DOI 10.1515/joc-2014-0003 — J. Opt. Commun. 2014; 35(2): 109–116

A.M. Balamurugan* and A. Sivasubramanian

A Novel QKD-based Secure Edge Router Architecture Design for Burst Confidentiality in Optical Burst Switched Networks

Abstract: The Optical Burst Switching (OBS) is an emergent result to the technology issue that could achieve a viable network in future. They have the ability to meet the bandwidth requisite of those applications that call for intensive bandwidth. The field of optical transmission has undergone numerous advancements and is still being researched mainly due to the fact that optical data transmission can be done at enormous speeds. The concept of OBS is still far from perfection facing issues in case of security threat. The transfer of optical switching paradigm to optical burst switching faces serious downfall in the fields of burst aggregation, routing, authentication, dispute resolution and quality of service (QoS). This paper proposes a framework based on QKD based secure edge router architecture design to provide burst confidentiality. The QKD protocol offers high level of confidentiality as it is indestructible. The design architecture was implemented in FPGA using diverse models and the results were taken. The results show that the proposed model is suitable for real time secure routing applications of the Optical burst switched networks.

Keywords: optical burst switching, quantum key, burst confidentiality, stream cipher

PACS® (2010). 42.81.Uv, 42.79.Sz, 42.50.Nn

***Corresponding author: A.M. Balamurugan:** Department of Electronics and Communication Engineering, St. Joseph's College of Engineering, Chennai, Tamilnadu, India.
E-mail: bala_am2000@yahoo.com
A. Sivasubramanian: Department of Electronics and Communication Engineering, St. Joseph's College of Engineering, Chennai, Tamilnadu, India

1 Introduction

As the demand for traffic keeps on increasing thoroughly during the recent years, many new technologies have been introduced. The main reason for the upcoming technologies is the demand for bandwidth to a greater extent. More and more user networks are emerging as a result of which the demand for the bandwidth also increases. The internet traffic demand has an exponential increase due to large amount of efficient users. Internet is termed as "network of networks" due to information transfer globally. These are supported to provide high speed, performance and cost service depending on the demands of their customers. One is an Optical to Electrical to Optical (O/E/O) Switching, and the other is an all-Optical switching. O/E/O switching is the physical switching architecture used in the existing network. In O/E/O switching, incoming optical data is converted to the electrical domain before it is stored in the switch for processing. The data then is converted back to the optical domain for outgoing transmission. On the contrary, data in all-optical switching is switched through the switch all optically without converting it to the electrical domain. There are some potential benefits for all-optical switching over O/E/O switching [1]. First, the operation of O/E/O switching is based on a store-and-forward architecture while all-optical switching is cut-through in nature. Therefore, O/E/O switching introduces some transmission delays in intermediate nodes while all-optical switching does not. Secondly, the main advantage of all-optical switching, is that they simply switch data streams of light without any O/E/O conversion in intermediate nodes. Thus, services and/or protocols are transparent to the network. This gives an opportunity for providing a flexible and future proof network. However, all-optical switching still has some drawbacks when compared to O/E/O switching. First, all-optical switching is still an emerging technology while O/E/O switching is a proven technology, which has already been deployed in the current network. Second optical processing is very limited in the current technology. The major two classifications of O/E/O switching are: Optical circuit switching (OCS) and Optical packet switching (OPS) [2]. Each and every technology has its own outcomes of priority and pit fall. A WDM optical packet network consists of optical packet switches interconnected by WDM fiber links. Optical packet switches are fixed size packets which operate in slotted manner. The demand for more bandwidth is fuelled by packet switched

IP traffic and the traffic generated by higher layer protocols and applications, such as the World Wide Web. Optical burst switching (OBS) combines the best of optical circuit switching and packet switching and can be used to carry IP over DWDM [3].

