EPR state given by eqn (4). The superposition photon state is called as anti-correlation state because there is 50% probability of obtaining two photons respective of Alice and Bob in $|\downarrow_A\uparrow_B>$ and 50% probability of obtaining $|\uparrow_A\downarrow_B>$ respectively. Hence Eve can't predict the exact spin states of photons.

4.1.2 Test of separability

This is another important test that is to be done with the generation of photons at superposition state. This test verifies that two photons are separable or not if the superposition state or mixed state of two photons is separable then they will not be in entanglement, so that a mixed quantum state will either be in a product state or in entanglement.

Let two photons in mixed state $|\Phi>$, comprising of the photon states of A and B users, will be separable if the fractional division of the mixed state holds and that give equivalent result of $|\Phi> = |\Psi_A> |\Psi_B>$, this is also called as the product state. Such that Ket A and B are in tensor product to each other. Therefore if two photons mixed state represents a tensor product then they are not in entanglement and these photons are liable to be dropped because they will never carry quantum information processing.

4.2. Quantum Information processing

Processing of quantum information is carried out according to the steps given below.

Step-1: A spin-0 photon at pump frequency ω_p is generated by the laser and passed through non-linear optical crystal.

Step-2: This spin-0 photon breaks into two spin-1/2 particles at frequency ω_s and ω_i whose quantum mechanical state is given by eqn (4),

$$|\Psi> = \frac{1}{\sqrt{2}}(|01> + |10>) \quad (4)$$

at wavelength λ_i and λ_s.

Step-3: Idler photons are destined for A-side users at respective wavelengths λ_1, λ_2, λ_3, λ_4 are formed a wavepacket and then transmitted through the optical fiber. Similary, all of the signal photons at wavelengths $\lambda_1^{'}$, $\lambda_2^{'}$, $\lambda_3^{'}$, $\lambda_4^{'}$ are formed a wavepacket and transmitted through optical fiber towards the B-side user.
Step-4: Idler photons from different crystal sources are made to pass through multiplexing them by using different Hadmard gates.
Step-5: Now considering six basis coplanar angles of A and B-user, considering for A 0°, 45° and 90° are the fixed angles whereas for Bob it is considered to be 45°, 90° and 135° both users basis angles are coplanar.
Step-6: These 6 basis states are categorized into two part compatible and incompatible states. Such as (45°, 135°), (0°, 90°) of (A, B) are Rectilinear and Diagonal compatible states and measurement will result up spin/down spin, so that up spin represented by qubit state with arrow upwards $|\uparrow>$ and down spin with arrow downwards $|\downarrow>$ or a superposition state qubit represented by $|+>/|->$.

Such that, $|+> = \frac{(|0>+|1>)}{\sqrt{2}}$ and $|-> = \frac{(|0>-|1>)}{\sqrt{2}}$

Step-7: To obtain DWDM multiplexed entangled photons we use the concept of Quantum parallelism using parallel Hadmard gates with photons at different wavelength. Qubit-0, $|0>$ and qubit-1, $|1>$ is transformed according to Eqn. (1) and (2).
Step-8: Thus obtaining actual WDM packet in the larger Hilbert space by tensor product of all individual photon superposition states. Thus we are showing results for single photon state after Hadmard transform. So that,

$$H|\Psi> = |\Psi'>$$

$$= H\left(\frac{|01> + |10>}{\sqrt{2}}\right)$$

$$= \frac{H|0>|1> + H|1>|0>}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}}\left(\frac{|0> + |1>}{\sqrt{2}}|1> + \frac{|0> - |1>}{\sqrt{2}}|0>\right)$$

$$= \frac{1}{2}(|01> + |11> + |00> - |10>)$$

$$|\Psi'> = \frac{1}{2}(|00> + |01> - |10> + |11>) \quad (9)$$

Therefore, according to the theory of quantum parallelism,

$$|\Phi> = |\Psi'> \otimes |\Psi'> \otimes |\Psi'> \otimes |\Psi'>$$

Above is the tensor product of four qubit states obtained from different entanglement sources and gives the Hadmard transform of 4th order to the quantum state $|\Psi'>$.
Such that,

$$|\Psi'> \otimes |\Psi'> =$$

$$1/4\ (|0000> + |0001> - |0010> + |0011> + |0100> + |0101> - |0110> + |0111> - |1000> - |1001> + |1010> - |1011> + |1100> + |1101> - |1110> + |1111>)$$

We can represent in matrix form qubit state $|\Psi'>$ as,

$$[\Psi'] = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \quad (10)$$

Similarly, for the order of 2 it can be represented in the matrix form as following,

$$[\Psi']^{\otimes 2} = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad (11)$$

Therefore, obtaining similarly for the order of 3 in the matrix form,

$$[\Psi']^{\otimes 3} = \frac{1}{8}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{pmatrix} \quad (12)$$

On the same line we can obtain the matrix form of 4th order Hadmard transform such that,
$[\Phi] = [\Psi']^{\otimes 4} = [\Phi_i] = [\Phi_s]$, this will be a square matrix of 16 ×16.

