Hindawi
Security and Communication Networks
Volume 2018, Article ID 8214619, 7 pages
https://doi.org/10.1155/2018/8214619

Research Article

Quantum Cryptography for the Future Internet and the Security Analysis

Tianqi Zhou,[1] Jian Shen ,[1,2] Xiong Li,[3] Chen Wang,[1] and Jun Shen[1]

[1]*Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing, China*
[2]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China*
[3]*Hunan University of Science and Technology, Xiangtan, China*

Correspondence should be addressed to Jian Shen; s_shenjian@126.com

Received 28 December 2017; Accepted 29 January 2018; Published 21 February 2018

Academic Editor: Guojun Wang

Cyberspace has become the most popular carrier of information exchange in every corner of our life, which is beneficial for our life in almost all aspects. With the continuous development of science and technology, especially the quantum computer, cyberspace security has become the most critical problem for the Internet in near future. In this paper, we focus on analyzing characteristics of the quantum cryptography and exploring of the advantages of it in the future Internet. It is worth noting that we analyze the quantum key distribution (QKD) protocol in the noise-free channel. Moreover, in order to simulate real situations in the future Internet, we also search the QKD protocol in the noisy channel. The results reflect the unconditional security of quantum cryptography theoretically, which is suitable for the Internet as ever-increasing challenges are inevitable in the future.

1. Introduction

With the popularization and rapid development of the Internet, human society has entered the information age. Nowadays, all walks of people and all aspects of life can not be separated from the network. In 1990s, the term "cyberspace" was used to represent many new ideas and phenomena in the Internet, networking, and digital communication [1]. Nowadays, this term is used to describe the domain of the global technology environment by experts and researchers of technical strategy, security, government, military, and industry and enterprises. Also, this term is used to refer to anything associated with the Internet. Using this global network, people can engage in all kinds of activities such as communicating ideas, sharing information, providing social support, conducting business, directing actions, creating artistic media, playing games, and engaging in political discussion. Typical applications based on cyberspace include cloud computing [2, 3] and personalized recommender systems [4].

Despite all benefits and advantages of cyberspace, it is regarded as the largest unregulated and uncontrolled field in human history. Therefore, the problem of information security is the primary problem of cyberspace. On the one hand, information technology and industry have entered an unprecedented stage of prosperity. On the other hand, the means of all kinds of attacks emerge in an endless stream. Attacks, like hacker attacks, malicious software invade, and computer viruses, pose a great threat to cyberspace information security. Moreover, the progress of science and technology also poses new challenges to cyberspace security.

Due to the characteristics of the quantum computer, many existing public key cryptography (RSA [5, 6], ELGamal [7], elliptic curve cryptography (ECC) [8], and so on) will be no longer safe in the quantum computer. Namely, the well-known discrete logarithm problem (DLP) or the integer factorization problem will no longer be difficult under quantum computer. This suggests that in order to resist quantum computers, new cryptosystems that are not based on discrete logarithms problem or the large factor decomposition problem should be explored. Only in this way can the information security of cyberspace be ensured in the future Internet.

Taking protective measures at all levels and scope of the network is the basic idea of cyberspace security [9]. These measures aim at detecting and discovering all kinds of network security threats and taking corresponding response actions.

Quantum cryptography is still in its infancy. But we can not ignore the challenges it brings to the security of existing cyberspace. In 1994, mathematician Shor has proposed the quantum algorithm [10] by which the integer factorization problem and the discrete logarithm problem can be efficiently solved in polynomial time. Note that so far researchers have not found the classical algorithm to solve the large integer decomposition and the discrete logarithm problem efficiently under the Turing machine model. Therefore, the challenge of the emergence of quantum computers to the traditional cryptosystems can not be ignored even if it is still in its infancy.

Cryptography and network security are the key technologies to ensure the security of the information system [11]. Quantum cryptography is an important branch of cryptography, which is the combination of quantum mechanics and classical cryptography. The security of communication can be guaranteed by Heisenberg's uncertainty principle and quantum no-cloning theory [12]. The main goal of the study of quantum cryptography is to design cryptographic algorithms and protocols, which is against quantum computing attacks.