Optical burst switching is a new technology that it is currently under research. Unlike optical packet switching, it does not require optical buffering. It combines the recompenses optical packet switching and circuit switching. It is regarded as a viable solution for transmitting bursts over an optical network [4]. A connection is setup uniquely for the transmission of a single burst. An OBS network consists of OBS nodes interconnected with WDM fiber in a mesh topology. An OBS node is an OXC which has a very low configuration time, due to the fact that connection does not stay up for a long time. OBS network consist of two routers-edge and core router. Edge router is again classified as ingress and egress node. In general, ingress node performs the action of assembling the packets into bursts from various sources which can be of variable size [5]. The work of ingress node is assembling, scheduling, routing wavelength assignment. Each burst is formed once it reaches a certain threshold limit or time. On an average a burst consist of minimum of 40,000 packets. Egress node performs the disassembly of bursts into packets. Egress node works on disassembling and forwarding packets to higher network layer. Core node performs controlling and signaling action [6]. These bursts are transported directly over the WDM link. For each burst, it first sends a SETUP message to the network, to announce its intention to transmit. Transmission of the burst takes place after a delay known as offset [7]. The network nodes allocate resources for this single burst.

The major advantage is that there is no synchronization required, since the data burst and the header travel on a separate WDM channel. Though OBS network has added advantages there are certain disadvantages too. The normal behavior of each node follows certain security concepts such as confidentiality, integrity and authentication. Vulnerability is happens when the normal behavior of the node is not obeyed. The OBS also suffers from security and vulnerability issues. Each and every data burst has to pass through a number of intermediate nodes. If any one intermediate node compromises to some factor it becomes malicious and there comes the problem of security.

2 Edge router model

In OBS networks, data are accumulated into variable size data bursts, and are transported directly over K wavelength channels. For each data burst a burst header is created, and is sent on a dedicated control channel before transmission of the data burst. The data bursts can remain in the optical domain and can pass through OBS routers transparently. This discards the requirement for optical buffers in these kinds of networks. In addition, since burst headers and data bursts are sent on separate channels, there is no call for for synchronization requirement. OBS edge routers are responsible for assembly of packets into data bursts according to the requirement of next edge router address. A burst is created when it either reaches the pre-defined maximum burst size, or the burst assembly time reaches the timeout value. Once a burst is created, the ingress edge router creates a burst header and it is sent on a dedicated control channel. The burst header contains the length of the burst, and the offset time between the data burst and the burst header. When the burst header reaches the OBS core router, it is converted to electronic signal and processed electronically. By processing the burst header and depending on availability of channel, at least one outgoing WDM channel which is available for the duration of the burst is selected and a channel will be selected to carry the data burst. If not, the data burst will be dropped. When data bursts reach the egress edge router, data bursts will be disassembled back to packets and forwarded to proper network interfaces. The burst assembly as well as disassembly functionality is provided only at the OBS edge routers. There is no reassembly of burst in the OBS core network. There is a one-to-one correspondence between the burst header and its corresponding burst. The burst headers are responsible for setting up optical data paths for their data bursts. The data bursts will simply follow the light paths set up by burst headers and are transparent to OBS core routers [8]. The OBS edge router is shown in Fig. 1.

3 Security issues in OBS edge router

OBS networks can prove to be cost effective interconnection solutions to the ever growing Internet. However, OBS network is not free of security issues. In this section, the need to take 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

