Integrated Optics-Based Quantum Communication Devices

Rohit K Ramakrishnan*[a], Shafeek A Samad [a], Archana K [a], Yadunath T R[a,b], Partha P Das[b], Srinivas Talabattula[a]

[a]Applied Photonics Lab, ECE Department, Indian Institute of Science, Bangalore, India - 560 012;
[b]Dept. of Physics, National Institute of Technology Karnataka, Surathkal, India - 575 025.

ABSTRACT

Quantum communication or more specifically quantum information processing is considered as the future of information science and technology. In this paper we propose a scheme to implement quantum communication at the device level using integrated optics. We implement the quantum communication protocol BB84, in a waveguide based circuit using integrated optics. We also propose a high dimensional quantum key distribution method implementation using integrated optics. In the earlier one polarized photons are used as the carriers of quantum information, while in second one electromagnetic modes in the waveguide are used to carry quantum information. The high dimensional quantum communication method is used to increase the information content of protocol thus increasing on the data rates. This is done by encoding into a larger state space. We have used electromagnetic modes for encoding since the polarization method is not efficient to carry information in a larger state space.

1. INTRODUCTION

Quantum Communication or more specifically quantum information processing has changed our perception about communication especially the way information is processed [1]. Though it promises unbreakable secure communications, it is still a long way from practical implementation. The most successful quantum communication method in terms of implementation is Quantum Key distribution (QKD), which is the technique of sharing a secret key between two users that trust each other, in the presence of an adversary. The limitation of QKD is its data rate [2]. High Dimensional Quantum Key Distribution (HD QKD) was proposed to overcome the limitations of QKD. The practical implantation schemes for HD QKD are still in the early stages. In this paper, we present an integrated optics based circuit to implement conventional QKD and HD QKD. In conventional QKD polarized photons are used to carry units of quantum information. In HD QKD electromagnetic modes in the waveguides are used for carrying quantum information.

Keywords: Quantum Communication, QKD, High Dimensional QKD, BB84 protocol, Integrated Optics, Multi-mode interference (MMI).

2. QUANTUM KEY DISTRIBUTION USING INTEGRATED OPTICS

2.1 BB84 Protocol

Quantum Communication has been proven effective in the area of secure communication. QKD protocols has been proposed and verified for 100% secure communication. In quantum information processing quantum bits - "qubits" are the carriers of information. BB84 protocol was the first protocol for QKD proposed by Bennett and Brassard in 1984. This method uses polarized photons and the principle of quantum superposition for secure communication [3, 4]

*rohitkr@ece.iisc.ernet.in

Advances in Photonics of Quantum Computing, Memory, and Communication X, edited by Zameer Ul Hasan, Philip R. Hemmer, Hwang Lee, Alan L. Migdall, Proc. of SPIE Vol. 10118, 1011813
 · doi: 10.1117/12.2251091

The realization of the BB84 protocol using integrated optics is shown in figure 1. This is realized using a waveguide-based circuit. Alice, the sender codes the incoming message into polarized photons. This is done by connecting 2 single photon sources with polarizers of two types attached to them. These two types of polarizers are the two bases for measurement. To select the base randomly, we use a switching device controlled by a random number generator (RNG) that chooses between two sources in random manner. This is sent through waveguide that supports single photon transmission [5, 6]. At the receiving end, Bob does the measurement by choosing the bases randomly. This is done again using a RNG. The RNG randomly selects the detector to which the photons are to be sent. The outputs of both RNGs are compared later through a classical channel and the bases are discarded when they are not matched. The data stream is filtered according to this.