As stated previously, exploring quantum cryptographic protocols will be an essential part of cyberspace security issues for future Internet. In this paper, we concentrate on analyzing and exploring the quantum key distribution protocol target for cyberspace security for the future Internet.

1.1. Organization. The rest of this paper is organized as follows. Section 2 introduces some related works about quantum cryptography. Section 3 presents preliminaries of quantum physics and quantum communication. Section 4 presents benefits that quantum cryptography brings to the future Internet and analyze the security of it. Section 5 concludes our paper.

2. Relate Works

Quantum cryptography stems from the concept of quantum money, which was proposed by Wiesner in 1969. Limited by the level of technology in history, this novel and creative idea cannot be realized, which makes it remain unpublished until 1983 [13].

The first practical QKD protocol [14] was proposed by Bennett and Brassard, in 2011. By leveraging single photon polarization, they pioneered the implementation of the quantum key distribution protocol. After that, a lot of effort was put into QKD in order to improve security and efficiency. In 1991, Ekert proposed the protocol [15] that is based on Bells theorem. Note that [15] employs a pair of quantum bits (i.e., an EPR pair), which is essentially the same as [14]. Subsequently, in 1992, the improvement [16] of the scheme [14] was put forward by Bennett. Employing any two nonorthogonal states, the improvement is more efficient and simple. After that, many QKD protocols [17, 18] using the basic principles of quantum mechanics have been proposed successively.

As an important cryptographic basic protocol, the oblivious transfer protocol is one of the key technologies for privacy protection in cryptography [19]. The oblivious transfer protocol is a protocol, where the sender sends many potential information to the receiver, but the sender itself is not aware of the specific content of the transmission. The concept of quantum oblivious transfer (QOT) [20] was fist put forward by Crépeau in 1994. After that, many works have been devoted to the QOT protocol. In 1994, the the "oblivious transfer" security of [21] against any individual measurement allowed by quantum mechanics was proved by Mayers and Salvail in [22]. In 1998, the protocol [23] was proposed, which proves the security of the QOT protocol under an eavesdropper. Other protocols [24, 25] were proposed to improve QOT protocol to varying degrees.

Quantum authentication (QA) protocol is also one of the quantum cryptographic protocols. It was proposed in [26] in 2001. After that, many QA protocols [27, 28] have been proposed one after another.

The quantum cryptography protocol has developed many branches now. In addition to the protocols (i.e., QKD protocol, QOT protocol, and QA protocol) we discussed above, quantum cryptography protocols also include quantum bit commitment (QBC) protocols [29, 30] and quantum signature (QS) protocols [31, 32].

3. Preliminaries

In many respects, quantum communication and information processing are superior to that of classical, which is rooted in the characteristics of quantum information.

3.1. Properties of Quantum Information. Properties of quantum information mainly include uncertainty principle, quantum no-cloning theory, the quantum teleportation, and the hidden characteristics of quantum information, which can be employed to resist attack (passive or active attack [33]) in cyberspace communication.

Heisenberg's uncertainty principle and quantum no-cloning theory [12].

(i) Uncertainty principle: it is known as Heisenberg's uncertainty principle, which was introduced in 1927 by the German physicist Heisenberg [34]. The main idea of uncertainty principle is that the particle position in the micro world is impossible to be determined, and it always exists in different places with different probability.

(ii) Quantum no-cloning theory [12]: quantum no-cloning theory is the uncloned and undeleting properties of the unknown quantum state. Cloning means producing a completely identical quantum state in another system. Scientists have proved that machines capable of replicating quantum systems do not exist [35]. The undeleting principle can guarantee that any deleting and damaging effect of the enemy on the quantum information will leave a trace in secure

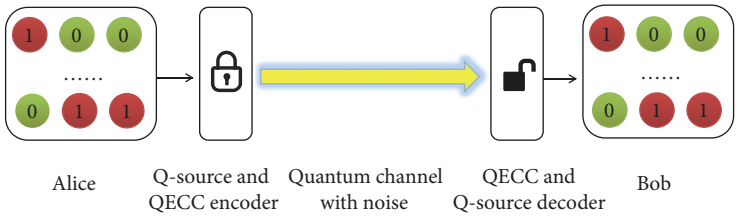

Figure 1: Quantum direct communication model.

communication. It was proposed in [36] in Nature that deleting a copy of an arbitrary quantum state is not allowed by linearity of quantum theory.

