Digital Object Identifier:

Quantum Cryptography for Internet of Things Security

Alekha Parimal Bhatt | Anand Sharma*

***Abstract*—**Internet of things (IoT) is a developing technology with a lot of scope in the future. It can ease various different tasks for us. On one hand, IoT is useful for us, on the other hand, it has many serious security threats, like data breaches, side-channel attacks, and virus and data authentication. Classical cryptographic algorithms, like the Rivest-Shamir-Adleman (RSA) algorithm, work well under the classical computers. But the technology is slowly shifting towards quantum computing, which has immense processing power and is more than enough to break the current cryptographic algorithms easily. So it is required that we have to design quantum cryptographic algorithms to prevent our systems from security breaches even before quantum computers come in the market for commercial uses. IoT will also be one of the disciplines, which needs to be secured to prevent any malicious activities. In this paper, we review the common security threats in IoT and the presently available solutions with their drawbacks. Then quantum cryptography is introduced with some of its variations. And finally, the analysis has been carried out in terms of the pros and cons of implementing quantum cryptography for IoT security.

***Index Terms*—**Internet of things, quantum computing, quantum cryptography, security.

1. Introduction

Computers these days offer all types of services for us. Having and using computers ease up so many tasks in our lives. But computers also have a risk of security with every each task that they perform[1]. Hence it is important for us to ensure the total security of our valuable and personal information. Sustaining computer security comprises of employing suitable anticipatory measures, detecting budding vulnerabilities, possible coercion, and compromised systems, and handling incidents[2]. The computer security is growing as a more and more important field due to the widespread use of the Internet, Wi-Fi, and bluetooth. There are many different types of misuse that can occur over a computer network like hacking, phishing, spreading computer viruses, worms, or Trojans. Misuse may also include the damage to the hardware, software, or electronic data sources.

With the development in technologies, a new field of interest called the Internet of things (IoT) is undergrowth, in which more processes are being automated and more user data are available on the Internet. Hence the need for security has increased nowadays.

Convergence of multiple technologies, machine learning, goods sensors, wireless detector networks,

*Corresponding author
Manuscript received 2019-05-22; revised 2019-07-01.
A. P. Bhatt and A. Sharma are with the Department of Computer Science and Engineering, Mody University of Science and Technology, Sikar 33231 (e-mail: alekhabhatt365@gmail.com; anand_glee@yahoo.co.in).
Publishing editor: Xuan Xie

management systems, and automation (including home and building automation), all contribute to facultative IoT[3]. IoT involves the extending web property on the far side customary devices, from desktops, laptops, smartphones, and tablets, to any variation of historically non-internet-enabled physical devices and everyday objects. Embedded with technologies, these devices will communicate and move over the net, and that they will be remotely monitored and controlled. Having such widespread applications makes IoT prone to many security attacks and breaches. So we have to be careful while developing or using the IoT applications.

2. Security Issues in IoT Systems

This section will describe the various security issues in IoT systems[4],[5].

• Data breaches

The IoT applications collect tons of users' data to operate and function properly. Also, most of the data consist of the user's personal information. So it must be protected by encryption.

• Data authentication

Even when data are successfully encrypted, likelihoods of the device itself being hacked are still there. If there is no way to establish the authenticity of the data communicated to and from an IoT device, the security is conceded.

• Side-channel attacks

These are the attacks which are based on the data and information gained from the implementation of a system, rather than the weaknesses in the algorithm of implementation. Power consumption, electromagnetic leak, or sound can be enough to exploit the system.

• Irregular/no updates

There are plenty of IoT devices in the world and the number is expected to increase in the near future. While developing the devices, the developers often do not pay much attention to the future updates of the device and hence a device considered to be secure when it was manufactured may not be secure any more after 2 years to 3 years or less if it is not updated regularly.

• Malware and ransomware

An example of malware can be the Mirai Botnet which infects the IoT devices that run on Argonaut reduced instruction-set computer core (ARC) processors. If the default username and password combination is not changed for the device, it is very easy for Mirai to infect the device. Ransomware is malevolent software that tends to lock the users out of their devices and threaten the users to leak out their personal data unless a ransom amount is paid.

2.1. Traditional Security Techniques

IoT also comes with many benefits and various risks. As security is the prime concern for any communications, the traditional security techniques are described in this section[6],[7].

