Technical University of Varna
Annual Journal
ISSN 2603-316X (Online)
DOI: 10.29114/ajtuv.vol1.iss1.27
Vol.1 Issue 1 (2017):
Published: 2017-12-28

Quantum secure communication models comparison

Georgi Petrov Bebrov[1], *Rozalina Stefanova Dimova*[1]

1-Technical University of Varna, Department of Telecommunications, 9010, 1 Studentska Street, Varna, Bulgaria

Corresponding author contact: g.bebrov@tu-varna.bg

Abstract. *The paper concerns the quantum cryptography, more specifically, the quantum secure communication type of schemes. The main focus here is on making comparison between the distinct secure quantum communication models – quantum secure direct communication and deterministic secure quantum communication, in terms of three parameters: resource efficiency, eavesdropping check efficiency, and security (degree of preserving the confidentiality).*

Keywords: quantum cryptography, quantum secure communication, quantum teleportation, super-dense coding

1 Introduction

Communication, in its general sense, is a sharing of information between two or more parties by any means regardless of the distance. There are two main aspects that ensure the proper communication process. They are information security that involves CIA (Confidentiality, Integrity, Availability) (Nieles, 2017) and reliability. In the following, we shall consider ourselves only with the security, in particular, the confidentiality. A solution to the confidentiality problem in communication systems is the encryption of the sharing data during its transfer, i.e., making use of cryptographic primitives in the communications.

In the world of classical cryptography, one can distinguish two main classes of cryptographic primitives: symmetric and asymmetric (Stallings, 2017). Aside from their assets though, these types of primitives have substantial drawbacks, which could lead to compromising the confidentiality of communication systems. The problem of symmetric cryptography is related to not having reliable key distribution, whereas the problem of the common asymmetric cryptography is not the key distribution, but not being quantum-resistant, that is, it can be easily broken by algorithms run on quantum computers. However, there exist classical crypto methods not having such drawbacks, i.e., being assumed to be completely secure (Cheng, 2017). Although secure nowadays, the latter, for their being computational-complexity-based, could in some future instant of time be broken by discovering appropriate algorithms.

Luckily, alongside the quantum computing, the field of quantum cryptography has blossomed as well. The latter could be even resistant to possible quantum attacks, that is to say, it is the only known technique at this time that provides an unconditional privacy in data transfer. As opposed to its classical counterpart, the quantum cryptography secureness is due to its utter reliance on the physical laws governing the microscopic world of fundamental particles (e.g. photons). In order to break the cryptography of this kind, one has to get over the laws of Nature, an action unlikely to be done.

This kind of cryptography consists in using fundamental particles as data carriers. The information is encoded into the properties of the particles, which manifest quantum character whose fuzziness and strangeness provide uncracking masquerade of the data. In addition to that, the quantum cryptography has the advantage over its classical counterpart in that it is able to not only conceal the information transmitted over an insecure channel but also to reveal the presence of an unauthorized person, an eavesdropper, in a communication link. That is why, for the two reasons just mentioned, the quantum cryptographic primitives are regarded as probably the most powerful tool against any kind of attacks known to date.

In general, there exist two main types of quantum primitives – quantum secure communication (QSC) and quantum key distribution (QKD), which are considered in Section 2. Particular attention will

Technical University of Varna
Annual Journal
DOI: 10.29114/ajtuv.vol1.iss1.27
Vol.1 Issue 1 (2017):
Published: 2017-12-28
ISSN 2603-316X (Online)