(iii) Quantum teleportation: the classic information is obtained by the sender measuring the quantum state of the original, which will be told by the sender in the way of classical communication. Quantum information is the rest of the information that the sender does not extract in the measurement, and it is passed to the recipient by measurement. In 1993, the scheme that teleports an unknown quantum state was proposed in [37].

(iv) Hidden characteristics of quantum information: quantum information has unique properties that classical information does not possess. Specifically, the information of the quantum code in the entangled state can not be obtained by the local measurement operation, which can only be revealed by joint measurement. The works about quantum information concealment was proposed in 2001 by Terhal et al. in [38].

3.2. Quantum Communication System. The quantum communication can be divided into quantum direct communication and quantum teleportation communication. Quantum direct transmission model is the simplest mode to realize the transmission of quantum signals in different places. Figure 1 depicts quantum direct communication model.

In this Figure 1, Alice wants to communicate with Bob through a quantum channel. In the quantum direct transmission model, Alice first needs to produce a series of photons through the preparation device according to the message she wants to share with Bob. After the generation of the quantum source, this information also needs to be processed by quantum source encoder and quantum error correcting code (QECC) encoder. Then, the quantum information can be transmitted directly to the quantum channel (optical fiber or atmosphere). Here, the quantum channel is easily disturbed by external noise. Therefore, the receiver Bob first performs QECC encoding to the received signal and then performs quantum source encoding. Finally, Bob obtains the initial quantum message.

The other quantum communication is the quantum teleportation. Unlike the classical communication, the qubits not only can be in a variety of orthogonal superposition states but also can be in the entangled state. The principle of quantum teleportation is to establish a quantum channel

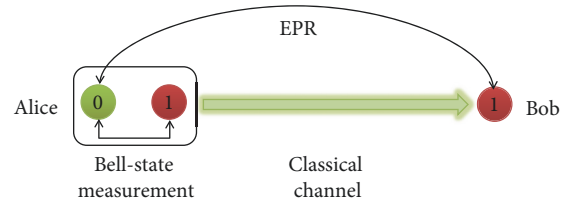

Figure 2: Quantum teleportation.

by using the maximum entangled state of two particles. Then the message is transmitted by the quantum operation. Note that selection of communication channels is the difference between the teleportation and the direct communication. Model of the quantum teleportation is illustrated in Figure 2.

In this model, we depict that Alice who wants to transmit one-bit quantum whit Bob in other place. Firstly, an EPR pair is generated by the EPR entanglement source. Secondly, one of the particles is sent to Alice and the other is sent to the receiver Bob through the quantum channel. Thirdly, in order to transmit information, Alice needs to measure the particles in the EPR entangled pairs and the pending bits she holds. And then, Alice informs Bob of measurement results. Finally, based on the measurement results of Alice and the measurement of the EPR pair of himself, Bob can obtain information about the particles to be transmitted.

4. Quantum Cryptography for Future Internet

Security for cyberspace in the future Internet should be guaranteed as it is the collection of all information systems and the information environment for human survival. For the growing security problem in cyberspace, quantum cryptography becomes the first consideration.

4.1. Unconditional Security. Cable and light are the main carriers of today's Internet communication. This communication system model is shown in Figure 3. Alice and Bob are legitimate users in the system while Eve is an eavesdropper. In order to ensure security, they encrypt messages and then transmit it on the public channel. The classical cryptosystem is roughly divided into two kinds, which are symmetric key cryptosystems and asymmetric key cryptosystems. For these two cryptosystems, their security is mostly based on the complexity of computing. However, the rapid development of hardware equipment and the proposed new advanced algorithms have brought unprecedented challenges to the

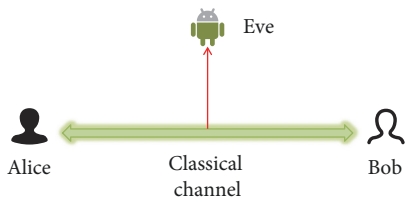

Figure 3: Classical communication model.

