Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 11 (2016) pp. 031-038

Quantum Cryptography: A Comprehensive Survey

Noor Ul Ain[1], Atta-ur-Rahman[2]

[1]School of Electrical Engineering and Computer Science (SEECS), NUST,
Islamabad, 44000, Pakistan
13msccsnaain@seecs.edu.pk

[2]Barani Institute of Information Technology (BIIT), PMAS-AA University,
Rawalpindi, 46000, Pakistan
atta@biit.edu.pk

***Abstract*: Quantum cryptography is one of the most prominent fields in modern world of information security. Quantum cryptography is considered to be a future replica of classical cryptography along with a vital stance to break existing classical cryptography. Quantum computers innovated by a Canadian D-wave company in collaboration with Google, NSA and Martin Lockheed seems to possess strong computational power as compared to existing machines. This shows that if successfully implemented, it is expected that in future classical cryptographic algorithms including RSA will be broken and sensitive information will become insecure. In this survey paper firstly motivations behind the innovation of quantum cryptography and existing quantum protocols for information security are described. Then the existing hardware of quantum computer are discussed. After that some active research areas in quantum physics are discussed. Finally a comparison of existing trends in quantum cryptography in terms of existing quantum products by different manufacturers is performed.**

Keywords: Quantum Cryptography, RSA, Quantum encryptors, Quantum computer, D-wave, QKD MiTM, SQUID

I. Introduction

This paper is an extended version of our recently published work [37]. Quantum cryptography is all about using quantum physics to perform cryptographic tasks as well as to break cryptographic systems [2]. In terms of performing cryptographic tasks, these systems are able to provide enhanced Quantum Key Distribution. In terms of breaking cryptographic systems, enhanced computational strengths offered by quantum systems are expected to break any complex cryptographic algorithm. Another important feature of quantum systems is quantum no-cloning theorem [2] which mitigates both active and passive eavesdropping. Moreover, the need for quantum computer is also very important because in upcoming years Moore's Law will fail, thus from then onwards Rose's Law will overtake this technology advance. Purpose of this paper is to provide the readers with up-to-date progress in the field of quantum cryptography. This is accomplished in the way that first the motivation behind this field are given in detail that why this is an emerging area in security, second a brief introduction of quantum computers is given that how the implementation is made possible, an introduction to the research group that are currently known as working in this field, is presented. Moreover quantum products, quantum standards and its applications are presented in detail.

Rest of the paper is divided in following sections: Section 2 focuses the need of Quantum Cryptography Section 3 discusses the general architecture of Quantum Computer Section 4 provides various Quantum protocols for Quantum Cryptography. Section 5 is about the active Quantum Research groups along with their research areas. Section 6 discusses generic Quantum timeline and finally section 7 provides major Quantum cryptographic products.

II. Motivations

The motivation behind preferring quantum cryptography over classical is because of the inherent features offered by quantum mechanics as compared to classical cryptography. It is often asked that what will happen when today's crypto-systems will be broken. According to [38], it is projected that Quantum computers will break the crypto-systems of the current days including RSA, DSA and ECDSA. It is therefore, a big need of the time to come up with, to design and investigate such algorithms, techniques and protocols that can resist Quantum Computers attacks for example, post-quantum public-key signature systems and post-quantum public-key encryption systems etc. Ex-

perts are investigating the state of the art in quantum cryptography like lattice based cryptography, hash based cryptography, code based cryptography and multivariable cryptographic systems.

Quantum no-cloning theorem says that it is impossible for anyone to create an exact replica of an existing quantum. This feature of quantum cryptography is a counter measure against MiTM attack. Similarly quantum measurement rule states that no one can eavesdrop the information being transmitted in the channel without being noticed [2]. Whenever someone tries to eavesdrop the qubits (unit of information in quantum systems) state of the qubits change and the attacker gets noticed by both parties and thus the communication [43] is aborted. Another reason for choosing quantum cryptography over classical cryptography is that the advanced computation power offered by quantum computers as compared to classical [14].

According to prior research, as mentioned earlier, Moore's Law will no longer be supportive and thus a new Law is required to show ongoing technology advances. This new law can only be possible if quantum systems are deployed rather than classical systems. A representation of both Moore's Law and Rose's Law is shown in fig-2. According to the research, Moore's Law will not be valid because it states that after every eighteen months chip size will be reduced and number of transistors will be doubled, which will not be valid after 2020, while the Rose's law suggests to increase the number of qubits instead of reducing chip size for continuous technology growth. This is one of the main reasons to choose quantum computer for future computing along with other reasons as described before.