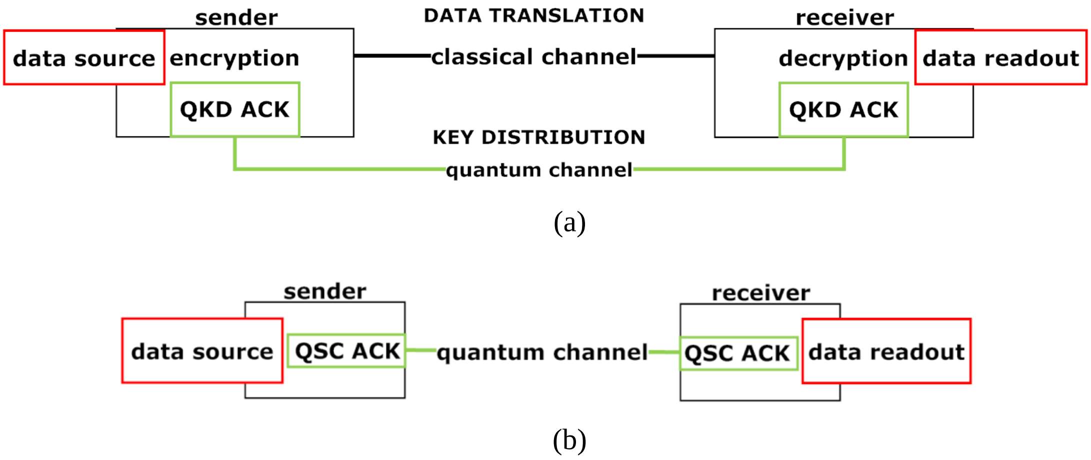
be paid on QSC systems, as the latter will be classified and analyzed. The main idea of the paper, however, is presenting a comparison between the different classes of QSC with respect to three parameters: resource efficiency, check efficiency, and security, as shown in Section 3.

2 Quantum primitives

All in all, these primitives are quantum communication processes between two or more parties following a certain sequence of steps: (i) establishing a quantum channel, (ii) performing eavesdropping check, (iii) data translation over the quantum channel secured.

Clearly, the protagonist in the foregoing steps is the quantum channel, which is a set of devices and systems, whereby quantum systems (fundamental particles) are conveyed; one system at a time. For the quantum particles used in the quantum communications are photons, the quantum primitives can be deployed into the already installed telecommunication optical resource, but with one exception: in some cases, the terminal devices that are to be used for implementing quantum communications have to be of one-photon type (Bebrov, 2017), (Diamanti, 2016). Establishing a quantum channel means sharing quantum particles between two or more parties. Eavesdropping check, in turn, is a supplementary process included into the primitives so as to be verified whether or not the quantum channel is intercepted. Whereas data translation consists in transferring, processing and reading out the information encoded into the quantum systems conveyed over the quantum channel.

Based on the above-stated points, the most common and prominent quantum primitives existing to date have been developed: the quantum key distribution (Bebrov, 2017; Diamanti, 2016) and quantum secure communication (Long, 2007). The QKD is the process of securely sharing a key between parties in a quantum way, i.e., transferring the key information particle by particle, as shown in Fig.1a. In turn, the QSC is the process of quantum data transfer in a secure fashion. In the latter the communication does not resort to encryption/decryption procedures, the translation of information is performed in a direct manner, as shown in Fig.1b.



(a)

(b)

Fig. 1. General block schemes of (a) quantum key distribution and (b) quantum secure communication.

In Fig.1, QSC ACK and QKD ACK are sets of devices facilitating the implementation of (i, ii, iii), i.e., detection, generation, processing of quantum particles, and acknowledgment of the quantum channel security, for the needs, respectively, of QSC and QKD.

Though both QKD and QSC provide security as great as the other, they could introduce a delay to the information transfer due to their exhaustive eavesdropping check procedures. That especially holds for QKD-involved communications having not only check procedure but also encryption and decryption processes, which further roll out in time the communication process. For this reason, QSC-involved communication is thought to be more efficient with respect to the time frame, i.e., not as cumbersome as QKD-involved one. So, in the lines hereafter we shall concentrate on QSC type of schemes, which draw more and more attention in the recent years.

