Future of Data Security with the Emergence of Quantum Paradigm

Muhammad Anwaar Saeed†, K. Ahmed††

†Department of Computer Science, NCBA&E Lahore, Pakistan&Faculty Member, Virtual University of Pakistan
††Department of Computer Science, NCBA&E Lahore, Pakistan

Summary
In the emerging era of communication and data processing, security is becoming the prime concern, though since the invention of computation machines / computers, scientists are proposing / improving various mechanisms and theories to address this specific concern. Most of the methods used to secure data are categorized as cryptographic methods; which are normally derived from a mathematical concept and dependent upon the hardness of the mathematical problem. In computation, mathematical problems are linked to the processing capability of the machine, therefore, as the processing capability is enhancing, various known and trusted cryptographic methodologies has been compromised. Quantum computing is one of the strong contenders which is providing processing power and logic to break the conventional cryptographic methods. This paper is focused on providing the review of existing methodologies and way forward for further exploration.

Key words:
Quantum Cryptography, QKD, ECC, NTRU, BB84, BB92

1. Introduction

Humans have the nature to share information with others which is considered to be secure for sharing. Even this sharing varies during the interactions with different people. While communicating within a clan/group of people, they have developed mechanisms of secure communication to hide their secrets like Scytale by Spartans around 400 BC, Caesar's substitution method etc. At the same time opponents have tried to uncover the secret by adopting different methods. These deciphering attempts have compelled the researchers to develop more sophisticated mechanisms for security like poly alphabetic ciphers which remain unbreakable for almost two centuries. One time pads are used to make data more secure and unbreakable. With the invention of modern communication systems, a new public key method was introduced. These methods require a secure mechanism for sharing respective keys among parties which is considered to be an important part of public key ciphers. RSA, ECC, Diffie-Hellman are some of the examples. Most of the current mechanisms depend on the computational hardness of the problem like RSA based on factoring etc. Now these systems are considered to be compromised with the emergence of quantum computing era as explained by Shor's method. Scientists are now trying to devise mechanisms for quantum computing environment by using the quantum properties like entanglement etc. [1]. Quantum mechanics introduces the research community towards a new and multifold dimension of quantum cryptography that is based on no-cloning theorem i.e. a qubit can neither be cloned nor enhanced without unsettling its existing state, this stance makes the distribution key reiable. Bell inequality test exposes the quantum connection between qubit states to provide the entanglement and super-poisitioning characteristics of qubits which has changed the whole scenario of security and encryption regiem.

2. Discussion

Quantum cryptography is the Wiesner's idea which became a focused area of many scientists who are conducting research in this paradighm. BB84 is the first unconditionally secure quantum ker distribution protocol introduced in 1984. A major milestone of this field is the cracking of RSA's factoring problem by Shor in 1994. Communication over a larger distance is an issue in quantum computing till the development of a functional quantum repeater [2]. Zurek suggested that classical systems benefit from the quantum coherence's natural loss, which result into de-coherence and it is important for quantum to classical transition [3].
In 2004, Gene Itkis highlighted the key exposure issue and proposed the solution to detect such exposure or security key tempering, interestingly this tamper detection required no input except the two key signatures, has no dependence on hardware or infrastructure [4].
It is not an easy task to construct quality quantum codes. The quantum error correcting code finding task is converted into the task of calculating the additive self orthogonal codes. [5] Shamir's idea is used to develop a three pass quantum protocol considering the no-cloning properties of quantum mechanics [6]. Either prepare & measure or entanglement is used to develop Quantum Key Distribution (QKD) protocols and provide the basis for their category. PNS attack is possible on BB84 without any detection. Whereas its proposed solution i.e. B92

Manuscript received August 5, 2017
Manuscript revised September 20, 2017

protocol is vulnerable to intercept resend attack. A combination of these two protocols is proposed by Huttner et al. Burb has proposed a generalized BB84 for six states which is more secure. PNS attack is overcome through SARG04 by Sacarani et al. and decoy state protocol. Concept of entanglement is first time used by Ekert [7]. While distributing keys in classical environment, interception is evident and this defficiency can only be filled by QKD e.g. BB84, Ekert etc. Due to the limitations of existing photon emitters, beam splitter attack is considred to exist [8]. Security is dependent on physical properties instead of computational complexities in quantum cryptography. Scheme proposed by Tittel et al. is capable of detecting an opponent activity. A non-zero value of quantum bit error ratio is always observed in all QKD schemes even if there is no attack [9].

