© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Limit of Privacy and Quantum Cryptography

Bhavesh Prajapati
Assistant Professor, IT Department, L. D. College of Engineering, Ahmedabad, Gujarat, India

ABSTRACT

Recent developments in quantum cryptography have started affecting security and privacy of modern classical cryptography. Just in 1994, Peter Shor represented algorithm for factoring large prime numbers which forced cryptographers and security experts to give attention to quantum cryptography. Modern classical Public Key Infrastructures depends on difficulty of factoring large prime numbers using RSA. Shor's algorithm challenges this and makes jeopardy of modern PKI. For example, when we try to break 2048 bit RSA key using classical computers it will take billion years to break. But same can be broken within few seconds with mature quantum computing architecture. Having said this, quantum computers have their own limitations. They are having small memories, limited processing power and works on comparatively smaller distances. In this paper we discusses quantum cryptography and limitation of classical and quantum cryptography in providing privacy.

Keywords : Quantum Cryptography, Integrated Circuit, Quantum Theory, Quantum Algorithm, PKI, RSA, QKD

I. INTRODUCTION

According to Moore's law the number of transistors on integrated circuit (IC) chips doubles approximately every two years, with the transistors becoming smaller and processing faster. Moore's law still works, but one day it will no longer apply. Energy consumption and heat production are becoming greater challenges as the number of transistors on a chip increases. Quantum theory also gives an excellent resolution for energy consumption and heat production.

In 1994 Shor proposed a quantum algorithm that could dramatically reduce the time spent on integer factorization. The most important issue is that it could also carry out prime factor decomposition, which is the core part of Rivest, Shamir, and Adleman (RSA, which uses different keys in encryption and decryption periods, also called the asymmetric key algorithm or public key cryptosystems). RSA is the most widely used cryptographic system. It takes 13 months to decrypt its encryption using a desktop computer with 4 cores running at 2.8 GHz. However, the same situation becomes different in the quantum world. If we apply Shor's algorithm to find the prime factors, only 1 s is required. Quantum algorithms provide a huge improvement.

The question to ask is, "How long does your data need to be secure?" If the answer is 30 years or more, you are already behind the power curve.

In classical cryptography, the secret key can be created by the sender alone, the sender and the receiver, or the third party. In complicated procedures, the secret key should only be used once. In addition, the key should be adapted in certain protocols where the key contains an extraordinary amount of bits that may equal the length of the plain text. A secured key will ensure a safe method of transferring information between parties. The more

IJSRSET1849149 | Received : 01 April 2018 | Accepted : 20 April 2018 | March – April 2018 [(4) 4 : 1567-1571]

complex the secured key, the safer the information transfer. So classical cryptography is the process that occurs within an unexpected amount of time through the execution of complex mathematical sequences. As a result, must constantly strive to improve communication security. Table 1 displays limitations of today's most popular classical algorithms against development in quantum cryptography.

