International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:13, No:2, 2019

Proposal of Optimality Evaluation for Quantum Secure Communication Protocols by Taking the Average of the Main Protocol Parameters: Efficiency, Security and Practicality

Georgi Bebrov, Rozalina Dimova

***Abstract*—**In the field of quantum secure communication, there is no evaluation that characterizes quantum secure communication (QSC) protocols in a complete, general manner. The current paper addresses the problem concerning the lack of such an evaluation for QSC protocols by introducing an optimality evaluation, which is expressed as the average over the three main parameters of QSC protocols: efficiency, security, and practicality. For the efficiency evaluation, the common expression of this parameter is used, which incorporates all the classical and quantum resources (bits and qubits) utilized for transferring a certain amount of information (bits) in a secure manner. By using criteria approach whether or not certain criteria are met, an expression for the practicality evaluation is presented, which accounts for the complexity of the QSC practical realization. Based on the error rates that the common quantum attacks (Measurement and resend, Intercept and resend, probe attack, and entanglement swapping attack) induce, the security evaluation for a QSC protocol is proposed as the minimum function taken over the error rates of the mentioned quantum attacks. For the sake of clarity, an example is presented in order to show how the optimality is calculated.

***Keywords*—**Quantum cryptography, quantum secure communcation, quantum secure direct communcation security, quantum secure direct communcation efficiency, quantum secure direct communcation practicality.

I. Introduction

THE application of quantum mechanics to the field of telecommunications gives rise to the so-called quantum communications. It appears to be an important area of research in the modern and future information age due to the influx of focusing on the quantum computing, which enforces the emergence of quantum technologies into the communications. To be more precise, the uprise of quantum computing leads to the burst of quantum cryptography. The latter is concerned with transferring information in a confidential manner based on the laws of quantum physics. The most common and well-known representatives of this field are the quantumkey distribution (QKD) and quantum secure communication (QSC). The former offers reliable sharing of a secret cryptographic key between two parties before their communication, so that confidential data transfer could subsequently take place.

Georgi Bebrov is with the Technical University of Varna, Bulgaria (e-mail: g.bebrov@tu-varna.bg),
Rozalina Dimova is with the Technical University of Varna, Bulgaria (e-mail: rdim@abv.bg).

The latter achieves communication secureness without resorting to cryptographic tasks, i.e. encryption/decryption and key distribution are not needed. QSC, in turn, is divided into two branches: quantum secure direct communication (QSDC) [1]-[7] and deterministic secure quantum communication (DSQC) [1], [8], [9]. In the former, the message to be kept in secret is directly translated over a quantum communication channel, that is, a transmission not resorting to encryption and auxiliary classical channels. On the other hand, in the latter the secret message translation resorts to using at least 1-bit auxiliary classical channel.

In attempting to judge the success of a QSC model, we may ask ourselves three questions: (1) "Is the protocol secure?", (2) "Is the protocol efficient?", and (3) "Does the protocol rely on practical setup?". So, only in the case when positive answers are given to these question we may say that a model is satisfactory, optimal. That is, in order to determine whether a QSC protocol is optimal, we should first answer to the above three questions. Answers to the questions could be given by means of the three parameters: *efficiency* that is judged by the amount of resources used to transfer given amount of information; *security* that is judged by the extent to which a scheme is liable to existing attacks or could be more precisely defined by the probability of detecting the presence of an eavesdropper; and *practicality* that is judged by the complexity of the given model and the devices used for its realization. In terms of the efficiency of QSC protocols, there is a common evaluation proposed by [10]

$$E = \frac{b_s}{q_t + b_t}, \tag{1}$$

b_s being the information, in bits, sent from sender to receiver; q_t and b_t being the qubits and bits, respectively, used to facilitate sending b_s in a secure manner. However, there are no general, straightforward "answers" (evaluations) for the security and practicality – evaluations convenient for common use. As in the case of security and practicality, there does not exist an "answer" to the question "Is the protocol optimal?", i.e., there is no general optimality evaluation for QSC protocols (an evaluation incorporating all the parameters that characterize a protocol) by means of which we could completely evaluate and compare all the existing QSC protocols. For the latter reasons, in the current paper we aim to present general, straightforward evaluations for the security,

practicality and optimality of QSC protocols.

