iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** Issue **Issue:** ssue-1 **Month of publication:** October 2014

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology(IJRASET)

# Study and Implementation of 3 Stage Quantum Cryptography in Optical Networks

T.Godhavari[1] , Libi Balakrishnan[2], Srikrishnan[3]

[2] *PG Student- M.Tech. Communication system*
[1,3]*Assitant Professor*
*Dept. Electronics and Communication Engineering*
*Dr.MGR Educational and Research Institute, University*
*Chennai, Tamil Nadu, India.*

***Abstract: This paper presents a quantum protocol based on public key cryptography for secure transmission of data over a public channel. The security of the protocol derives from the fact that Alice and Bob each use secret keys in the multiple exchange of the qubit. Unlike the BB84 protocol and its many variants where the qubits are transmitted in only one direction and classical information exchanged thereafter, the communication in the proposed protocol remains quantum in each stage. In the BB84 protocol, each transmitted qubit is in one of four different states; in the proposed protocol, the transmitted qubit can be in any arbitrary state. Disparate and heterogeneous networks will be a growing reality in the future. Additionally, some of the regulatory, national interest, and security requirements might force a geographic boundary between networks.***
***Keywords: Optical Network, OBS,WDM Quantum computing***

## I. INTRODUCTION

The Internet is rapidly becoming a 'network of networks' as a logical outcome of the growth of a global information economy where geographically or functionally distinct networks 'owned' by functionally distinct networks 'owned' by identities can cooperate to provide high speed, high performance, and cost effective service, on demand ,to their customers. We obtain the highest level of interconnection at the *optical* level. Optical switching technologies can be categorized into optical circuit switching, optical packet switching, and optical burst switching (OBS). Optical circuit switching, also known as lambda switching, can only switch at the wavelength level, and is not suitable for bursty Internet traffic. Optical packet switching which can switch at the packet level with a fine granularity is not practical in the foreseeable future. The two main obstacles are the lack of random access optical buffers, and optical synchronization of the packet header and payload.

OBS is considered the most promising form of optical switching technology. OBS can provide a cost effective means of interconnecting heterogeneous networks regardless of the lower-level protocols used in these networks For example, an OBS network is able to transport 10 Gigabit per second Ethernet traffic between two sub-networks without the need to interpret lower level protocols or to make two geographically distant wireless networks to act as an integrated whole without protocol translations. Unfortunately, OBS networks suffer from security vulnerabilities . Although IPSec can be used to secure IP networks, OBS networks can provide security services to traffic that do not necessarily have an IP layer, as illustrated in Figure 1.

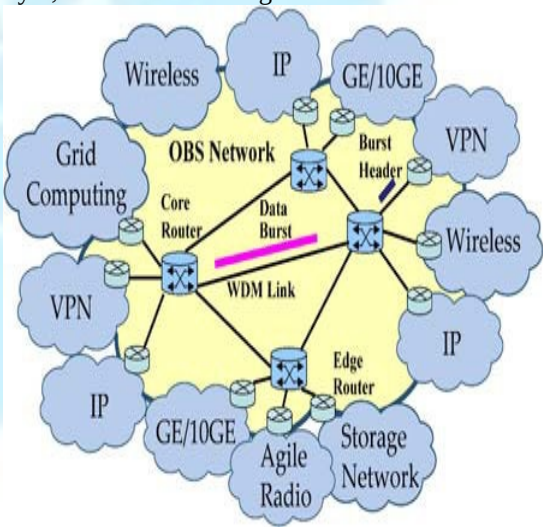



Fig.1 Illustration of OBS network

This will likely be the case for the majority of traffic served by the OBS layer. For example, native Ethernet traffic can be transported directly over OBS networks. There is no single security measure that can accommodate the security needs of different modalities of traffic that interface with the OBS networks. It is clear that the security of communication within the OBS network has to be sufficiently addressed in

order for OBS to fulfil its promise. In addition, as computing power increases in the future, classical cryptography and key management schemes based on computational complexity become increasingly susceptible to brute force and cryptanalytic attacks.

On the other hand, quantum cryptography uses the quantum mechanism to provide security, which is theoretically unbreakable. Given the optical modality Fig. 1. Illustration of optical burst switching (OBS) network.of all information within the OBS network, introducing quantum cryptography in OBS networks appears to be a natural choice. Since the OBS network itself allows a one-to-one correspondence between a header and its associated burst, the same relationship could be exploited to tie the same key to the header and the burst. The quantum-based methodology will allow a secure distribution of keys which could be potentially used to encrypt and decrypt each burst with a unique key. However, it must be stressed that classical cryptography and key distribution schemes will co-exist with quantum-based techniques for a long time. Therefore, we propose an integrated security framework for OBS networks which exploits the strengths of both classical and quantum cryptography schemes, and allows a seamless migration to quantum techniques as as the technology evolves. In addition, by embedding security components in the OBS native router architecture and incorporating quantum techniques for key distribution, the proposed approach can achieve a robust level of security while combining the strengths of both quantum and classical technologies. The integrated framework will make it possible to offer different levels of security for different applications.