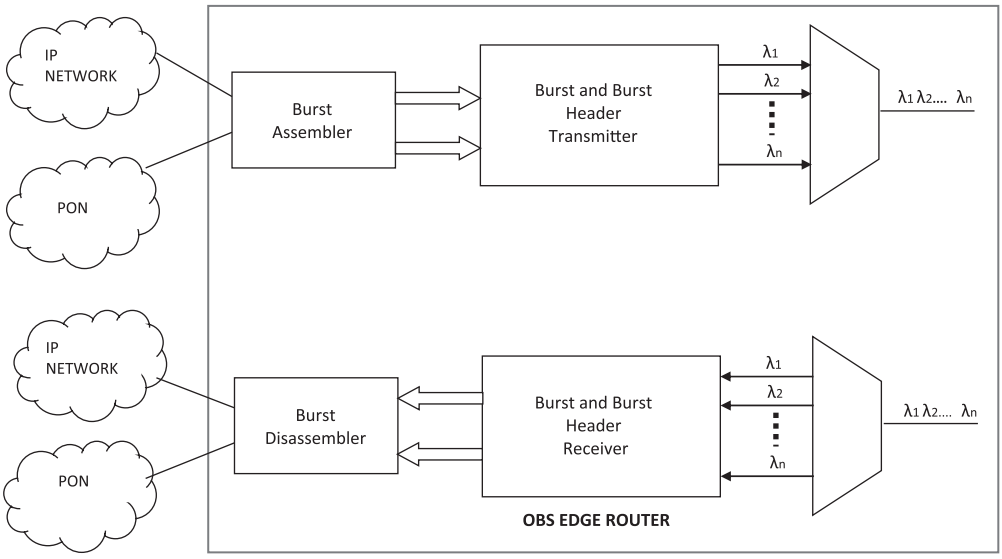

Fig. 1: OBS edge router

for the arriving burst. Since the burst has been sent, it is will arrive at the input of the core router. Then the burst is no longer connected with its header and becomes an orphan burst. As a result, these orphan data bursts can be tapped off by some undesirable party, thereby compromising its security [8].

Redirection of data bursts: The one-to-one correspondence between the burst header and its corresponding burst is indicated by the offset time present in the burst header. This one-to-one correspondence can be violated by sending a malicious header corresponding to the same burst. This results in the route and the destination for the burst being modified by the malicious header, even though a valid path has been set up by the authentic header.

Replay: Replay attack refers to capturing a valid but expired burst and transmitting that at a later time, or by sending an expired burst header to make the optical burst to circulate in the OBS network, thereby delaying its delivery to the final destination.

Burst header flooding attacks: The intruders compromises any one node and copies and replicate its original Burst address. The Duplicated Copies of the Burst address are then feed to the next intermediate node of the compromised node. The subsequently intermediate node upon receiving such burst header tries to reserve for such duplicate address. Therein the intermediate node is under Buffer with overflow. At last, it results in not permitting the intermediate node to reserve any resource even if they are effective burst header. This is named as Burst Header Flooding attack [9].

Fake burst header attack: The intruder tries to send malicious burst control header to the particular node. These headers redirect all the data to a fake destination that is controlled by the attacker. The original destination will be ignorant of this tapping and the security being compromised as the fake destination forwards to the real destination disguised as the source and sends through the same data burst [9].

Denial of service attack: The OBS core that decides the path of the data burst follows the unoccupied or unused outgoing Wavelength division Multiplexing (WDM) channels to make their decisions in deciding their path. Whenever there is a non availability of WDM, the burst packets that are to be transited are thrown away. The routers having routed the control packet with their destination does not have well defined mechanism to Counter check the burst sent upon they reaching their destination. This loophole can be used to exploit the network by setting up a malicious burst header that would push WDM to be labeled as busy at all times when in reality they network is completely free.

Hence the OBS network has to be designed in such a way that the networks is free from all the above mentioned security threats. All this is possible only with a framework for every node in the network that is capable of tackling these issues. One such model is discussed and analyzed which tries to provide burst confidentiality.

4 Model of proposed secured edge router

In this architecture, the various input traffic patterns like Internet protocol, passive optical network, gigabit Ethernet, wireless and many more are sent as input to the line interface from where these inputs are assembled together in a form known as burst. Burst is a collection of packets. Bursts are usually transported directly over wavelength division multiplexing (WDM) links. Burst consists of a header known as the burst header which is generated for each data burst and is sent on a separate control channel ahead of the data burst. Burst assembler is used to assemble all the input packets in the form of a burst. From there, the burst is encrypted and the key used for this encryption is the quantum key. This key is then encrypted in the burst header using the classical key.