Table 1: Measurement results.

Results	Polarization	
	⊕	⊗
Bases		
↔	1	0: 50%; 1: 50%
↕	0	0: 50%; 1: 50%
↗	0: 50%; 1: 50%	0
↖	0: 50%; 1: 50%	1

security of classical cryptosystems. Moreover, the rapid development of quantum computing has also made many difficult problems in classical mathematics have the solvability in the field of quantum physics. For example, the DLP and the integer factorization problem have been solved in [10] in 1994. Therefore, exploring quantum cryptographic protocols will be an essential part of cyberspace security issues for future Internet.

Shannon, the founder of the information theory, made a pioneering study of unconditional security in the 50s of last century [39]. In this study, unconditional security conditions of "one-time-pad" were given. Namely, rather than the pseudo-random number, the encryption/decryption key is real random. And this key is used only once. Furthermore, the key length is equal to the plaintext and performs the exclusive or operation with the plaintext by bit. However, the problem of key distribution at one-time pad has never been solved. It is worth noting that this problem of key distribution can be solved by the principle of quantum mechanics.

Figure 4 illustrates the model of the famous QKD protocol [14].

In this model, sender wants to share a common conference key with his/her counterpart, which can be used to encrypt/decrypt messages they communicate. In this QKD protocol, the real randomness of the key is guaranteed by the essential properties of the quantum: uncertainty principle. Moreover, an attacker is definitely detected if it exists.

4.2. Sniffing Detection. In Figure 3, Alice and Bob exchange information in public channel. In order to ensure confidentiality, their information is encrypted, but they cannot prevent an attacker from eavesdropping on the channel. Moreover, because of the characteristics of the device itself, the eavesdropper can not be detected whether it is in cable communications or in optical fiber communications. In cable communications, the listener can use a multimeter or oscilloscope to monitor. In optical fiber communications, the eavesdropper can get information from a part of the light signal. Note that the fiber loss is influenced by environmental factors, such as temperature and pressure, which makes the loss caused by eavesdropping not be perceived.

In quantum communication, the eavesdropper is sure to be detected owing to quantum no-cloning theory. Specifically, in Figure 4, if an eavesdropper monitors the quantum channel, for a bit of quantum information, he will choose the same measuring base with the sender with a 50% probability. Therefore, the eavesdropper will be detected at a 50% probability for a bit of quantum information. Note that, for the quantum information of n-bit, the probability of the eavesdropper being detected is $1 - (1/2)^n$.

4.3. Security of the QKD. In this subsection, in order to simulate real situations in the future Internet, we first analyze the quantum key distribution protocol in noise-free channel. Moreover, we further search the quantum key distribution protocol in noisy channel.

In order to analysis security of QKD protocol, we list the encoding of quantum information and the measurement results under different measurement bases in Table 1. The two parties agree in advance that the horizontal and oblique downwards polarization represents "1" while the vertical and oblique upward polarization represents "0."

The probability of the existence of a eavesdropper on the QKD protocol is as follows.

$$\Pr = \Pr\left\{\text{Base}_A = \text{Base}_B \wedge \text{Measure}_A \neq \text{Measure}_B\right\}. \quad (1)$$

The probability that the eavesdropper is found for 1-bit quantum information is calculated as $1/2 \times 1/2 \times 1/2 = 1/8$.