The proposed security architecture is also consistent with the potential use of quantum data encryption in the future, as one can envisage the possibility of using a quantum technique to encrypt such as by using a Vernam cipher to make the encryption theoretically unbreakable. The rest of the paper is organized as follows. Section 2 provides the background of OBS networks. In Section 3, we describe security vulnerabilities in OBS networks, discuss the embedded security services to secure the OBS network.

The rest of the paper is organized as follows. Section 2 provides the background of OBS networks. In Section 3, we describe security vulnerabilities in OBS networks, discuss the embedded security services to secure the OBS networks, and propose the integrated secure OBS router architecture which allows both classical and quantum cryptography techniques..

## II. OPTICAL BURST SWITCHING (OBS)BACKGROUND

In OBS networks, data are aggregated into variable size data bursts, and are transported directly over wavelength division multiplexing (WDM) links. A burst header is generated for each data burst, and is sent on a separate control channel ahead of the data burst. The OBS routers will set up a light path for the duration of the data burst according to the information carried in the burst header. Data bursts can stay in the optical domain and pass through OBS routers transparently. This eliminates the need for optical buffers in such networks. In addition, since burst headers and data bursts are sent on separate WDM channels, there is no stringent synchronization requirement. Figure 1 illustrates an OBS network interconnecting heterogeneous networks. OBS ingress edge routers are responsible for assembling packets into data bursts according to the egress edge router addresses and possibly quality-of-service (QoS) levels. A burst is formed when it either reaches the pre-defined maximum burst size, or the burst assembly time reaches the timeout value. Adaptive burst assembly schemes can be used as well. Once a burst is formed, the ingress edge router generates a burst header which is sent on a separate control channel. The burst header specifies the length of the burst, and the offset time between the burst header and the data burst. The data burst is then launched on one of the WDM data channels. When the burst header reaches the OBS core router, it is converted to electronic signal and processed electronically. Since burst headers carry complete information about data bursts, the OBS core router can make efficient scheduling decisions in selecting the outgoing WDM channels for data bursts by simply processing burst headers. If at least one outgoing WDM channel is available for the duration of the burst, a channel will be selected to carry the data burst. Otherwise, the data burst will be dropped. Before the data burst reaches the OBS core router, the optical interconnects in the OBS core router will be configured to route the optical data burst to the desired output channel. The data burst can traverse the OBS core network as an optical entity transparently without encountering O/E/O conversion. When data bursts reach the egress edge router, data bursts will be disassembled back to packets and forwarded to proper network interfaces.

Note that burst assembly/disassembly functionality is only provided at OBS edge routers. There is no burst reassembly in the OBS core network. There is a one-to-one correspondence between the burst header and its associated burst. Burst headers are responsible for setting up optical data paths for their data bursts. Data bursts will simply follow the light paths set up by burst headers and are transparent to OBS core routers.

## III. PROPOSED EMBEDDED SECURITY SERVICES AND INTEGRATED SECURE OBS ROUTER ARCHITECTURE

### 3.1.Security vulnerabilities in OBS networks

OBS networks show great promise in providing cost effective interconnection solutions to the ever growing Internet. However, OBS network is not free of security concerns . In

this section, the need to bring security measures to OBS networks is discussed.

*Orphan Bursts*: The burst header is responsible for making the WDM channel reservation for its corresponding burst. If the scheduling request is rejected at one of the OBS core routers, there will be no valid optical path set up for the arriving burst. Since the burst has been launched, it is going to arrive at the input of the core router in any case. At this point, the burst is no longer connected with its header and becomes an orphan burst as shown in Figure 2(a). As a result, orphan data bursts can be tapped off by some undesirable party, compromising its security.