Up to the present relatively many schemes for quantum secure communication have been worked out (Hassanpour, 2015; Joy, 2017; Liu, 2013; Long, 2007; Yan, 2004; Zhang, 2017), taking into account the fact that the field of quantum communication is really juvenile.

In QSC, (iii) can be realized in two ways: (*) entirely quantum translation; (**) quantum translation supported by classical one. In this regard, QSC is divided into two classes of protocols, as shown in Fig.2: quantum secure direct communication (QSDC) (Liu, 2013; Long, 2007; Zhang, 2017) for which (*) holds, and deterministic secure quantum communication (DSQC) (Hassanpour, 2015; Joy, 2017; Yan, 2004) for which (**) holds. In other words, in the former the message to be kept in secret is directly translated over a quantum communication channel, that is, a transmission without resorting to encryption and auxiliary classical channels, whereas in the latter the secret message translation resorts to using at least 1-bit auxiliary classical channel.

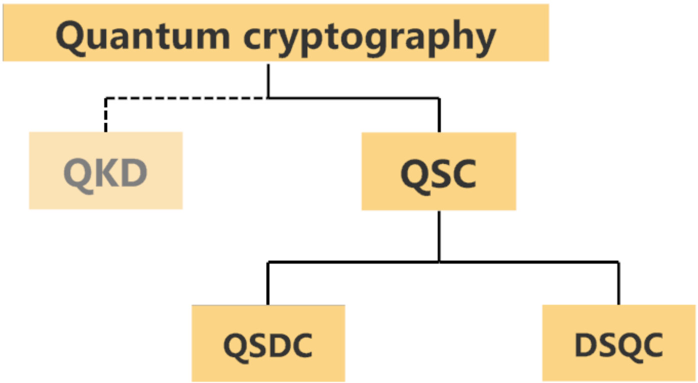


Fig. 2. General classification of quantum secure communication schemes.

3 Comparison of distinct quantum secure communication models

In order to make the comparison between the two kinds of quantum secure communication models, we shall first choose a representative for each one and then contrast them. The differences between the protocols will be evaluated by three factors to be introduced in the section. This will enable us to make inference about which kind of QSC is more appropriate

To begin with, it is the representative of each kind of QSC that we wish to specify before comparing the two distinct models. For QSDC a superdense coding scheme (Liu, 2013; Wang, 2005) in its simplest form (when two qubits are used) is chosen. It is a consecutive transfer of quantum systems, as between two transfers an eavesdropping check takes place. It turns out that this type of scheme is the most eminent. For DSQC a teleportation scheme (Yan, 2004) is chosen, as the most significant. It is an information transfer without resorting to actual translation of the quantum systems carrying the data. For such information process to be achieved an interaction between the carrying system and the quantum channel must be executed as well as an auxiliary classical is to be availed of. The eavesdropping check is performed before putting into effect the interaction just mentioned. There exist different types of teleportation schemes such as those reviewed in (Joy, 2017; Yan, 2004), which are defined by their features: type of quantum channel, amount of information transferred per one procedure, number of check processes per one procedure. Since the different features lead to different efficiencies, the teleportation schemes are assumed to differ mainly in efficiency, as can be seen in (Joy, 2017). Therefore, we pick as a representative of the direct secure quantum communication class the superior one in this respect, that is, the setup introduced in (Joy, 2017).

The comparison consists of evaluating and contrasting the different protocols in terms of three parameters – resource efficiency, check efficiency, and security, as shown along the following lines of this section.