In 2004, Scarani et al., has provided evidence in favor of quantum computation proving that quantum key distribution is more secure and efficient way in cryptography condition to the transforming of classical bits into sets of on-orthogonal qubits state, as QKD is a non-cloning theorem therefore it is not possible to make duplicates of signals [10]. Yang has introduced QSDC (Quantum Secure Direct Communication) protocol in 2011, these are two fault tolerant protocols made from four-qubit decoherence free states with two logical qubits. These protocols haved proved respective resistence against collective-sephasing noise and collective-rotation noise, in comparison to other protocols yang et al has provided higher performance of qubits efficiency and also showed conformity to Deng-Long criteria that demands the unconditional security [11].

In 2012 Liu et al., came up with another interesting quantum secure director communication protocol based on single photon in both polarization and spatial-mode degree of freedom. The salient feature of this protocol is related to the high channel capacity because each photon carry 02 bits which is twice in comparison to others. Similarly, hyper dense coding aspect made it easy to manage the single-photon quantum state in polarization and spatial mode degree of freedom [12].

Quantum Key Distribution (QKD), Quantum Secure Direct Communication (QSDC), Quantum Secret Sharing (QSS) are examples of tangible achievements in the domain of quantum and specifically security that resulted into opening many new debates and research dimensions to be explored by scientists. Yang et al., has provided two authenticated quantum direct communication (AQDC) protocols using bell states which are used during transmission to ensure the sender and receiver based correlation of bell states [13].

In cryptosystems, major focus is given to encryption key and the mechanism of making and distribution of these keys, conventional as well as quantum cryptosystems show multiple commendable exploration and results with this reference. The origin of public key cryptography is mathematics, and since inception it has been dominated by two important segments i.e. integer factorization like Rabin-Williams and RSA and discrete logarithm like Diffie-Hellman, DSA, ECC, El Gamal. In the same reference, such encryptions based on elliptic curve discrete logarithm have the features of small key size with moderate encryption/decryption time [14]. The performance of public key is based on size, bandwidth and computational overheads, RSA is an example which has been used in many scenarios though large key length and computational power require respective hardware/processing support for keys of 1024 or higher, another example as an alternate is NTRU that requires minimal computing power with better performance and high security [15], these comparisons lead towards highlighting parameters which are essential to be considered while evaluating public key i.e. computational cost, length, key exchange message length, length of signature and key lifetime [16].

Adaptive Cryptographic Engine (ACE) has been proposed by Dandalis et al. in 2004 for IPSec architecture to improve performance and flexibility for encryption, it is important to highlight that results showed better key-setup latency and throughput as compare to software solutions [17]. In same year Huang experimented the hash-chain based group key schema which worked well for systems with moderate group size and stable population. From performance perspective it was observed that group key scheme showed minimal overheads with reasonable security level [18]. Another development from keys / schema development reference is in 2008, Cheon proposed an identity based encryption using timed-released public key encryption based on bilinear mapping [19].