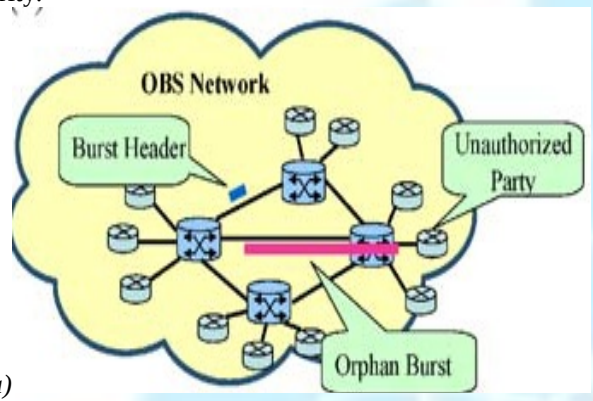
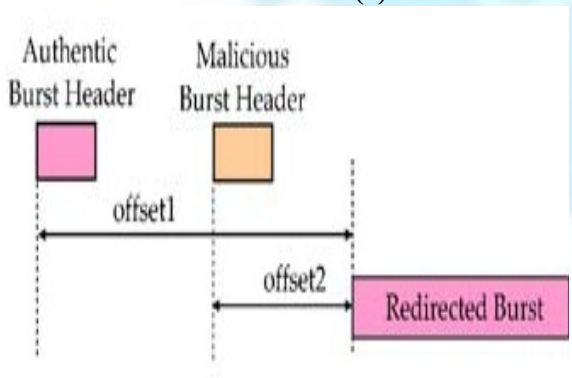



*FIG2(a)*

*Redirection of Data Bursts*: The one-to-one correspondence between the burst header and its associated burst is implied by the offset time carried in the burst header. Such one-to-one correspondence can be violated by injecting a malicious header corresponding to the same burst, as shown in Figure 2(b). As a result, the route and the destination for the burst can be altered by the malicious header, even though a legitimate path has been set up by the authentic header.

FIG:2(b)




*Replay*: Replay attack can be launched by capturing a legitimate but expired burst and transmitting at a later time, or by injecting a expired burst header to cause the optical burst to circulate in the OBS network, delaying its delivery to the final destination.

Fig. 2. (a) Example of an orphan burst, (b) example of violation of one-to-one correspondence in redirected burst.

*Denial of Service*: OBS core routers make scheduling decisions based on the availability of their outgoing WDM channels. When a burst is scheduled, the core router will mark the WDM channel 'busy' for the duration of the burst. In the case where no 'idle' WDM channel can be found for the upcoming burst, the burst is discarded. Note that all scheduling decisions are made by processing burst information carried in burst headers on-the-fly. The OBS core routers have no ability to verify if indeed the scheduled optical burst arrived at the designated time. This can be used to launch a denial-of-service attack by simply injecting malicious burst headers, causing the core routers to mark WDM channels 'busy' and thus blocking real traffic passing through the OBS network. As we can see, an OBS network is under severe security threats. Effective security measures must be implemented in order to make the OBS network a viable solution for the future Internet.

3.2 Embedded Security Services

In the section, we propose to embed security services which integrate classical and quantum cryptography in the OBS network architecture, as opposed to a layer on top of it.

*End-to-end data burst confidentiality*: In OBS networks, data bursts assembled at the ingress edge router stay in the optical domain in the OBS core network, and are only disassembled at egress edge router. Since data bursts switch transparently across the OBS core routers, the end-to-end confidentiality of data bursts within the OBS domain can be provided by encrypting data bursts at the ingress edge router and decrypting at the egress edge router. An effective encryption scheme for securing data bursts can be implemented using the advanced encryption standard (AES) since it can function at high speed while also providing a high degree of cryptographic strength. The keys can be transferred using either classical techniques, or quantum-based key distribution schemes.

*Per-hop burst header authentication*: Unlike data bursts, which retain optical modality in the core OBS network, burst headers are converted back to an electronic form and are processed at every OBS core router along the path. Therefore, per hop burst header authentication is needed to ensure that no malicious headers are injected into the network. Authenticating burst headers at each hop can mitigate several active attacks such as misdirection of data bursts, replay, and denial of service.

*Burst integrity with burst retransmission*: In OBS networks, when there is no outgoing WDM channel available, the burst will be dropped. In order to ensure the integrity of burst transmission, we propose to implement the following mechanism. In case a burst
is dropped due to lack of WDM resources, the burst integrity service will trigger burst drop notification with optional burst retransmission at the ingress edge router. Burst integrity service also ensures that no injection or replay occurs during burst transportation. Such service is dependent upon direct access to the burst transmission control, and can only be implemented as an embedded service.

*Integrated classical and quantum cryptography*:
Classical cryptography relies on the assumption that performing certain mathematical functions is intrinsically hard using available computing resources. However, as computing power will inevitably increase in the future, such an assumption is increasingly questionable. In contrast, quantum cryptography, or quantum key distribution (QKD) built upon the principles of quantum mechanics is theoretically unbreakable since observing the state of a transmitted photon will corrupt its state. However, quantum cryptography still faces technical challenges and will not completely replace classical cryptography in the near future. Therefore, we propose to provide a security framework which entails both classical and quantum components.