III. Quantum Computer

Quantum computers are also termed as super-computers. These are the devices that are involved in complex computations and data operations in form of qubits rather than bits. Qubits are different in the sense that classical bit can be either 1 or 0 at a time but qubit can be a superposition of both at a time.

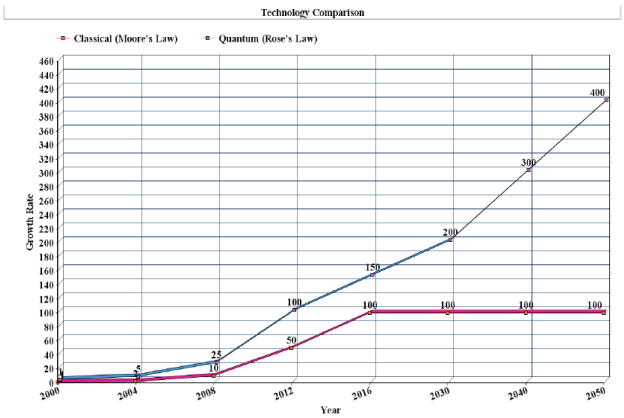

Fig. 1. Moore's Law v/s Rose Law for Technology Comparison

This feature enables qubits to store infinite amount of information and computational power as compared to classical computers. A general quantum processor architecture is shown below:

Fig-2 shows basic Quantum Strategy i.e. how quantum architecture is designed along with the subfields of quantum computation that are considered to be a necessary element of a quantum computer. Here QEC refers to Quantum Error Correction and FT refers to Fault Tolerant. Firstly Quantum theorems including Quantum measurement rule and Quantum No-cloning theorem are the main reason of Quantum Complexity along with other quantum algorithms including algorithms for QKD and Quantum Signatures [7]. The next important element is quantum programming languages that are a major part of quantum development. Another feature is Quantum hardware architecture itself, which shows the hardware elements to be used. Moreover, it also includes features to reduce errors and overcome quantum system faults. Finally Qubit Interconnect Technologies along with qubit storage and various quantum gates are most important building blocks of quantum system architecture. On basis of work done in quantum computer architecture, here is a top to bottom list to show the depth of work done in respective areas.

A survey on computational assumptions used in the crypt-analysis broken or not according to Shor's algorithm is presented by Zhu in [39]. In this research it was mentioned that quantum theorems are becoming a threat for all the existing algorithms of the day regardless of the key size used. This is majorly because, quantum enhanced parallelism, according to which the quantum theorems has a brutal capability to achieve exponential speedup factor for certain problems like error correcting codes, knapsack problem etc.

In his Master's thesis, Macro A. Barreno [40], presented the future of cryptography under Quantum Computers. He further added, that with the possible emergence of quantum computers and the kind of behaviors they exhibit like fast and growing computational speedup and convergence rate, a new paradigm shift in cryptography can easily be predicted. Quantum computers may have the capability to break the most modern encryption standards eventually. So this security seems useless against a quantum-enabled adversary. The aim of this thesis was to characterize this convergence of cryptography and quantum computation.

The Fig-3 above describes the hierarchy of quantum computer architecture to show which areas are most explored in field of quantum cryptography. As it can be seen in the figure, most of the work is done in developing quantum complexity theory to propose various quantum algorithms to be used including BB84, SARG04, E91, SDC and others. After that researchers are side by side working on designing quantum gates to be used in quantum operations including NOT, OR, Identity, Hadamard gate and others. Moreover, currently few researchers are also working on developing quantum languages to be used in quantum computers to ensure quantum software development as well. Another research area is quantum system organi-

zation in which the main researcher organizations involved are D-wave, SeQureNet, MagiQ Tech and others who design quantum hardware and develop ways to use them. The area which is least explored and is creating a lot of difficulties for successful quantum communication is to develop ways to ensure error free communication over the channel along with fault tolerance.