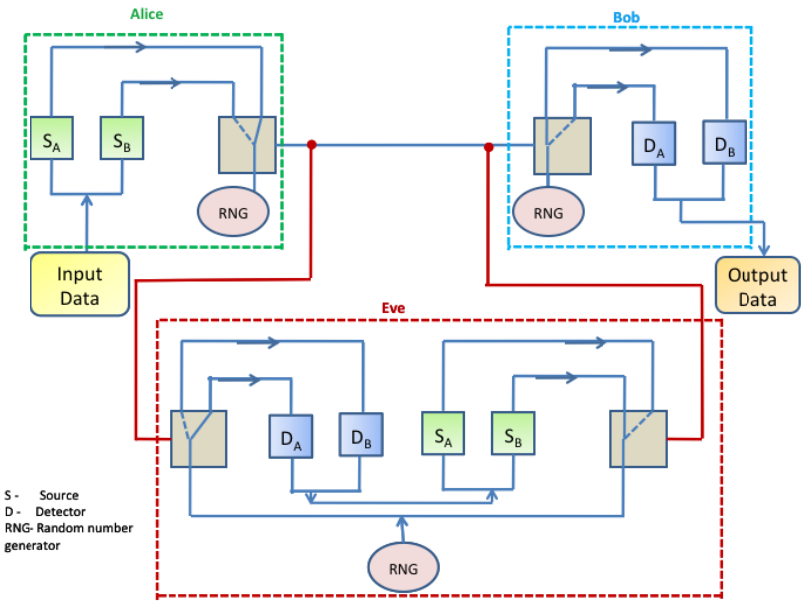

Fig1: Integrated optic method to implement BB84 Protocol

Consider the situation when somebody tries to eavesdrop. We consider Eve as an eavesdropper. If Eve drops in between, he/she may need a similar device for generating bases and sending data. We use another integrated optic circuit to realize Eve, which will have the same type of circuitry as Alice and Bob. But, since the output of Random Number generators of Eve and Bob can't be the same, the data mismatch will indicate the presence of eavesdropper. Most optical detectors are intensity detectors that are insensitive to the polarization of light. However, a superconducting nanowire single photon detector (SNSPD) that is naturally sensitive to polarization due to its nanowire structure is reported in [7]. In this study, SNSPD with high polarization sensitivity is studied by adjusting the width and pitch of the nanowire.

3. HIGH DIMENSIONAL QKD USING INTEGRATED OPTICS

3.1 High Dimensional QKD

The existing QKD protocols use a two-dimensional Hilbert space or two conjugate continuous variables for key encoding. High Dimensional Quantum Key Distribution (HD QKD) is a new approach to QKD that is to encode multiple bits per photon pair, similar to the way pulse-position modulation is used in classical optical communication under photon-starved conditions [8]. In this method instead of qubits we use "qudits". Qudit is a generalization of qubit to d-dimensional Hilbert space. However its implementation within a framework of proven security for multiple bits per photon is remaining as a long-standing challenge.

3.2 High Dimensional BB84 Protocol

The protocol requires that Alice has d processes to generate qudits that are to be sent to Bob. BB84 protocol uses polarized states of photons as qubits. The conventional protocol uses two bases from which two states are chosen as 0 and 1. In HD QKD however we need *d* states to denote qudits in *d*-dimensions. Randomness is one of the factors on which security of BB84 protocol depends [8]. In HD encoding Alice uses a Random Number Generator (RNG) to select from a set of *d* bases. The protocol starts when Alice selects a base to encode the information she has. The first "bit" is encoded and sent to Bob via a quantum channel.

Bob upon receiving the qudit performs the measurement on a base randomly chosen from the set of *d* bases, for which Bob also need to use a Random Number Generator. However both Alice and Bob keep track of the bases they have chosen to encode and preformed measurement with. Consider Eve, an eavesdropper trying to steal information. Intercepting the quantum channel and reading the qudits can only do this. The measurement process essentially destroys the quantum information since quantum information cannot be cloned [9]. So now, Eve has to generate quantum information again by choosing a quantum state preparation process that can give *d* bases. Here, Eve also need to use a RNG for random selection of bases. Once the transmission is completed Alice and Bob compare their bases via the classical communication channel. When choices of base of Alice and Bob coincide exactly the qudits give same measurement results. If they do not coincide the qudits give random results. Only the coinciding bases are chosen and the measurements carried out during the rest of cycles are discarded. The measurement results in the clock cycles where bases are same are also compared. But if Eve has read the data in between, the information Bob received was from qudits sent by Eve. The data may be the same but bases may be different since random choices of bases of Alice and Eve will not agree completely. This will result in data mismatch when Alice and Bob compare data. Thus the intrusion can be detected [10].