3.3 Integrated Classical And Quantum Cryptography Services

*Supervisory security protocol*: The supervisory protocol manages security in the OBS network on a per user basis. Specifically, it assigns keys to users and stores their hash values and sets up the sequence that needs to be followed to authenticate the users by password authenticated key exchange (PAKE) or some other procedure. Once the users have identified themselves for a session, a session key is generated either by a classical or QKD techniques
for different levels of security guarantees. Such a service will affect the burst assembly process, and has to be implemented as an embedded service in the OBS network architecture. The supervisory security protocol is essential for the prevention of man-in-the middle attacks.

3.3 Integrated Secure OBS Router Architecture

In this section, we show how to embed the proposed security services as part of the native OBS network architecture. The integrated router architecture to support both classical and quantum cryptography is also presented.

*sQ-channel for quantum key distribution*: The proposed realization of QKD in OBS networks is as follows. As mentioned earlier, OBS preserves the photonic modality of information within its domain. We additionally introduce the constraint of optical passivity within the OBS boundary, specifically, so far as the channel that carries the quantum key Fig. 3. Creating a Q-channel between edge routers. information (called the Q-channel in this paper) is the photon on the Q-channel on an end-to-end basis. Since WDM technology is used for interconnecting the edge and the core routers, one (or several) of these channels (wavelengths) would carry the photon whose polarization would convey information regarding the key. Figure 3 shows the creation of a Q-channel between a pair of edge routers. The support for Q-channels in OBS routers is further explained below.

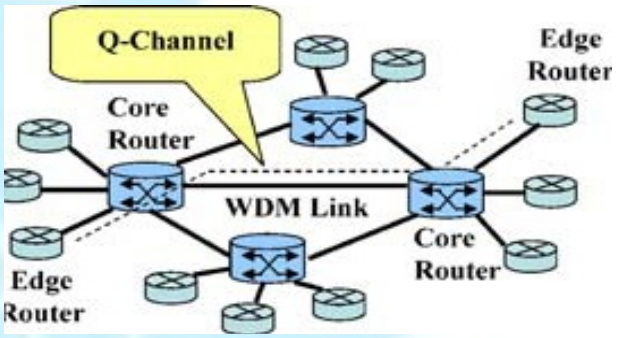



Fig 3

*Secure edge router architecture*:

The OBS edge router aggregates traffic into bursts based on destination edge router addresses, and possibly QoS parameters. The basic operation of an edge router can be found in Reference [10]. We extend the basic OBS edge router architecture to support embedded OBS security services as shown in Figure 4. At the point of ingress direction, the assembled bursts and their corresponding headers are encrypted before transmission onto the optical link. At the point of egress direction, the received burst headers are authenticated before their corresponding bursts are decrypted and disassembled. The key management functions include both classical and quantum components. The classical key distribution protocol uses the control channel, while the QKD is *via* Q-channels. The burst integrity control interacts with the burst assembly process in the burst transmitter and retransmits bursts as necessary.

*Secure core router architecture*:

OBS core routers electronically process the burst headers sent on the control channel while allowing optical bursts to pass transparently [10]. The integrated secure OBS core router architecture shown in Figure 5 supports Q channels for QKD, as well as classical key distribution protocols. The key manager in the core router architecture is for burst header authentication, and is transparent to the burst encryption key exchanged on an end-to-end basis. The burst scheduling process is only executed when the burst header is

authenticated. When bursts cannot be scheduled due to lack of available outgoing WDM channels, the burst scheduling process interacts with the burst integrity control unit to inform the ingress router, and trigger burst retransmission.

High performance electronics such as field programmable gate arrays (FPGAs) can be used to implement the proposed embedded security services in the secure edge and core routers, in much the same way as the burst assembly and burst scheduling blocks are implemented

