Enhancing Grid Security using Quantum Key Distribution

Muhammad Mubashir Khan[1] and Jie Xu[2]

[1]*NED University of Engineering & Technology, Pakistan*
[2]*School of Computing, University of Leeds, UK*
mmkhan@neduet.edu.pk, j.xu@leeds.ac.uk

Abstract

Quantum Key Distribution (QKD) is a secure key distribution technology, which provides information theoretic or unconditional security. BBN DARPA quantum network and SECOQC network of secrets are the examples of such networks. Research is also in progress for the integration of QKD with the protocols in different layers of OSI model. Integration of QKD in point-to-point protocol (PPP) OSI layer 2 and with IPSEC at OSI layer-3 are the examples of such research efforts. All these steps are leading towards the utilization of QKD technology for enhancing the security of modern computing applications on the Internet. This paper presents a model for the exploitation of QKD security networks in high performance distributed computing applications, such as grid computing.

Keywords: *Quantum Key Distribution, Quantum Cryptography, Information Security, Security Protocols*

1. Introduction

In the beginning of 21st century two companies of the world one from USA, MagiQ Tech, and another from Switzerland, idQuantique, presented the commercial products of Quantum Key Distribution (QKD). The practical realization of QKD unveiled new arena of research in the area of Network and Information Security. At the time of writing this paper, QKD is assumed to be more secure than any other known cryptosystem against classical as well as quantum computer attacks.

Extensive research underway for sophisticated implementation of QKD in practical communication networks. Built by BBN Technologies, the *DARPA Quantum Network* was jointly developed by researchers at Harvard University, Boston University and BBN Technologies in 2004 [1]. The main goal of this point-to-point quantum network was to exploit QKD technology for securing standard Internet traffic. The EU funded FP6 project SECOQC (Secure Communication based on Quantum Cryptography) [2-4], clearly shows the feasibility of constructing highly integrated QKD-networks. The SECOQC network prototype presented a splendid practical example for the development and operation of a point-to-point QKD network architecture with sophisticated protocols. There are a number of other approaches and models for the utilization of QKD technology in a network fashion, see for example [5-8]. Furthermore, research is also underway for the integration of QKD protocols with the existing classical protocols like PPP, IPSec and SSL-TLS, which are widely used on the internet for secure communication [9-13], cf. Figure 1.

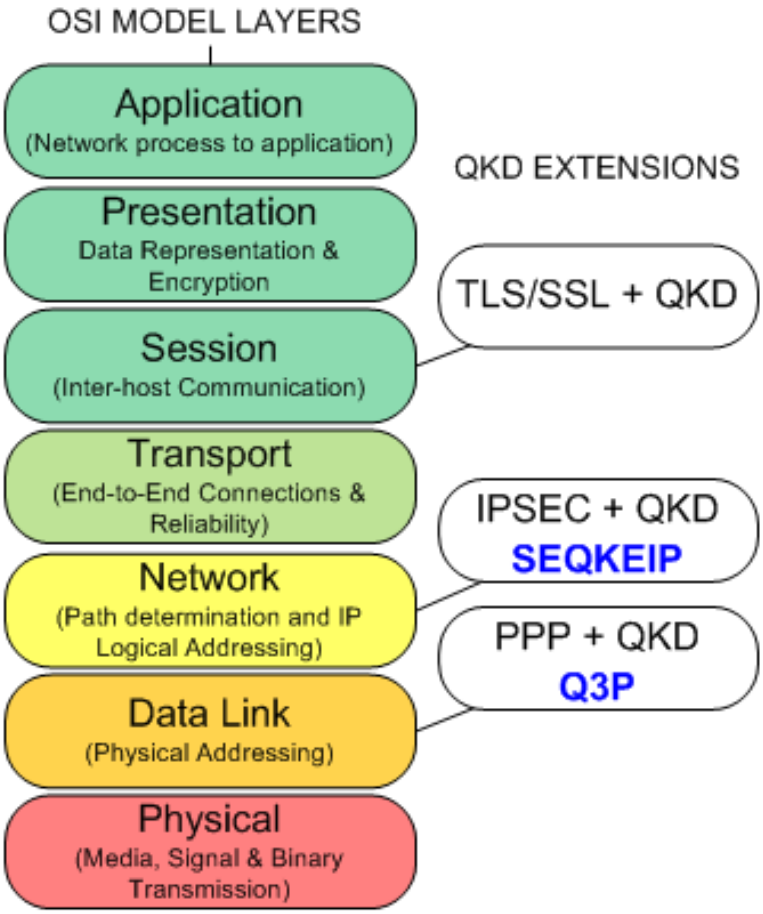

Figure 1. Integration of QKD with Different Layers of OSI Model

The above-mentioned progress reveals that the QKD network technology has great potential for securing the modern high performance distributed computing applications. In the next section we explain the potential weaknesses and requirements of the emerging distributed computing applications taking grid computing as an example.