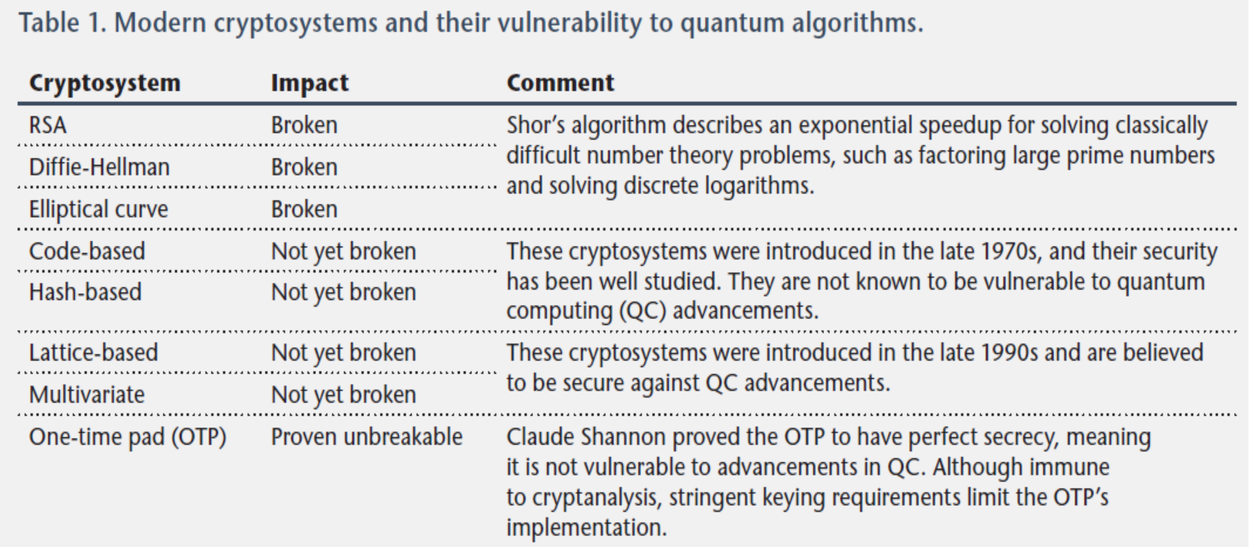

Table 1. Modern cryptosystems and their vulnerability to quantum algorithms.

Cryptosystem	Impact	Comment
RSA	Broken	Shor's algorithm describes an exponential speedup for solving classically difficult number theory problems, such as factoring large prime numbers and solving discrete logarithms.
Diffie-Hellman	Broken	
Elliptical curve	Broken	
Code-based	Not yet broken	These cryptosystems were introduced in the late 1970s, and their security has been well studied. They are not known to be vulnerable to quantum computing (QC) advancements.
Hash-based	Not yet broken	
Lattice-based	Not yet broken	These cryptosystems were introduced in the late 1990s and are believed to be secure against QC advancements.
Multivariate	Not yet broken	
One-time pad (OTP)	Proven unbreakable	Claude Shannon proved the OTP to have perfect secrecy, meaning it is not vulnerable to advancements in QC. Although immune to cryptanalysis, stringent keying requirements limit the OTP's implementation.

II. INTRODUCTION TO QUANTUM CRYPTOGRAPHY

Quantum physics inhibits some typical properties which cannot be easily explained by normal physics. For example:

- ✓ The no-cloning theorem states that one cannot create a copy of an unknown quantum state or qubit.
- ✓ One cannot measure a system without disturbing it.
- ✓ The uncertainty principle states that one cannot simultaneously measure two properties (such as position and momentum of a particle)
- ✓ with arbitrarily high precision.

Above characteristics can be considered negative but these drawbacks are turned into positive applications for quantum cryptography. Heisenberg Uncertainty principle says that we cannot measure quantum state of system without disturbing it. So when light particle is polarized, we can know the polarization only at the time of measuring it.

Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984. Bennet and Brassad stated that an encryption key can be created depending on the amount of photons reaching a recipient and how they were received. Photons can be polarized for different angles and their orientation can be used to represent information in form of zero and one. In a way a system for producing and delivering key in secure way can be developed. The representation of bits through orientation of polarized bits is base of quantum cryptography. Classical cryptography depends on computational limitations while quantum cryptography depends on basic rules of physics and not on processing power of computations.

Let us understand use of quantum cryptography to distribute keys. This includes a sender, "Alice", a receiver, "Bob". Alice sends a message to Bob using a photon gun to send a stream of photons randomly chosen in one of four polarizations that correspond to vertical, horizontal or diagonal in opposing directions (0,45,90 or 135 degrees).

Bob receives each photon from stream and chooses a random filter to measure the polarization of received photon, whether it is in rectilinear (0 or 90 degrees) or diagonal (45 or 135 degrees) bases. Bob also keeps record of results of which measurements are correct with reference to Alice's selection. All photons will not reach to Bob due to distance and noise.

Alice and Bob discusses over pubic channel about types of measurements done, which bases are used and which photons are registered. The in correctly measured photons were discarded. While correctly measured photons are converted in to bits based on their polarization.

Here Alice and Bob cannot determine the key in advance as key is generated based on their random choices of polarization angles and correctly received bits. In a way quantum cryptography makes secure distribution of keys possible.