3.3 Implementation of HD BB84 Protocol

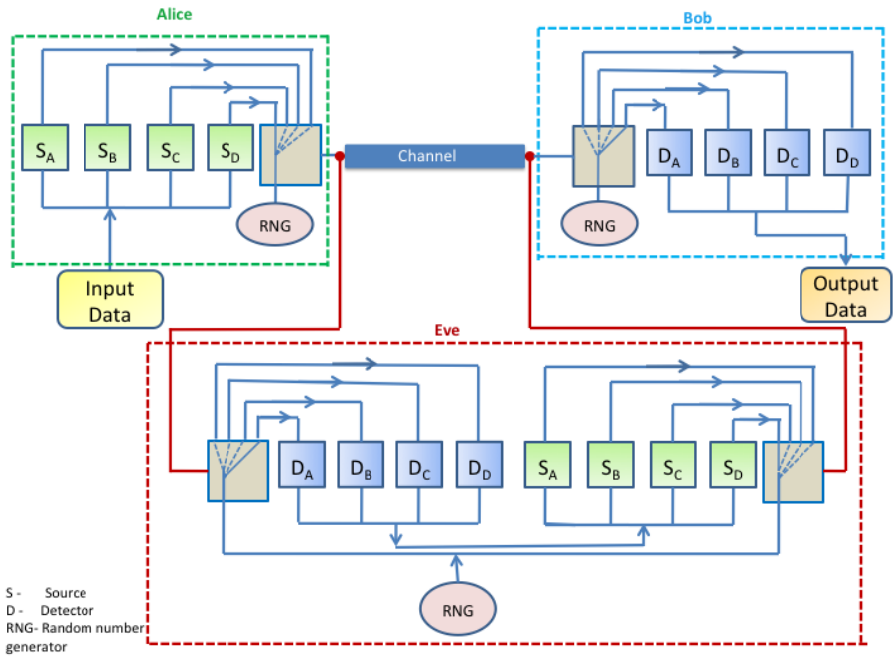

Fig 2. Implementation of HD-QKD Using Integrated Optics

Instead of polarized photons here we chose electromagnetic modes to represent quantum information [11]. The base *d* is selected as 4 here. The schematic to implement HD QKD using electro-magnetic modes as bases is shown in figure 2.

The incoming binary bits are grouped into two, forming the four combinations 00, 01, 10, and 11. Each source generates four modes M_1, M_2, M_3, and M_4. These can be chosen as the four modes of a waveguide for example, TE_0, TE_1, TE_2, and TE_3. The selection of the source is made by the sequence generated by the random number generator (RNG). Commercially available RNGs from [12] can be used to generate four random numbers. The data is encoded into the EM modes. The electro-optic switching circuit will take the input from the random number and selects one of the sources. Switches based on MMI can also be used as reported in [13].

Depending on the data combination, a particular mode will be chosen from the source. The implementation details are shown in fig 3. The continuous wave laser at a wavelength from the c-band (1530 to 1565 nm) is chosen as the source. The incoming light is split equally into the four arms of a 1x4 power divider. A waveguide splitter based on MMI can be used. MMI-based device is used for both power splitting and mode conversion because of its inherent advantages like compact size, low loss, high tolerance to fabrication errors, and relatively large optical bandwidth [13]. Power dividers based on Y-splitters have very stringent fabrication tolerances because of the sharp bends.

Multimode Interference (MMI) devices are based on the principle of self-imaging. Self-imaging is a property of multimode waveguides by which an input field profile is reproduced in single or multiple images at periodic intervals along the propagation direction of the guide [14]. The dimension of the MMI splitter can be chosen according to the mathematical formulae in [15].

The MMI device consists of the input and the output access waveguides and the central multimode interference region. As the modes in the MMI region couple at different phases, light in the MMI region exhibits various distributions as it propagates to different positions determined by L_π, which is the beat length of the first two modes and can be expressed as:

$$L_\pi = \frac{\pi}{\beta_0 - \beta_1} = \frac{4 n_c W_e^2}{3\lambda_0} \quad (1)$$

where β_0 and β_1 are the propagation constants of the first two guided modes, n_c is the refractive index of the core layer, W_e is the effective width of the MMI region and λ_0 is the application wavelength. For normal MMI couplers, field distribution will reappear after a propagation distance of $6L_\pi$, while a reversed image will appear at $3L_\pi$.