DOI: 10.29114/ajtuv.vol1.iss1.27
Vol.1 Issue 1 (2017):
Published: 2017-12-28
ISSN 2603-316X (Online)

3.1 Resource efficiency

The resource efficiency is an important economic factor having an important role in one's choosing an appropriate model for deployment in practice. For quantum secure communication protocols, this efficiency is defined by the ratio of securely translating amount of information to the amount of quantum resources and classical ones supporting them, if there are any, necessary for secure communication to be attained. Therefore, it is given by the expression (Cabello, 2000; Joy, 2017)

$$\eta_r = b_s/(q_t + b_t), \tag{1}$$

where b_s being the secure information, in bits, translated, q_t and b_t being the qubits and bits, respectively, used to facilitate sending b_s in a secure manner. Having presented this factor, let us now evaluate it for the different QSC models so that we could compare them. In accordance with (Long, 2007), we find for the super-dense coding (QSDC representative) that its resource efficiency resides in the value 1, i.e., the maximally possible one. Accordingly, based on (Joy, 2017) we obtain for the teleportation-based scheme (DSQC representative) a resource efficiency of 0.4 (40%).

So, taking into account the above, we can arrive at that in this respect QSDC is assumed to significantly excel DSQC, i.e., the former is much more economically efficient than the latter. This is due to the fact that the QSDC schemes exploit only quantum channels, unlike DSQC in which both quantum and classical channels are involved in the process of secure information translation.

3.2 Check efficiency

Since the eavesdropping check process plays an important role in every quantum secure communication protocol, it would be of great benefit for one to be able to assess the efficiency of the distinct protocols with regard to this process in order to contrast them. To do so, in the following, we shall introduce a parameter giving an account of the extent to which a particular protocol has an efficient check process performance.

The parameter of concern, denoted by η_c, is defined by the ratio of the number of bits transferred in the (overall) secure communication, n_b, to the number of check processes carried out, n_c. That is, it is given by

$$\eta_c = n_b/n_c \tag{2}$$

and called *check efficiency*. Let us now make the comparison of QSDC and DSQC protocols with regard to this efficiency, as we calculate the latter for the two cases: super-dense coding and teleportation-based scheme. According to (Long, 2007), as can be easily verified, the super-dense coding protocol has check efficiency of value 1. For the teleportation-based DSQC (Joy, 2017) this type of efficiency resides in the same value – for securely transferring two bits of information, two check procedures are necessary.

So, with respect to the parameter recently introduced here DSQC and QSDC can be assumed to be on equal terms.

3.3 Security

Previously, we evaluated and contrasted the efficiencies of different types of secure quantum communication. Let us now proceed with the security of the distinct models.

Providing information security in the quantum communications is based mainly on eavesdropping check process. As said earlier, it enables detecting the presence of an intruder in quantum communication connection. The security is more precisely determined by whether the check process is effective and implemented at the right time. QSDC is a scheme in which the secure communication is achieved by modulating the quantum channel with respect to the information desired to be conveyed over it, whilst DSQC is a scheme in which the secure communication is achieved by modulating quantum systems interacting with the quantum channel. Modulating the quantum system, we are able then to modulate the channel by carrying out the interaction between the system and the channel. The advantage here is that the information translation can be executed after doing eavesdropping check of the channel. It is known that both modulations enable effective check processes to be carried out, that is, a detection of intruders is possible regardless of the attacks they launch (Joy, 2017). However, the second condition – well-timed check implementation – for a quantum communication to be secured is not fulfilled by the QSDC protocols (Long, 2007). That being the case, because in QSDC only two out of the three processes inherent to quantum communication procedure are implemented: in a somewhat extent (ii) and (iii) are combined, that is, they are executed together. This, on one hand, leads to higher resource efficiency, but, on the other hand, also to dropping off the level of security to some extent. For this reason, the QSDC is assumed to be less secure on account of that it does not allow thorough performing the eavesdropping check before the data to be translated. To put it simply, there is liable to be information leakage in performing QSDC protocols.

3.4 Conclusions

In brief, as summarized in Table 1, we have found that QSDC excels DSQC in resource efficiency, which is a really important parameter in economic terms and is on par with the latter in terms of check efficiency, it fails in security. On the ground that in the cryptographic world the secureness of a scheme is of utmost importance, we are thus forced to conclude that even though QSDC may seem superior, DSQC is a more satisfactory model. This is justified by the fact that it shines brighter in the most important task the primitives are made for – preserving the confidentiality of communications.