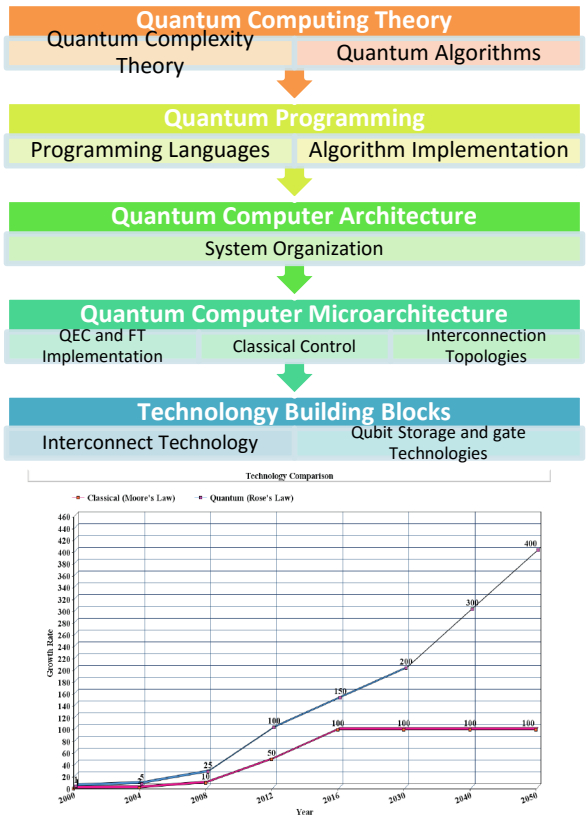

Fig. 2. Quantum Computer Architecture and Computation

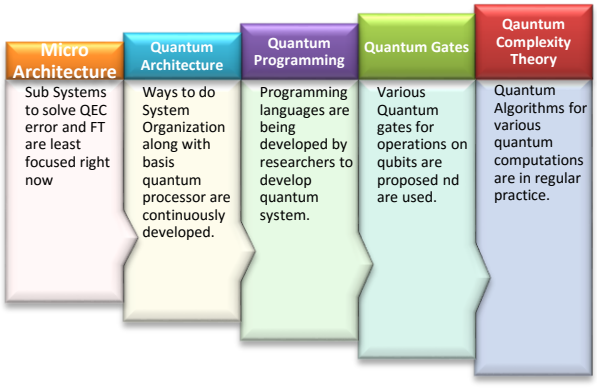

Fig. 3. Progress in Most Active to Least Active Quantum Computer Development Phases in Right to Left

According to D-wave research team, quantum processor is made of SQUID- quantum transistor [11]. This processor is named as quantum annealing and the currently available quantum computer operates on 512 qubits [11] and it is expected to be in a range 1024-2048 qubits [21] in a few years. Some of the current applications of quantum computers in field of information security are as follows:

It can break strong encryptions in the world. It is Useful for large time taking calculations. Quantum computer is a good remedy for eaves dropping phenomenon. It has the ability to factorize large prime numbers to break public key cryptography. It can search out large database in very less time as compared to classical methods to find out collisions in hashes.

Fig. 4. D-wave Quantum Computer [21]

IV. Quantum Computing in News

Currently quantum computer manufactured by D-wave in collaboration with NSA had some specific reasons as exposed by Snowden. The main reason of NSA to get this system is to do successful online surveillance program for getting information of every person in the world. Currently NSA has two active programs in this regard: Penetrating Hard Targets and Owning the Net [24].

The first program consumed $79.7 million and its objective was to sustain and enhance research operations at NSA. The objective of second program was to use quantum computers to break encryptions thus to extract worldwide sensitive information to spy popular web services online. Google and Microsoft are working on this as well and their purpose is to encrypt data as it moves along public channels, private lines and large data centers to ensure the secrecy of all sort of information. Moreover, NASA is also involved in this program and their objective is to investigate whether these systems can optimize the search for exoplanets (planets that are outside of our own solar system). Another active group named as Quantum Hacking Group in Norway is involved in finding flaws in quantum hardware and propose ways to do quantum eavesdropping to achieve absolute security for quantum systems in the future.

V. Quantum Processor

Quantum Processor by D-wave is named as Quantum Annealing Processor. It is made of SQUID quantum transistor. It is designed by joint work of D-wave and NSA. Currently 512 qubits are used in available quantum processor. In 2015, 1024-2048 qubit quantum core processor

is expected. Some of the issues in quantum Processor are still there including Quantum noise during transmission and improper control implementation during transmission.