2. Motivation

In computing, grid is a system architecture that coordinates resources, which are not subject to centralized control; using standard, open, general-purpose protocols and interfaces and delivers non-trivial quality of service. Grid computing has emerged as a modern technology to fulfill the high performance computing requirements of users, institutions and business organizations worldwide.

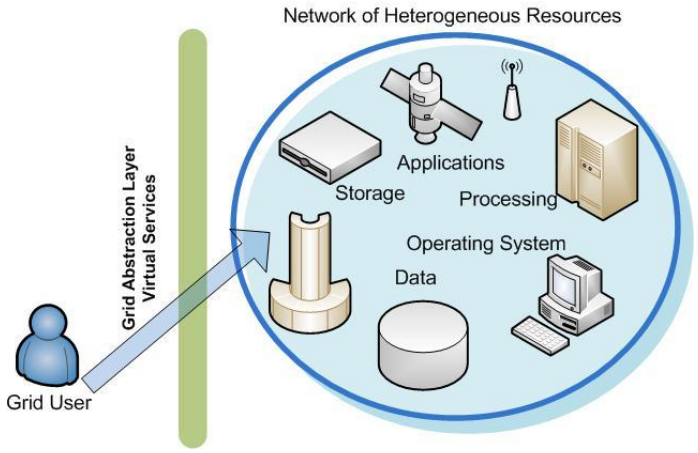

Figure 2. Grid Computing (Distributed computing over a network of heterogeneous resources using open standard)

Although there are many important aspects of grid computing but the biggest barrier against the widespread adoption of grid computing is security. According to [14], there are a number of different security issues in grid computing, like data protection, job starvation, denial of service, policy mapping, and information security. Confidentiality, integrity and authentication are the key concerns in information security. These issues are normally tackled by applying the PKI (Public Key Infrastructure).

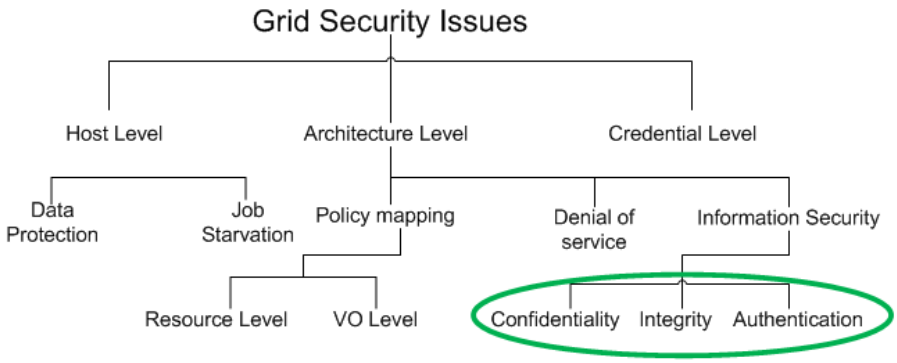

Figure 3. Classification of Grid Computing Security Issues

There are certain issues pertaining to the PKI authentication mechanism in grid systems [15]. PKI is based upon Asymmetric Key Cryptography which does not provide unconditional security, rather it depends upon the unproven assumption of computing power, i.e. the attackers equipped with sufficient computing power, which may not be possible with the current technology, would be able to crack the cryptographic key. According to [16], key distribution techniques based on public key cryptography only provide computational security. Finding efficient algorithms to compute the inverse of one-way-functions has not been proven impossible and emerging powerful computers might pose real threats to their security.

3. Quantum Network Infrastructure Framework for Grid Computing

We propose to integrate the QKD technology with PKI to achieve unconditional security in distributed computing. A conceptual model of quantum network infrastructure framework for grid computing is presented, taking the SECOQC QKD network as a model. This framework is based upon the concepts of integrating QKD network and protocol with the classical network and protocols.

We propose to create a virtual organization (VO) among the users connected with the QKD network, i.e. a grid computing environment secured by QKD technology, see Figure 4.