Step-9: Now the optical fiber channel is supposed to transmit the signal photon wavepacket $[\Phi_s]$ the 4th order matrix as extended form of Eqn. (12) from central source to the B-side user, similarly idler photons wavepacket $[\Phi_i]$ from central source to the A-side user.

Step-10: De-multiplexing at B and A's location is being done by using a wavelength selective filtering and parallel Hadmard transform again. Therefore the overall n^{th} order hilbert space tensor product collapses into 1st order Hadmard transform of quantum mechanical states of photons. Such that it can be proved easily that applying a Hadmard gate again results into same entangled state generated by the central source. Thus,

$$H|\Psi' > = |\Psi > \quad (13)$$

Step-11: Polarization analyzer of authentic B-user as well as the A-user will have to perform polarization measurement of the photons received by their detectors. The measurement is done in compatible basis to realize the actual bit independent to each other.

Step-12: A tabular representation is shown below, representing the polarization analysis of 10 successive photons transmitted by the central sourse for switching between users A-1 & B-2, so that user A-1 wants to share the secret key with user B-2. The detection results finally into a shifted key of certain bit length depending on the number of compatible states.

Table-2: Ten successive photon distribution analysis between user A-1 & B-2

A-1, Spin	$\|\downarrow>$	$\|+>$	$\|\downarrow>$	$\|\downarrow>$	$\|\downarrow>$	$\|+>$	$\|\uparrow>$	$\|->$	$\|+>$	$\|\uparrow>$
A-1, Basis	0°	45°	0°	90°	90°	45°	0°	45°	45°	90°
B-2, Spin	$\|\downarrow>$	$\|\downarrow>$	$\|\uparrow>$	$\|\uparrow>$	$\|+>$	$\|->$	$\|->$	$\|+>$	$\|\downarrow>$	$\|\downarrow>$
B-2, Basis	45°	90°	90°	90°	135°	135°	135°	45°	90°	90°
Compatibility	No	No	Yes	Yes	No	Yes	No	Yes	No	Yes
Information bit	X	X	1	1	X	0	X	1	X	0

Hence the shifted key shared between users A-1 and B-2 according to the table is 11010. Similarly other pair of A-side and B-side user can share their one time pad key.

5. COMPARING WITH CLASSICAL CRYPTOGRAPHY

Classical cryptography in one hand represents its strength on the number of bits present in the key on the other hand considering Quantum cryptography the security threats to communication are minimized due to quantum mechanics. It is a general concept of present day's cryptography that more the numbers of bits more secure is our key to brute force or other attacks. However the evolution of certain Quantum algorithms in the history had given the solution of most typical classical world's problem. It is a fear that as soon as the

Quantum computers come into application classical communication/cryptography will be not secured. Therefore Quantum cryptography and related technologies will be the need of secured communication in coming years. The no-cloning theorem forbids the threats of storing or capturing of quantum information. At the same time the Heisenbergs uncertainty principle gives strength to quantum communication so that Eve can not predict or measure the actual quantum information if she does then her presence can be detected easily so that measurement of one parameter of quantum mechanics changes the values of others.

6. CONCLUSION

The next generation communication technology will be benefited by the enormous level of security provided by QKD or Quantum Cryptography. In this paper we have shown a way of getting multi-party secret key transferred through a network, where the objective goal was the distribution of one time pad key sharing using entangled photon distribution. Since Quantum communication is searching for a still to come mile-stone. A theoretical model of a Quantum cryptography network has been proposed that can be helpful in designing of a next generation communication network where security and good data rate at minimum cost and time is desirable. Our model is an approach towards multi-functional Quantum networks, where we have shown just one feature of such a network that is of secret key sharing. We have shown that using parallel Hadmard gates performing Hadmard operation on photons at different wavelength generated by SPDC (Spontaneous Parametric down Conversion) photon sources in parallel will result into a wavepacket similar to wavelength division multiplexing. Further photons are detected at the end users location so that their polarization analysis when in compatible measurement basis gives the secret key shared between pair of users. Photon entanglement distribution is an interesting concept from Quantum mechanics which can effectively be utilized to give good results and will prove more fruitful in coming years. Further discretization of spectral and temporal parameters in time-bins and conjugate frequency-bins correlations and also intermixing of correlation randomly will increase complexity and will be typical for Eve's calculation. At the same time use of quantum dots for single entangled photon transmission can give a new hope to the process developers. It is worth to say that the next generation metropolitan area network will be a Quantum communication network.

REFERENCES

[1] C.H.Bennett, *et al.,* "Quantum Cryptography: Public key distribution and coin tossing", in *IEEE International Conference on Computers, Systems and Signal Processing*, 1984, pp. 175.