VI. Quantum Protocols

Some of the major protocols used in field of quantum cryptography to provide Quantum Key Distribution are discussed in a tabular form. The comparison is done on basis of Tolerable Quantum Bit Error Rate and Qubits Depolarization Rate [6]. Moreover relationship between these two elements is also shown for each of them. The protocol to be chosen depends on the requirements of the user. Generally the protocol with maximum tolerable QBER and QDPR is preferred.

TABLE-1
Comparison of Quantum Protocols in terms of QBER and DPR [6]

Protocol	Tolerable QBER(e_b)	Tolerable DPR(p)	Relation
BB84	0.1100	0.1650	$e_b=2p/3$
Six State	0.1261	0.1891	$e_b=2p/3$
SARG04	0.09689	0.08046	$e_b=4p/(3+4p)$
Sym. 3 State	0.09812	0.1161	$e_b=8p/(9+4p)$
Asym. 3 state	0.04356	0.06534	$e_b=2p/3$

Here e_b is tolerable QBER which refers to acceptable Quantum bit error rate during transmission over a channel and prefers to tolerable DPR i.e: acceptable quantum depolarization rate over a noisy quantum channel.

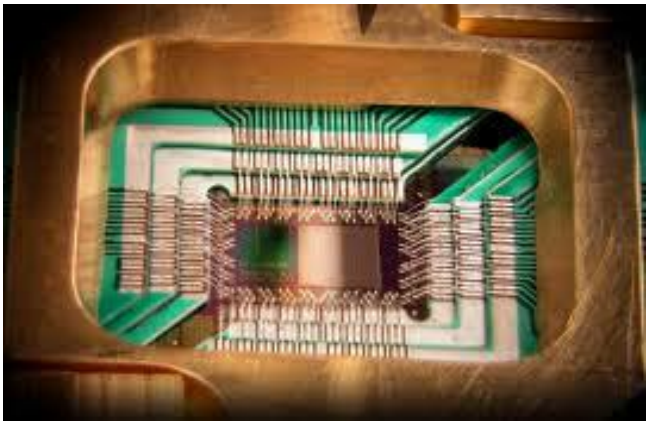

Fig. 5. D-wave Quantum Annealing Processor [23]

Fig-6 shows comparison between some Quantum Key Distribution protocols[42] including six state QKD protocol, BB84 Key distribution protocol, SARG04, Symmetric three-State protocol and asymmetric three-state QKD protocol. These protocols are compared in terms of their key generation rate along with their distance transmission capability. According to the graph six-state QKD protocol is best in terms of its key generation rate along with large distance transmission.

VII. Quantum Research Groups

Following are some of the major research groups along with the researchers and research areas in the field of quantum computing:

1) The McGill University

The research group at McGill University is doing research work in field of Quantum computing, Quantum Information and quantum mechanics, Quantum cryptography, Algorithms, Complexity Theory.

2) The University of Michigan

The research work in University of Michigan is related to Quantum Computer Architecture and Quantum Design Automation, Simulation of Quantum Circuits on Classical Computers, Synthesis of Quantum and Classical Reversible Circuits, Modelling of Faults and Errors in Quantum Circuits, Circuit Equivalence Checking (Formal Verification). The research is done in collaboration with Columbia University, NIST and MIT.

3) The University Of WaterLoo

The quantum research group in University of WaterLoo is doing projects in domain of Quantum Computing, Communications in Quantum, Quantum Sensing. The research work is done in collaboration with Institute for Quantum Computing, QCSYS, USEQIP.

4) Quantum Hacking Group Norway

The main interest of Quantum hacking group Norway is to identify flaws in Quantum Hardware, to identify Quantum Systems imperfections, eavesdropping, absolute security. University of WaterLoo Canada and IdQuantique are supporting Quantum Hacking Group in the research.

5) Quantum Communication Victoria

The research group in Quantum Communication Victoria is doing research activities in Quantum Computation, Quantum Technology, Quantum Communication Devices, Photon source. Research activities in QCV are funded by The University of Melbourne, MagiQ Technologies Inc., Qucor Pty Ltd, Silicon Graphics Inc.

6) SEECS, NUST

Currently, School of Electrical Engineering and Computer Science (SEECS) at National University of Sceince and Technology (NUST), Pakistan is working in the field of quantum non-locality and quantum cryptography. It includes the ways to develop a secure algorithm which addresses a comparatively new and wide field of quantum secret sharing via entanglement and teleportation mechanism.

