A survey on Quantum key Distribution and Huffman Coding Compression Algorithm

Mohit Shukla[1], Sarvesh Patel[2]

[1,2]Department of Computer Science & Engineering, Rama University, Kanpur(U.P)

ABSTRACT:- This paper proposes a new data transmission technique that uses Quantum Key Distribution (QKD) method, One Time Pad (OTP) encryption technique and Huffman encoding compression algorithm to transmit the data more securely and efficiently. While data is transmitted, requirements like secrecy, less overhead through compression etc are crucial issues. QKD is one of the most promising methods which provide unconditional security. It relies upon the immutable laws of quantum physics rather than computational complexity as the basis of its secrecy. To establish the trust between the sender and the receiver, this paper considers a trusted center that distributes and verifies the key. Also it uses Huffman encoding- a lossless compression algorithm to compress the transmitted data over the classical channel that reduces the data transmission overhead. Moreover for data encryption, it applies OTP technique with the key randomly generated by the QKD method that ensures the secrecy of the transmitted data over the classical channel. Thus the overhead of both quantum and classical channels are reduced. Finally the time requirements for encoding-decoding and encryption-decryption for the proposed technique are evaluated.

Keywords-Quantum Key Distribution; Huffman encoding algorithm; One Time Pad

Introduction

Quantum key distribution (QKD) involves the generation of a shared secret key between two parties via quantum signal transmission. (Among other possible terms, we will often use the more appropriate ``generation'' in lieu of ``distribution,'' ignoring their ne distinction in conventional cryptography QKD is widely perceived to have been proved secure in various protocols , in contrast to the lack of security proofs for conventional methods of encryption for privacy or key distribution. Security proofs in QKD are highly technical and are also multi-disciplinary in nature, as is the case with the subject area of quantum cryptography itself. Theoretical QKD involves in its description and treatment various areas in quantum physics, information theory, and cryptography at an abstract and conceptual level. It is dif cult for non-experts in QKD security to make sense of the literature; moreover, even experts are often not aware of certain basics in some of the relevant fields. Many who perform assessments on QKD security follow the vague community consensus on QKD security being guaranteed by rigorous proofs. A common perception is that QKD gives ``perfect secrecy,'' as asserted for example in a useful recent monograph on conventional cryptography.

In this paper, we will describe the actual security theory situation of QKD with just enough technical materials for accurate statements on the results. We will be able to describe some main security issues without going into the physics, and we can treat everything at a *classical* probability level, to which a *quantum* description invariably reduces. We will discuss in what ways these security issues have been handled inadequately. Some major work in the QKD security liter-ature will be mentioned and also discussed in Appendix I, which may help clarify the issues and illuminate the develop-ment that led to the current security situation. In Appendix II, we compare QKD to conventional cryptography and provide a preliminary assessment on the usefulness of QKD when conventional cryptography appears adequate. (Note that cryp-tography is a small and relatively minor subarea of computer security. It is the latter that results in news headlines.) In Appendix III, some possible objections to certain points of this paper from the viewpoint of the current QKD literature are answered. Table 1 in Section VIII.B gives a summary comparison of various numerical values.

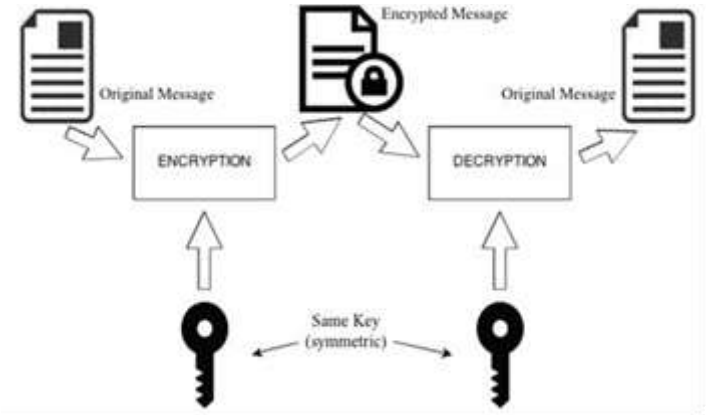
Generally, perfect security cannot be obtained in any key distribution scheme with security dependent on physical characteristics due to system imperfections mixed with the attacker's disturbance, which must be considered in the security model. This is especially the case with QKD, which involves small signal levels. We use the term ``QKD'' in this paper to *refer* to protocols with security depending on information-disturbance trade-offs, excluding those based on other principles such as the ``KCQ'' approach in, which permits stronger signals and for which no general security proof has yet been claimed. In QKD, one can at best generate a key that is close to perfect in some sense. This immediately raises the issue of a security criterion, its operational signifiscance and its quantitative level. Security is very much a quantitative issue. Quantitative security is quite hard to properly de ne and to rigorously evaluate; thus, there are few such results in the literature on conventional mathematics-based cryptography. It is at least as hard in physics-based cryptography, and there is yet no true valid quantisation of QKD security under all possible attacks.