In parallel to conventional cryptosystem development and progress, quantum related concerns were also addressed by researchers. MPQC protocol is an example, focused on soundness, completeness and privacy for variable quantum secret sharing. At conventional front, a verifiable secret sharing is a two phased protocol with one node as dealer, which shares the secret among players, in response the players reconstruct the secret publicly, while in quantum, a dealer node share its state, as quantum states cannot be cloned therefore, the reconstruction is not required, instead it is dealt by another entangled designated player. [20]

With emerging technology, challenges for quantum key experimentation are getting more complex e.g. reaching high key rates over large distances, photonic transition can be done through optical fiber or even in free space. At university of Geneva, Zbinden and Gisin have conducted the experiment on optical fiber covering 67km, the results were successful with transmission of secret key at 130 bit per second. A similar experiment has been done by

Weinfurter at LMU Munich covering 23.4 km with a transmission rate of 1000 bits per second. These results shows that emerging technology is enabling us to deploy quantum key distribution protocols for security and cryptosystems [21]. In 2013, Bernien have shared the results and observation of experiment which incorporates a long distant quantum network developed by using solid state registers. Two entangled qubits have been used, result showed the existence of non-local quantum relation by various readouts in dissimilar basis on qubits. These results lead towards the development of solid state quantum networks [22].
In 2014 Chen et al., shared their observations on correlation between entangled particles and distributed nodes, they have used quantum secret sharing (QSS) to derive quantum key while for validity they have used quantum circuit to identify the equivalence of the original states and states in quantum blind signature [23]. In same year, Bhatia et al. proposed the engagement of polarized photons for quantum encryption in wireless environment. With reference to key distribution, they have used IEEE 802.11 standards along with features of quantum cryptography, results show the reduction in the adversary success ratio [24].

In 2015, Thayananthan et al. have provided a less complex way of quantum cryptography by using Grover's algorithm and related validation methods for mobile data security and privacy issues due to existing cryptographic mechanisms. The method proposed the use of quantum cryptography with two handshake based PairHand protocol for authentication of mobile user which reduces the computational cost with increased handover efficiency by using the quantum properties of visible light as medium along with PairHand protocol. [25]

In 2016, Gaborit have provided an argument on syndrome decoding problem by generating pseudo random method, they have used rank matric method in quantum computing environment with a customized pseudo random generator. They have also explained some parameters that can be used to enhance the resistance level against classical and quantum attacks [26]. Buhari et al. have also shared a simulation tool for quantum cryptography without entanglement. The tool named QuCCs, can build a link between devices and the qubit by using the mesoscopic simulation. Because of its object oriented architecture, the proposed framework can be enhanced to facilitate the entangled environment's requirement. [27]

Similar to encryption techniques, signatures have the same issue that they become insecure in quantum computing environment because of their dependency on computational hardness of problem. Thus most of existing signature techniques becomes improper to use in quantum computing. Due to quantum computational power, if we ignore the efficiency factor then P2 protocol is a suitable candidate for conversion into a quantum signature protocol. Quantum channels of low quality can be used for signature construction. Any improvement in the linear relation of signature and message length will increase the efficiency. An optimization is required to keep the quantum signature techniques inexpensive in terms of pairwise channel acquisition when participants are increased. [28] A four phased handshake technique is suggested for a QKD protocol in combination with IEEE 802.11 standard for unconditional security. [29]

3. Conclusion

From the above discussion we can say that data security is the major concern with the emergence of quantum era. Researchers are trying to develop techniques to provide the optimum security for data, keys, or signatures. From the cited work, it is clear that quantum properties like entanglement provide us the liberty to attain adversary detection features without any extra effort. Similarly, perfect photon emitters eliminate the man in middle attack. Moreover, no-cloning properties enable us to detect any malicious activity when occurred. From the cited work, it is also evident that some of the classical paradigm techniques can be transformed to quantum paradigm techniques with a minimum or no effort like NTRU and P2 protocol. Based on this we can say that it is possible to develop techniques which can be utilized in both paradigms equally and effectively.

While going through the cited work we can observe a pattern that core component of security mechanisms are vulnerable even in the classical paradigm and with the increasing computational power in classical world, then strength of security component need to be enhanced e.g. the key length of RSA etc. It is clear that data is considered a separate entity and has no consideration while defining the security measures. When it comes to the quantum paradigm, the hardest classical problem is under threat of being solved. Therefore we need to reconsider the existing practices of security applications. We can measure the hardness of a certain problem in classical environment by just considering its complexity in quantum computers. If time complexity in quantum is high then considering the existing fact it will be a very tough problem to be solved in classical environment.