[2] C.H.Bennett, *et al.,* "Experimental Quantum Cryptography", *J. Cryptography*, vol. 5, pp. 3-28, 1992.

[3] S.J. Wiesner, "Conjugate Coding" , *SIGACT News*, Vol. 15, No. 1, pp. 7888, 1983.

[4] A. Einstien, et al., "Can Quantum-Mechanicanical Description of Physical Reality Be Considered Complete?" *Phys. Rev.*, Vol. 47, No. 10, pp. 777-780, 1935.

[5] J. S. Bell, "On the Einstein Podolosky Rosen Paradox", *Physics*, Vol. 1, pp. 195-200, 1964.

[6] Artur K. Ekert, "Quantum Cryptography based on Bell's theorem", *Phys. Rev.*, Vol. 67, No. 6, pp. 661-663, 1991.

[7] Nikolina Ilic, "The Ekert Protocol", *J. Phy.*, Vol. 334, No. 1, 2007.

[8] P. Kumar, *et al.,* "All-Fiber Photon-Pair Source for Quantum Communication" , *IEEE Photonics Technology Letters*, Vol. 14, No. 7, pp. 983-985, 2002.

[9] G. Brassard, *et al.,* "Multiuser Quantum Key Distribution using Wavelength Division Multiplexing" in *Proceedings of SPIE 5260: Applications of Photonics Technology*, 2003, pp. 149-153.

[10] G. Brassard, *et al.,* "Entanglement and Wavelength division Multiplexing for Quantum Cryptography Networks" in *AIP conference Proceedings QCMC-04*, 2004, Vol. 734, pp. 323-326.

[11] E. Meyer-Scott, *et al.,* "Quantum Entanglement Distribution in Telecommunications Optic Fibre Network", *Physics In Canada*, Vol. 66, No. 3, pp. 180-182, 2010.

[12] J. Mower, *et al.,* "Dense wavelength division multiplexed quantum key distribution using entangled photons", arXiv: 1110.4867v1 [quant-ph], 2011.

[13] C. Holloway, *et al.,* "Optimal pair generation rate for Entanglement-based QKD", arXiv: 1210.0209v1 [quant-ph], 2012.

[14] C. Holloway, "Towards real-world adoption of quantum key distribution using entangled photons", in *Master of Science thesis IQC (Waterloo)*, 2012.

[15] C. E. Shannon (1949), Communication theory of secrecy systems , Bell Systems Technical Journal, Vol. 28, No. 4, pp. 656-715.

[16] J. R .Johansson, *et al.,* "QuTiP: An open-source Python framework for the dynamics of open quantum systems, Computer Physics Communications", Vol. 183, No. 8, pp.1760-1772.

[17] Prem Kumar, *et al.,* "Quantum Communications: Present status and future prospects", in *ECOC-2010(Italy)*, 2010.

[18] D. McMahon, "Quantum computing explained", *IEEE Computer Society*, Wiley-Interscience publication (New Jersey), 2007.

[19] R. Hadfield, "Single photon detectors for optical quantum information application", *Nature Photonics*, Vol. 3, pp. 696-705, 2009.

BIOGRAPHIES OF AUTHORS

Vikas Kumar Jha, (B.E. in Electronics & Communication Engg. From RGPV Bhopal in 2010) is a Master of Technology student from Atal Bihari Vajpayee – Indian Institute of Information Technology & Management Gwalior, with specialization in Advanced Networks. He is doing his M.Tech thesis in Quantum Communication Networks under Quantum Computing & Information Group at ABV-IIITM Gwalior, under the supervision of Dr. Pankaj Srivastava.

Dr. Pankaj Srivastava, Ph.D. (Allahabad University, India) is an associate professor in Atal Bihari Vajpayee – Indian Institute of Information Technology & Management Gwalior. He achieved his doctoral degree in physics from physics department, Allahabad University. His doctoral research includes the physical properties of semiconducting surfaces. During the course of doctoral research he has visited International Centre for Theoretical Physics (ICTP), Trieste, Italy to carry out his research work in the Condensed Matter theory group. His current area of research is nanotechnology investigating various physical properties of materials in the form of nanowires, nanoclusters, nanotubes, nanoribbons w.r.t. electronic devices and information technology applications employing first principles approach. Dr. Srivastava is also working in the area of Quantum Computing and Information and many other projects on nanoCMOS and nanoMOSFET technology. He has published more than 95 papers in peer reviewed journals of international repute apart from presenting papers and chairing sessions in national and international seminars/conferences in the area of Nanoscience and Technology. He has been awarded various national scholarships & fellowships of UGC, DST and ISRO. He is member of many professional and academic bodies viz. ISTE-New Delhi, ICTP-Italy, MRSI-Bangalore. He is research paper referee of Elsevier Science journals, RSC publications etc. International Biographical Centre, Cambridge, England has awarded Foremost Scientists of the World-2008.