That there are problems and gaps in QKD security proofs has been discussed since 2003 in, Appendixes A and B, Appendix A, and culminating in the numerical adequacy issue in in 2012, which provides the trace distance criterion level for a so-called ``near-perfect'' key. This last numerical adequacy point is emphasized in , and a reply is given in , which in turn is replied to in no further exchange on this topic has resulted. The basic point of is that a trace distance level of is sufficient for security. There have since been several arXiv papers that elaborate upon the several QKD security issues that have yet to be resolved. This paper summarizes and super sedes those papers in a coherent framework for analysing QKD security.

Classical Cryptography Techniques

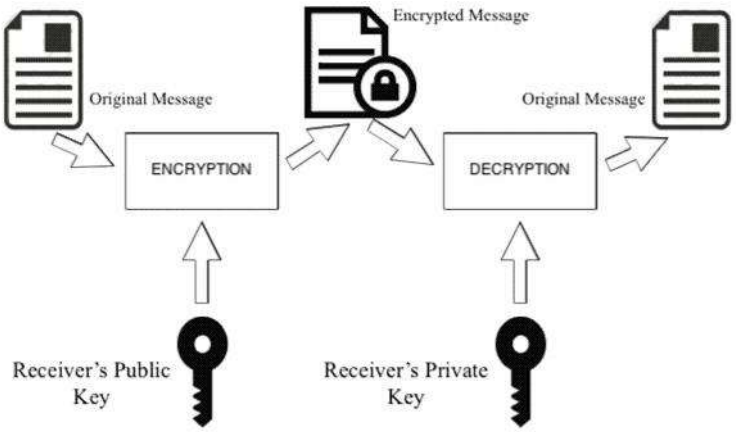
Symmetric Key Cryptography

Cryptosystems that make use of symmetric key distribution use same key for encryption and decryption. This method is also known as secret key cryptography. Secure communication channel in key management is achieved only if the symmetric keys are pre-distributed in to every pair of interactive systems. Fig. 4. Shows the process of symmetric key cryptography



Asymmetric Key Cryptography

Cryptosystems that make use of asymmetric key distribution use a public key system that consists of two parts: a Private key, which is kept secret and a Public key, which is distributed over the network. The sender encrypts the message using the public key of the receiver. The receiver makes use of its private key to decrypt the message. In such a distribution the private key is never in transit and hence less vulnerable to security issues. Fig. 5. Shows the process of asymmetric key cryptography.



Related works

Quantum cryptography is described as a point-to-point secure key generation technology that has emerged in recent times in providing absolute security. Researchers have started studying new innovative approaches to exploit the security of QKD for a large-scale communication system. A number of approaches and models for utilization of QKD for secure communication have been developed.

The uncertainty principle in quantum mechanics created a new paradigm for QKD [21]. One of the approaches for use of QKD involved network fashioned security. BBN DARPA quantum network is an example of such network. Researchers at Boston, Harvard University, and BBN technologies jointly developed the DARPA Quantum Network in 2004 [14]. The main goal was point-to-point Quantum network that exploited QKD technology for end-to-end network security via high speed QKD.

Other approaches and models equipped with QKD in network fashion are introduced in the literature as, A different approach that this paper deals with is using QKD in existing protocols, which are widely used on the Internet to enhance security with main objective of unconditional security. Papers present models and schemes to integrate QKD in classical security protocols like IPsec, PPP and TLS.