The paper is organized as follows. In Section II, the expressions for the security, practicality, and optimality evaluations are sequentially given. Also, in the end of the section, an example is shown of how the optimality of a QSC protocol is calculated. The conclusions are set out in Section III.

II. Optimality Evaluation of QSC Protocols

In order to present the optimality evaluation of QSC protocols, we first introduce the expressions for evaluation of both the security (Section II.A) and practicality (Section II.B). For the sake of clarity, we end up the section with an example that demonstrates how the optimality of a QSC protocol is calculated.

A. Security Evaluation

Up to the present the only characteristic that we have considered on a QSC and described by an expression is the efficiency. We shall now go on to discuss the security for a general QSC model and in that connection it will be defined in terms of both the classical and quantum channels.

In general, for a QSC protocol to be secure, it has not to succumb to both quantum and classical channel attacks. For the evaluation of quantum channel succumbing we subject the given QSC protocol to common attacks (Measure and resend attack, Intercept and resend attack, Probe attack, Entanglement swapping attack) [8], [9] in order to verify whether or not the scheme is secure and to what extent it is secure — what is the probability of detecting the presence of an eavesdropper. Besides the quantum channel, both the auxiliary classical channel (in DSQC models) and classical channel used for check procedures could also pose a threat, thus giving rise to information leakage to somewhat extent.

Being unevaluated mathematically so far in a general and straightforward manner, along the following lines of this section the security in terms of both quantum and classical channels is aimed to be examined and expressed.

1) Classical Channel Security: Loophole in the classical channel (auxiliary or public one) and its evaluation:

The loophole occurring is that an eavesdropper could gain information about the data transferred over the quantum channel, when monitoring the auxiliary or public classical channel. If we assume that the quantum channel is completely secure, that is, the eavesdropper does not have access to the quanta shared, his/her only option is to monitor the classical channels (auxiliary or public one). In general, not knowing the content of data running through an informational (quantum) channel, one has the only option — to pick out in a random way one of the possible data sequences that the message is presented by (e.g., 0 and 1). For example, suppose the data transferred is 00. Being unaware of the data content, but aware of the length of a data sequence, one could give oneself a try to guess the original bit sequence. In this case, the probability of occurring a positive outcome out of this trial for the eavesdropper is 1/4 or 25%, because there are four possible sequences of length two and from eavesdropper's standpoint they are equiprobable. That is, the entropy in the eavesdropper's informational frame of reference is

$$H_e = -\sum_{i=1}^{4} p(x_i)\log_2 p(x_i) = -\log_2 \frac{1}{4} = 2\,\text{bits}, \quad (2)$$

where $p(00) = p(01) = p(10) = p(11) = 0.25$. The problem posed here is the fact that there is a classical channel tightly related to the data transfer, which can be wiretapped in an unhindered manner by an eavesdropper.

Let us now observe a case in which the eavesdropper wiretaps the classical channel only (i.e., launches classical channel attack) for a two-bit procedure of a QSC protocol. Here, knowing the information passing through the classical channel, it is possible for the eavesdropper to be aware of the fact that only two two-bit information sequences can occur in the procedure, for instance, the probabilities of '01' and '10' to occur are $p(01) = p(10) = 0.5$. That is, unaware of the quantum procedure, one gains some information about the data transferred. Thus, in this case for the entropy of the eavesdropper we get

$$\begin{aligned} H'_e = &-\sum_{i=1}^{4} p(x_i)\log_2 p(x_i) = \\ &- p(00)\log_2 p(00) - p(01)\log_2 p(01) \\ &- p(10)\log_2 p(10) - p(11)\log_2 p(11) \\ = &-0\log_2 0 - 0.5\log_2 0.5 - 0.5\log_2 0.5 - 0\log_2 0 = 1\,\text{bit}. \end{aligned} \quad (3)$$