The access waveguides of the MMI can be designed to support the required four modes. The waveguide is designed so that the wave function is a superposition of 4 modes. Once the choice of source is made by the optical switching circuit based on the RNG output, the mode field to be transmitted is decided based on the input dual-bit pattern. The output of the switching circuit is a superposition of the modes. To extract the desired mode, two approaches can be used. The first method is to taper the multimode waveguide to a single mode waveguide, so that only fundamental mode exists in the single mode waveguide. This can be converted to the higher order mode using an MMI mode converter. The conversion of TE0 to TE1 mode in the wavelength range of 1280–1320 nm on InP substrates is demonstrated in [13]. Using 4x4 and 3x3 MMIs, mode conversion efficiencies of 50% and 66% are reported in this paper. This TE0 to TE1 mode conversion is also reported in [16]. It is shown in [17] that the efficiency can be significantly improved by an appropriate combination of different MMI couplers with phase shifters. The second method is to use multiple waveguides, each one carefully engineered to allow a particular mode by matching the propagation constants to those in the multimode waveguide. The waveguides have to be designed such that maximum power will be coupled only to the desired mode.

The input data combination and the output of RNG are fed to a digital circuit whose output will control the voltages applied to an MZI based device. The voltages are applied such that the sum of the outputs of the four MZIs in the circuit will have only the required mode. Rest is cancelled by destructive interference.

This mode generated corresponding to the incoming dual-bit is transmitted through the channel. The channel is assumed to be ideal, which preserves the transmitted mode field. If the eavesdropper taps the signal in the channel, he/she cannot find out from which source the mode was generated, as all sources will generate identical set of modes. The authorized receiver who has the key for decryption will only be able to identify the source. This is analogous to the identical qubits

produced by the two sources at the transmitter (Alice) of the conventional quantum version implementation of the BB84 protocol.

At the detector end, the received modes are identified. The selection of detectors is also randomly done using the random number generator. Bases selected by random number generators at both Alice and Bob are compared and the matching bases are selected and the rest is discarded. From the modes, the corresponding data is recovered.