From there, the burst is sent through the burst control channel transmitter to the burst control channel receiver where the burst is received and first the burst header decryption is done using the classical key followed by the burst decryption using the quantum key. The burst is then sent to the burst disassembler which disassembles the burst. This is an effective way to secure the burst. Securing the burst is very important as there are many possibilities that the bursts can be tapped off by some undesirable source. There are also possibilities that a malicious header be inserted in the middle to divert the path of the burst [10]. There can also be an injection of an expired burst header in order to cause delay in getting delivered to its final destination. Moreover, whenever a burst is scheduled, the WDM channel will be marked as 'busy' by the core router for that particular duration of the burst so that no other burst is delivered at this time. This proposed architecture provides an idea of how a burst can be maintained confidential and how it can be kept away from the tappers. Security is an aspect which should be considered of highest importance when it comes to data bursts. Without security, the bursts can be easily tapped or altered in any way. It is therefore very important to consider the confidentiality of the burst and this is the proposed architecture to demonstrate the Integrated Secured OBS Router. The proposed Edge Router architecture is shown in Fig. 2.

4.1 Burst encryption

The conventional method of encryption implemented in the Optical Burst Switching is Block cipher using the AES algorithm. The AES algorithm uses fixed key sizes. The sizes are optimally chosen between 128, 192 or 256 bits. The fixed key nature is a major disadvantage in the optical domain since fixed sizes would result in identical cipher text which eliminates the need to cipher the data at all. Moreover, Block cipher uses blocks of data for encryption but the eavesdropper can replace the actual block with a fake block to cause chaos. To overcome all the above disadvantage we have proposed to use the stream cipher using the RC4 algorithm [11]. This method is preferred over the majority of other methods owing to its remarkable simplicity and speed of processing. The key generation is deployed utilizing the Quantum key distribution. Thus we would never end up with identical key since QKD is based on the properties of photons. The stream cipher is also known as the state cipher due to the fact that the encryption standard is based on the current state of the bit to be encrypted [12].

In OBS networks the ingress routers consists of the collection of data which stay in the OBS core network in the optical domain and only at the egress edge router they are dissembled. Thus, encrypting the data at the ingress router and decrypting it at the egress router ensures End-to-end data burst confidentiality. The data burst is maintained confidential since the remaining routers act only as a medium of travel and need not necessarily know about the data in the encrypted burst. The data can be stolen from many intermediate attacker nodes while data traversal. The act of eavesdropping can happen in the two ways: one, by direct physical tampering of the optical cable. Two, residual cross talk from the adjacent channel. The second method of the attack can take place in the WDM networks where various subscribers use various wavelengths causing leaking of optical power from the adjacent channel. But, the confidentiality of the data is still preserved because practical difficulty in eavesdropping is very high, assuming it to be impossible.

Theoretically, if the length of the data equals the data speed, the outcome of the operation would be an unbreakable cipher. Here we are using symmetric key using quantum key distribution for encrypting and decrypting the text. The quantum key distribution uses a separate channel to transmit the key. The bits carrying the quantum key are called Q-bits. The security provided by the QKD is called the "unconditional security" without posing any restrictions on the abilities of the eavesdropper. The QKD is ideally suited for OBS since its based on the quantum properties of photons. Thus, the QKD helps to achieve the theoretically unbreakable and non-identical cipher [13].

