Quantum Cryptography for IoT: APerspective

Sudhir K. Routray, Mahesh K. Jha, Laxmi Sharma, Rahul Nyamangoudar, Abhishek Javali
Department of Telecommunication Engineering
CMR Institute of Technology, Bangalore, India
{sudhirkumar.r, mahesh.j, laxmi.s, rahul.n, abhishek.j}@cmrit.ac.in

Sutapa Sarkar
Department of Electronics and Communication Engineering
CMR Institute of Technology, Bangalore, India
sutapa.s@cmrit.ac.in

***Abstract*-Internet of things (IoT) is going to be an integral part of our lives in the next few years. It will be found as direct service provider in our surroundings through the connected sensor based networks. Even indirectly, it will serve us in several forms as value added services over the cellular platforms. However, it is very much vulnerable from several security threats. The current security level is not very strong for the future applications of IoT. There is a need of a robust crypto-system for IoT. In this article, we propose quantum cryptography as a security solution for IoT in the long term. We explain the motivation behind this idea and the potential applications in IoT in the near future.**

Keywords—Internet of things; security for IoT; cryptography for IoT; quantum cryptography; quantum cryptography for IoT

I. INTRODUCTION

Internet of Things (IoT) is an emerging technology which can disrupt the current trends in ICT. Its financial potentials are also huge [1]. It has been proposed as an integral part of connected living. Thus in the next decade, IoT will have ubiquitous presence in the inhabited areas [2]. As it is going to be an important aspect of the lives of people there are several challenges. It will deal with a large amount of sensitive data. These data need appropriate security and integrity. In the current scenarios elliptic curve cryptosystems (ECCs) are the popular choices for IoT security [3]. However, IoT is seen as a long term solution for several applications. In the next few decades the quantum computers are expected to arrive and that will certainly decode all the ECCs quite easily. Therefore, IoT does not have a proper security framework in the long run. That is the main motivation for us to propose quantum cryptography (QC) for IoT as a robust security which can sustain the threats from the quantum computers.

In [1], control and management of security in systems is achieved using QC. It depicts the security strength of QC. In [2], some of the recent advances of security framework along with its characteristics are presented. This paper provides relevant questions for the researchers in the fields of quantum optics, quantum information processing and quantum communications. In [3], the practical resource trade-offs are highlighted in the context of QC and related algorithms. In [4], entangled pairs connecting the earth and orbiting satellites are presented which gives the scope for the next generation quantum cryptographic systems at a large scale. In [5], the applications of the quantum theory are depicted for security over the Internet. It addresses the increasing number of research branches associated with QC. It also discusses the protocols which address many real scenarios such as e-commerce. In [6], some of the present experimental accomplishments, future enhancements, ideas and patents on QC are discussed. This work compares the nature of quantum data with the classical data, and highlights the fact that quantum data cannot be read without modifying it. This work also addresses the complexity involved in bringing the quantum machines into the real world. In [7], a fully secure quantum key exchange is demonstrated over a 1.9 km free-space range using the concept of QC. A long-term goal of this work is to illustrate the key exchange to a satellite orbiting at 300 to 1200 km altitude. In [8], the current advancements in China in developing Internet of Things (IoT) are highlighted. It addresses the methodologies; research and development plans for the widespread deployment of IoT. It also depicts a generalized IoT architecture with three platforms to realize the challenging architecture of IoT. In [9], present state-of-the-art of industrial IoT is systematically recapitulated. It introduces the contextual and service oriented architectures of IoT. It also addresses the vital machineries that might be used in IoT. In [10], an overview of IoT is analyzed, emphasizing the need for healthier unification among IoT facilities. Long Term Evolution (LTE) based cellular IoT solutions are emphasized in [11], giving importance to low cost, low power consumption and longer battery life. It also considers the security aspects of IoT. In [12], the impact of IoT on the forthcoming future is analyzed. It also highlights eight prominent research topics on IoT, addressing some of the key research problems.

In this article, we present the importance of a reliable security system for IoT. We show that QC is the right choice for the long term security of IoT. In the long run, the currently used techniques will fail. QC can sustain all the foreseeable security threats.

The remaining parts of this article are organized in 4 different sections. In Section 2, we present the basics of QC. In Section 3, we present the basics of IoT and the essence of security in it. In Section 4, we present QC for IoT and its deployment issues. In Section 5 we conclude the chapter with the main summarizing points of this article.

II. Quantum Cryptography

Cryptography is the science of secret communication. It is utilized to design and implement techniques of secret communication between two trusted parties in the presence of continuous effort from a third party to eavesdrop. QC is based on the fundamental and consistent principles of quantum mechanics. QC involved in 20th century, is based on quantum mechanics and on the Heisenberg Uncertainty principle and the principle of photon polarization. According to the Heisenberg's uncertainty principle, without disturbing the system, it is tough to measure the quantum state of any system. Thus, the polarization of light or a photon particle can only be measured at the particular time of measurement. This principle plays a critical role in opposing the attempts of eavesdroppers in a cryptosystem based on QC. On the other hand, the photon polarization principle describes the way light photons can be polarized or oriented in specific directions. Moreover, a photon filter with the correct polarization is able to detect only a polarized photon or else the photon will be destroyed. It is this nonstop run of photons along with the Heisenberg Uncertainty principle which make QC an enticing option for ensuring the privacy of data and defeating eavesdroppers.