Moreover, another research area that has been focused in NUST is “Quantum Secure Positioning”. This system works to validate the users who are the part of secret communication and are actually present on the particular location that is been claimed by them.

VIII. Quantum Standards

Some of the Standards in terms of Quantum Key distribution along with their particular implementation are described here in form of a table.

1) GS QKD 002 [35]:
This Standard is for different use cases including offsite backup, management, critical infrastructure, Metropolitan Area Network, backbone protection, High Security Access Network and Long Haul Service.

2) GS QKD 003 [31]:
This standard defines various standard components and internal interfaces to be used in quantum systems including photo detectors, QKD sources and system components.

3) GS QKD 004 [34]:
This standard defines standard Application Interface specifications and descriptions to be used in quantum systems.

4) GS QKD 005 [32]:
This standard is specific for security related matters including framework for security statements in QKD implementation devices. It also defines classical protocols to be used in quantum systems including error correction methods, reconciliation and privacy amplification.

5) GS QKD 008 [33]:
This standard is specific to QKD module security including self-test, Sensitive Security Parameters Management, Software and operational Level security.

TABLE-2 Quantum Standards

SR.	STANDARD	STANDARD TITLE
1	GS QKD 002	Quantum Key Distribution: Use Cases
2	GS QKD 003	Quantum Key Distribution: Components and Internal Interfaces
3	GS QKD 004	Quantum Key Distribution: Application Interface
4	GS QKD 005	Quantum Key Distribution: Security Proofs
5	GS QKD 008	Quantum Key Distribution: QKD Module and Security Specifications

IX. Quantum Products

A wide range of quantum products is available in the market including Quantum Encryptors, Optical Quantum Sources, Quantum Random Number Generators, Quantum Computers, Disk Backups and many others. As the theme of this article is to conduct a survey on quantum trends in field of information security, so the focus here will be on the products specific for information security domain. Thus various discrete and continuous quantum key distribution devices are compared here on the basis of:

a) QKD form (Continuous/ Discrete)
b) Prominent Features
c) Key Strength in terms of Key Refresh Rate
d) Particular QKD role in Networks
e) Authentication mechanism used
f) Supporting Hardware
g) Underlying QKD and Classical Crypto Algorithms

The important things to note here are that the latest form of QKD in the market is CVQKD manufactured by SeQureNet in 2013.The difference between Discrete and continuous Variable QKD is that in case of DQKD individual photons are sent whereas in case of CVQKD photon beams are sent with various available variations of photon beams. Another important term here is *Key Refresh Rate.* This term refers to the capability of a device to refresh its key per second time unit. Another element in this comparison is authentication. Authentication mechanism is still classical and this is the main reason of failures in quantum mechanisms. Researchers are aiming to generate successful foolproof authentication mechanisms in quantum systems to overcome this flaw. Various ways to overcome this issue are being proposed including quantum digital signatures. Quantum products are being used on industrial scale in various forms including server, point to point and security gateways. Below is a comparison among some popular Quantum Key Distribution devices. Remember that all these devices are hybrid of classical and Quantum Cryptographic ways. A table for this comparison is also given in the end.

Cerberis [36]**:** Cerberis is manufactured by IDQuantique. It works as DQKD with a key refresh rate of 1key/min for 12 devices connected. In the network it plays the role of server and uses BB84, SARG, RSA and AES. Authentication is performed via access control methods. The transmission capability of this device is successful upto 100 km after which Depolarization and noise are introduced.

Clavis^2 [8]**:** Clavis^2 is manufactured by IDQuantique. It works as DQKD with a key refresh rate of 1000 bits/sec. in the network it plays role of connector that connects two stations and controls them via some external computer. It uses BB84, SARG04 for key generation and uses universal hashing mechanism with OTP for authentication. The transmission capability of this device is successful up-to 50 km.

Q-Box [12]**:** Q-Box is manufactured by MagiQ Technologies. It uses DQKD with a key refresh rate of 1000 bits/sec. moreover for key generation it uses combination of BB84 and DH. Authentication in Q-box is performed through DSS authentication. The transmission capability of Q-box is maximum 50 km. it is used for peer to peer key sharing.