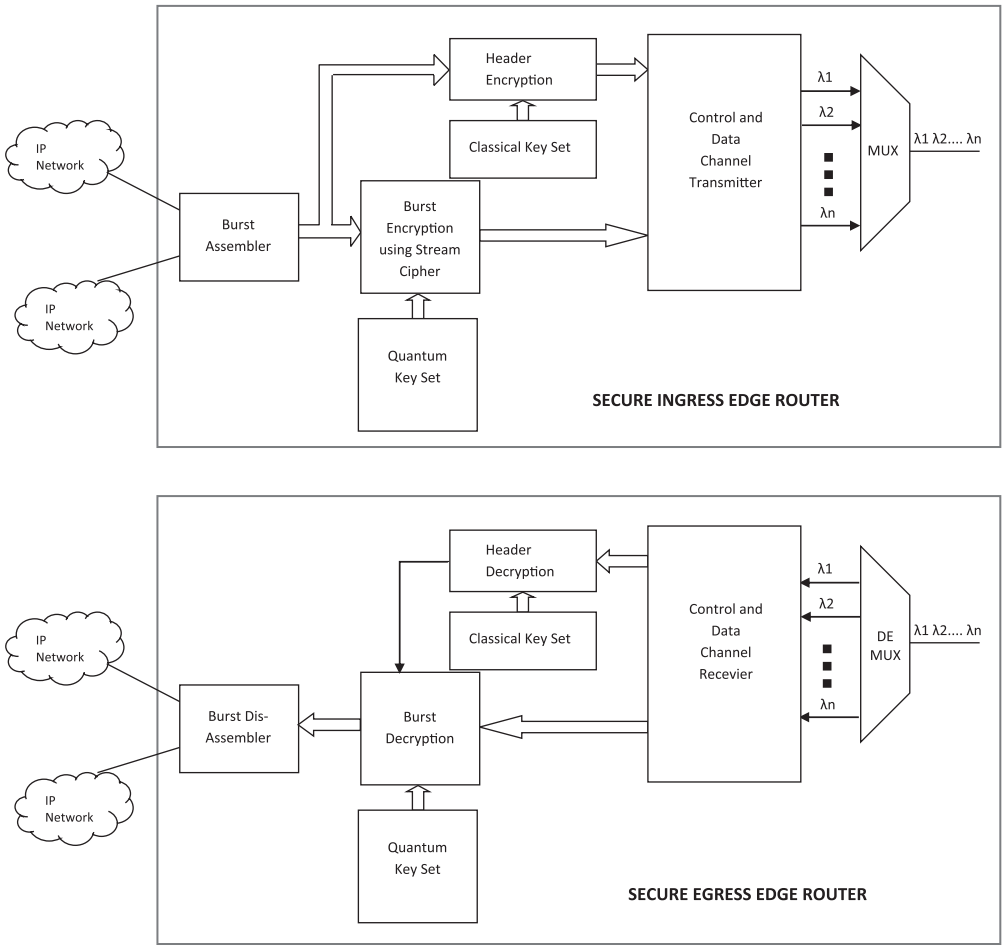

Fig. 2: Secure edge router model

4.1.1 RC4 realization

RC4 uses a variable length key from 1 to 256 bytes to initialize a 256-byte state table. The state table is used for subsequent generation of pseudo-random bytes and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text. Each element in the state table is swapped at least once. The RC4 algorithm works in two phases, key setup and ciphering. Key setup is the first and most difficult phase of this algorithm. During a N-bit key setup, the encryption key is used to generate an encrypting variable using two arrays, state and key, and N-number of mixing operations [14]. These mixing operations consist of swapping bytes, modulo operations, and other formulas. Once the encrypting variable is produced from the key setup, it enters the ciphering phase, where it is XORed with the plain text message to create an encrypted message. XOR is the logical operation of comparing two binary bits. If the bits are different, the result is 1. If the bits are the same, the result is 0. Once the receiver gets the encrypted message, he decrypts it by XORing the encrypted message with the same encrypting variable [15]. Now, the keys K used in our proposal is implemented or derived from the QKD algorithm called quantum keys. Adapting the quantum unbreakable keys of the QKD in the RC4 algorithm is the key strength to this proposal.