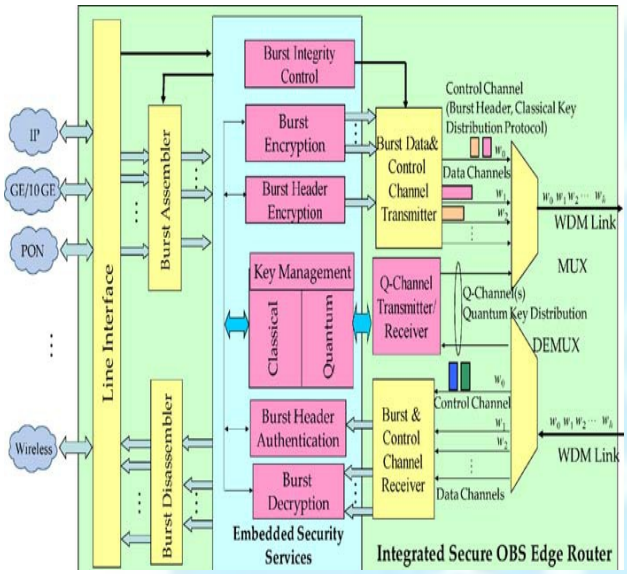



Fig 4.Integrated secure OBS edge router architecture

## IV. QUANTUM CRYPTOGRAPHY FOR ENHANCED SECURITY

### 4.1.Quantum Cryptography Background

It is proven that should the length of a random key equal the length of the message (in other words, if the rate at which the key can be transported equals the data speed), the encryption performed on the message through a simple technique such as the exclusive OR operation will lead to a theoretically unbreakable cipher Since there is no secure way of sending the random key over a public channel, the use of quantum cryptography can be envisaged as matching the performance of the theoretically unbreakable cipher. The first quantum-based scheme for exchanging secure keys was made by Bennett and Brassard in 1984 and it is called the BB84 protocol , which is the most popular QKD method. QKD is effective because of the no-cloning theorem that identical copies of an arbitrary unknown quantum state cannot be created. The BB84 protocol and its variants use qubits (quantum bits) in one pass and this is followed by two additional passes of classical data transmission. If Eve tries to differentiate between two non-orthogonal states, it is not possible to achieve information gain without collapsing the state of at least one of them . Proofs of the security of quantum cryptography are given variously in References pactical issues have been considered in References, and optical implementations are discussed in References . The issue of using attenuated lasers rather than single photon sources is considered .. In short, quantum cryptography is ideally suited for OBS since it is fundamentally based on the quantum properties of a photon. Besides leading to a theoretically unbreakable encryption scheme, the quantum-based encryption technology is well matched for use in an end-to-end photonic environment, which the OBS environment typifies.

### 4.2. BB84 Quantum Cryptography Protocol and Siphoning Attacks

We first describe how BB84 quantum cryptography protocol works. Unlike classical states, a quantum state is a superposition of several mutually exclusive component states. The weights of the component states are complex and their squared magnitude represents the probability of obtaining that specific component state. The quantum state *X*, if it is a two component state, or a qubit, will be written as: $|X\_ = a\ |0\_ + b\ |1\_$ where $|a|2 + |b|2 = 1$. Suppose, Alice and Bob each has two polarizers, with 0/90 degrees and with 45/135 degrees. If Alice and Bob use the same basis frames, then they can communicate different binary states with each transmission. The two bases may be represented two bases may be represented graphically as + and x, respectively.

We assume that Alice sends the string 0101100 using the two bases. Since Bob does not know the bases used by Alice, he chooses random bases as shown in Figure 6(b) and makes measurements. Bob sends the chosen basis vectors to Alice who can now estimate as to which measurement bases chosen by Bob were correct; this is communicated by Alice to Bob through a classical communication channel. Bob discards un-matched bits, and the resultant bits . Since only the polarizers at locations 1, 3, 4, 6, 7 correspond to the choices made by Alice, Bob obtains the raw key of sub-string 00100. The steps of BB84 protocol are summarized as follows:

*Step 1*: Alice randomly chooses polarizers to generate photons and sends them to Bob.
*Step 2*: Bob receives those photons with randomly chosen polarizers.
*Step 3*: Alice and Bob match their bases and discard the data for un-matched polarizers.

However, BB84 is susceptible to siphoning attacks. The unconditional security of BB84 and its variants can only be guaranteed if one's light source emits nothing but single photons. Since this is not possible with current light sources, eavesdropping attacks are possible.

In particular, the eavesdropper siphons off individual photons and measures them to determine what the legitimate receiver has obtained. To reduce the probability that pulses will contain multiple photons, current implementations of BB84 and its variants limit the intensity of each pulse and reduce the bit rate at which they are sent. But the weaker a pulse is, the less distance it can travel, and a slower bit rate reduces the speed at which keys can be distributed. The problem of siphoning attack plagues all variants of the BB84 protocol and, therefore, it is essential to have a new quantum cryptography protocol where the siphoned photons do not reveal any information about the transmitted bit.

4.3. 3-Stage Quantum Cryptography

Protocol for Secure Optical Burst Switching Quantum cryptography allows one to go beyond the classical paradigm and, therefore, overcome the fundamental limitations that the classical techniques suffer from. However, it also faces new challenges related to performance in the presence of noise and certain limitations of the single-photon generators. Our proposed integrated secure OBS architecture is fully compatible with the well-known BB84 protocol.
However, to deal with the technical challenge of siphoning attack on the practical multi-photon sources in the BB84 protocol, we propose to use a new 3-stage quantum cryptography protocol for the secure OBS framework. Unlike BB84 and its variants, the 3-stage quantum cryptography protocol is immune to siphoning attacks and therefore, multiple photons can be safely used in the quantum key communication.