QPN [13]**:** QPN is manufactured by MagiQ Technologies. It works as DQKD with a key refresh rate of 100 256 bit keys/sec. in network it plays the role of Gateway and performs error free communication up-to 140km. the protocols used for key generation and distribution are BB84, AES, 3-DES along with IPSec for security. Moreover authentication is performed via DSS authentication mechanism.

QKD GHz System [27]**:** This device is manufactured by Toshiba. It also works as QKD with a key refresh rate of 1Mbits/sec. in the networks it performs P2P key distribution. The protocols used for QKD in this case are SDC and AES with OTP. The transmission capability of this device is at least 100km. Authentication is performed using Decoy Pulses.

Cygnus [1]**:** Cygnus is manufactured by SeQureNet and is the most advanced CVQKD available in Quantum market. The key refresh rate for this device is 10K bits/sec on 20km 100 bits/sec on 80km. In the networks it offers peer to peer key generation mechanisms. The protocols used for QKD are E91, AES with OTP, DH, SHA-1 and RSA. Transmission capability of Cygnus is maximum 80km. authentication is performed via HMAC and Digital Signatures [9].

EPR SYS405 [15]**:** EPR SYS405 is manufactured by AIT. It uses DQKD mechanism for key generation and distribution. In the networks it is part of backbone. Key refresh rate of EPR SYS4005 is 2K bits keys/sec on 5km. It uses BB84, SARG04 and DH for key generation. Authentication is performed using digital signatures. Transmission capability of this device is less than 5km.

On the basis of QKD[41] variations Cygnus with CVQKD is considered to be the best. But on basis of key refresh rate QKD GHz System by Toshiba with a capability of 1M bits/sec seems to be best. Similarly on basis of error free transmission QPN with 140km is considered to be best. On basis of authentication mechanism used, QKD GHz System by Toshiba looks best because it deploys decoy pulses for authentication. On basis of variety of protocols for selection, Cerberis by IDQuantique is best with greater variations. Most advanced system overall in the market is Cygnus manufactured by SeQureNet.

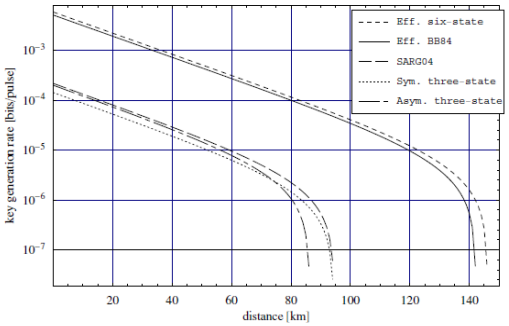

Fig. 6. Comparison between the various QKD protocols using the decoy-state method in a realistic situation where a coherent source and imperfect detectors are used. [6]

X. Quantum Applications

Some of the popular quantum applications include Quantum cryptography along with Quantum key distribution, Quantum based secure position verification, Quantum secret sharing, Quantum hash functions, Quantum digital signatures and Quantum languages. Quantum digital signatures are yet to be unleashed and quantum languages are still immature and a lot of work is needed to be done in order to develop an efficient quantum computer.

XI. Conclusions

Quantum Computer and quantum based devices seem to be innovation in field of Information security. It is expected that quantum computers will be the most powerful computers and will be able to solve any complex computational problem. This poses a serious threat to classical cryptography. Various quantum products are available in the market with variety of features depending on user requirement.

Researchers are aiming to get a quantum computer with their own reasons. As revealed by Edward Snowden, NSA [24] is working to decrypt the communication, for which it has started some projects as well. At the same time Google and Microsoft [30] are trying to get a quantum computer to provide security to their users by encrypting all the communication when it travels through public channels to achieve secrecy of an individual. Similarly NASA wants to get a quantum computer to enhance its research to exo-planets.

Overall at this time, things are still in hand as quantum computer is not completely active, but the issue needs to be addressed properly. Moreover, another group named as Quantum Hacking Group in Norway is also working on quantum hardware to find flaws in them and propose ways to achieve eavesdropping with aim to get absolute security via quantum systems.