• Hashed passwords

Hashing is a common technique to encrypt the passwords for devices. Hash is a function which takes a string as input and produces a unique and consistent set of bits. The Hash code can be cracked using a technique called rainbow table. It is a table which contains the Hash key for the very common password strings, which lets anyone do quick look-up to crack the password. The reverse look-up of the rainbow table can be avoided using an entity called salt. It is a small string of random characters which is appended to every Hash key and is unique for each key. Creating a rainbow table for such long sequences is a time taking and expensive task.

• Private key authentication

Private key cryptography is asymmetric encryption which provides two keys, one public and one private. If data are encrypted with the private key, it can only be decrypted with the public key, and vice versa. Doing so preserves

the security of the system and makes communications with other devices safer. This can be useful when a new device needs to connect to the IoT network and in the verification of messages passed between devices.

• Signed firmware

While creating the firmware, the developer puts a secret digital signature with it, preventing hackers from replacing the actual firmware with a malicious one as they will not be able to replicate authenticated signatures. Also, a technique called secure boot is used to check if each code that runs on the device is signed appropriately.

All these techniques mentioned above are not realizable to a very good extent in real-life systems due to resource constraints. A restricted amount of processing power and memory poses a big hurdle for developers. These techniques may be theoretically perfect but there are various different examples where we can still see security breaches in IoT systems. Examples of some malicious attacks are:

• The Mirai botnet or Dyn attack;
• hackable cardiac monitoring devices from St. Jude;
• the owlet Wi-Fi baby monitor vulnerabilities;
• the TRENDnet webcam hack;
• Stuxnet.

This clearly signifies that we need some more powerful cryptographic and security algorithms to prevent the threats discussed above.

3. Quantum Cryptography

Quantum cryptography is a very interesting field that makes use of the rules of quantum mechanics to develop a cryptosystem that is believed to be the most secure system[8]. It cannot be breached by anyone without getting noticed by the sender or the receiver of the message. Quantum cryptography is based on using photons and their fundamental quantum properties to develop an indestructible cryptosystem because it is not possible to measure the quantum state of any system without alarming the system[9].

Currently, the cryptographic algorithms are using the principles of mathematics to try and develop efficient cryptosystems. An example of a mathematics based cryptographic algorithm is where the 'key' is a combination of a large set of prime factors of large numbers generated at random. Cracking such keys may be an extraordinary task for a normal computer but it is not impossible.

So, scientists are now moving from mathematics towards physics and trying to develop systems which will replace the currently used systems for the better. Using quantum mechanics to send/receive messages is believed to be 100% unhackable and secure[10].

The root of quantum cryptography lies in the fact that it uses the smallest individual particles that exist in nature, i.e. photons. These photons have a property to exist in more than one state simultaneously and they change their states only when they are measured. That is the main property exploited by the quantum cryptography algorithms. Whenever a message is travelling through a channel from the sender to the receiver and any malicious entity tries to intercept the communications, the change in the state of the photon is immediately visible to the sender/receiver.

Also, there is a variation of a technique which makes use of a property called quantum entanglement[11],[12]. Quantum entanglement is a property in which even if two quantum particles/photons are separated by a physical distance, a change in any one of the photons leads to a change in another one, making it easy to detect the intruder in a network.

3.1. Shor's Algorithm for Factoring

Shor's algorithm is one of the most famous algorithms in the field of quantum computing. It shows the

efficient way of factoring large non-prime numbers in polynomial time which takes up exponential time when performed in a classical way.

The motivation behind this algorithm is that the current cryptographic algorithms, like the Rivest-Shamir-Adleman (RSA) algorithm, are based on the principle of factoring large numbers, and the inability of classical computers to solve the problem in polynomial time is the main reason of the success of such algorithms. But quantum computers are very fast and efficient in calculating the factors and hence these algorithms can be easily breached shortly soon. So, to avoid this we need some algorithms that are based on the quantum background.

Generally, classical algorithms take up the time of $O((\log N)^k)$ and the quantum algorithm takes up the time of $O(\log N)$. Also, the run time differs largely: The classical computers take up the run time of $O(\exp(L^{1/3}(\log L)^{2/3})$ and the quantum computers take up the run time of $O((L)^3)$, where L is the length of the number N in bits[13].