Experimental Results and Discussions

Employing the proposed technique, the time requirement for compression-decompression is presented. Also the time requirement for encryption-decryption is presented. Here, plaintexts with different lengths are chosen to depict the result. In both cases, when the size of the data increases, the time requirement also increases and it is easily observable from the figures. It also shows that for the proposed technique, the time requirement of decompression is larger than that of compression while the size of the plaintext increases. It also shows that for the proposed technique, the time requirement of decryption is larger than that of encryption.

Conclusions

The proposed data transmission technique based on QKD along with Huffman coding compression algorithm and OTP enriches the level secrecy and efficiency of the transmitted data. Here to breach the security of ciphertext, the attacker needs to perform all possible combinations of checking before breaching the secrecy of the data which is expected to be quite difficult. The reason is, the decryption of data of the proposed technique relies on the strength of Huffman algorithm, along with OTP in which the key is generated randomly using QKD. For this reason the proposed technique ensures better secrecy and efficiency than other related techniques, and it is powerful against intruders and eavesdroppers. The main concern of this work is to ensure secrecy and efficiency while data transmission. Over the classical channel, the use of OTP makes the data more secure and the use of Huffman algorithm makes the data transmission faster i.e. efficient.

Reference

1. K. S. Kabir, T. Chakraborty, and A.B.M. Alim Al Islam, “SuperCrypt: A Technique for Quantum Cryptography through Simultaneously Improving Both Security Level and Data Rate”, Proc. of 2016 Int. Conf. on Networking Systems and Security, pp. 25-33, 2016.

2. D. Bruss, G. Erdelyi, T. Meyer, T. Riege, and J. Rothe, “Quantum cryptography: A survey,” ACM Computing Surveys (CSUR), Vol. 39, No. 2, pp. 1-27, 2007.

3. W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” Nature, Vol. 299, pp. 802-803, 1982.

4. N. S. Yanofsky and M. A. Mannucci, “Quantum computing for computer scientists,” Vol. 20, Cambridge University Press, 2008.

5. M. Alshowkan, K. Elleithy, A. Odeh, and E. Abdelfattah, “A new algorithm for three-party Quantum key distribution,” in 2013 IEEE 3rd Int. Conf. on Innovative Computing Technology (INTECH), pp. 208-212, August, 2013.

6. A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Physical review letters, 67.6, pp. 661-663, 1991.

7. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proceedings of IEEE Int. Conf. on Computers,Systems and Signal Processing, 1984.

8. Z. Quan and T. Chaojing, “Simple proof of the unconditional security of the Bennett 1992 quantum key distribution protocol,” Physical Review A, Vol. 65, No. 6, p. 062301, 2002.

9. D. Gottesman and J. Preskill, “Secure quantum key distribution using squeezed states,” Physical Review A, vol. 63, p. 022309, 2001.

10. H.-C. Chen, S.-Z. Lin, and T.-L. Kung, "Three-Party Authenticated Quantum Key Distribution Protocol with Time Constraint," in 2012 Sixth Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp. 506-511, 2012.

11. S. Ali, O. Mahmoud, and A. A. Hasan, "Multicast network security using quantum key distribution (QKD)," in 2012 Int. Conf. on Computer and Communication Engineering (ICCCE), pp. 941-947, 2012.

12. X. Zhang and S. Xie, "Three-party quantum secure direct communication base on partially entangled states," in 2011 Int. Conf. on Mechatronic Science, Electric Engineering and Computer (MEC), pp. 1555-1558, 2011.

13. F. Zamani and P. K. Verma, "A QKD protocol with a two-way quantum channel," in 2011 IEEE 5th Int. Conf. on Advanced Networks and Telecommunication Systems (ANTS), pp. 1-6, 2011.

14. R. Sarath, A. S. Nargunam, and R. Sumithra, "Dual channel authentication in cryptography using quantum stratagem," in 2012 Int. Conf. on Computing, Electronics and Electrical Technologies (ICCEET), pp. 1044-1048, 2012.

15. M. Sharma. "Compression Using Huffman Coding," IJCSNS: Int. Journal of Computer Science and Network Security, Vol.10, No.5, May 2010.

16. "Eclipse Luna", Software available ahttps://eclipse.org/luna/,on April 2017.