The existing quantum hardware is not suitable enough to establish a complete quantum communication and data storage model altogether. Therefore, we need to use the quantum properties not only for the available quantum computers but also for the available classical infrastructure

as well. Key sharing is a concerned area in classical computing. We can use the QKD protocols using optical fiber for key sharing instead of classical ways. It will enable us to utilize the quantum features for a classical paradigm. By mingling both paradigms we can cater the existing data security issue on internet or cloud etc. As discussed above that data has no linkage with the key, therefore if key is compromised then the whole security is vanished. But if we have a certain link between data and key then at least we can detect at early stages that the system is being compromised and certain measure can be taken to cater the situation. This feature can easily be accommodated in quantum computers by using quantum properties like entanglement. And it can be implemented in classical paradigm as well by transforming the quantum procedures into classical procedures. Further research is required to develop this transformation either at hardware level or software level.

References

[1] A. Ekert, "Quantum Cryptography," in Quantum Communications and Cryptography, Taylor & Francis Group, 2006, pp. 1-15.

[2] D. Chait, "A Survey of Quantum and Classical Cryptography," http://www.sci.tamucc.edu/ccsc/E-Journal/2008/Papers/P-0006-final.pdf, Vol. 1, Apr 2008.

[3] W. H. Zurek, "Decoherence and the Transition from Quantum to Classical - Revisited," Los Alamos Science, pp. 2-25, 27 November 2002.

[4] G. Itkis, "Cryptographic Tamper Evidence," in Proceedings of the 10th ACM conference on Computer and Communication Security, Washington DC, USA, 2003.

[5] Z. Varbanov , "On Quantum Information and the Protection by Quantum Codes," in International Conference on Computer Systems and Technologies (CompSysTech'10), Sofia, Bulgaria, Jun 2010.

[6] Y. Kanamori, S.-M. Yoo and M. Al-Shurman, "A Quantum Non-key Protocol for Secure Data Communication," in 43rd ACM SE Conference, Mar 18-20, 2005,, Kennesaw, GA, USA, Mar 2005.

[7] J. Mobin and A. Khurram, "A Survey of Quantum Key Distribution Protocols," in Frontier Information Technology, FIT'09, Abbottabad, Pakistan, Dec 2009.

[8] T. Jennewein , C. Simon and G. Weih, "Quantum Cryptography with Entangled Photons," Physical Review Letters, vol. 84, no. 20, p. 4729 – 4732, 2000.

[9] W. Tittel, J. Brendel, H. Zbinden and N. Gisin, "Quantum Cryptography using Entangled Photons in Energy-Time Bell States," Physical Review Letters, Vol. 84(20), p. 4737 – 4740, May 2000.

[10] V. Scarani, A. Acin, G. Ribordy and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulses Implementations," Physical Review Letters, Vol. 92(5), pp. 7901-7904, Feb 2004.

[11] C. Yang, C. Tsai and T. Hwang, "Fault tolerant two-step quantum secure direct communication protocol against collective noises," Science China Physics, Mechanics & Astronomy, vol. 54, no. 3, pp. 496-501, March 2011.

[12] D. Liu, J.-L. Chen and W. Jiang, "High-Capacity Quantum Secure Direct Communication with Single Photons in Both Polarization and Spatial-Mode Degrees of Freedom," International Journal of Theoretical Physics, vol. 51, no. 9, pp. 2923-2929, September 2012.

[13] Y.-G. Yang, J. Tian, J. Xia and H. Zhang, "Quantum Authenticated Direct Communication Using Bell States," International Journal of Theoretical Physics, September 2012.

[14] D. M. Galindo, T. S. Takagi and J. L. Villar, "A Provably Secure Elliptic Curve Scheme with Fast Encryption," in Proceedings of Progress in Cryptology - INDOCRYPT 2004,5th International Conference on Cryptology in India, Chennai, India, 2004.