XII. References

1. *Quantum key distribution.* Wikipedia, 2014.
2. *A closer look-512 qubit processor gallery.* Physicsandcake. Vesuvius,2011.
3. Anthony, S. *The NSA is building a quantum computer to crack almost every kind of encryption.* USA: NSA, 2014.
4. Bunky, P. I. *Architectural considerations in the design of a superconducting quantum annealing processor.* Canada: arXiv. pp. 4-5, 2014.
5. Clavis, R. P. *The Most Versatile Quantum Key Distribution Research Platform.* Geneva Switzerland, 2010.
6. *Cygnus X3 Hardware Security Module (XHSM) Security Policy.* Mailing Solutions Management Engineering, 2012.
7. *CygnusState-of-the-art Continuous-Variable Quantum Key Distribution Module.* Paris: SeQureNet SARL,Bat B, 12 villa de la croix Nivert, 75015 pp 1-4, 2013.
8. D.Dodan.. *Updating Quantum Cryptography.* USA: Masahide Sasaki (NICT), 2009.
9. D-WAVE. *The Quantum Computing Company.* Burnaby, 2014.
10. *Emerging Trends in Quantum Computing.* European commission, 2014.
11. Fung, C.-H. F. A survey on quantum cryptographic protocols. *IEEE proceedings on Quantum Computer* . pp 5-7, 2007.
12. Grossman, L. The quantum quest for a revolutionary computer.pp 3-6, 2014.
13. *Introduction to the D-wave quantum hardware.* D-wave The quantum computing company, 2014.
14. Jackson,]. J. *IBM questions the performance of D-Wave's quantum computer, 2014.*
15. Jacques, P. J.. *Experimental Demonstration of Continous Varible Quantum Key Distribution over 80 km of Standard Telecom Fiber.* Paris: SeQureNet. pp 2-5, 2012.

16. Kurtciefer, C. Quantum Cryptography A Step towards global key distribution. *Nature, Vol. 419*, 2012.
17. Meter, R. V. *A Blueprint for Building a Quantum Computer.* Communications of the Acm . pp 84-93, 2013.
18. METZ, C. *Google can repel the attack of NSA quantum computer.* USA: NSA, 2014.
19. *Network Encryption-Photon counting-Randomness.* IDQ from Vision to Technology, 2014.
20. QKD. *Components and Internal Interfaces.* ETSI GS QKD 003 V1.1.1. pp 7-11, 2011.
21. QPN, M. *Uncompromising VPN Security Gateway.* New York: MagiQ Technologies. pp 1-4, 2007.
22. *Quantum Computer System.* Inc., 2014.
23. *Quantum Key Distribution Application Interface.* ETSI GS QKD 004 V1.1.1 Industry Specification Group.pp 6-11, 2012.
24. *Quantum Key Distribution Security Proofs.* ETSI GS QKD 005 V1.1.1 Industry Specification Group.pp 6-11, 2012.
25. *Quantum Key Distribution (QKD):QKD Module Security Specification.* , ETSI GS QKD 008 V1.1.1 Industry Specification Group. pp 7-21, 2012.
26. *Quantum Key Distribution Use Cases.* ETSI GS QKD 002 V1.1.1 Industry Specification Group .pp 4-7, 2012.
27. R. Renner. (n.d.).SeQre. *Progress in Quantum Cryptography.* Poland: 5th Symposium of Laboratory of Physical Foundation of Information Processing, 2014.
28. Shin. " How Quantum is the D-Wave machine., 2014.
29. Silverman, J.. *What will quantum computers be used in the future*, 2011.
30. T.Lanting. *Entanglement in a Quantum annealing processor.* Canada: arXiv. pp 1-3, 2014.
31. Technology, A. I. *Quantum Key Distribution Recent developments and state of the art.* Antipolis, France: ETSI Security Workshop. pp 7-20, 2012.
32. *The best of classical and quantum worldsCerberis",Layer 2 Link Encryption.* Switzerland: IDQuantique, 2012.
33. *Toshiba delivers ' Unconditionally Secure' network encryption technology*, 2007.
34. Vinci, W. *Distinguishing Classical and Quantum Models for the D-Wave Device.* UK: arXiv. pp 2-6, 2014.
35. Workbench, Q.-B. *Uncompromising QKD Research.* New York: MagiQ Technologies, 2003.
36. *World's Largest Quantum Computation Uses 48 Qubits.* New York: MIT Technology Review, 2014.
37. *Quantum Cryptography Trends*: A Milestone in Information Security, Hybrid Intelligent Systems (HIS'15), Springer, 2015.
38. Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen (editors). *Post-quantum cryptography*. Springer, Berlin,. ISBN 978-3-540-88701-0. pp 1-30, 2009.
39. Hong Zhu. "*Survey of computational assumptions used in cryptography broken or not by Shor's algorithm*." Master's thesis. pp 13-20, 2001.
40. Marco A. Barreno. "*The future of cryptography under quantum computers*." Senior thesis, 2002.
41. Hoi-Kwong Lo, Marcos Curty and Kiyoshi Tamaki. "*Secure Quantum Key Distribution*." Nature Photonics 8.8: 595-604, 2015.
42. Matthew Campagna, Lidong Chen et al. *"Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges".* Mark Pecen, Approach Infinity, Inc. pp 8-26, 2015.
43. Chunnilall, Christopher J. *"Metrology for quantum communications."* Lasers and Electro-Optics (CLEO), 2015 Conference on. IEEE. pp 1-2, 2015.