The algorithm depends on three main factors:

• Modular arithmetic;

• quantum parallelism;

• quantum Fourier transform.

The problem statement for the algorithm is: Given an odd composite number N, find an integer d, strictly between 1 and N, which divides N.

There are 2 parts of this algorithm:

• Conversion of the problem of factoring to the problem of finding the period. This can be solved classically.

• Finding the period using the quantum Fourier transform which is responsible for quantum speedup.

3.2. Quantum Key Distribution (QKD)

Quantum key distribution is a very basic technique used in quantum cryptography. As we know that quantum computing uses a stream of photons to transmit data. These photons have a property called a 'spin'. There are basically 4 types of spins: Horizontal, vertical, 45° diagonal, and −45° diagonal. The horizontal and vertical filters are put under the rectilinear scheme and the 2 diagonal filters are put under the diagonal scheme. Generally, the horizontal and 45° filters represent the binary 1 and the vertical and −45° filters represent the binary 0[14].

A very interesting principle in physics known as the Heisenberg uncertainty principle states that we cannot measure all the properties of a particle without disturbing its current state. This principle applies to the photons, too. If we try to measure the spin of the photons, the spin will change, which may change the value of the photon. Thus we can know that the stream of communicating photons is interrupted by an unwanted entity[15]-[18].

Alice sends to Bob a stream of polarized photons, selecting in random between the polarizations. Once receiving a photon, Bob chooses in random between + and x bases. Once the transmission is complete, Bob sends Alice the sequence of bases he used to measure the photons. These communications will be utterly public. Alice tells Bob that which of the bases was similar ones she used. These communications may be public. Alice and Bob discard the measurement that Bob used a different basis[19],[20]. On average, Bob can guess the proper basis with the possibility of 50%, and can thus get a similar polarization as Alice sent. The key is then the interpretation of the sequence of remaining photons as 0s and 1s. Eve will hear the messages between Alice and Bob about the sequences of bases they used and learn the bases that Bob guessed properly. However, this tells her nothing regarding the key, because Alice's polarizations was chosen at random. If Bob guessed + as the correct polarization, Eve does not understand whether or not Alice sent a 0 or a 1 polarized photon, and so is aware of nothing regarding the key bit the photon represents. Once Eve measures a

photon, its state is altered to evolve to the basis Eve used, thus Bob can get the incorrect end in some similar basis with the possibility of 50%, Eve's measurement adds an error of 25%[20],[21].

3.3. Device-Independent Quantum Cryptography

In general communications networks, it is often seen that two computers do not communicate directly. There are always some intermediate measurement devices that help the message to go from the source to the destination. Now in such a case, we cannot trust the third-party devices to be completely safe and secure. They may be tampered with by some malicious entity or by the developers themselves. Also, the risk of side-channel attacks is to be worried[22]. The device-independent quantum key distribution aims at modifying the original quantum key distribution to be safe in case of untrusted third-party devices. The aim of quantum key distribution is for two computers, Alice and Bob, to share a common cryptographic key through communications over public channels. It is known that the BB84 protocol (the quantum cryptographic protocol) is safe even under the channel noise and possible detector faults at the end of Bob, with the assumption that the apparatus used at Alice's side are perfectly working to produce photons. But when we work in reality, this assumption does not hold good because there are high possibilities of faulty apparatus at Alice's side, too, which could hamper the security of the private string shared by Alice and Bob for communications.

For the solution of this problem, we need some devices which have the capabilities of self-testing. After passing these tests the device is said to be secure for communications[23]. Also, cross-checking the polarizations and their probability distributions can be a solution. There are various implementations for the solution of these problems.

4. Quantum Cryptography Implementation with IoT

IoT devices have many loopholes in terms of the security of the devices, users, or the network. The current classical architecture of the IoT does not provide any provisions to detect the eavesdropper in the communications channel[24]. Also, there can be some attacks wherein only one device in the whole IoT network can be infected with some virus and other devices trust the infected device and continue communications until it is detected. The fault might not be detected until a late time point and by then a sufficiently large amount of information could be transmitted to any malicious entity[25]. Some viruses may affect the systems in a manner that they can only be removed by rebooting the systems and the industrial and enterprise systems are not rebooted for a very long time. Hence, there are multiple different points of vulnerability and IoT systems are highly susceptible to attacks. Here, we study the possible solution of IoT security through quantum cryptography[26].