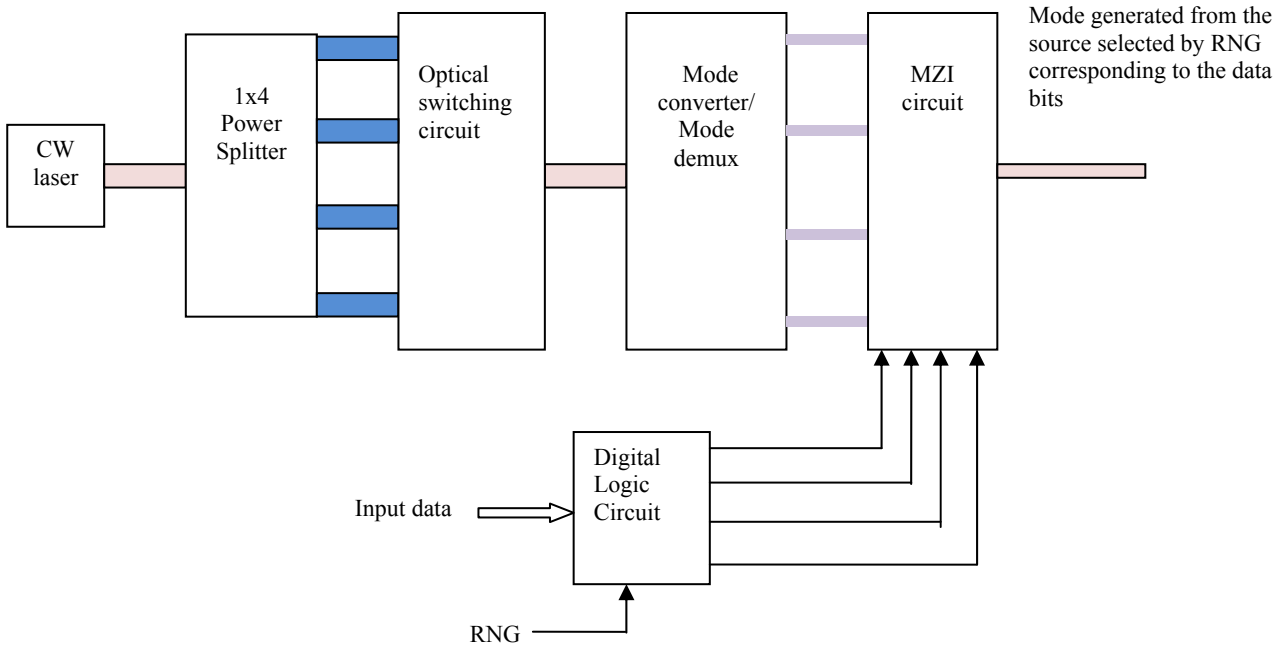

Fig 3. Proposed scheme for Transmitter of HD-QKD using Integrated Optics

4. CONCLUSION

We present integrated optics based circuits for realizing quantum key distribution. We have presented two proposals for implmenting BB84 and HD version of BB84. A novel idea of using the electromagnetic modes as analogues of quantum states and realsing them for HD QKD is proposed in this paper. This paves the way for highly secured systems using integrated optic device. The fabrication of the devices are planned for the future.

REFERENCES

[1] Nielsen, M A. and Chuang I L [Quantum Computation and Quantum Information], Cambridge Univ. Press, Cambridge (2001).

[2] Alléaume, R et al., "Using quantum key distribution for cryptographic purposes: a survey" Theor. Comput. Sci. 560, 62-81 (2014).

[3] Bennett, C. H. and Brassard, G., "Quantum Cryptography: Public key distribution and coin tossing", Proc. IEEE International Conference on Computers, Systems & Signal Processing, Bangalore India, 175-179 (1984).

[4] Bennett, C. H., Brassard, G., Crépeau, C., Maurer, U.M. "Generalized privacy amplification", IEEE Transactions on Information Theory 41, 1915-1923 (1995).

[5] Politi, A, et.al.,"Integrate Quantum Photonics" IEEE J. Sel. Top. Quantum Electron. 15, 1673-1684 (2009).

[6] Politi, A, et al., "Silica-on-Silicon Wave-guide Quantum Circuits," Science 320(5876), 646-649 (2008)

[7] Qi Guo, et.al., "Single photon detector with high polarization sensitivity," Sci. Rep. 5(09616), (2015)

[8] Zhong, Tian et al., "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding", New Journal of Physics 17, (2015).

[9] Wootters, W K., Zurek, W H.,"A Single Quantum Cannot be Cloned", Nature 299, 802-803 (1982).

[10] Ramakrishnan, Rohit K. and Srinivas, Talabattula.,"Photonic Crystal based Quantum Hadamard Gate" Proc. SPIE 7420, 7420R (2009).

[11] Ramakrishnan, Rohit K. and Srinivas, Talabattula., "High Dimensional Quantum Key Distribution: BB84 Protocol Using Qudits," Proc. 13th International Conference on Fiber Optics and Photonics, OSA Th3A.77 (2016).

[12] Symul, T., Assad, S M. and Lam, P K., "Real time demonstration of high bit rate quantum random number generation with coherent laser light" Appl.Phys.Lett. 98, 231103 (2011).

[13] Yin, Rui.,, Teng, Jinghua. and Chua, Soojin., "A 1 to 2 optical switch using one multi-mode interference region", Optics Communications 281, 4616–4618 (2008).

[14] Guo, Fei., et.al., "Two-Mode Converters at 1.3 μm Based on Multi-mode Interference Couplers on InP Substrates", Chin. Phys. Lett. 33(2) (2016).

[15] Ulrich, R. and Ankele, G., "Self-imaging in homogeneous planar optical wave-guides", Applied Physics Letters. 27(6), 15 (1975).

[16] Ferreras, A., et.al., "Useful Formulas for Multimode Interference Power Splitter/Combiner, Design", IEEE Photonics Technology Letters, 5(10), (1993)

[17] Awasthi, Ashish., Srinivas, Talabattula., Shivaleela, E.S., "Low loss mode multiplexer/ De-multiplexer for Mode Division over two mode fiber," Proc. IEEE Workshop on Recent Advances in Photonics (WRAP), 1-4, (2015)