TABLE 1 QUANTUM KEY DISTRIBUTION (QKD) PROTOCOLS.

QKD Protocol	Inventor/s	Scheme of cryptography
BB84 protocol	Bennett and Brassard	Polarization state of a single particle
BBM92	Bennett, Brassard, and Mermin	Polarization state of single particle
SARG04	Scarano, Acin, Ribordy, and Gisin	Polarization state of single particle
E91	Ekert	Polarization state of Entangled particles

The concept of QC was developed by Charles H. Bennet and Gilles Brassard in 1984 as part of a study between physics and information. QC does not transmit any message signal instead it is only used to produce and distribute a key. This key could be created depending on the amount of photons reaching a recipient and how they were received. Polarization of the photons can be done at various orientations, and these orientations can be used to represent bits containing ones and zeros. A user can suggest a key by sending a series of photons with random polarizations. The representation of bits through polarized photons is the foundation of QC, known as quantum key distribution.

In case if the key is intercepted, this can be detected without any consequences, since it is only a set of random bits and can be tossed out. The sender can then transmit another key. Once a key is received securely, this can be used to encrypt a message, transmitted by communication means like: telephone, e-mail.

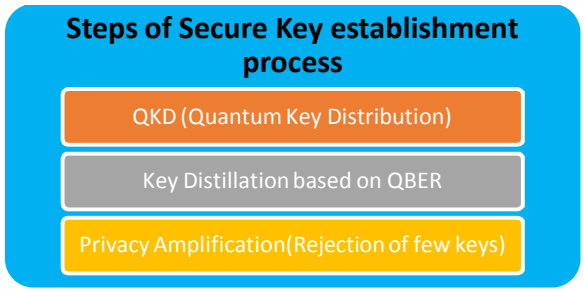

Fig. 1. Steps of secure key establishment process

In QC, a bit of quantum of information is called a 'qubit'. Here a photon is characterized using its plane of polarization, ranging from 0° to 180°. QC uses the property that if a diagonally polarized photon is passed through a linear polarizer it randomly 'chooses' either the horizontal or vertical state of polarization with a probability of 0.5. The representation of bits through polarized photons is the foundation of quantum cryptography, known as Quantum Key Distribution (QKD). In QKD the encryption key is transmitted through quantum channel to the end users. In this case, two types of channels are used: (a) Quantum channel: to transmit the secret key and (b) Public channel: used by the end users(usually in literature, Alice, the transmitter and BOB, the receiver) to verify if the transmitted key is distorted indicating eavesdropping (presence of EVE). The polarization state of a photon is used to represent the bits. A summary of the steps of secure key establishment process are presented in Fig. 1.

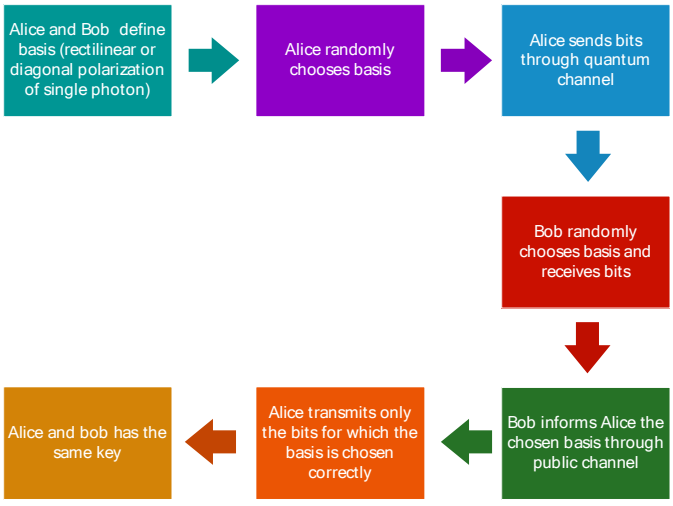

Fig. 2. Summary of the steps of QKD of BB84 protocol

QKD requires the most elaborate mechanism. There are a number of QKD protocols developed till date. Some of them involve detection of polarization state of a single photon and some of them use the entangled photons to establish the secure key communication. Among these protocols, the most popular one is the BB84 protocol, the steps of which are summarized in Fig. 2 (which is suitable for IoT security).