A very basic aspect of the quantum cryptography is a quantum key distribution which is discussed above[27]. The best feature in the quantum key distribution is the ability of the channel to detect the presence of any eavesdropper in the architecture of the system. This is in sharp contrast to classical algorithms for cryptography.

There are several variations of the quantum cryptographic protocol, BB84, but the main problem in the physical implementation of these protocols is the maximum distance that can be traveled by the photons. Photons are essentially light particles and they can easily be distorted by the environmental or natural calamities. The photons need to travel a very long distance in cases where the IoT networks are wide and stretch across many cities/countries. Here, quantum computing fails to do so. Also, quantum devices are very big, bulky, and expensive. These cannot be afforded by every organization. The existing quantum key distribution protocol is designed to work with only 2 devices. This is not possible in actual IoT systems which connect hundreds of devices together to communicate[28].

So to cure these problems we can give a solution wherein we combine both the classical and quantum approaches. One solution is proposed, which keeps the current semiconductor chips but uses quantum techniques to create a long and unique cryptographic key for each device. This can be done using quantum random number generation (QRNG), which generates a noise source with a high level of randomness. Quantum computing is capable of generating such large numbers quite efficiently and at a fast speed. Thus, it will be very difficult to guess the key and each device will have its unique key. The only way to get the key is to access the physical device configuration and trying to do so without getting noticed is very difficult. Hence, the key can be secured and the communications can be safe[29].

Additionally, the device-independent quantum cryptography can be used to ensure that the manufactured devices are trustworthy.

5. Conclusions

Finally, it has been concluded that although quantum computing and quantum cryptography have developed very efficiently, there is some more advancement that is required for them to become a reality in the commercial systems. Many algorithms are an advanced version of the quantum key distribution, like the coherent one way (COW) quantum key distribution, which aim at amending the drawbacks of the original quantum key distribution algorithm. But to implement quantum systems in the commercial use for IoT is a big challenge due to the large scale and expensive quantum apparatus which cannot be afforded by every organization. Also, the distance which quantum communications can be done is very less due to the properties of photons, which restrict them to travel long distances. If these issues are resolved, we can have successful IoT systems with quantum cryptography applied to them, making them the most secure systems to date.

References

[1] V. Kharchenko, M. Kolisnyk, I. Piskachova, and N. Bardis, "Reliability and security issues for IoT-based smart business center: Architecture and markov model," in *Proc. of the 3rd Intl. Conf. on Mathematics and Computers in Sciences and in Industry*, Chania, 2016, pp. 313-318.

[2] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3-9, Feb. 2014.

[3] IEEE. (2017). Internet of things—IEEE standards enabling products with real-world applications. [Online]. Available: https://standards.ieee.org/initiatives/iot/stds.html

[4] SecureRF. (February 2019). Will enterprise prioritize IoT security over innovation in 2019? [Online]. Available: https://www.securerf.com/will-enterprise-prioritize-iot-security-over-innovation-in-2019/

[5] Y.-C. Yang, L.-F. Wu, G.-S. Yin, L.-J. Li, and H.-B. Zhao, "A survey on security and privacy issues in Internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

[6] *Internet Security Threat Report*, Symantec, Cupertino, 2016.

[7] J. Shen, T.-Q. Zhou, X.-C. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," *IEEE Trans. on Information Forensics and Security*, vol. 13, no. 4, pp. 912-925, Apr. 2018.

[8] R. P. Feynman, "Simulating physics with computers," *Intl. Journal of Theoretical Physics*, vol. 21, no. 6-7, pp. 467-488, Jun. 1982.

[9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of IEEE Intl. Conf. Computers, Systems and Signal Processing*, Bangalore, 1984, pp. 175-179.

[10] D. Deutsch, A. Barenco, and A. Ekert, "Universality in quantum computation," *Proc. of the Royal Society A: Mathematical and Physical Sciences*, vol. 449, no. 1937, pp. 669-677, Jun. 1995.