Therefore, comparing this result to the above one (2), it is evident that H_e falls out from its maximum. Accordingly, this means that the uncertainty about the data bit sequence obtained for the latter case is lower than the former one. As can be readily seen, the H_e decreases by a factor of two:

$$\frac{H'_e}{H_e} = \frac{1}{2}. \quad (4)$$

Hence, this ratio can be used to evaluate the security of a QSC model in the presence of classical channel attack. So, let us call it *classical channel immunity* and denote it by χ, i.e.,

$$\chi = \frac{H'_e}{H_e}, \quad (5)$$

where H'_e is the entropy when eavesdropper monitors the classical channel and H_e is that when the eavesdropper does not observe the classical channel.

2) Quantum Channel Security: Generally, the security of the QSC in terms of the quantum channel attacks is evaluated with regard to the robustness against quantum attacks (e.g., Measure and resend attack, Intercept and resend attack, Probe attack, Entanglement swapping attack [8], [9]) — the protocol is either secure or insecure, depending on whether or not it is resilient to the attacks. In other words, the security could be in this way evaluated by 0 (insecure) and 1 (secure). To make the evaluation more granular, we resort to utilizing the fact that the security is conditioned by the statistical nature of the process of detecting eavesdroppers. Therefore, the expression defining to what extent a quantum channel is secure can be

given by the lowest value of the error rates (ER) expected each quantum attack to evoke, that is,

$$\lambda = \min(ER_k), [\%] \tag{6}$$

where k is the number of quantum attacks taken into account.

3) Overall Security: In this work, the overall security of a quantum secure communication protocol is proposed to be evaluated by the following expression

$$\Sigma = \frac{\chi + \lambda}{2}, \tag{7}$$

i.e., as the average taken over the classical and quantum channels securities.

B. Practicality Evaluation

The approach to evaluate the practicality of a quantum secure communication is the following. It consists in determining whether or not a quantum secure communication protocol meets the criteria:

- c_1: usage of exotic (special) quantum state in a QSC protocol. For instance, the states used both for quantum channels and data quantum systems (quantum systems carrying the information) in [8].
- c_2: usage of more than one type of quantum channel in a QSC protocol (i.e., using more than one type of quantum channel to transmit a message). For example, using both single-qubit and two-qubit channels to transmit binary information in a protocol. The latter requires the utilization of two quantum sources. Another example is the case in which two or more quantum channels are used in a protocol, which differ from one another by a quantum operation or quantum operations (performing quantum gates) – Hadamard gate is an exception.
- c_3: usage of additional classical operation in a QSC protocol, which requires deploying certain classical device. An example of an additional classical operation is the process of encoding. As is known, it requires the realization of an encoder, whose presence leads to decrease in the practicality.

The criteria can be represented by a binary vector. For we have three criteria, the vector is composed of three elements

$$\mathbf{c} = c_i = [c_1\ c_2\ c_3],$$

where i runs from 1 to 3. Because the vector is of binary type, each element of it could either be '0' or '1'. In this representation, the binary digit '0' is assigned to a criterion when it is met and the binary digit '1' is assigned to a criterion when it is not met by a QSC protocol. Using the above criteria approach, the practicality can be mathematically represented by the expression

$$\xi = \sum_{i=1}^{n} \frac{1}{n} \cdot c_i. \tag{8}$$

It is evident from Equation (8) that the possible values of the practicality lie within the interval $[0, 1]$, i.e., $\xi \in [0, 1]$.

C. Optimality Evaluation of QSC Protocols

The optimality incorporates the efficiency E, the security Σ, and the practicality ξ of a QSC model (protocol). It is evaluated as follows

$$\zeta = \frac{E + \Sigma + \xi}{3}. \tag{9}$$

That is, the optimality is the average taken over all the three main parameters of a QSC. Because $E \in [0, 1]$, $\Sigma \in [0, 1]$, and $\xi \in [0, 1]$, the optimality also lies within the interval $[0, 1]$.