3-stage quantum cryptography protocol is based on random rotations which can better protect duplicate copies of the photons than in non-single qubit transmissions of the BB84 protocol. This also means that the new protocol can use attenuated pulse lasers
rather than single-photon sources in the quantum key exchange, which will potentially extend the transmission distance. The 3-stage quantum cryptography protocol for security services in OBS is described as follows.

Consider transferring state X from Alice to Bob. The state X is one of two orthogonal states and it may represent 0 and 1 by prior agreement of the parties. To transmit the quantum cryptographic key, Alice and
Bob apply secret transformations *UA* and *UB* that are commutative. The protocol can be summarized as follows:

*Step 1*: Alice applies a unitary transformation *UA* on quantum information *X* and sends the qubits to Bob.
*Step 2*: Bob applies *UB* on the received qubits *UA*(*X*), which gives *UBUA*(*X*) and sends it back to Alice.
*Step 3*: Alice applies *U†A* (transpose of the complex conjugate of *UA*) on the received qubits to get *U†AUBUA*(*X*) = *U†AUAUB*(*X*) = *UB*(*X*) (since *UA*& *UB are commutative)*

Fig. 7. Illustration of recommended quantum cryptography protocol for security services in OBS networks .and *UB* commutate, *UBUA*(*X*) = *UAUB*(*X*))

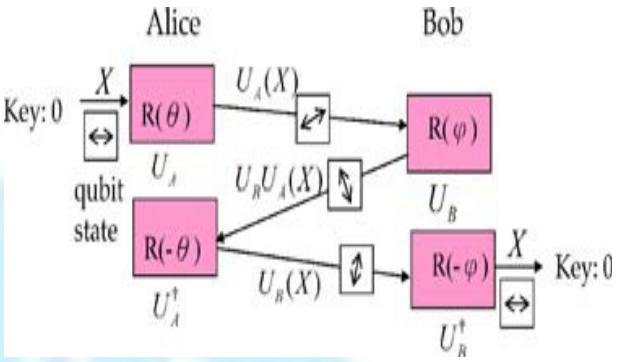



Fig 7.Illustration of recommended quantum cryptography protocol .

and sends it back to Bob. Bob then applies *U†B* on *UB*(*X*) to get the quantum information *X*. The use of random transformations, which Alice and Bob can change from one qubit to another, guarantees that from the perspective of the eavesdropper, the probability of collapsing into |0_ and |1_ states has equal probability, which is desirable for cryptographic security. An example of the proposed new protocol is illustrated in Figure 7. As we can see, while the actual quantum state of *X* is never exposed on the link, Bob is able to restore *X* and receives key 0 successfully.
The commutative of the rotation operator

$$R(\theta) = \begin{matrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{matrix}$$

is clear from the relation

$$R(\theta)\cdot R(\varphi) = \begin{matrix} (\cos\theta & -\sin\theta) \\ (\sin\theta & \cos\theta) \end{matrix} \times \begin{matrix} (\cos\varphi & -\sin\varphi) \\ (\sin\varphi & \cos\varphi) \end{matrix}$$

$$= \begin{matrix} \cos(\theta+\varphi) & -\sin(\theta+\varphi) \\ \sin(\theta+\varphi) & \cos(\theta+\varphi) \end{matrix}$$

unlike the BB84 protocol which is vulnerable to siphoning of photons in an attenuated pulsed laser system, the proposed 3-stage protocol is immune to such an attack since the actual quantum state of the key is never revealed in the communication. This property is of significant importance in terms of using quantum cryptography in a practical network environment where an optical path can potentially be extended beyond trusted routers.

## V. IMPLEMENTATION

In this section, we discuss the implementation aspects of the protocol and practical realization of the rotation operators, which are crucial to providing secure data transfers. The section also highlights the use of transformations that apply on multiple qubits simultaneously. One possible implementation is to apply Pauli transformations. They are convenient to use, and entail less precision requirements. The only condition for applying any new transformation in the operation of the three-stage protocol is that the transformations should map into the |0> and |1> states with equal probability so that the requirement for cryptographic security remains intact. The simplest group consist of the basic single-qubit operators *X, Y, Z.*