Figure 5 illustrates the probability of the eavesdropper being detected in noise-free channel. From the graph we can see that when the number of transmissions exceeds 40, the probabilities of the eavesdropper are close to 100%. While Figure 6 illustrates the probability of the eavesdropper being detected in the channel with 30% noise. The graph shows that when the number of transmitted photons is close to 80, the probability of the eavesdropper being detected is close to 100%. From the above two figures we can conclude that the eavesdropping behavior in quantum communication is certain to be detected. In particular, the more the number of transmission data the higher the probability of the eavesdropper being detected, no matter whether there is noise interference or not.

Figure 7 shows the probability of error in the receiver when the eavesdropper eavesdrops on the channel in different probability. It indicates that the error rate of the receiver is 25% in the absence of eavesdropper, while that of the receiver is about 31% when the eavesdropper monitors the channel with a probability of 50% and that of the receiver rises to about 37% when the eavesdropper monitors every bit of the channel.

Figure 8 shows the eavesdropper being detected when he/she eavesdrops on the channel in different probability. In this picture, the purple line represents that the attacker monitors the channel in the possibility of 100% while the green line and the red line represent that the attacker

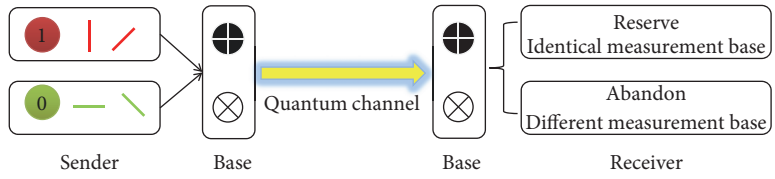

Figure 4: Model of QKD protocol.

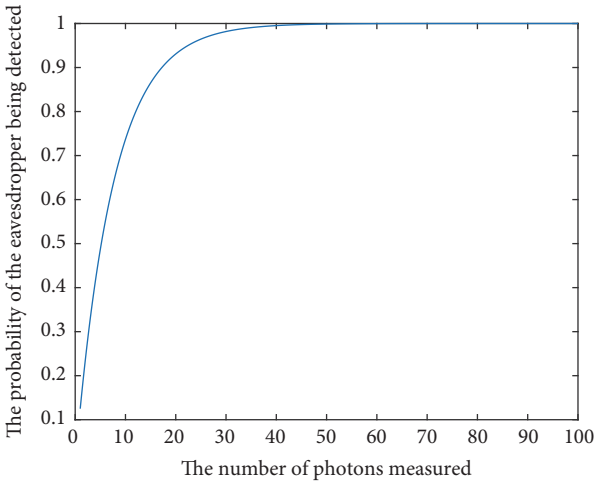

Figure 5: QKD protocol in noise free channel.

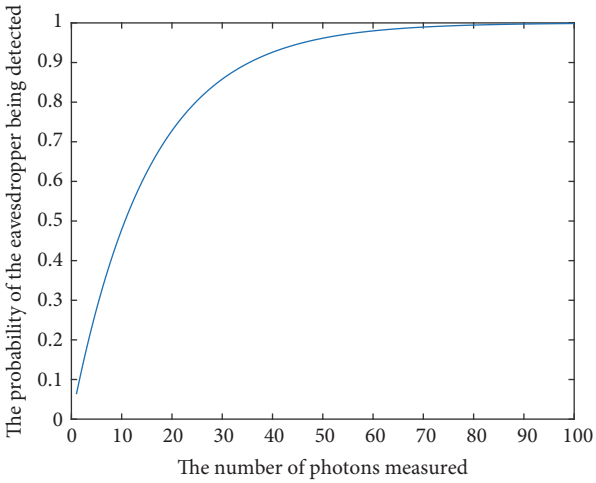

Figure 6: QKD protocol with 30% noise.