Key setup implementation:

```
For i from 0 to 255
        S[i] = i;
End
j = 0;
for i from 0 to 255
j = (j + s[i] + key[i mod key length]) mod 256
        swap values of s[i] and s[j]
end for
```

Ciphering implementation:

```
i = 0;
j = 0;
while generating output
        i = (i + 1) mod 256;
        j = (j + S[i]) mod 256;
        swap values of S[i] and S[j];
K = S[(S[i] + S[j]) mod 256];
```

The quantum keys are shared uniquely among the many of the ingress to egress paths for data security and ease of decryption. The Quantum keys are stored in the RAM of the routers that have optimal memory allocation at their respective places. These RAMs prove to be cost effective too.

4.2 Quantum key generation

It is built based on Heisenberg's uncertainty principle. It states that certain pairs of physical properties cannot be calculated simultaneously. If one of them is calculated, other gets disturbed and becomes impossible to compute. Quantum key distribution uses a separate channel to transmit key. It carries photons of random polarization and is known as Q-bits. Photons get altered when they are measured. Thus data through this channel cannot be intercepted without being detected. This is achieved by sender encoding the bits of the key as quantum data and sending them to receiver. If third party tries to learn these bits, then the messages will be disturbed and both the Sender and Receiver will notice thereby making it unbreakable. The key is thus typically used for encrypted communication. The security of QKD can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something that is not possible with classical key distribution [16]. This is frequently described as "unconditional security", even though there are some minimal assumptions required including that the laws of quantum mechanics apply and that Sender and Receiver are able to authenticate each other, i.e. Third party should not be able to impersonate Sender or Receiver as otherwise a man-in-the-middle attack would be possible. QKD is the only example of commercially available quantum cryptography [17]. There are three main security protocols for QKD namely B92, BB84 and Entanglement based QKD. In this paper we use two stage Quantum key generation using B92 and BB84 protocol. In BB84 protocol we use two polarization states called rectilinear (R) and diagonal (D). The single photon could be polarized as four states: H, V, $|45°\rangle$ and $|135°\rangle$ which is shown in Table 1.

Table 1: Polarization states for QKD

State/bit	0	1
Rectilinear	H	V
Diagonal	$\|45°\rangle$	$\|135°\rangle$

4.3 Two-stage QKD protocol (Stage 1: B92 & Stage 2: BB84)

This protocol makes use of both B92 and BB84. In the first stage, Ingress node sends a random sequence of photon using B92, and in the second stage, Egress node will use BB84 or B92 to send the photons in which Egress node's measurement results are "N" in the first stage.

Ingress node sends a random sequence of photons, $|H\rangle$-photon and $|135°\rangle$-diagonal photon. Egress node randomly chooses its detector basis from $|45°\rangle$-diagonal basis or $|V\rangle$-basis to measure each photon, and the bases are interpreted as a binary sequence. Results of Egress node's measurement are taken. Egress node choose its basis according Egress node's bit, and then it sends a random sequence of photons, $|H\rangle$-photon, $|V\rangle$-photon, $|45°\rangle$-photon, and $|135°\rangle$-photon where its measurement results are "N". Ingress chooses its detector bases according Ingress node's bits. To measure each photon, results of Ingress node's measurement are taken. Then, the states are interpreted as a binary sequence. Ingress node reports its detector bases for each photon. Egress tells Ingress which bases were correct. Ingress and Egress will share the bits where the results are "Y" in 2nd stage, neglecting all other bits. Ingress and Egress will get the final shared secret key which are shown in Table 2. For a k-bit sequence in the two stage QKD protocol, the idealized maximum shared bits between Ingress node and Egress node are $k \times 1/4$ in the first stage. Egress node resends $3k/4$ bits in the second stage and Ingress node may get maximum correct $3k/4 \times 2/3$ bits.