In the following lines of the section, we present an example that clarifies the process of calculating the optimality of a QSC protocol – the optimality of the protocol [3] is evaluated.

Example of optimality evaluation:

1) Efficiency: Taking into account the evaluation [10] and the efficiency analysis introduced in [3], the efficiency of the protocol proposed by Deng et al. is

$$E = \frac{b_s}{q_t + b_t} = \frac{2}{2 + 0} = 1. \tag{10}$$

2) Practicality: The protocol [3] is characterized with the following features:

- The protocol does not utilize exotic (special) quantum channel [3] – it utilizes Bell state quantum channel.
- The protocol uses only one type of quantum channel for transferring information – Bell state quantum channel.
- There is no additional classical operation in the protocol.

Therefore, according to Equation (8) and the criteria approach given in Section II.B, the practicality of the protocol [3] is

$$\xi = \frac{1}{3} \cdot 1 + \frac{1}{3} \cdot 1 + \frac{1}{3} \cdot 1 = 1. \tag{11}$$

3) Security: We shall now consider the security of the protocol proposed in [3] with respect to four common quantum attacks: Measure and resend attack, Intercept and resend attack, Probe attack, and Entanglement swapping attack.

Measure and resend attack. Here the eavesdropper, conventionally called Eve, captures the particles from the travel groups of the sender, Alice, measures them and then resends them to the recipient, Bob. If the decoys are prepared both in $(+)$ or $(\times)$ basis, Eve conducts measurements on the intercepted by her particles in $(+)$ or $(\times)$ chosen at random. Being of unknown to Eve state, each particle intercepted by her is then characterized by the well-known expressions

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \text{ when Eve uses } (+), \tag{12}$$

$$|\psi\rangle = \alpha\,|+\rangle + \beta\,|-\rangle \text{ when Eve uses } (\times), \tag{13}$$

where α and β — probability amplitudes, display the statistics of the states. In the case now considered, the statistics depends on the state in which the particle is generated (sent), or more precisely, on the basis in which is sent. For instance, given $(+)$ is used by Eve and the particle intercepted is sent in the $(+)$ basis, then either α or β is unity, i.e. $\alpha = 1, \beta = 0$ or $\alpha = 0, \beta = 1$. However, if it is sent in $(\times)$ basis, then $|\alpha| = |\beta| \rightarrow |\alpha| = |\beta| = 1/\sqrt{2}$. Taking into consideration the

above lines, we could summarize for the instance when $(+)$ basis is used by Eve the following

$$|0\rangle \rightarrow |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{\text{measuring}} |0\rangle\,; \alpha = 1, \beta = 0$$
$$|1\rangle \rightarrow |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{\text{measuring}} |1\rangle\,; \alpha = 0, \beta = 1$$
$$|+\rangle \rightarrow |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \xrightarrow{\text{measuring}} |0\rangle \text{ or } |1\rangle\,; \alpha = \frac{1}{\sqrt{2}} = \beta$$
$$|-\rangle \rightarrow |\psi\rangle = \alpha\,|0\rangle - \beta\,|1\rangle \xrightarrow{\text{measuring}} |0\rangle \text{ or } |1\rangle\,; \alpha = \frac{1}{\sqrt{2}},$$
$$\beta = -\frac{1}{\sqrt{2}}. \quad (14)$$

But, if Eve uses $(\times)$ basis, then the following occurs

$$|+\rangle \rightarrow |\psi\rangle = \alpha\,|+\rangle + \beta\,|-\rangle \xrightarrow{\text{measuring}} |+\rangle\,; \alpha = 1, \beta = 0$$
$$|-\rangle \rightarrow |\psi\rangle = \alpha\,|+\rangle + \beta\,|-\rangle \xrightarrow{\text{measuring}} |-\rangle\,; \alpha = 0, \beta = 1$$
$$|0\rangle \rightarrow |\psi\rangle = \alpha\,|+\rangle + \beta\,|-\rangle \xrightarrow{\text{measuring}} |+\rangle \text{ or } |-\rangle\,; \alpha = \frac{1}{\sqrt{2}} = \beta$$
$$|1\rangle \rightarrow |\psi\rangle = \alpha\,|+\rangle - \beta\,|-\rangle \xrightarrow{\text{measuring}} |+\rangle \text{ or } |-\rangle\,; \alpha = \frac{1}{\sqrt{2}},$$
$$\beta = -\frac{1}{\sqrt{2}}. \quad (15)$$

