A Review on Quantum Cryptography and Quantum Key Distribution

Ritu Rani

Lecturer, Department of Physics, CRM Jat College, Hisar

Abstract: **- Quantum cryptography uses our current knowledge of physics to develop a cryptosystem that is not able to be defeated - that is, one that is completely secure against being compromised without knowledge of the sender or the receiver of the messages. Quantum cryptography promises to reform secure communication by providing security based on the elementary laws of physics, instead of the current state of mathematical algorithms or computing technology. This paper describes an overview about Quantum cryptography and Quantum key distribution technology, and how this technology contributes to the network security.**

Keywords:- **Quantum cryptography, public-key encryption, Secret key encryption, Quantum key distribution technology**

I. INTRODUCTION

The word quantum itself refers to the most fundamental behavior of the smallest particles of matter and energy: quantum theory explains everything that exists and nothing can be in violation of it. Quantum cryptography is the science of exploiting quantum mechanical properties to perform cryptographic tasks. The best known example of quantum cryptography is quantum key distribution which offers an information-theoretically secure solution to the key exchange problem. Currently used popular public-key encryption and signature schemes (e.g., RSA and ElGamal) can be broken by quantum adversaries. There are two main fields of modern cryptographic techniques: Public key encryption and Secret key encryption . Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication. With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale. The symmetric key was found to be non-practical due to challenges it faced for key management. This gave rise to the public key cryptosystems. Public-key cryptography, or asymmetric cryptography, is an encryption scheme that uses two mathematically related, but not identical, keys - a public key and a private key. Unlike symmetric key algorithms that rely on one key to both encrypt and decrypt, each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt. public-key encryption uses two different keys at once -- a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. The main disadvantage of a secret-key cryptosystem is related to the exchange of keys. Symmetric encryption is based on the exchange of a secret (keys). Secret key cryptography systems are often classified to be either stream ciphers or block ciphers. Stream ciphers work on a single bit at a time and also use some kind of feedback mechanism so that the key changes regularly. The goal of position-based quantum cryptography is to use the geographical location of a player as its (only) credential. A quantum cryptographic protocol is device-independent if its security does not rely on trusting that the quantum devices used are truthful. Thus the security analysis of such a protocol needs to consider scenarios of imperfect or even malicious devices. Quantum computers may become a technological reality; it is therefore important to study cryptographic schemes used against adversaries with access to a quantum computer. The study of such schemes is often referred to as post-quantum cryptography.

II. QUANTUM KEY DISTRIBUTION TECHNOLOGY

Quantum Key Distribution uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. Quantum key distribution is not only based on the principles of quantum physics, it also relies on classical information theory. The distributed key must be both common and secret. First, the transmission errors must be corrected, whether they are caused by eavesdropping or by imperfections in the setup. Second, a potential eavesdropper must know nothing about the key. To achieve these two goals, techniques from classical information theory, collectively denoted as secret-key distillation, must be used. One aspect of quantum key distribution is that it is secure against quantum computers. Its strength does not depend on mathematical complexity, like post-quantum cryptography, but on physical principles. The value of the bit, a 1 or a 0, is determined by states of the photon such as polarization or spin. At the sender's end, a laser generates a series of single photons, each in one of two polarizations: horizontal or vertical. QKD will become necessary for any form of secure data transfer, thus paving the way for the development of Quantum Cities and national and international Quantum Grids.

III. ADVANTAGES AND DISADVANTAGES OF QUANTUM CRYPTOGRAPHY

Advantages of Quantum cryptography:

- Virtually un-hackable
- Simple to use
- Less resources needed to maintain it

Disadvantages of Quantum cryptography

- The signal is currently limited to 90 miles
- Could replace a lot of jobs

IV. APPLICATION OF QUANTUM CRYPTOGRAPHY

The signal is currently limited to 90 milesCould replace a lot of jobs Quantum cryptography use in every sphere like ultra-secure voting, secure communication with space, a smarter power grid, quantum internet, Key Agreement, Data Encryption , Digital Signature, Analysis of DNA Structure, Analysis of Brain Function , Maintaining security etc.

V. LIMITATIONS OF QUANTUM CRYPTOGRAPHY

- Quantum cryptography is good for secrecy but cannot be used to sign public documents (some authentication of private messages is possible)
- Bruce Schneier, an American cryptographer, says " I don't see any commercial value in it. I don't believe it solves any security problem that needs solving. I don't believe that it's worth paying for. I can't imagine anyone but a few technophiles buying and deploying it. Systems that use it don't magically become unbreakable, because the quantum part doesn't address the weak points of the system.
- Quantum cryptography does not guarantee that you can communicate securely.
- Quantum cryptography doesn't "solve" all of cryptography: The keys are exchanged with photons, but a conventional mathematical algorithm takes over for the actual encryption

VI. CONCLUSION

In this paper we are summarize about Quantum cryptography and . Quantum cryptography comes with its own load of weaknesses. It was recognized in 2010, for instance, that a hacker could blind a detector with a strong pulse, rendering it unable to see the secret-keeping photons. Security is a broad issue and this report has only addressed a narrow area of techniques that, provided appropriate security policies are defined and adhered to, will facilitate a secure system. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical communication.