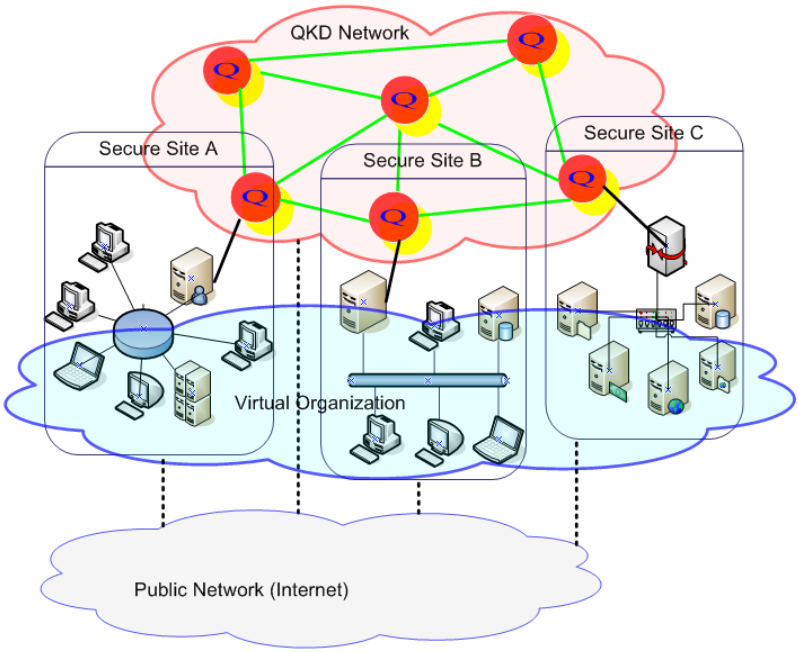

Figure 4. Conceptual Model of Grid Computing based on QKD Network

There are following main features in the proposed scheme.

- All the grid communities participating in this scheme are connected with the QKD network as well as with the public network, i.e. the Internet.
- It is assumed that all the users connected to the quantum network nodes are present in one of the secure sites, as shown in the Figure 4.
- The QKD network provides a key management and user authentication system with unconditional security based on QKD technology; hence replacing the vulnerabilities of PKI authentication mechanism against classical as well as quantum computer attack.
- The basic secure communication link between the two parties is possible via the SECOQC QKD network functionality. As explained in detail in [2], no upper layer application requires extra modification in order to exploit the unconditionally secure key material.
- In addition to the quantum key distribution capability all the QKD nodes are capable of acting like a Certificate Authority (CA), same as traditional PKI system.

- Since the vision of grid is global, the proposed model is designed keeping in view the fact that the grid system secured by QKD network can be a subset of the larger grid system, which is secured by the classical PKI technology.

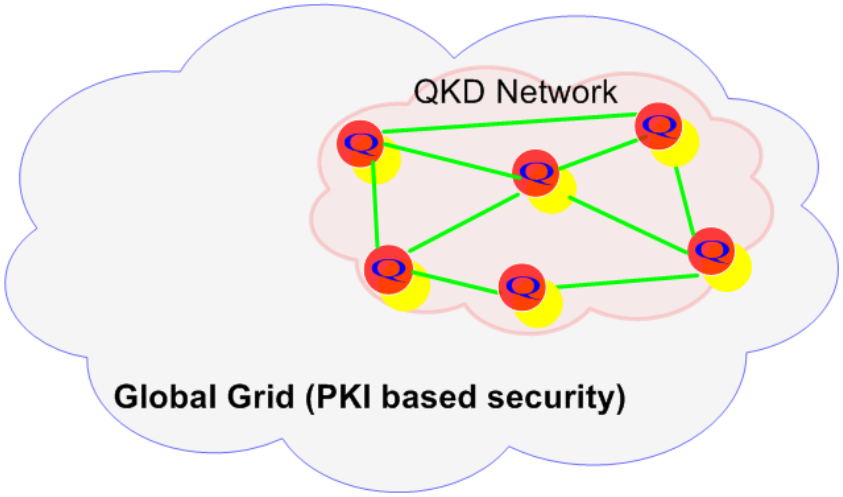

Figure 5. Status of the QKD Secured Grid Communities in the Global Grid

4. Authentication Mechanism in QKD Connected Communities

In this section we describe the simple authentication mechanism between the user and the resource, which are connected with the QKD Network, refer to Figure 6.