[15] C. Narasimham and P. Jayaram, "Performance Analysis of Public key Cryptographic Systems RSA and NTRU," IJCSNS International Journal of Computer Science and Network Security, vol. 7, no. 8, pp. 87-96, 2007.

[16] R. A. Perlner and D. A. Cooper, "Quantum Resistant Public Key Cryptography: A Survey," in IDtrust '09, Gaithersburg, MD, 2009.

[17] A. Dandalis and V. K. Prasanna, "An Adaptive Cryptographic Engine for Internet Protocol Security Architectures," ACM Transactions on Design Automation of Electronic Systems, vol. 9, no. 3, pp. 333-353, 2004.

[18] D. Huang and D. Mehdi, "A Key Chain-Based Keying Scheme for Many-to-Many Secure Group Communication," ACM Transaction on Information and System Security, vol. 7, no. 4, pp. 523-552, 2004.

[19] J. H. Cheon, N. Hopper, Y. Kim and I. Osipkov, "Provably Secure Timed-Release Public Key Encryption," ACM Transactions on Information and Systems Security, vol. 11, no. 2, 2008.

[20] C. Crepeau, D. Gottesman and A. Smith, "Secure Multiparty Quantum Computation," in STOC'02, May 19-21, 2002, Montreal, Quebec, Canada., Montreal, Quebec, Canada, 2002.

[21] D. Bruss, G. E. Lyi, T. Meyer, T. Riege and J. R. Rothe, "Quantum Cryptography: A Survey," ACM Computing Surveys, vol. 39, no. 2, June 2007.

[22] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress and R. Hanson, "Heralded entanglement between solid-state qubits separated by three metres," Nature, vol. 497, pp. 86-90, 2 May 2013.

[23] Y. Chen, T.-S. Lin, T.-H. Chang, C.-Y. Lu and S.-Y. Kuo, "A Novel Quantum Key in Distributed Networks," in Proceedings of the 14th IEEE International Conference on Nanotechnology, Toronto, Canada, 2014.

[24] P. Bhatia and R. Sumbaly, "Framework for wireless network security using quantum cryptography," International Journal of Computer Networks & Communications (IJCNC), vol. 6, no. 6, November 2014.

[25] V. Thayananthan and A. Albeshri, "Big data security issues based on quantum cryptography and privacy with authentication for mobile data center," Procedia Computer Science, vol. 50, pp. 149-156, 2015.

[26] P. Gaborit, A. Hauteville and J. P. Tillich, "RankSynd a PRNG Based on Rank Metric," in proceedings Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, February 24-26, Fukuoka, Japan, 2016.

[27] A. Buhari, Z. A. Zukarnain, R. Khalid and W. J. A. Z. Dato, "A Generic Simulation Framework for Non-Entangled based Experimental Quantum Cryptography and Communication: Quantum Cryptography and Communication Simulator (QuCCs)," in IOP Conference Series: Materials Science and Engineering, 2016.
[28] R. Amiri and E. Andersson, "Unconditionally Secure Quantum Signatures," Entropy, vol. 17, no. 8, pp. 5635-5659, 2015.
[29] J. Ahmed, A. K. Garg, M. Singh, S. Bansal and M. Amir, "Quantum Cryptography Implementation in Wireless," International Journal of Science and Research (IJSR), vol. 3, no. 4, pp. 129-133, April 2014.

Muhammad Anwaar Saeed is a PhD scholar of the School of computer Sciences in National College of Business administration and Economics (NCBA&E), Lahore Pakistan. He is also working in Virtual University of Pakistan as an Assistant Professor in Computer Science Department. His area of research is agent based data encryption and information security. He is also interested in Quantum Computing especially encryption mechanisms used in this field. He is the author of a monograph on framework for Self Organizing Encryption in Ubiquitous Environment, published by VDM Verlag in 2010. He has also published research papers on his area of interest. Before joining VU, he has ample experience of both software development and network management.

Khalil Ahmed is PhD from Washington University USA. He is an expert academician and passionately engaged in research. His area of research is machine consciousness, A.I. and knowledge management.