REFERENCES

[1]. Introduction to Quantum Cryptography and Secret-Key Distillation by Gilles Van Assche http://gva.noekeon.org/QCandSKD/QCandSKD-introduction.html

[2]. Quantum Cryptography and Secret-Key Distillation, © Cambridge University Press

[3]. Crépeau, Claude; Joe, Kilian (1988). Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract). FOCS 1988. IEEE. pp. 42–52.

[4]. How Encryption Works http://computer.howstuffworks.com/encryption3.htm

[5]. Kilian, Joe (1988). Founding cryptography on oblivious transfer. STOC 1988. ACM. pp. 20–31.

[6]. Brassard, Gilles; Claude, Crépeau; Jozsa, Richard; Langlois, Denis (1993). A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties. FOCS 1993. IEEE. pp. 362–371.

[7]. What is Public-key Cryptography? https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/

[8]. Mayers, Dominic (1997). "Unconditionally Secure Quantum Bit Commitment is Impossible". Physical Review Letters. APS. **78** (17): 3414–3417. arXiv:quant-ph/9605044.Bibcode:1997PhRvL..78.3414M. doi:10.1103/PhysRevLett.78.3414. Preprint atarXiv:quant-ph/9605044v2

[9]. Public Key Encryption https://www.tutorialspoint.com/cryptography/public_key_encryption.htm

[10]. "Experimental Bit Commitment Based on Quantum Communication and Special Relativity".

[11]. ^ Jump up to:[a] [b] Damgård, Ivan; Fehr, Serge; Salvail, Louis; Schaffner, Christian (2005). Cryptography In the Bounded Quantum-Storage Model. FOCS 2005. IEEE. pp. 449–458. A full version is available at arXiv:quant-ph/0508222.

[12]. Private-key (or secret-key) cryptography http://ccm.net/contents/130-private-key-or-secret-key-cryptography

[13]. Wehner, Stephanie; Schaffner, Christian; Terhal, Barbara M. (2008). "Cryptography from Noisy Storage". Physical Review Letters. APS. **100** (22): 220502. arXiv:0711.2895 .Bibcode:2008PhRvL.100v0502W. doi:10.1103/PhysRevLett.100.220502.PMID 18643410. A full version is available at arXiv:0711.2895.

[14]. Secret Key https://www.techopedia.com/definition/24865/secret-key

[15]. Koenig, Robert; Wehner, Stephanie; Wullschleger, Juerg. "Unconditional security from noisy quantum storage". A full version is available at arXiv:0906.1030.

[16]. A Comparison of a Public and a Secret Key Cryptosystem by Adam Donlin, SE4H. 29th February, 1995. http://www.dcs.ed.ac.uk/home/adamd/essays/crypto.html

[17]. Kent, Adrian; Munro, Bill; Spiller, Tim (2010). "Quantum Tagging with Cryptographically Secure Tags". A full version is available at arXiv:1008.2147.

[18]. Lau, Hoi-Kwan; Lo, Hoi-Kwong (2010). "Insecurity of position-based quantum-cryptography protocols against entanglement attacks". Physical Review A. APS. **83**: 012322. arXiv:1009.2256. Bibcode:2011PhRvA..83a2322L.doi:10.1103/PhysRevA.83.012322. A full version is available at arXiv:1009.2256.

[19]. Malaney, Robert A. (2010). "Location-dependent communications using quantum entanglement". Physical Review A. **81**: 042319. arXiv:1003.0949 .Bibcode:2010PhRvA..81d2319M. doi:10.1103/PhysRevA.81.042319.

[20]. How quantum cryptography works: And by the way, it's breakable By Michael Kassner http://www.techrepublic.com/blog/it-security/how-quantum-cryptography-works-and-by-the-way-its-breakable/

[21]. Buhrman, Harry; Chandran, Nishanth; Fehr, Serge; Gelles, Ran; Goyal, Vipul; Ostrovsky, Rafail; Schaffner, Christian (2010). "Position-Based Quantum Cryptography: Impossibility and Constructions". A full version is available at arXiv:1009.2490.