Finally the efficiency of our two stage QKD protocol will be

$$\frac{k \times \frac{1}{4} + \frac{3k}{4} \times \frac{2}{3}}{k + \frac{3k}{4}} = 42.9\%.$$

Thus, the average complexity order of two stage QKD is calculated as follows. There are k photons with two polarization states in 1st stage (B92), and $3k/4$ photons with

Table 2: An 8-bit sample for two stage QKD protocol

Sequence of bits		1	2	3	4	5	6	7	8
Stage 1									
1	Ingress node bit	1	0	1	0	1	1	0	0
	Ingress node polarization	135°	H	135°	H	135°	135°	H	H
2	Egress node detector basis	45°	45°	V	V	45°	45°	45°	V
	Egress node bit	0	0	1	1	0	0	0	1
3	Egress node measurement	N	N	Y	N	N	N	Y	N
	Shared secret key in 1st stage	–	–	1	–		–	0	–
Stage 2									
4	Egress node source basis	R	R	–	D	R	R	–	D
	Egress node bit	1	0	–	0	0	1	–	1
	Egress node polarization	V	H	–	45°	H	V	–	135°
5	Ingress node detector basis	R	D	–	D	R	R	–	D
6	Ingress node measurement	V	45°	–	45°	H	V	–	135°
	Ingress node bit	1	0	–	0	0	1	–	1
7	Ingress node reports basis	R	D	–	D	R	R	–	D
8	Egress node response	Y	N	–	Y	Y	Y	–	Y
9	Shared secret key in 1st stage	1	–	–	0	0	1	–	1
10	Final shared secret key	1	–	1	0	0	1	0	1

four polarization states in 2nd stage (BB84). The average complexity order is given by

$$\frac{2\times k+4\times \frac{3\times k}{4}}{k+\frac{3\times k}{4}}=2.86.$$

5 Implementation of proposed model

Implementation of proposed model has been attempted and achieved successfully on COTS FPGA'S using Xilinx ISE 14.1 simulator. The HDL used is Verilog. Table 4 below gives the details of the resource utilization for each of the realizations on the FPGA's. The Simulation criteria is shown in Table 3.

Table 3: The simulation criteria

HDL	Verilog
Version	Xilinx ISE 14.1
Burst size	2048 bits
Number of IP source	2
Packet size	1024 bits
Number of packets/Burst	2
Burst assembly algorithm	Threshold based
Traffic pattern	Self similar
Encryption algorithm	Stream cipher (RC4)
Size of key	256 bytes
Ciphering technique	XOR

SPARTON 6, VIRTEX 4, VIRTEX 6, VIRTEX 7 have been used. From the table it is observed that slice logic utilization varies from just 2% to 22% only. The LUT utilization ratio is between 20% to 97%.

The minimum period for each of the designed architecture is seen to vary from just 0.84 μsec to 0.2 μsec. Thus, it can be inferred that this architecture can be initiated for real time secure routing applications of the Optical burst switched networks. These low values of delay are an added advantage, obtained by realizing this architecture in hardware.

Further analysis shows that a major part of the delay is due to routing between the modules, which could be further optimized by back annotating the place and route (PAR) technique of the implementation. Also from the results of the logic utilization, it is seen that scalability of the system is not seen to be a difficult problem. Thus scalability and real time routing of the network is also achieved.

6 Conclusion

From the results obtained it can be concluded that this architecture can be appropriate for real time secure routing applications of the Optical burst switched networks. Also from the results of the logic utilization, it is seen that scalability of the system is not seen to be a difficult problem. Thus scalability and real time routing of the network is

Table 4: Device utilization summary

Model	Device	Slice			LUTs			Minimum period & clock period
		Available	Used	Percentage	Available	Used	Percentage	
VIRTEX 4	xc4vfx40-12-ff672	37248	8368	22%	37248	36357	97%	0.97 µs (80.273ns logic, 17.416ns route) (82.2% logic, 17.8% route)
SPARTAN 6	xc6slx100-3-fgg484	126576	8408	6%	63288	39714	62%	0.2 µs (38.570ns logic, 170.584ns route) (18.4% logic, 81.6% route)
VIRTEX 6	xc6vcx75t-2-ff484	93120	8403	9%	46560	35732	76%	0.18 µs (26.133ns logic, 154.123ns route) (14.5% logic, 85.5% route)
VIRTEX 7	xc7vx330t-3-ffg1157	408000	8410	2%	204000	41348	20%	0.084 µs (16.374ns logic, 67.805ns route) (19.5% logic, 80.5% route)

also achieved. Hence this proves to be an elucidation for burst confidentiality in OBS networks.