But, how come Eve knows which basis to use? The answer is that she does not know. Thus, measuring in a basis selected at random, Eve at some instances introduces errors that are detected by Alice and Bob.

Using similar approach as [11], we evaluate the error rate occurred in this type of attack. We divide the analysis into two cases: $(+)$ basis chosen by Eve; and $(\times)$ chosen by Eve, and for each of them calculate the error rate. Then, we combine the two error rates obtained to get the total one, which characterizes the Measurement and resend attack.

Let us first start off with the $(+)$ case. As shown in Equation (14), two states could occur for Eve in the measurement — $|0\rangle$ or $|1\rangle$. When $|0\rangle$ (or $|1\rangle$) occurs, it is evident that either $|0\rangle$ ($|1\rangle$) or $|+\rangle$ or $|-\rangle$ is sent by Alice to Bob and since Eve does not know the basis of the particle sent, she chooses at random (probabilities $p(|0\rangle) = p(|+\rangle) = p(|-\rangle) = 33.33\%$) a state to resend. In this case, $(+)$-sent particle implies that $33.33\% + 66.66\% \cdot 50\%$ of the cases Eve will resend a correct particle state and 33.33% an incorrect state, whereas $(\times)$-sent particle implies that $33.33\% \cdot 50\% + 66.66\% \cdot 50\%$ of the cases Eve will resend an incorrect state and 50% a correct one. Summing up, for the error rate in this case we get on average $33.33\% \cdot 50\% + (33.33\% \cdot 50\% + 66.66\% \cdot 50\%) \cdot 50\%$, that is, 41.66%.

Because the $(\times)$ case is symmetric to the above one, the error rate obtained for it is the same — 41.66%.

The overall (the average) error rate, accounting for both randomly $(+)$- and $(\times)$-chosen cases, is therefore

$$ER = 50\% \cdot 41.66\% + 50\% \cdot 41.66\% = 41.66\%. \quad (16)$$

Intercept and resend attack. Eve intercepts the particles of the first travel block and after that sends her own prepared group of particles to Bob. In this way, she introduces errors into the decoys' states because of her ignorance of the original ones. Therefore, Eve can be detected during the first eavesdropping check process. The reason for this is the fact that $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ states could occur for a particle intercepted by Eve, since either $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ or $|\Phi^+\rangle = (|{+}{+}\rangle + |{-}{-}\rangle)/\sqrt{2}$ state is used for the two-qubit decoy systems. Since these two two-qubit states are equally likely, the single-qubit states aforementioned are then equiprobable — they share probability of 25%. In this case, the probability of success attack is 50%, or equivalently, the error rate is 50%. This is so due to the relations presented below in Table I.

TABLE I
RESENT-POSSIBLE STATES RELATIONS

Resent	Possible	Success probability
$\|0\rangle$	$\|0\rangle$	25%
$\|0\rangle$	$\|1\rangle$	0%
$\|0\rangle$	$\|+\rangle$	$25\% \cdot 50\% = 12.5\%$
$\|0\rangle$	$\|-\rangle$	$25\% \cdot 50\% = 12.5\%$

The overall success probability is a sum of the success probabilities of the relations shown. The relations for the other states ($|1\rangle$, $|+\rangle$,$|-\rangle$) that could be resent are the same. So, the overall error rate can be assumed to be equal to 50%.

According to analyses put forward in [8], [9], the **Probe attack** and **Entanglement swaping attack** for the protocol [3] have one and the same error rate values: 50%.