[22]. Beigi, Salman; König, Robert (2011). "Simplified instantaneous non-local quantum computation with applications to position-based cryptography". arXiv:1101.1065
[23]. Quantum Cryptography Applications in Electronic Commerce Jonathan Jones Oxford Centre for Quantum Computation http://www.qubit.org
[24]. quantum cryptography http://searchsecurity.techtarget.com/definition/quantum-cryptography
[25]. Mayers, Dominic; Yao, Andrew C.-C. (1998). Quantum Cryptography with Imperfect Apparatus. IEEE Symposium on Foundations of Computer Science (FOCS). arXiv:quant-ph/9809039
[26]. Colbeck, Roger (December 2006). "Chapter 5". Quantum And Relativistic Protocols For Secure Multi-Party Computation (Thesis). University of Cambridge. arXiv:0911.3814.
[27]. How quantum key distribution works By William Jackson Oct 29, 2013 https://gcn.com/articles/2013/10/29/how-quantum-key-distribution-works.aspx
[28]. Vazirani, Umesh; Vidick, Thomas (2014). "Fully Device-Independent Quantum Key Distribution". Physical Review Letters. **113**: 140501. arXiv:1403.3830.Bibcode:2014PhRvL.113b0501A. doi:10.1103/PhysRevLett.113.020501.
[29]. Miller, Carl; Shi, Yaoyun (2014). "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices". arXiv:1402.0489.
[30]. Miller, Carl; Shi, Yaoyun (2015). "Universal security for randomness expansion".arXiv:1411.6608.
[31]. Chung, Kai-Min; Shi, Yaoyun; Wu, Xiaodi (2014). "Physical Randomness Extractors: Generating Random Numbers with Minimal Assumptions". arXiv:1402.4797.
[32]. Quantum Cryptography: Definition, Advantage and Limitation By Naveen Thakur · October 7, 2012 http://www.whitec0de.com/quantum-cryptography/
[33]. "Post-quantum cryptography". Retrieved 29 August 2010.
[34]. Bernstein, Daniel J.; Buchmann, Johannes; Dahmen, Erik, eds. (2009). Post-quantum cryptography. Springer. ISBN 978-3-540-88701-0.
[35]. Watrous, John (2009). "Zero-Knowledge against Quantum Attacks". SIAM J. Comput. **39**(1): 25–58. doi:10.1137/060670997.
[36]. "NSA Suite B Cryptography". Retrieved 29 December 2015.
[37]. Laws of Physics Say Quantum Cryptography Is Unhackable. It's Not by Adam Mann. https://www.wired.com/2013/06/quantum-cryptography-hack/
[38]. Heisenberg, W. (1927), "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik", Zeitschrift für Physik (in German), 43 (3–4): 172–198, Bibcode:1927ZPhy...43..172H, doi:10.1007/BF01397280.. Annotated pre-publication proof sheet of Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, March 21, 1927.
[39]. W. Wootters and W. Zurek, "The no-cloning theorem", Phys. Today, vol. 62, no. 2, pp. 76–77, 2009.
[40]. J. Hilgevoord and J. Uffink, "The Uncertainty Principle", Plato.stanford.edu, 2001. [Online]. Available: http://plato.stanford.edu/entries/qt-uncertainty/. [Accessed: 07-Oct-2016].
[41]. "How Quantum Suicide Works", HowStuffWorks, 2007. [Online]. Available:http://science.howstuffworks.com/innovation/science-questions/quantum-suicide2.htm. [Accessed: 07-Oct-2016].
[42]. C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum key- distribution Protocols," Phys. Rev. Avol. 73, 2006.
[43]. Cachin, Christian; Crépeau, Claude; Marcil, Julien (1998). Oblivious Transfer with a Memory-Bounded Receiver. FOCS 1998. IEEE. pp. 493–502.
[44]. Quantum Key Distribution http://quantum.ukzn.ac.za/research/quantum-key-distribution
[45]. Dziembowski, Stefan; Ueli, Maurer (2004). On Generating the Initial Key in the Bounded-Storage Model. Eurocrypt 2004. LNCS. **3027**. Springer. pp. 126–137.
[46]. https://en.wikipedia.org/wiki/Quantum_cryptography
[47]. Chandran, Nishanth; Moriarty, Ryan; Goyal, Vipul; Ostrovsky, Rafail (2009). Position-Based Cryptography. A full version is available at IACR eprint:2009/364.
[48]. US 7075438, issued 2006-07-11
[49]. Simmon, G. J. ,"Symmetric and asymmetric encryption", ACM Computing Surveys, 11(4), 1979, pp. 305-330
[50]. Bennett, C.H. and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984.
[51]. Ekert. A. Physical Review Letters, 67, pp. 661–663, (1991)
[52]. Kak, S., A three-stage quantum cryptography protocol. Foundations of Physics Letters, vol. 19, pp. 293–296, 2006.
[53]. Chen, Y. et al., Embedded security framework for integrated classical and quantum cryptography in optical burst switching networks. Security and Communication Networks, vol. 2, pp. 546–554, 2009.