Author Biographies

Noor Ul Ain is currently doing Masters in Information Security from SEECS- NUST, Islamabad Pakistan. Her main area of research is Quantum Secret Sharing. Noor-ul-ain has the BS Electronics Engineering from University of Engineering and Technology Taxila.

Dr. Atta-ur-Rahman is currently working at Barani Institute of Information Technology (BIIT), Rawalpindi, Pakistan, as Associate Professor & Deputy Director (R&D). He has completed his BS degree in Computer Science from University of The Punjab, Lahore, Pakistan; MS degree in Electronic Engineering from International Islamic University, Islamabad, Pakistan and PhD degree in Electronic Engineering from ISRA University, Islamabad Campus, Islamabad, Pakistan in years 2004, 2008 and 2012, respectively. His research interests include information and coding theory, wireless/digital communication, digital signal processing, data security, soft/evolutionary computing and hybrid intelligent systems.

TABLE-3 Quantum Products Comparison

Product	Manufac-turer	Type	Features	Key Strength in terms of Refresh Rate	Category	Authentication	Supporting Hardware	Protocols used
Cerberis	IDQuantique	QKD	Secure P-P backbone Latency(<15us) Highly secure, scalable, versatile 10Gbps bandwidth Dual key agreement Upto 100km transmission	1 key/min for 12 encryptors	Server	Role based identification for access control	Centauris Encryptors Fiber Channel (FC-1G, FC-2G, FC-4G) Quantis Quantum Random number generator	BB84, SARG, RSA (Dual Key) AES-256, CFB(1Gbps), CTR(10Gbps) Encryption Algorithms
Clavis[2]	IDQuantique	QKD	Key reconciliation Privacy amplification Up to 50km transmission	1000bits/sec	External Connector	Universal hashing with one time pad	Quantis, Centauris, Cerberis	BB84, SARG04
Q-Box[12]	MagiQ Tech	QKD	Symmetric Key Distribution P-P single photon based Upto 50km transmission	1000 bits/sec	Peer to Peer	DSS Authenti-cation	True random number generator	BB84, Diffie Helmen,
QPN	MagiQ Tech	QKD	Compatible with DWDM Latency(<10us) Remote monitoring Integrated with PKI In-transit data security Access to SAN Upto 140 km transmission	100 256bit keys/sec	Gateway	DSS Authenti-cation	Quantum and Classical Channels Upto 1G tunnel	BB84, 3DES, AES, IPSec
QKD GHz Sys-tem[27]	Toshiba	QKD	Key management and distribu-tion Side channel attacks counter-measures >100km transmission	1M bits keys/sec on 50km	Point to point	Decoy Pulses	Random Number Genera-tor	SDC, AES with OTP
Cyg-nus[1]	SeQureNet[1]	CVQK D[1]	LDPC based error correction Low SNR WDM compatible Upto 80km transmission Privacy Amplification[1,9]	10K bits keys/sec on 20km 100 bits keys/sec on 80km[1]	Peer to peer	256 bit HMAC based authenti-cation Digital Signa-tures (ECDSA)[9]	Continuous RNG, IdQuan-tique Quantum RNG[1,10]	E91,AES with OTP, DH, SHA-1, RSA[10]
EPR SYS-405 Sys-tem[15]	AIT	QKD	Error correction Side Channel controls WDM integration Privacy amplification >5km transmission	2K bits keys/sec on 5km	Backbone networks	Digital Signa-tures based authentication	BBO,Pump laser diode, Free Space optical tele-scopes.	BB84, SARG04, Diffie Helmen