[11] A. Ekert and C. Macchiavello, "Quantum error correction for communication," *Physical Review Letters*, vol. 77, no. 12, pp. 2585-2588, Sept. 1996.

[12] E. Rieffel and W. Polak, "An introduction to quantum computing for non-physicists," *ACM Computing Surveys*, vol. 32, no. 3, pp. 300-335, Sept. 2000.

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145-195, Jan. 2002.

[14] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, pp. 057901:1-4, Aug. 2003.

[15] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters*, vol. 87, no. 19, pp. 194108:1-3, Nov. 2005.

[16] N. Gisin and R. Thew, "Quantum communication," *Nature Photonics*, vol. 1, no. 3, pp. 165-171, Mar. 2007.

[17] A. Sharma, R. C. Belwal, V. Ojha, and G. Agarwal, "Password based authentication: Philosophical survey," in *Proc. of 2010 IEEE Intl. Conf. on Intelligent Computing and Intelligent Systems*, Xiamen, 2010, pp. 619-622.

[18] A. Sharma, V. Ojha, and V. Goar, "Security aspect of quantum key distribution," *Intl. Journal of Computer Applications*, vol. 2, no. 2, pp. 58-62, May 2010.

[19] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge: Cambridge University Press, 2017.

[20] T. Cubitt, D. Elkouss, W. Matthews, *et al.*, "Unbounded number of channel uses may be required to detect quantum capacity," *Nature Communications*, vol. 6, pp. 6739:1-4, May 2015.

[21] V. Ojha, A. Sharma, V. Goar, and P. Trivedi, "Limitations of practical quantum cryptography," *Intl. Journal of Computer Trends and Technology*, vol. 1, no. 1, pp. 90-93, 2011.

[22] S. Pirandola, C. Ottaviani, G. Spedalieri, *et al.*, "High-rate measurement-device-independent quantum cryptography," *Nature Photonics*, vol. 9, no. 6, pp. 397-402, May 2015.

[23] F.-H. Xu, M. Curty, B. Qi, and H. K. Lo, "Measurement-device-independent quantum cryptography," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 6601111:1-11, May 2015.

[24] A. P. Bhatt, T. Babuta, and A. Sharma, "Quantum information processing and communication: Asian perspective," *Intl. Journal of Computer and Mathematical Sciences*, vol. 7, no. 2, pp. 616-621, Feb. 2018.

[25] L. S. Bishop, S. Bravyi, A. Cross, J. M. Gambetta, and J. Smolin. (March 2017). Quantum volume. [Online]. Available: https://pdfs.semanticscholar.org/650c/3fa2a231cd77cf3d882e1659ee14175c01d5.pdf

[26] Nicola Jones. (June 2013). Computing: The quantum company. *Nature*. [Online]. Available: https://www.nature.com/news/computing-the-quantum-company-1.13212

[27] Timothy Hollebeek. (May 2019). Future-proofing security in a post-quantum cryptography world. [Online]. Available: https://securityboulevard.com/2019/05/futureproofing-security-in-post-quantum-cryptography-world/

[28] S. Gupta and C. Dutta, "Internet of things security analysis of networks using quantum key distribution," *Indian Journal of Science and Technology*, vol. 9, no. 48, pp. 105551:1-11, 2016.

[29] R. Pell. (January 2018). IoT security algorithm accepted by NIST for quantum cryptography project. [Online]. Available: https://www.eenewseurope.com/news/iot-security-algorithm-accepted-nist-quantum-cryptography-project

Alekha Parimal Bhatt was born in Surat in 1997. Currently, she is pursuing her B.Tech. degree with the Department of Computer Science and Engineering, Mody University of Science and Technology (MUST), Sikar. Her research interests include quantum computing and data science.

Anand Sharma was born in Bikaner in 1981. He received his Ph.D. degree in engineering from MUST in 2016, his M.Tech. degree from Atal Bihari Vajpayee-Indian Institute of Information Technology and Management (ABV-IIITM), Gwalior in 2008, and his B.E. degree from University of Technology of Madhya Pradesh (RGPV), Bhopal in 2004. He is currently working with MUST as an assistant professor. His research interests include information theory and coding, information security, quantum cryptography, and IoT. He is serving in several international journals as the editorial member and in international conferences as the technical programme committee/organizing committee.