Received: January 15, 2014. Accepted: February 6, 2014.

References

[1] I. Chlamtac, A. Ganz, G. Karmi (1992). Lightpath communications: an approach to high bandwidth optical WAN's. IEEE Transactions on Communications, pp. 1171–1182.

[2] C. Qiao, M. Yoo (1999). Optical burst switching (OBS) – A new paradigm for an optical internet. Journal of High Speed Networks, Vol. 8, No. 1, pp. 69–84.

[3] A.M. Balamurugan, A. Sivasubramanian (2013). Optical burst switching issues and its features. International Journal of Emerging Trends & Technology in Computer Science, Vol. 2, No. 3, pp. 306–315.

[4] H.E. Fletcher (1983). A PCM frame switching concept leading to burst switching network architecture. IEEE Communications Magazine, Vol. 21, No. 6, pp. 13–19.

[5] K. Koduru (2005). New Contention Resolution Techniques for Optical Burst Switching. Master's thesis, Louisiana State University, May 2005.

[6] L.R. Garg, A. Kumar (2012). Survey on contention resolution techniques for optical burst switching networks. International Journal of Engineering Research and Applications (IJERA), Vol. 2, No. 1, pp. 956–961.

[7] C. Gauger, K. Dolzer, J. Späth, S. Bodamer (2001). Service differentiation in optical burst switching networks. Photonic Networks, March 2001, pp. 124–132.

[8] Y.H. Chen, P.K. Verma, S. Kak (2009). Embedded security framework for integrated classical and quantum cryptography services in optical burst switching networks. Security and Communication Networks, Vol. 2, No. 6, pp. 546–554.

[9] N. Sreenath, K. Muthuraj, G. Vinoth (2012). Threats and vulnerabilities on TCP/OBS networks. International Conference on Computer Communication and Informatics (ICCCI), January 2012, pp. 1–5.

[10] M.P. Fok, Z.X. Wang, Y.H. Deng, P.R. Prucnal (2011). Optical layer security in fiber-optic networks. IEEE Transactions on Information Forensics and Security, Vol. 6, No. 3, pp. 725–736.

[11] A.M. Balamurugan, A. Sivasubramanian. Quantum key based data burst confidentiality in optical burst switched networks. Scientific World Journal (accepted for publication).

[12] P.D. Townsend, S.J.D. Phoenix, K.J. Blow, S.M. Barnett (1994). Design of quantum cryptography systems for passive optical network. Electronic Letters, Vol. 30, No. 22, pp. 1875–1877.

[13] C.H. Bennet, G. Brassard (1984). Quantum cryptography: public key distribution and coin tossing. Proceedings of IEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, Dec. 1984, pp. 175–179.

[14] A. Mousa, A. Hamad (2006). Evaluation of the RC4 algorithm for data encryption. International Journal of Computer Science & Applications, Vol. 3, No. 2, pp. 44–56.

[15] N. Singhal, J.P.S. Raina (2011). Comparative analysis of AES and RC4 algorithms for better utilization. International Journal of Computer Trends and Technology, Vol. 79, No. 14, pp. 177–181.

[16] D.N. Kartheek, G. Amarnath, P.V. Reddy (2013). Security in quantum computing using quantum key distribution protocols. International Conference on Automation, Computing, Communication, Control and Compressed Sensing, 2013, pp. 19–25.

[17] A. Tanaka, M. Fujiwara, K. Yoshino, S. Takahashi, Y. Nambu, Akihisa Tomita, S. Miki, T. Yamashita, Wang Zhen, M. Sasaki, A. Tajima (2012). High-speed quantum key distribution system for 1-Mbps real-time key generation. IEEE Journal of Quantum Electronics, Vol. 48, No. 4, pp. 542–550.