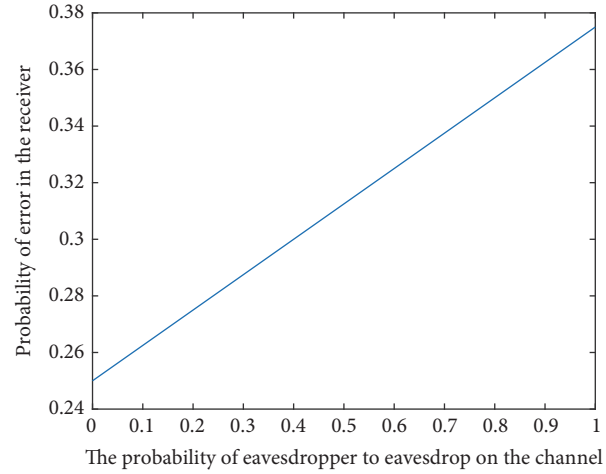

Figure 7: The effect of eavesdropping on the rate of error.

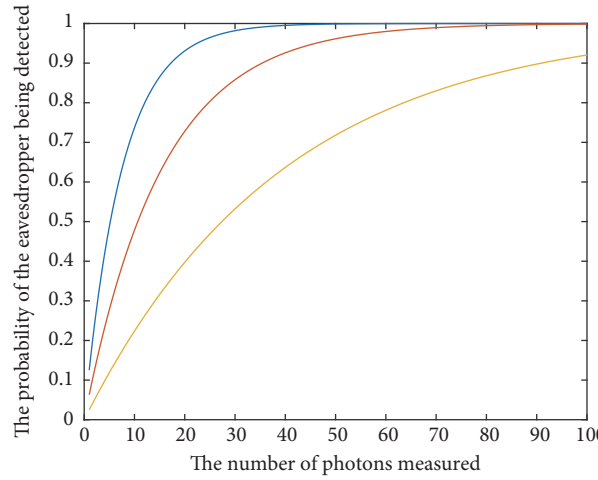

Figure 8: The eavesdropper detects the channel with different probability.

monitors the channel in the possibility of 50% and 20%, respectively. From these three curves, we can observe that regardless of probability of the eavesdrop monitoring the channel, the probability of him/her being detected is nearly 100% as the number of transmitted bits is rising.

From the above discussion, we can conclude that the quantum cryptography offers unconditional security and the sniffing detection properties for secure communication. These properties can ensure security for cyberspace in the future Internet.

5. Conclusion

Based on quantum mechanics and classical cryptography, quantum cryptography is a novel one in the field of cryptography. Compared with classical cryptography, its ultimate advantages are the unconditional security and the sniffing detection. These characteristics can solve cyberspace security critical problem for the future Internet. In particular, quantum cryptography provides security for various applications (e.g., Internet of things and smart cities [40]) in cyberspace

for the future Internet. Our experimental analysis results show the unconditional security and sniffing detection of quantum cryptography, which makes it suitable for future Internet.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Science Foundation of China under Grants no. 61672295 and no. 61672290, the State Key Laboratory of Information Security under Grant no. 2017-MS-10, the CICAEET fund, and the PAPD fund.

References

[1] L. Strate, "The varieties of cyberspace: Problems in definition and delimitation," *Western Journal of Communication*, vol. 63, no. 3, pp. 382–412, 1999.

[2] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," *IEEE Transactions on Information Forensics and Security*, vol. 12, pp. 2402–2415, 2017.

[3] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, 2017.

[4] T. Zhou, L. Chen, and J. Shen, "Movie Recommendation System Employing the User-Based CF in Cloud Computing," in *Proceedings of the 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 46–50, Guangzhou, China, July 2017.

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[6] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and Traceable Group Data Sharing in Cloud Computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 912–925, 2018.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[8] Y.-M. Tseng, "An efficient two-party identity-based key exchange protocol," *Informatica*, vol. 18, no. 1, pp. 125–136, 2007.

[9] J. Shen, T. Miao, Q. Liu, S. Ji, C. Wang, and D. Liu, "S-SurF: An Enhanced Secure Bulk Data Dissemination in Wireless Sensor Networks," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, vol. 10656 of *Lecture Notes in Computer Science*, pp. 395–408, Springer International Publishing, Cham, 2017.

[10] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (SFCS '94)*, pp. 124–134, IEEE, 1994.

[11] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things," *IEEE Internet of Things Journal*, pp. 1-1.

[12] A. Peres, *Quantum Theory: Concepts And Methods*, Springer Science & Business Media, 2006.