So far, so nice. But what about attacker? Let us assume the obvious possibility of attacker try to gain the key from quantum key distribution system. Let us name this malicious attacker "Eve". When Eve tries to measure , she have equal chance of selecting the correct filter as Bob have but will not be able to confirm with Alice regarding her choice of bases. Eve may try when Alice and Bob are confirming with each other about the matching bases used for measurements. But still this information is of no use as Eve does not know the exact polarization used by Alice for each photon. Due to this Eve will never be able to gain the correct key.

As per Heisenberg Uncertainty principle, we cannot copy quantum bit as when we try to measure it, its state will be changed. Alice and Bob need to fix the number of photons required to be communicated to generate a key before starting a procedure. Mathematically Bob should receive at least twenty five percent of photons correctly if they are not sniffed in between. If Eve detects a photon she cannot pass the same to Bob as she cannot copy the photon. And if Eve sends her own photons with randomly chosen orientation error rate will increase suggesting presence of malicious attacker.

III. LIMITATION OF QUANTUM CRYPTOGRAPHY

Theory of quantum cryptography is mature enough but practical implementation of quantum cryptography is little far away from efficient implementation. Following are key issues need to be addressed for real life implementation of Quantum cryptography applications.

a. Point to Point links and Denial of Service

The quantum channel is a specialized piece of equipment, which by its very nature is a point-to-point connection: X and Y have to be at each end of it, with their photon sources and detectors. The point-to-point nature of QKD restricts potential growth, and gives rise to the possibility of a denial-of-service attack: if Z can't obtain key information, then cutting the physical link will mean X and Y can't either, which might serve Z's purposes just as well [7].

b. High Bit Errors Rate

The bit error rate of a quantum key distribution is several percentages higher than an optical communication system, which can be devastating in terms of practicality.[7].

c. Authentication

QKD does not in itself provide authentication. Current strategies for authentication in QKD systems include prepositioning of secret keys at pairs of devices, to be used in hash-based authentication schemes, or hybrid QKD-public key techniques. Neither approach is entirely appealing. Prepositioned secret keys require some means of distributing these keys before QKD itself begins, e.g., by human courier, which may be costly and logistically challenging. Furthermore, this approach appears open to denial of service attacks in which an adversary forces a QKD system to exhaust its stockpile of key material, at which point it can no longer perform authentication.

On the other hand, hybrid QKD-public key schemes inherit the possible vulnerabilities of public key systems to cracking via quantum computers or unexpected advances in mathematics.

d. Sufficiently Rapid Key Delivery

Key distribution systems must deliver keys fast enough so that encryption devices do not exhaust their supply of key bits. This is a race between the rates at which keying material is put into place and the rate at which it is consumed for encryption or decryption activities. Today's QKD systems achieve on the order of 1,000bits/second throughput for keying material, in realistic settings, and often run at much lower rates. This is unacceptably low if one uses these keys in certain ways, e.g., as one-time pads for high speed traffic flows.

e. Distances and Location Independence

In the ideal world, any entity can agree upon keying material with any other (authorized) entity in the world. Rather remarkably, the Internet's security architecture does offer this feature – any Computer on the Internet can form a security association with any other, agreeing upon keys through the Internet IPSec protocols. This feature is notably lacking in QKD, which requires the two entities to have a direct and unencumbered path for photons between them, and which can only operate for a few tens of kilometers through fiber.

IV. CONCLUSION

Quantum cryptography applications seem promising despite having implementation challenges. Still there is a lot to be done to develop quantum cryptography infrastructure. Many government agencies and corporate have started planning for quantum proof security arrangements. It is impossible to predict the future but scientists are expecting practical quantum computer by 2045 to be a reality. This does not mean that quantum computers are going to replace classical computers; still there is a need to define protocols and architecture to interface both worlds together.