So, the quantum channel security for the protocol of [3] obtains the value

$$\lambda = \min(ER_1, ER_2, ER_3, ER_4) = \min(41.66\%, 50\%, 50\%, 50\%) = 41.66\% \approx 0.42, \quad (17)$$

where ER_1 corresponds to the error rate in Measurement and resend attack, ER_2 corresponds to the error rate in Intercept and resend attack, ER_3 corresponds to the error rate in Probe (Entaglement) attack, and ER_4 corresponds to the error rate in Entanglement swapping attack.

On the other hand, the classical communication carried out in the protocol of [3] demonstrates that the classical channel security resides in the value of

$$\chi = \frac{H_e'}{H_e} = \frac{2}{2} = 1. \quad (18)$$

Therefore, for the overall security of the protocol, we obtain

$$\Sigma = \frac{\chi + \lambda}{2} = \frac{1 + 0.42}{2} = 0.71. \quad (19)$$

4) Optimality: According to Equation (9) and the values obtained above for the efficiency, practicality, and security, the optimality of the protocol is

$$\zeta = \frac{E + \Sigma + \xi}{3} = \frac{1 + 0.71 + 1}{3} \approx 0.9. \quad (20)$$

III. CONCLUSION

In summary, mathematical expressions for the security and practicality of QSC protocols were introduced. Also, the three main parameters of QSC protocols: efficiency, security, and practicality, were incorporated into a more general parameter, called optimality. The latter was proposed in order

to characterize any existing QSC protocol in a complete manner. An example is presented demonstrating how the optimality of the protocol [3] is calculated. It is furthermore evident that the optimality can be used as parameter by means of which one can compare distinct protocols.

Acknowledgment

The work is supported by the projects 07/10-2016 and 01/05-2018, funded by National Science Fund, Ministry of Education and Science, Bulgaria.

References

[1] G. Long, F. Deng, C. Wang, X. Li, K. Wen, and W. Wang, *Quantum secure direct communication and deterministic secure quantum communication*, Front. Phys., 2, 25, Springer, 2007.
[2] C. H. Bennett and S. J. Wiesner, *Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States*, Phys. Rev. Lett., 69, 2881, American Physical Society, 1992.
[3] F. G. Deng, G. L. Long, and X. S. Liu, *Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block*, Phys. Rev. A, 68, 042317, American Physical Society, 2003.
[4] C. Wang, F. Deng, Y. Li, X. Liu, and G. Long, *Quantum secure direct communication with high-dimension quantum superdense coding*, Phys. Rev. A, 71, 044305, American Physical Society, 2005.
[5] F. G. Deng and G. L. Long, *Secure direct communication with a quantum one-time pad*, Phys. Rev. A, 69, 052319, American Physical Society, 2004.
[6] A. Banerjee and A. Pathak, *Maximally efficient protocols for direct secure quantum communication*, Phys. Lett. A, 376, 2944, Elsevier, 2012.
[7] C. W. Tsai, C. R. Hsieh, and T. Hwang, *Dense coding using cluster states and its application on deterministic secure quantum communication*, Eur. Phys. J. D, 61, 783, Springer, 2011.
[8] D. oy, S. Surendran, and M. Sabir, *Efficient Deterministic Secure Quantum Communication protocols using multipartite entangled states*, Quantum Inf Process, 16, 157, Springer, 2017.
[9] F. Yan and X. Zhang, *A scheme for secure direct communication using EPR pairs and teleportation*, Euro. Phys. J. B, 41, 7578, Springer, 2004.
[10] A. Cabello, *Quantum Key Distribution in the Holevo Limit*, Phys. Rev. Lett., 85, 5635, American Physical Society, 2000.
[11] Z. Cao, D. Song, J. Peng, C. He, and J. Feng, *High Security Quantum Secure Direct Communication Protocol Based on Three - particle GHZ States*, Proceedings of the 17th IEEE International Conference on Nanotechnology, USA, pp. 40-43, 25-28 July 2017.