[13] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[14] C. H. Bennett and G. Brassard, "WITHDRAWN: Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, 2011.

[15] A. K. Ekert, "Quantum cryptography based on Bellâs theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, 1991.

[16] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters*, vol. 68, no. 21, pp. 3121–3124, 1992.

[17] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Physical Review A: Atomic, Molecular and Optical Physics*, vol. 51, no. 3, pp. 1863–1869, 1995.

[18] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, no. 14, pp. 3018–3021, 1998.

[19] P. Li, J. Li, Z. Huang, C.-Z. Gao, W.-B. Chen, and K. Chen, "Privacy-preserving outsourced classification in cloud computing," *Cluster Computing*, pp. 1–10, 2017.

[20] C. Crépeau, "Quantum oblivious transfer," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2445–2454, 1994.

[21] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer," in *Annual International Cryptology Conference*, pp. 351–366, Springer.

[22] D. Mayers and L. Salvail, "Quantum oblivious transfer is secure against all individual measurements," in *Proceedings of the Workshop on Physics and Computation. PhysComp '94*, pp. 69–77, Dallas, TX, USA.

[23] D. Mayers, "On the security of the quantum oblivious transfer and key distribution protocols," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 963, pp. 124–135, 1995.

[24] S. Winkler and J. Wullschleger, "On the efficiency of classical and quantum oblivious transfer reductions," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 6223, pp. 707–723, 2010.

[25] A. Chailloux, I. Kerenidis, and J. Sikora, "Lower bounds for quantum oblivious transfer," *Quantum Information & Computation*, vol. 13, no. 1-2, pp. 0158–0177, 2013.

[26] M. Curty and D. J. Santos, "Quantum authentication of classical messages," *Physical Review A: Atomic, Molecular and Optical Physics*, vol. 64, no. 6, 2001.

[27] B.-S. Shi, J. Li, J.-M. Liu, X.-F. Fan, and G.-C. Guo, "Quantum key distribution and quantum authentication based on entangled state," *Physics Letters A*, vol. 281, no. 2-3, pp. 83–87, 2001.

[28] D. Zhang and X. Li, "Quantum authentication using orthogonal product states," in *Proceedings of the 3rd International Conference on Natural Computation, ICNC 2007*, pp. 608–612, China, August 2007.

[29] G. Brassard and C. Crépeau, "Quantum bit commitment and coin tossing protocols in," in *Proceedings of the Conference on the Theory and Application of Cryptography*, pp. 49–61, Springer.

[30] N. K. Langford, R. B. Dalton, M. D. Harvey et al., "Measuring entangled qutrits and their use for quantum bit commitment," *Physical Review Letters*, vol. 93, no. 5, Article ID 053601, pp. 1–53601, 2004.

[31] G. Zeng and C. H. Keitel, "Arbitrated quantum-signature scheme," *Physical Review A: Atomic, Molecular and Optical Physics*, vol. 65, no. 4, 2002.

[32] X. Lü and D. Feng, "An Arbitrated Quantum Message Signature Scheme," in *Computational and Information Science*, vol. 3314 of *Lecture Notes in Computer Science*, pp. 1054–1060, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[33] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. PP, no. 99, 2017.

[34] W. Heisenberg, "Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik," in *Original Scientific Papers Wissenschaftliche Originalarbeiten*, pp. 478–504, Springer, 1985.

[35] A. Peres and L. E. Ballentine, "Quantum Theory: Concepts and Methods," *American Journal of Physics*, vol. 63, no. 3, pp. 285-286, 1995.

[36] A. K. Pati and S. L. Braunstein, "Impossibility of deleting an unknown quantum state," *Nature*, vol. 404, no. 6774, pp. 164-165, 2000.

[37] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1899, 1993.

[38] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, "Hiding bits in bell states," *Physical Review Letters*, vol. 86, no. 25, pp. 5807–5810, 2001.

[39] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[40] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," *Pervasive and Mobile Computing*, vol. 41, pp. 219–230, 2017.