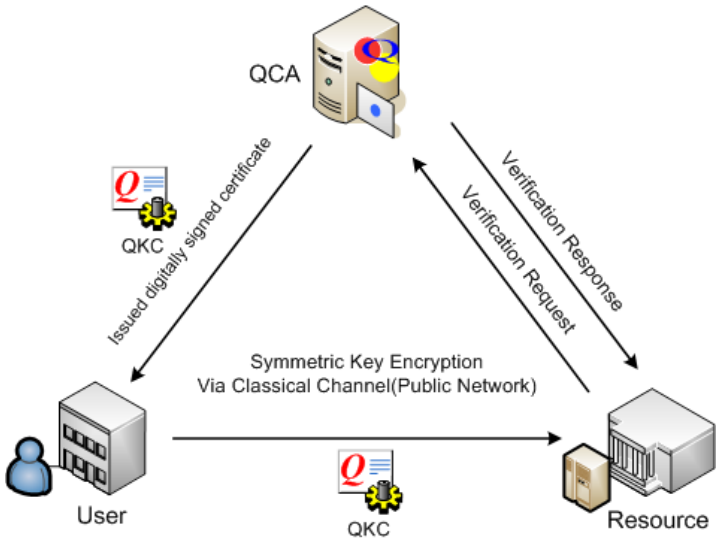

Figure 6. Authentication between User and Resource Connected with the same QKD Network

Here we introduced two new components the Quantum Certificate Authority (QCA) and the Quantum Key Certificate (QKC). Let's first explain these components in detail.

4.1. The Quantum Certificate Authority (QCA)

The status of the QCA is a trusted third party, which can issue the authentication certificates to the communicating parties registered with the Registration Authority (RA) in a Virtual Organization (VO), on request. The QCA can act as a complete traditional CA with the added functionality that it can operate on both the symmetric and asymmetric key cryptographic mechanisms. Hence, the authentication certificate issued by the QCA, the Quantum Key Certificate (QKC) in our model, is capable of providing the authentication in the QKD connected grid communities as well as in classically secure communities.

4.2. The Quantum Key Certificate (QKC)

QKC is a more protected form of a normal PKI Authentication Certificate, which contains all the fields of normal PKI certificate. Additionally, it is protected by the Hash-based Message Authentication Code (HMAC) symmetric key digital signature.

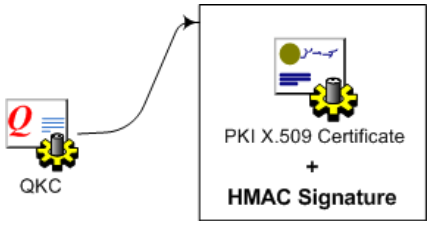

Figure 7. Quantum Key Certificate (QKC)

HMAC makes use of a strong hash algorithm (e.g., MD5, SHA1, SHA256) to create a check-word over the data and an embedded key. A receiver, who possessed the secret key, would re-generate the same check-word by performing the same hash function over the concatenated data and key. If the check-word received matches the one re-generated, then the authenticity and integrity of the received data is assured.

4.3. The Authentication Mechanism

The Quantum Certificate Authority (QCA) is a node of the QKD network with additional functionality of acting as a trusted third party certificate authority (CA). On request from the user the QCA issues a certificate QKC, explained in the previous section, to the User via QKD network. The user then encrypts the certificate using its shared secret key with the Resource and sends it to the Resource via public network. The Resource on receiving the certificate decrypts the certificate using its shared secret key with the User. The Resource then sends the check-word from the QKC to the QCA for verification.

4.4. Verification of QKC

There are three possible approaches of verifying the integrity and authenticity of the QKC.

First approach: The Resource sends the complete QKC. The QCA then calculates the check-word using the secret key of the User and matches it with the one mentioned in the QKC. On finding the exact mach the QCA sends the verification message to the Resource. In this approach the QCA must be a trusted party for the Resource.

Second approach: The Resource sends the QKC to QCA without the check-word. The Resource then calculates the check-word using the secret key of the user and sends the check-word via the QKD network. In this case the Resource doesn't completely rely on the QCA but

it can verify the QCA by getting the correct check-word. In case the Resource received the incorrect check-word it reveals that either the QKC's integrity is compromised or the QCA is compromised.

Third approach: The Resource requests the secret key of the User's QKC and calculates and verify the check-word itself.