V. REFERENCES

[1]. "Practical Challenges in quantum key distribution" by EleniDiamanti, Hoi-Kwong Lo, Nature Publications,2016

[2]. "Quantum cryptography and quantum key distribution Protocol: A Survey" by V. Padmavati, B. Visnuvardan, A.V.N. Krishna, IEEE 6th International Conference, 2016

[3]. "Post quantum cryptography what advancements in quantum computing mean for IT professionals" by Logan O. Mailoux, IEEE 2016

[4]. "QKDP's Comparison Based upon Quantum Cryptography Rules" by AbdulbastAbushgra, KhaledElleithy, IEEE, 2015

[5]. "Quantum cryptography and its applications over the internet" by Chi-Yuan Chen, Guo-jyunZeng, IEEE 2015

[6]. "A Tutorial on Quantum Key Distribution" by Baokang Zhao, Bo Liu, Ilsun You, IEEE 10th International Conference, 2015

[7]. "Quantum Cryptography: Pitfalls and Assets" by Deepshikha Sharma, IJERSTE, 2014

[8]. "How secure is quantum cryptography" by Renato Renner, Optical Society of America, 2013

[9]. "Key Distribution Protocol on Quantum Cryptography" by KondwaniMakanda, Jun-cheolJeon, IEEE, 2013

[10]. "Quantum cryptography and comparision of quantum key distribution protocols" by ErgumGumus, G.Zeynep, Journal of Electrical and Electronics engineering,2008.

[11]. "The formal study of quantum cryptography protocols" by Fan Yang, Yu-Jie, IEEE 2013

[12]. Bennett, C. H. & Brassard, G. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (ed. Goldwasser, S.) 175–179 (IEEE Press, 1984).

[13]. Scarani, A.Acin, Ribordy, G.Gisin.N."Quantum Cryptography protocols robust against Photon number Splitting attack." Physical Review

Letters, vol.92.2004 http://www.qci.jst.go.jp/eqsi03/program/papers/O26-Scarani.pdf

[14]. Secure communication with a publicly known key.C. K. A. Beige, B.-G. Englert and H. Weinfurter. ActaPhysicaPolonica A, 101(3):357–368,2002.

[15]. Quantum cryptography: Public key distribution and coin tossing. C. H. Bennett and G. Brassard. Theoretical Computer Science, 560, Part1(0):7 – 11, 2014. Theoretical Aspects of Quantum Cryptography,celebrating 30 years of fBB84g.

[16]. Quantum digital signatures without quantum memory. V. Dunjko, P. Wallden, and E. Andersson. Phys. Rev. Lett., 112:040502, Jan 2014.

[17]. Quantum cryptography based on bell's theorem.A. Ekert. Phys. Rev.Lett., 67:661–663, Aug 1991.

[18]. Differential phase-shift quantum key distribution systems. K. Inoue. Selected Topics in Quantum Electronics, IEEE Journal of, 21(3):1–7,May 2015.

[19]. Efficient quantum key distribution scheme and a proof of its unconditional security.H.-K. Lo, H. F. Chau, and M. Ardehali. J. Cryptol.,18(2):133–165, Apr. 2005.

[20]. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations V. Scarani, A. Acin, G. Ribordy, and N. Gisin..Phys. Rev. Lett., 92:057901, Feb 2004.

[21]. "Quantum Key Distribution Protocols: A Review," S. Reddy, Journal of Computational Information Systems, vol. 8, pp. 2839-2849, 2012.

[22]. M. M. Khan, M. Murphy, and A. Beige, New Journal of Physics,vol. 11, p. 063043, 2009.

[23]. "High error-rate quantum key distribution for long-distance communication," M. Elboukhari, M. Azizi, and A. Azizi, "Quantum key distribution protocols: A survey," International Journal of Universal ComputerSciences, vol. 1, pp. 59-67, 2010.

[24]. "Towards practical and fast quantum cryptography," N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, arXiv preprint quant-ph/0411022, 2004.

[25]. "Quantum Cryptography: A comprehensive study", Bhavesh Prajapati, 2014, IJSRSET

[26]. "A Brief Study of Quantum Cryptography Applications", Bhavesh Prajapati, 2015, International journal of scientific research in science and technology.

[27]. " Quantum Key Distribution : A Comprehensive Study", Bhavesh Prajapati, 2016, International Journal of Scientific Research in Science and Technology (IJSRST)

[28]. "Quantum Key Distribution Protocols : A Review". Bhavesh Prajapati, 2017, IJSRSET