Table 1. Comparison summary.

Resource efficiency η_r	**Check efficiency η_c**	**Security**
Superdense coding (QSDC) >> Teleportation (DSQC)	QSDC = DSQC	QSDC < DSQC
1 >> 0.4	1 = 1	Leakage of information is probable in QSDC

4 Summary

In short, we present in a brief manner the existing prominent quantum tools, in particular, the quantum secure communication models, for confidentiality preservation. Also, we compare the existing distinct quantum secure communication schemes in terms of three factors. In doing so, we arrived at the conclusion that DSQC is better than QSDC, for the reason that the former provides greater information security, more precisely, privacy, though it is not as efficient as the latter.

Based on the foregoing, in our future work, we intend to concentrate on working out a direct secure quantum communication protocol being both secure and efficient, as its resource efficiency approaches that of quantum secure direct communication models.

References

Bebrov, G., Dimova, R., & Pencheva, E. (2017). Quantum approach to the information privacy in Smart Grid. Optimization of Electrical and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP), Brasov, Romania, 971–976. doi:10.1109/OPTIM.2017.7975096

Cabello, A. (2000). Quantum key distribution in the Holevo limit, *Physical Review Letters*, 85(26 Pt 1), 5635-8. doi:10.1103/PhysRevLett.85.5635

Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a quantum world. *IEEE Communication magazine,* 25(2), 116–120. doi:10.1109/MCOM.2017.1600522CM

Diamanti, E., Lo, H., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution, *NPJ Quantum Information* 2, 16025. doi:10.1038/npjqi.2016.25

Gao, T. (2004). Efficient controlled quantum secure direct communication based on GHZ-like states. *Quantum Information Processing*, 14(2), 739–753. doi:10.1007/s11128-014-0866-z

Hassanpour, S. & Houshmand, M. (2015). Efficient controlled quantum secure direct communication based on GHZ-like states. *Quantum Information Processing*, 14(2), 739–753. doi:10.1007/s11128-014-0866-z

Joy, D., Surendran, S., & Sabir, M. (2017). Efficient Deterministic Secure Quantum Communication protocols using multipartite entangled states. *Quantum Information Processing*, 16(6), 1–11. doi:10.1007/s11128-017-1613-z

Liu, Z., Chen, H., Liu, W., Xu, J., Wang, d., & Li, Z. (2013). Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states. *Quantum Information Processing*, Volume 12, Issue 1, 587-599. doi:10.1007/s11128-012-0404-9

Long, G., Deng, F., Wang, C., Li, X., Wen, K., & Wang, W. (2007). Quantum secure direct communication and deterministic secure quantum communication. *Frontiers of Physics in China*, Volume 2, Issue 3, 251–272. doi:10.1007/s11467-007-0050-3

Nieles, M., Dempsey, K., & Pilliteri, V. (2017). An introduction to Information Security. *NIST Special Publication* 800-12, U.S. Department of Commerce. doi:10.6028/NIST.SP.800-12r1

Stallings, W. (2017). *Cryptography and Network Security*. *Principles and Practice*. Global Edition, Pearson Press.

Wang, C., Deng, F., Li, Y., Liu, X., & Long, G. (2005). Quantum secure direct communication and deterministic secure quantum communication. *Physical Review A*, Volume 71, Issue 4, 044305. doi:10.1103/PhysRevA.71.044305

Yan, F., Zhang, X. (2004). A scheme for secure direct communication using EPR pairs and teleportation. *The European Physical Journal B* 41, 75–78. doi:10.1140/epjb/e2004-00296-4

Zhang, W., Ding, D., Sheng, Y., Lan, Z., Shi, B. & Guo, G. (2017). Quantum secure direct communication with quantum memory. *Physical Review Letters*, Volume 118, Issue 22, 220501. doi:10.1103/PhysRevA.118.220501