In the first approach the Resource completely depends upon the QCA. The whole security lies in the security of the QKD Network and the pre-established trust between the QCA and the Resource. While in the second and third approach the Resource can check the integrity and authenticity of the QKC. While in case, if the calculated check-word doesn't mach it means that either the QCA or the QKC is compromised.

5. Grid Authentication Mechanism Among QKD Connected Communities

The authentication mechanism explained in the previous section can be extended to use in the Grid environment. Suppose the User and Resource connected to the QKD network are part of a virtual organization (VO). In this scenario both the User and Resource are registered with the Registration Authority (RA) of the VO. The process is explained in Figure 8.

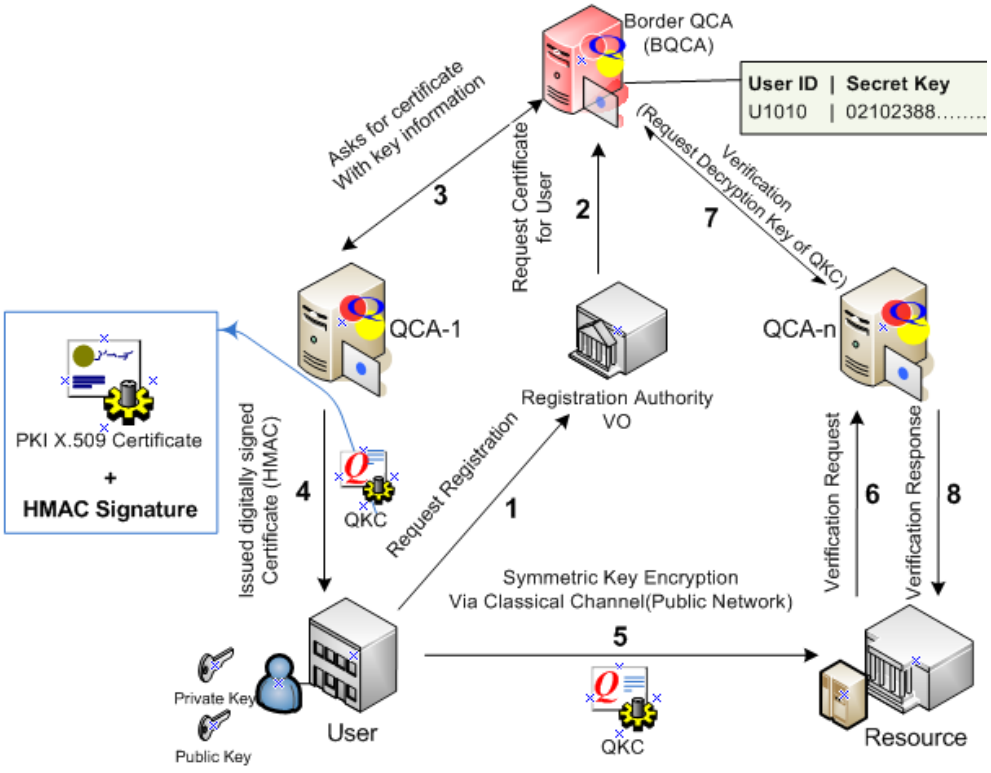

Figure 8. Authentication between User and Resource Present in the QKD Network

Let's explain the authentication mechanism when the User wants to send a request to the Resource.

Step 1: The user sends a registration request to the RA.

Step 2: After verification (depends upon the policy of VO) the RA directs the Border Quantum Certificate Authority (BQCA) to issue a QKC to the User. Refer to [2] for details of border QKD nodes.

Step 3: The BQCA generates a secret key for the User and sends a copy of that key with the User ID to its sub-QCA, in this case QCA-1, nearest to User in the QKD Network.

Step 4: QCA-1 generates a certificate similar to the PKI 8.509 certificate and digitally sign it with HMAC signature.

Step 5: QCA-1 sends the QKC to User by encrypting it with the key shared with User.

Step 6: The User, on receiving the QKC, verifies its integrity by calculating the HMAC check-word, and sends it to the Resource.

Step 7: The Resource, on receiving the QKC verifies it as explained in the previous section.

Step 8: After verification the Resource allows the User to use its services.

In the whole process of authentication we can see that our proposed solution of grid authentication with QKD provides unconditional security as compared to the other PKI based security mechanisms for grid. Hence it uses the unconditional security of QKD while stil utilizing the flexibility of PKI. No doubt that current PKI mechanisms based on conventional classical cryptography requires less overhead of small key size but it is also evident that after key distribution the symmetric key cryptography is many times faster than public key cryptography.