III. Typical Security Scenarios for IoT

IoT is quite broad and covers an overwhelming amount of information. To describe in short, IoT refers to the rapidly growing network of connected objects or devices that are able to collect and exchange data using sensors. With thriving and advancement of IoT, it finds new applications in various areas which include smart city, smart home, healthcare, smart wearable, connected car, and many more. The connected devices need to gather real-time information and communicate it to clouds to collect, store and analyze different data streams. All these processes deal with privacy and security sensitive information, for instance, health conditions of people such as ECG, blood pressure, or information related to whereabouts of the beloved ones through the use of wearables. When it comes to smart city, it can have critical data to control and monitor facilities, and also information influencing lives of people in the city. Security of this sensitive information from malicious attacks becomes an important aspect in IoT. Right now, the security fabric of IoT is problematic because of the lack of proper insight which is of minimal capacity, openness of the systems and physical accessibility. Apart from this, most devices communicate wirelessly and hence the IoT applications have to operate perfectly in the presence of security attacks. To deal with this security attacks there should be a provision in a system which can detect and diagnose the attack, and deploy countermeasures and repairs. Since the devices involved in IoT are of low capacity, the operations need to be performed in light weight manner to deal with such attacks. Considering present day mainframe security solutions which require heavyweight computations and large memory, it is a challenge to find solutions to this light weight security for IoT which leads to an open research issue. The future will see IoT security accelerating at an unprecedented rate due to hardware and software advances. Of course, some versions of IoT, i.e., NBIoT have the security of their legacy deployments such as LTE or GSM.

IV. Quantum Cryptography for IoT

QC has several advantages. In the quantum world it is the only cryptographic technology which can sustain. It is expected that in next few years quantum computers will be available for computing applications. In that scenario, all the currently existing cryptographic technologies will fail except for QC [3]. IoT will have widespread deployment across the sectors. All the common as well mission critical applications will have IoT as their part. In such conditions, the security provisioning will be very important. The quantum computers will pose new threats as all the common cryptographic methods can be decrypted. The need of quantum resistant cryptography is essential to handle such complexities [4]. QC can resist the threats of quantum computers as it is based on the quantum technologies. Of course the algorithms and the steps to be followed in that situation will be different from the current fabric of QC. Furthermore, QC can be applied both in the optical and wireless communications which is essentially an integral requirement of IoT security. The business paradigms of QC such as finance and banking already had been felt in the critical applications. QC has already been deployed for such critical infrastructure. In the future, IoT will take over all these sectors and QC will be its ammunition for security.

QC can be implemented at different levels. In the core networks, it can be a physical layer security detecting any intrusion into the system. This is very much same to the quantum optical cryptography currently in use is several secure communication links. It is also true for the metro and regional networks. In the access network if the optical fibers are used then it is possible to use the same principle. However, a hybrid network such as hybrid fiber coax or fiber digital subscriber line combination cannot provide the same level of security. In the wireless domain, the key distributions are done as mentioned in Section II. Thus, the implementations of QC at different levels have to be carefully chosen for different network configurations.

V. Conclusion

QC is a robust security technology. It can handle the security threats which are supposed to emerge from the quantum computers of the future. No other solution is visible currently which can be compared with QC. It is very much suitable for the IoT related applications. IoT will enter in to all critical aspects of connected living and smart environment. In the future, IoT applications will be pervasive and the security for all these applications will be paramount. Under such intensely secure environment, QC is presumed to be ubiquitous.

References

[1] M. Niemiec, A. R. Pach, "Management of Security in Quantum Cryptography," *IEEE Communications Magazine*, vol. 51, no. 8, pp. 36-41, Aug. 2013.

[2] F. Xu, M. Curty, B. Qi, H. Lo, "Measurement-Device-Independent Quantum Cryptography," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, Mar. 2015.

[3] L. O. Mailloux, C. D. Lewis, C. Riggs, M. R. Grimaila, "Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals," *IEEE IT Pro*. vol. 18, no. 5, pp. 42-47, May 2016.

[4] C. Elliot "Quantum Cryptography," *IEEE Security and Privacy*, vol. 2, no. 4, pp. 57-61, Apr. 2004.

[5] C. Y. Chen, G.-J. Zeng, F. J. Lin, Y. H. Chou, H. C., Chao, "Quantum Cryptography and Its Applications over the Internet," *IEEE Network*, vol. 29, no. 5, pp. 64-69, Oct. 2015.

[6] T. P. Spiller, "Quantum Information Processing: Cryptography, Computation, and Teleportation," *Proceedings of the IEEE*, vol. 84, no. 12, pp. 1719-1746, Dec. 1996.

[7] J. G. Rarity, P. M. Gorman, P. R. Tapster, “Secure key exchange over 1.9 km free-space range using quantum cryptography,” *Electronics Letters*, vol. 37, no. 8, pp. 512-514, Apr. 2001.

[8] S. Chen, H. Xu, D. Liu, B. Hu, H. Wang, “A Vision of IoT: Applications, Challenges, and Opportunities with China Perspective,” *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 349-359, Apr. 2014.

[9] L. D. Xu, W. He, S. Li, “Internet of Things in Industries: A Survey,” *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233-2243, Apr. 2014.

[10] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Communication Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Dec. 2015.

[11] Nokia white paper, *LTE evolution for IoT connectivity*, LTE evolution for IoT connectivity, 2015.

[12] J. A. Stankovic, “Research Directions for the Internet of Things,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 2327-4662, Jan. 2014.