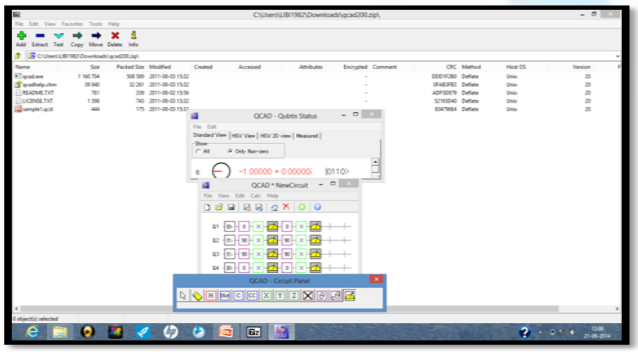
$$X = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \qquad Y = \begin{matrix} 0 & -i \\ i & 0 \end{matrix}$$

$$Z = \begin{matrix} 0 & -1 \\ -1 & 0 \end{matrix}$$

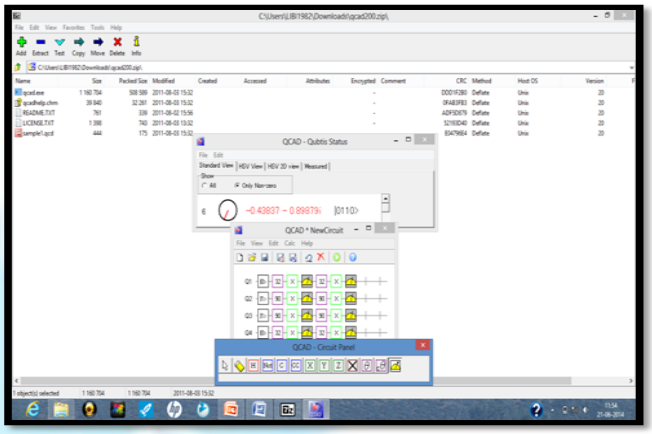
"QCAD" is a windows-based environment for quantum computing simulation which helps in designing circuits and simulating them. QCAD can simulate the designed the circuits and show results (states of qubits).

Here Alice is sending four qubits 0110 to Bob.Alice is sending 0 bit in 0 degree polarization & 1 bit in 90 degree polarization. After that each bit undergoes Pauli transformation(x) .Then the status is measured. Bob will use the same polarization & transformation on each bit. After measuring the status it is found that both the measured values are same.

The output obtained after doing this in QCAD is shown below.



For the same qubits with different polarization for each bit has done and measured the qubits status .The output is shown below.The measured values is different in both the cases