6. Conclusion

As a result of our proposed solution, we conclude that QKD Networks have strong applications in the high performance distributed computing. Issues of confidentiality, integrity and authentication, in grid computing, can be solved using QKD technology. Even though the vision of Grid computing is global, and QKD networks are very few and still in the testing phase, which is the biggest barrier against the wide spread exploitation of QKD technology on large scale distributed computing networks. Also the high cost of implementation of QKD Networks is also an issue for its exploitation on large-scale networks. Interoperability of QKD with other widely used security schemes like PKI and Kerberos is also possible, as a result of the proposed solution. Modern security applications should be designed keeping in view the requirements and limitations of QKD technology, so that as the QKD technology will become mature, it would be easier to exploit its unconditional security power in those applications.

Acknowledgment

The authors appreciate help and support from NED University of Engineering & Technology and DSS Group University of Leeds, UK, for this research work.

References

[1] C. Elliott, "The DARPA Quantum Network", Quantum Communications and Cryptography, **(2006)**.
[2] R. A. M. Dianati, M. Gagnaire and X. Shen, "Architecture and protocols of the future European quantum key distribution network", Security and Communication Networks, vol. 1, no. 1, **(2008)**, pp. 57 - 74.
[3] A. Poppe, M. Peev and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna", International Journal of Quantum Information, vol. 6, no. 2, **(2008)**, pp. 209-218.
[4] R. Alleaume, et. al., "SECOQC White Paper on Quantum Key Distribution and Cryptography", Arxiv preprint quant-ph/0701168, **(2007)**.
[5] M. M. Khan, et. al., "A Quantum Key Distribution Network through Single Mode Optical Fiber", Proceedings of the International Symposium on Collaborative Technologies and Systems, **(2006)**, pp. 386-391.
[6] Q. C. Le and P. Bellot, "Enhancement of AGT Telecommunication Security using Quantum Cryptography", Research, Innovation and Vision for the Future, 2006 International Conference on, (2006), pp. 7-16.
[7] H. J. Kimble, "The quantum internet", Nature, vol. 453, no. 7198, **(2008)**, pp. 1023.
[8] N. Gisin and R. Thew, "Quantum communication", Nature Photonics, vol. 1, no. 3, **(2007)**, pp. 165.
[9] T. M. T. Nguyen, M. A. Sfaxi and S. Ghernaouti-Hélie, "802.11 i Encryption Key Distribution Using Quantum Cryptography", Journal of Networks, vol. 1, no. 5, **(2006)**, pp. 9.
[10] S. Ghernaouti-Helie and M. Sfaxi, "Upgrading PPP security by quantum key distribution", NetCon 2005 conference, **(2005)**.
[11] S. Ghernaouti-Helie, et. al., "Using quantum key distribution within IPSEC to secure MAN communications", MAN 2005 conference, **(2005)**.
[12] S. Ghernaout-Helie and M. A. Sfaxi, "Applying QKD to reach unconditional security in communications".
[13] S. Rass, et. al., "Secure Message Relay over Networks with QKD-Links. Quantum, Nano and Micro Technologies", 2008 Second International Conference on, (2008), pp. 10-15.
[14] A. Chakrabarti, A. Damodaran and S. Sengupta, "Grid computing security: A taxonomy", IEEE Security & Privacy, vol. 6, no. 1, **(2008)**, pp. 44-51.
[15] S. A. Zhao, A. Kent, D. Robert, "PKI-Based Authentication Mechanisms in Grid Systems", Networking, Architecture, and Storage, NAS 2007, **(2007)**, pp. 83-90.
[16] M. Dianati and R. Alleaume, "Architecture of the Secoqc Quantum Key Distribution network", Arxiv preprint quant-ph/0610202, **(2006)**.

Authors

Dr. Muhammad Mubashir Khan is Associate Professor of Computer Science and Information Technology in NED University of Engineering and Technology, Karachi, Pakistan. He got his PhD degree from School of Computing, University of Leeds, UK, in 2011. His main area of research is Information Security (more specifically Quantum Key Distribution).

Professor Jie Xu is Chair of Computer Science at the School of Computing and leads the research at Leeds on Distributed Systems and Internet Computing. He has worked in the field of dependable distributed systems and fault-tolerant computing for over eighteen years. Professor Xu has published more than 120 edited books, book chapters and academic papers in areas of computer system fault diagnosis, fault-tolerant software and dependable distributed systems.