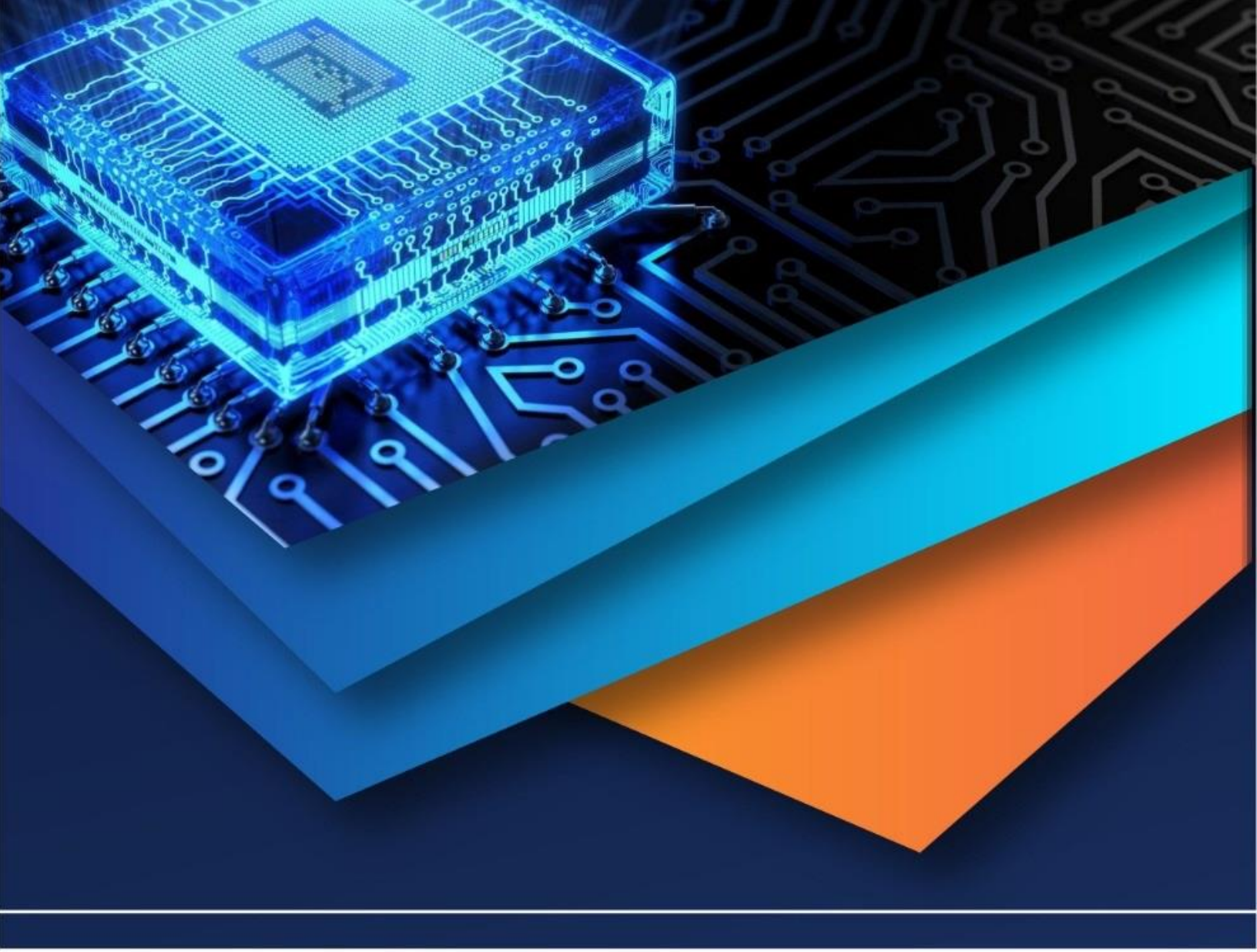


## VI. CONCLUSION

Practical implementations of BB'84 protocol are not secure with the presence of Eve. In contrast, the proposed implementation of the three-stage protocol allows multiple photons to be used in the secure communication, even with the presence of Eve.This paper has proposed an approach to embed a security framework in the native OBS network architecture, providing a means to secure the future Internet from the ground up. The proposed embedded security architecture allows the most suited classical and quantum cryptography techniques to be deployed, making it possible to offer robust security. While the proposed integrated security framework is fully compatible with the well-known BB84 quantum cryptography protocol, we recommend a new 3-stage quantum cryptography protocol based on random rotations of the polarization vector for the OBS security framework. Compared to the BB84 protocol, the 3-stage quantum cryptography protocol for security services in OBS networks has the following advantages: (1) it does not require single photon sources as required in the BB84 protocol (since practical photon sources produce many photons some of which may be siphoned off to break the protocol). Instead, multiple photons can be used in communication, increasing potential transmission distances, and reducing the protocol's sensitivity to noise; (2) while the BB84 protocol has one hop quantum communication followed by two hops of communications through classical channels, all three hops of communication in the new protocol are quantum, providing more security; (3) the newprotocol never reveals the actual quantum state of the key on the communication link, allowing the protocol to be
extended beyond trusted routers.

REFERENCES

[1] Farahmand F, Jue J. Supporting QoS with look-ahead window contention resolution in optical burst switched networks.ProceedingsoftheIEEEGlobalTelecommunications (GLOBECOM), San Francisco, CA, December 2003; 2699-- 2703.
[2] Qiao C, Wei W, Liu X. Extending generalized multiprotocol label switching (GMPLS) for polymorphous, agile, and transparent optical networks (PATON). IEEE Communications Magazine 2006; 44(12): 104--114.
[3] Phuritatkul J, Ji Y, Zhang Y. Blocking probability of a preemption-based bandwidth-allocation scheme for service differentiation in OBS networks. IEEE/OSA Journal of Lightwave Technology 2006.
[4] Chen Y, Turner J, Mo P. Optimal burst scheduling in optical burst switched networks. IEEE/OSA Journal of Lightwave Technology 2007.
[5] O'Mahony MJ, Politi C, Klonidis D, Nejabati R, Simeonidou D. Future optical networks. IEEE/OSA Journal of Lightwave Technology 2006; 24: 4684--4696.
[6] Chen Y, Verma PK. Secure optical burst switching (S-OBS)- --framework and research directions. IEEE Communications Magazine 2008; 46(8): 40--45.
[7] Stallings W. Cryptography and Network Security: Principles and Practice (4th edn), Prentice Hall: NJ, 2006,
[8] ChenY,TurnerJ,ZhaiZ.Designandimplementationofanultra fast pipelined wavelength scheduler for optical burst switching. Photonic Network Communications 2007; 14: 317--326.
[9] Wang L, Chen Y, Thaker M. Virtual burst assembly at ingress edge routers---a solution to out-of-order delivery in optical burst switching (OBS) networks. Proceedings of the IEEE
[10] Devetak I, Winter A. Relating quantum privacy and quantum coherence: an operational approach. Physical Review Letters 2004;.
[11] Kak S. A three-stage quantum cryptography protocol. Foundations of Physics Letters 2006; 19: 293--296.
[12] Yuhua Chen,Pramode K Verma. Embedded security frame work for integrated classical & quantum cryptography services in optical burst switching networks Security and communication networks -2009
[13] Sayonha Mandal ,James Sluss. Implementation of secure quantum protocol using multiple photons for communication-2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY