IET Quantum Communication

Research Article

Turbo-coded secure and reliable quantum teleportation

eISSN 2632-8925
Received on 21st January 2020
Revised 9th April 2020
Accepted on 14th April 2020
doi: 10.1049/iet-qtc.2020.0004
www.ietdl.org

Rosie Cane[1], Wanwan Xie[1], Soon Xin Ng[1] ✉
[1]School of Electronics and Computer Science, University of Southampton, Southampton, SO17 1BJ, UK
✉ *E-mail: sxn@ecs.soton.ac.uk*

Abstract: Quantum teleportation allows an unknown arbitrary quantum state to be transmitted between two separate locations. To achieve this, the system requires both classical and quantum channels, for communicating two classical bits and an entangled quantum bit from the transmitter to the receiver. It is commonly assumed that both channels are error-free, however, under realistic conditions, this is unlikely to be the case. This study proposed and investigated a secure and reliable quantum teleportation scheme when both classical and quantum channels exhibit errors. It was found that the security and reliability of the teleportation could be improved when powerful turbo codes are employed.

1 Introduction

Quantum teleportation (QT) is a communication protocol that transmits the information using an arbitrary and unknown quantum bit (qubit) without the physical transmission of that specific qubit [1]. The single qubit state can be represented by $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. This qubit can be teleported from the transmitter to the receiver by using the transmission of classical information and with the aid of an additional entangled pair of qubits. Without the transmission of the qubit $|\psi\rangle$ itself, the teleportation protocol reconstructs a replica of the original qubit at the receiver using the classical information communicated over the classical channel as well as one of the pre-shared entangled qubit that was communicated over the quantum channel. Hence, a QT system has a dual classical-quantum channel. More explicitly, information about the qubit $|\psi\rangle$ is extracted at the transmitter by a Bell measurement and the outcome is then communicated to the receiver over the classical channel. This information determines the appropriate application of single-qubit gates on the pre-shared qubit for reproducing the original state $|\psi\rangle$ of the teleported qubit at the receiver. Note that before the measurement, the quantum channel was used for sharing one of the entangled qubits from the transmitter to receiver.

However, the teleportation protocol is only effective provided that there is a low level of noise in the implementation hardware and both the classical and quantum transmissions are error-free. Hence, quantum error correction must be incorporated for protecting the transmission of the pre-shared entangled qubit. Similarly, classical error correction is also needed for reliable transmission of the measurement results from the transmitter to the receiver. It is also necessary to ensure the security of the transmission, especially in the quantum channel.

Error in either the classical or quantum channel (or both) can reduce the fidelity of the final teleported qubit. It is often assumed that channel error can be negligible in the teleportation protocol. However, this assumption must be removed when the teleportation scheme is implemented practically. On the one hand, teleportation has been widely considered for applications in secured communication, quantum networking, and quantum repeaters, as well as some conceptual applications in quantum information theory [2]. Further advances in quantum communications are available at [3–7]. However, practical investigation of error correction aided practical teleportation scheme is still lacking.

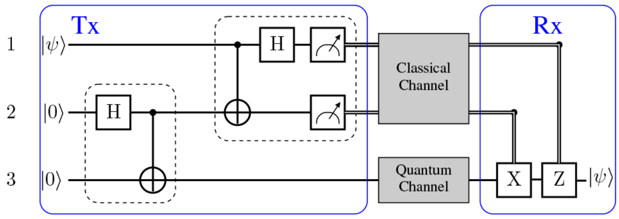


Fig. 1 *QT protocol [1]*

Against this backdrop, this study investigates a practical teleportation scheme, where both the classical and quantum channels exhibit errors. The effect of channel errors is investigated with the aid of both classical turbo codes (TCs) [8] and quantum TCs (QTCs) [9]. Then, secure QT protocols are explored by authenticating entangled qubit pairs via a trusted third-party and with the aid of quantum-secure-direct-communication (QSDC) [10] scheme.

The novel contributions of this study are as follows:

i. A practical teleportation scheme is investigated, where both the classical and quantum channels exhibit errors.
ii. Reliable teleportation with the aid of TC and QTC.
iii. Secure teleportation based on QSDC.

The rest of this paper is organised as follows. The protocol of QT over ideal channels is described in Section 2, while the teleportation over imperfect channels is investigated in Sections 3 and 4. A secure teleportation scheme is proposed and investigated in Section 5, while our conclusions are offered in Section 6.

2 Teleportation over perfect channels

In this section, the QT protocol [1] is described based on error-free classical and quantum channels. The aim of teleportation is to send the information of an arbitrary unknown qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ from the transmitter to the receiver without the transmission of the qubit itself. The circuit that can achieve teleportation is shown in Fig. 1.

As seen in Fig. 1, the protocol begins with three qubits. First of all, qubit 1 is the qubit for teleportation, which is in an arbitrary unknown state $|\psi\rangle$. Secondly, qubits 2 and 3, which are in the zero state, will be entangled and they will be shared between the transmitter and the receiver. This initial state can be described as follows:

$$\begin{aligned} |\psi\rangle \otimes |0\rangle \otimes |0\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \otimes |0\rangle \\ &= \alpha|000\rangle + \beta|100\rangle . \end{aligned} \tag{1}$$

Table 1 Gate operation applied to qubit 3 according to the measurement results

State	Measurement	Qubit 3 state	Gate correction
$\|00\rangle$	0, 0	$\alpha\|0\rangle+\beta\|1\rangle$	I
$\|01\rangle$	0, 1	$\alpha\|1\rangle+\beta\|0\rangle$	X
$\|10\rangle$	1, 0	$\alpha\|0\rangle-\beta\|1\rangle$	Z
$\|11\rangle$	1, 1	$\alpha\|1\rangle-\beta\|0\rangle$	XZ

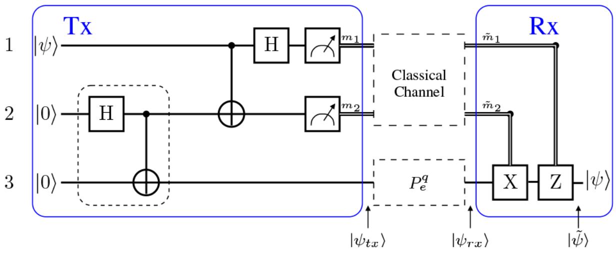


Fig. 2 *Reproduction of Fig. 1 with imperfect classical and quantum channel*

Note that the Hadamard gate (denoted *H*) is a quantum gate that has the following transformation on the computational basis states ($|0\rangle, |1\rangle$) [11]

$$\left|0\right\rangle \xrightarrow{H} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \qquad \left|1\right\rangle \xrightarrow{H} \frac{|0\rangle-|1\rangle}{\sqrt{2}}\,. \tag{2}$$

Applying a Hadamard gate to the second qubit in (1) would give (see (3)) . Then, a controlled-NOT (CNOT) gate is applied between qubit 2 and qubit 3. If a control qubit (qubit 2) is in the $|1\rangle$ state the CNOT gate applies a NOT gate to the target qubit (qubit 3), as exemplified below

$$\begin{aligned} &\left|10\right\rangle \xrightarrow{\text{CNOT}} \left|11\right\rangle \quad \left|00\right\rangle \xrightarrow{\text{CNOT}} \left|00\right\rangle \\ &\left|01\right\rangle \xrightarrow{\text{CNOT}} \left|01\right\rangle \quad \left|11\right\rangle \xrightarrow{\text{CNOT}} \left|10\right\rangle . \end{aligned} \tag{4}$$

Hence, the application of the CNOT gate to qubits 2 and 3 in (3) would give

$$\begin{aligned} &\frac{1}{\sqrt{2}}(\alpha|0\underline{00}\rangle+\alpha|0\underline{10}\rangle+\beta|1\underline{00}\rangle+\beta|1\underline{10}\rangle) \xrightarrow{\text{CNOT}} \\ &\frac{1}{\sqrt{2}}(\alpha|000\rangle+\alpha|011\rangle+\beta|100\rangle+\beta|111\rangle) \\ &=(\alpha|0\rangle+\beta|1\rangle)\otimes\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \end{aligned} \tag{5}$$

At this point, qubits 2 and 3 are entangled in the state $(1/\sqrt{2})(|00\rangle+|11\rangle)$, known as the Einstein–Podolsky–Rosen (EPR) pair [12]. At this point, qubit 3 of the entangled EPR pair can be transmitted to the receiver over an error-free quantum channel, while qubit 2 will be retained at the transmitter.

Next, a bell state measurement [13] will be applied to qubits 1 and 2, where qubit 1 is the unknown qubit for teleportation. To make a bell-state measurement, the CNOT and Hadamard gates are applied between qubits 1 and 2, as seen in Fig. 1, before the measurement [11]. The CNOT gate evolves (5) as follows:

$$\begin{aligned} &\frac{1}{\sqrt{2}}(\alpha|\underline{00}0\rangle+\alpha|\underline{01}1\rangle+\beta|\underline{10}0\rangle+\beta|\underline{11}1\rangle) \xrightarrow{\text{CNOT}} \\ &\frac{1}{\sqrt{2}}(\alpha|000\rangle+\alpha|011\rangle+\beta|110\rangle+\beta|101\rangle), \end{aligned} \tag{6}$$

while a Hadamard gate on qubit 1 would further transform (6) to

$$\begin{aligned} &\frac{1}{\sqrt{2}}(\alpha|\underline{0}00\rangle+\alpha|\underline{0}11\rangle+\beta|\underline{1}10\rangle+\beta|\underline{1}01\rangle) \\ &\xrightarrow{\text{H}} \frac{1}{\sqrt{2}}\left[\frac{\alpha|\underline{0}00\rangle+\alpha|\underline{1}00\rangle}{\sqrt{2}}+\frac{\alpha|\underline{0}11\rangle+\alpha|\underline{1}11\rangle}{\sqrt{2}}\right. \\ &\left.+\frac{\beta|\underline{0}10\rangle-\beta|\underline{1}10\rangle}{\sqrt{2}}+\frac{\beta|\underline{0}01\rangle-\beta|\underline{1}01\rangle}{\sqrt{2}}\right]. \end{aligned} \tag{7}$$

After collecting the terms with the same values in the first and second qubits in (7), we obtain

$$\begin{aligned} &\frac{1}{2}[(\alpha|000\rangle+\beta|001\rangle)+(\alpha|011\rangle+\beta|010\rangle) \\ &+(\alpha|100\rangle-\beta|101\rangle)+(\alpha|111\rangle-\beta|110\rangle)] \\ &=\left|00\right\rangle\frac{\alpha|0\rangle+\beta|1\rangle}{2}+\left|01\right\rangle\frac{\alpha|1\rangle+\beta|0\rangle}{2} \\ &\left|10\right\rangle\frac{\alpha|0\rangle-\beta|1\rangle}{2}+\left|11\right\rangle\frac{\alpha|1\rangle-\beta|0\rangle}{2}, \end{aligned} \tag{8}$$

which gives the system before the measurement at the transmitter. The measurements of qubits 1 and 2 could be in any of the following combinations: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. These measurements can then be communicated over a classical channel to the receiver as seen in Fig. 1. Note that after the measurement, qubit 1 has been destroyed.

If the measurement bits are given by 1, 0, then the state of the pre-shared qubit 3 has been changed to $(1/2)(\alpha|0\rangle-\beta|1\rangle)$. It is possible to transform qubit 3 to the state of qubit 1 (before measurement) based on the lookup table of Table 1, where *X* and *Z* refers to the bit and phase-flip gates defined by the *X* and *Z* Pauli operators [11]. More specifically, when the measurement results are 1, 0, the receiver should apply the *Z* gate to qubit 3. This will transform qubit 3 to the original state of qubit 1 as follows:

$$\alpha\left|0\right\rangle-\beta\left|1\right\rangle \xrightarrow{\text{Z}} \alpha\left|0\right\rangle+\beta\left|1\right\rangle=\left|\psi\right\rangle. \tag{9}$$

The corresponding lookup table mapping all possible measurement results to quantum gate operations is given in Table 1.

3 Teleportation over imperfect classical channel

In this simulation an unknown arbitrary qubit $|\psi\rangle$ is teleported based on a perfect quantum channel but an imperfect classical Rayleigh fading channel. As described in the previous section, the classical bits determine the activation of the *X* and *Z* gates at the receiver. The correctly applied combination of gates is essential to accurately resurrect the state of qubit 1 $|\psi\rangle$ at the receiver.

The classical bits $\tilde{m}_1$ and $\tilde{m}_2$ of Fig. 2 can take four combinations, namely 00, 01, 10, and 11. However, only when both m_1 and m_2 are transmitted perfectly can the *X* and *Z* gates be enabled or disabled properly at the receiver. For example, if qubit 1 is in the state $\alpha|0\rangle+\beta|1\rangle$ the measurement result for transmission would be 00. In this case, the identity gate *I* gate is applied at the receiver (see Table 1) to obtain the final state $|\psi\rangle$. However, if the corrupted classical bit sequence 01 is received instead, then an *X* gate is mistakenly applied as follows:

$$\begin{aligned} &\alpha\left|0\underline{0}0\right\rangle+\beta\left|1\underline{0}0\right\rangle \xrightarrow{\text{H}} \frac{\alpha|0\underline{0}0\rangle+\alpha|0\underline{1}0\rangle}{\sqrt{2}}+\frac{\beta|0\underline{0}0\rangle+\beta|0\underline{1}0\rangle}{\sqrt{2}} \\ &=\frac{1}{\sqrt{2}}(\alpha|000\rangle+\alpha|010\rangle+\beta|100\rangle+\beta|110\rangle)\,. \end{aligned} \tag{3}$$

$$\alpha\Big|0\Big\rangle + \beta\Big|1\Big\rangle \xrightarrow{X} \alpha\Big|1\Big\rangle + \beta\Big|0\Big\rangle \neq \Big|\psi\Big\rangle, \tag{10}$$

which produces a quantum bit-flip error in the reconstructed qubit 1. Therefore, an error in the classical channel can induce a quantum error on the teleported qubit 1.

Note that a single error on either m_1 or m_2 as well as simultaneous error, on both m_1, m_2, will result in only a single quantum error on the teleported qubit. For example, if the erroneous bit combination $\tilde{m}_1 = 0$, $\tilde{m}_2 = 1$ is applied at the receiver to the qubit in the previous example, then

$$\alpha\Big|0\Big\rangle + \beta\Big|1\Big\rangle \xrightarrow{XZ} \alpha\Big|1\Big\rangle - \beta\Big|0\Big\rangle \neq \Big|\psi\Big\rangle, \tag{11}$$

however, this will be counted as only a single qubit error.

3.1 Bit-error-ratio (BER)

If N classical bits are transmitted and N_ϵ is the number of erroneously received classical bits then the BER is given by

$$\text{BER} = N_\epsilon/N \ . \tag{12}$$

Likewise, the quantum-BER (QBER) is given by

$$\text{QBER} = N^q_f/N^q, \tag{13}$$

where N^q is the total number of teleported qubits and N^q_ϵ is the total number of erroneously teleported qubits.

More specifically, the teleportation of N_q number of qubit 1 (as shown in (1)) requires the transmission of $N = 2N_q$ classical bits for conveying the two measurement results from the transmitter to the receiver. If there are N_ϵ classical bit errors, the worst case would be when only one error occur in each of the two measurement results, giving rise to $N^q_\epsilon = N_\epsilon$ qubit errors. Hence, the corresponding QBER upper bound would be given by $\text{QBER} = N^q_\epsilon/N^q = N_\epsilon/(0.5N) = 2\text{BER}$.

3.2 Classical turbo-coded teleportation

Recall that for each recovered teleported qubit, two classical bits (m_1, m_2) must be accurately received. Fig. 3 shows the QBER/BER versus signal-to-noise ratio (SNR) performance when communicating over Rayleigh fading channel using uncoded modulation schemes. The SNR is defined as $\text{SNR} = h_r P_t/N_0$, where h_r is the Rayleigh fading channel coefficient, P_t is the transmit power, and N_0 is the variance of the additive White Gaussian noise. The effect on QBER is consistent with the relationship explained previously, which is given by

$$\text{QBER} \leq 2\text{BER} \,. \tag{14}$$

TCs [8] are popular classical channel coding schemes for mitigating the effect of channel fading and channel noise. TCs were first proposed in [8] and they showed a remarkable error correction performance under certain conditions, with only 0.7 dB disparity [14] compared to the Shannon limit, which was regarded as impossible before the invention of TCs. TCs take advantage of parallel-code concatenation at the encoder, having an interleaver between the two-component codes. At the decoding side, an iterative decoder based on two soft-input-soft-output decoders is invoked for exchanging soft extrinsic information between the two component decoders.

Fig. 4 shows that the QBER of the teleportation protocol can be improved by introducing TC in the classical transmission. Furthermore, an increased number of decoding iterations would allow the soft information from each decoder to be exchanged more effectively, leading to a more accurate bit recovery. However, to achieve a BER level of 10^{-5} the performance of the four-iteration- and eight-iteration-based schemes are relatively close. As a good trade-off between performance and complexity, the four-iteration-based TC scheme is chosen for our study.

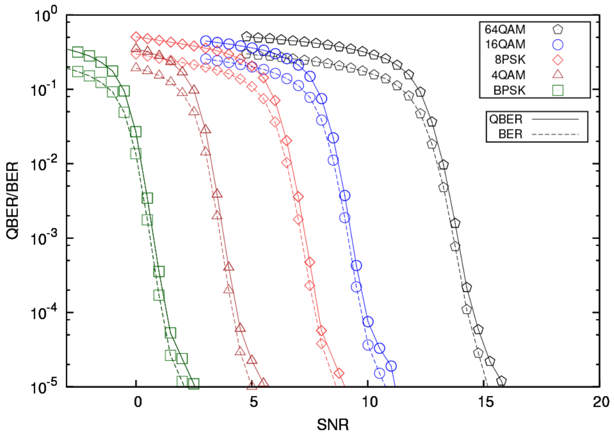


Fig. 3 *QBER/BER versus SNR performance when communicating over Rayleigh fading channel using uncoded binary phase-shift keying (BPSK), 4-quadrature amplitude modulation (4-QAM), 8-PSK, 16-QAM, and 64-QAM schemes*

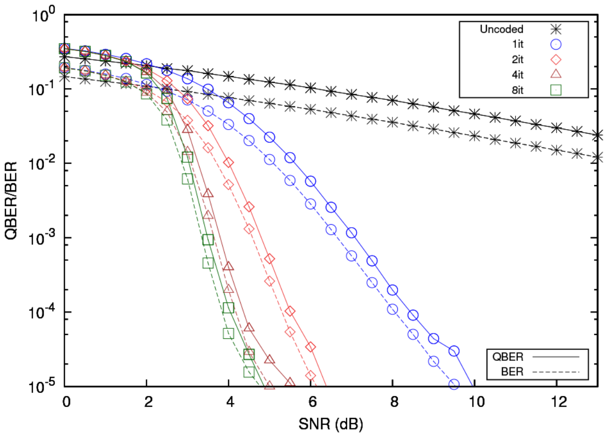


Fig. 4 *QBER/BER versus SNR performance when communicating over Rayleigh fading channel using uncoded BPSK and TC-4-QAM having 1, 2, and 8 decoding iterations*

4 Teleportation over imperfect quantum and classical channels

4.1 Quantum depolarising channel

We have shown that errors in the classical channel lead to quantum errors in the teleported qubits and that this can be improved by classical turbo coding. In this section, we consider errors in both the classical and quantum channels. Depolarising error probability P^q_ϵ is the probability having a quantum error in the quantum channel over which qubit 3 is transmitted, as shown in Fig. 2. The quantum depolarising channel [15] is characterised by three possible error events, namely the quantum bit-flip error, the phase flip error, and the combination of the two (the simultaneous occurrence of both bit and phase flip errors). Explicitly, a bit-flip error is equivalent to the transformation using a NOT gate (or Pauli X gate) and is similar to a classical bit-flip. For example, a bit-flip error has the effect that $|0\rangle \leftrightarrow |1\rangle$ on the computational basis states. On the other hand, a phase-flip error is equivalent to the transformation using the Z gate, where $|1\rangle \leftrightarrow -|1\rangle$ while $|0\rangle \leftrightarrow |0\rangle$ is left unchanged. Additionally, the bit-and-phase flip error is equivalent to the transformation using both X and Z gates, e.g. $|0\rangle \rightarrow -|1\rangle$. The probability each of these error events occurring is assumed to be equivalent in the standard quantum depolarising channel, i.e. each occurs with a probability of $P^q_\epsilon/3$.

Fig. 2 shows that the pre-shared qubit 3 (denoted as $|\psi_{\text{tx}}\rangle$) may arrive corrupted at the receiver (denoted as $|\psi_{\text{rx}}\rangle$) due to the

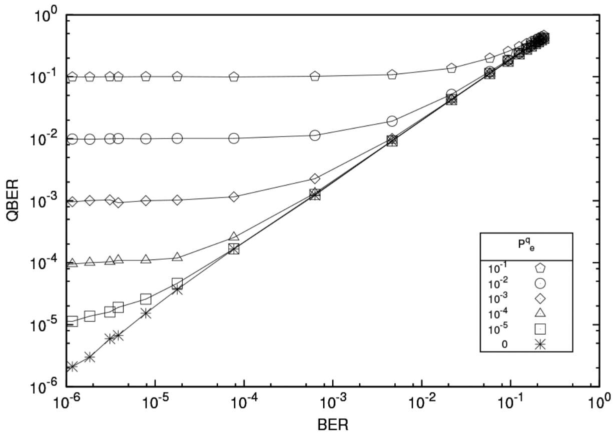


Fig. 5 *QBER versus BER curves of the turbo coded 8-PSK-assisted scheme when communicating over the Rayleigh fading channel. The qubit depolarising probability considered are* $P_e^q = (10^{-1}, 10^{-2}, 10^{-3}, 10^{-4}, 10^{-5}, 0)$

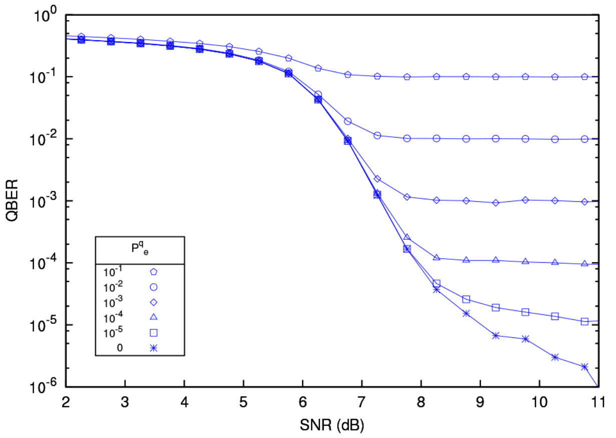


Fig. 6 *QBER versus SNR performance of the turbo-coded 8-PSK-assisted scheme when communicating over the Rayleigh fading channel. The qubit depolarising probability considered are* $P_e^q = (10^{-1}, 10^{-2}, 10^{-3}, 10^{-4}, 10^{-5}, 0)$

quantum depolarising channel. Let us consider this scenario in more details, assuming that $|\psi_{\text{tx}}\rangle = \alpha|1\rangle + \beta|0\rangle$ has a quantum bit-flip (X) error occurs during the transmission, then

$$\alpha\Big|1\rangle + \beta\Big|0\rangle \xrightarrow{X} \alpha\Big|0\rangle + \beta\Big|1\rangle. \tag{15}$$

This would lead to an error to the transported qubit 1 (denoted $|\psi\rangle$).

Let us now further describe the quantum channel error probability as P_e^q. For example, $P_e^q = 10^{-1}$ is equivalent to 1 corrupted qubit in ten pre-shared corrupted qubit 3 at the receiver, i.e. $|\psi_{\text{rx}}\rangle \neq |\psi_{\text{tx}}\rangle$. Let us define the total number of transmitted pre-shared qubits as N^q and the total number of corrupted transmitted qubits as $\overline{N}_e^q$. Then the QBER at the quantum channel is given by

$$P_e^q = \overline{N}_e^q / N^q \,. \tag{16}$$

4.2 Classical turbo-coded teleportation over imperfect quantum channel

As described in Section 3.1, the QBER is approximately twice the BER, when the quantum channel is error-free. With the addition of the imperfect quantum channel, the upper bound of the QBER is now given by

$$\text{QBER} \leq 2\text{BER} + P_e^q\,. \tag{17}$$

This is an upper bound since there are certain scenarios where the classical and quantum channel errors cancel each other. Fig. 5 shows various P_e^q values and the corresponding BER varying from 0.5 to 10^{-6}. The QBER follows the trend of (14), when P_e^q is small, as expected. For example, when the quantum channel error probability is given by $P_e^q = 10^{-4}$, we have QBER $\leq$ 2BER for BER $> 10^{-4}$. In this case, the classical channel error dominates the QBER in the region of BER $> 10^{-4}$. However, when $P_e^q >$ BER, the QBER converges to the P_e^q value in the form of an error floor. This is because the quantum error is now dominating the QBER, according to (17).

Fig. 6 shows the QBER versus SNR performance of the turbo coded 8-phase-shift keying (8-PSK)-assisted scheme when communicating over the Rayleigh fading channel. Since the BER of the classical channel reduces as SNR increases, we notice that the QBER has an error floor at P_e^q a high SNR region, as expected.

5 Quantum turbo-coded secure teleportation

As seen previously in Fig. 1, teleportation requires an entangled qubit pair (qubits 2 and 3), which are prepared at the transmitter and then one of them (qubit 3) is communicated to the receiver over the quantum channel. This section describes an alternative method whereby an EPR pair is distributed via an authentic third party, where each qubit in the entangled pair is communicated to the transmitter and receiver, separately. This way the teleportation protocol is applied at the transmitter without any knowledge of the location of the receiver. This adds a layer of security to the generation of the entangled qubits and the transmission of the EPR pairs. The only drawback of this approach is that a quantum memory is required to store the EPR pair before its distribution. However, this arrangement is more secure compared to that in Fig. 1.

When the entangled qubits are shared securely then the QT can be considered absolutely secure. This is because the measurement results are only beneficial to the eavesdropper when the transmitted qubit 3 is in the eavesdropper's possession. The addition of an authentic third-party means that QT can be used as a one-time-pad scheme and therefore can be employed for secure quantum communications [16]. Explicitly, an entangled qubit pair can be considered as a key for each teleportation. Once the security of the key is certified, then the transmission process can be deemed to have unconditional security [17].

However, provided that the EPR pairs are transmitted from an authenticated third party there exist a risk that the qubits can be exploited by an eavesdropper. The security of the EPR pair that is distributed via the quantum channel can be examined based on the characteristics of quantum entanglement. On the one hand, any measurements of either of the qubits in an entangled pair disturb the entanglement state, which ultimately results in an equivalent pure state. If the eavesdropper intercepts the transmission of the EPR pairs, it could, therefore, be discovered immediately. On the other hand, if the eavesdropper first intercepts the transmission of either qubit and re-sends it after some manipulations, the whole structure of the original entanglement is altered. Nevertheless, this attack can be detected if the transmitted and received qubit in the EPR pair are measured and the outcomes are compared [18].

For example, consider the transmission of the EPR pair $\big|AB^{00}\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$, where qubit A is kept at the transmitter and qubit B is transmitted to the receiver. If the eavesdropper prepares the same EPR pair, namely $\big|CD^{00}\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$, and then captures the qubit $|B\rangle$, then the system can be described by [19]

$$\begin{aligned}\big|AB^{00}\rangle\big|CD^{00}\rangle = \frac{1}{2}\big(\big|AC^{00}\rangle\big|BD^{00}\rangle \\ +\big|AC^{01}\rangle\big|BD^{01}\rangle\big|AC^{10}\rangle\big|BD^{10}\rangle + \big|AC^{11}\rangle\big|BD^{11}\rangle\big),\end{aligned} \tag{18}$$

where

$$
\begin{aligned}
|ij^{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)\\
|ij^{10}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad (19)\\
|ij^{11}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle).
\end{aligned}
$$

Equation (18) shows that if the eavesdropper measures $|BD^{00}\rangle$ then the other qubits are in the state $|AC^{00}\rangle$. Therefore the original entangled state $|AB^{00}\rangle$ is no longer valid and the qubits $|A\rangle$ and $|B\rangle$ are no longer entangled. When the qubits are no longer entangled, its measurement outcomes can no longer determine the measurement result of the other qubit. In other words, the QBER will be very high when the eavesdropper is the presence and this phenomenon can be used for secure quantum transmissions as explain in Section 5.1.

5.1 Secure and reliable teleportation

In this section, a secure and reliable QT based on the QTC of [9] and the QSDC of [10] is investigated. Provided that the security of pre-shared entangled qubit pairs has been ensured, the teleportation process would be unconditionally secure and therefore the protocol only concentrates on the security of the quantum channel. Furthermore, the QTC-decoded entangled pairs are more reliable compared to the uncoded scheme. Our proposed secure and reliable teleportation protocol, as seen in Fig. 7, can be explained below:

i. *Prepare n pairs of EPR qubits*: Half of these qubits are to be communicated from the transmitter and to the receiver via a quantum depolarising channel [If a third party is used to prepare these EPR qubit pairs, then half of the EPR pairs will be communicated to the transmitter and the other half to the receiver [16].] To do this, each of the n EPR pairs is prepared in the state $|\psi^{00}_{\rm tx,rx}\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$.

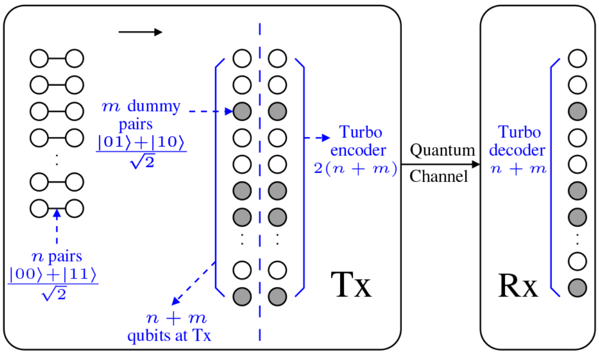
ii. *Prepare m dummy EPR pairs*: These qubits are to be inserted to the original EPR qubit pairs at secret locations. The dummy EPR pairs are in the state $|\psi^{01}_{\rm tx,rx}\rangle = (1/\sqrt{2})(|01\rangle + |10\rangle)$. This protocol becomes more precise for a larger value of m as the dummy EPR pairs are used to detect the eavesdropper.

iii. *Encode with QTC*: There are now $(n+m)$ EPR pairs, which are encoded with a 1/2-rate QTC to produce $2(n+m)$ qubit pairs in total.

iv. *Decode with QTC*: The corresponding QTC decoding process is implemented at the receiver [QTC decoding at the transmitter is also needed, if the EPR pairs are prepared by a third party [16].] and is based on the error syndromes [20, 21]. If the syndrome indicates that a qubit is erroneously bit flipped, an X gate correction is applied at the receiver. Then after QTC decoding, $(n+m)$ qubits are restored at the receiver.

v. *Measure m dummy qubits:* The measurement of the decoded dummy qubits can be used to determine the severity of eavesdropping that may have occurred. The location of the dummy qubits is communicated to the receiver. These qubits are measured at the receiver and the results are sent back to the transmitter. If there is no eavesdropper in the quantum channel, then the results obtained at the receiver should be opposite to that at the transmitter (since the dummy qubits are in state $(1/\sqrt{2})(|01\rangle + |10\rangle)$, when the quantum channel is error-free.

vi. *Evaluate the secure error ratio*: The quantum communication is deemed secure if the QBER of the dummy qubits is below a certain chosen security threshold (this threshold will be explained in Section 5.2). When the QBER of the dummy qubits is below the threshold, then the n pairs of pre-shared EPR qubits (qubits 2 and 3 of Fig. 1) are considered secure. Then the decoded EPR pairs can be used for teleportation. However, if the QBER of the dummy bits is higher than the threshold, then this indicates that the transmission has been intercepted and the whole transmission process should be discarded and the protocol should restart from step 1.



m dummy pairs $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$
n pairs $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
$n+m$ qubits at Tx
Turbo encoder $2(n+m)$
Quantum Channel
Turbo decoder $n+m$
Tx
Rx

Fig. 7 *QTC aided QSDC*

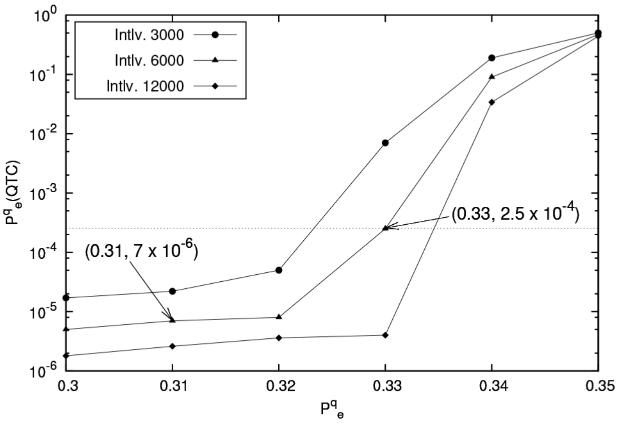


Fig. 8 *Channel depolarising error probability P^q_e (uncoded) versus QTC-decoded error probability $P^q_e(QTC)$. The QTC of [21] was considered*

vii. *Teleportation of information qubits*: When the EPR pairs are secure and reliable, then the teleportation of information qubits (qubit 1 in Fig. 1) based on classical measurement bits, as described in Section 2 can proceed correspondingly.

Note that dummy entangled qubit pairs are used in QSDC, while random entangled qubit pairs are also needed for the Bell inequality testing in the device-independent quantum key distribution. Hence, it is a good future research to compare the performance of these systems, in terms of the efficiency in using these entangled qubit pairs.

5.2 Secure error ratio threshold with QTC

Step 6 in the previous section requires a secure error ratio threshold to compare with the error ratio of the dummy qubits in order to establish if an eavesdropper was present during the qubit transmission. This must be determined carefully with the aid of the QTC. The secure error ratio can be specified from Fig. 8, where the x-axis P^q_e corresponds to the depolarising error probability in the quantum channel, while the y-axis shows the corresponding error ratio (denoted as P^q_e(QTC)) after applying the QTC.

Suppose that the channel depolarising probability without eavesdropping is given by $P^q_e = 0.31$. It is reasonable to assume that eavesdropper would introduce at least further 10% of error to the channel depolarising probability. This would make the overall channel-plus-eavesdropper depolarising probability to be $P^q_e > 0.41$. As we can see from Fig. 8 that after the application of the QTC of [21], say, with an interleaver length of 6000 qubits the corresponding QBERs are $P^q_e(\text{QTC}) = 7 \times 10^{-6}$ for $P^q_e = 0.31$ and $P^q_e(\text{QTC}) > 0.4$ for $P^q_e < 0.41$. Hence, without QTC, the 10% additional error introduced by the eavesdropper may be hard to detect when the quantum channel has a high depolarising error probability. However, with the aid of QTC, the QBER difference between the cases for having no eavesdropper ($P^q_e(\text{QTC}) = 7 \times 10^{-6}$) and with eavesdropper ($P^q_e(\text{QTC}) > 0.4$) is

Table 2 Tolerated quantum channel depolarising probability (P_e^q) as a function of the turbo interleaver length and the target QTC-decoded QBER (P_e^q(QTC)). This is based on Fig. 8

P_e^q(QTC)	Intlv. 3000	Intlv. 6000	Intlv. 12,000
10^{-2}	0.331	0.336	0.339
10^{-3}	0.326	0.332	0.336
10^{-4}	0.321	0.327	0.334
10^{-5}	0.281	0.321	0.331

significantly larger. In other words, the employment of QTC would make the detection of the eavesdropper easier. The reliability of the pre-shared qubits is also significantly improved from $P_e^q = 0.31$ to $P_e^q(\text{QTC}) = 7 \times 10^{-6}$, when the eavesdropper is not presence. Interested readers are referred to [21] for details of QTC.

5.3 Reliable QT

Based on the discussions so far, it is clear that both classical TC and QTC can be used to improve the reliability of the teleportation scheme. More explicitly, when QTC is employed, the over QBER of teleported qubits (qubit 1 of Fig. 1) given in (17) can be rewritten as

$$\text{QBER} = 2\text{BER} + P_e^q(\text{QTC}) \,, \tag{20}$$

where P_e^q(QTC) is the QBER of the QTC-aided transmission of the pre-shared qubits over the quantum channel. If the BER is controlled to a relatively low level using the classical TC, then the QBER error floor can be reached with lower SNR in the classical channel as seen in Fig. 5.

As seen in Fig. 5, in order to attain QBER < 10^{-4} the corresponding BER must also be BER < 10^{-4}. Fig. 6 shows that this condition can be met with an SNR >8 dB. In addition, with the implementation of QTC, $P_e^q(\text{QTC}) = 10^{-4}$ is achieved when the depolarising probability is $P_e^q = 0.327$ with the application of a 6000 interleaver, as shown in Table 2. A larger depolarising probability of $P_e^q = 0.334$ can be tolerated if the interleaver length is doubled to 12,000. Hence, the stronger the encoding scheme, the more reliable and secure the teleportation system become.

6 Conclusion

We have investigated the performance of a TC and QTC aided QT scheme when communicating over a Rayleigh fading channel and an imperfect quantum channel. The upper bound of the quantum error ratio was derived, which depends on the quality of both classical and quantum channels.

A QTC-aided secure transmission of pre-shared entangled qubits based on the QSDC protocol was investigated. More explicitly, the employment of QTC was found to be very useful for detecting eavesdroppers when the quantum channel is imperfect, as explained in Section 5.2.

More quantitatively, the proposed secure and reliable QT scheme can achieve QBER = 10^{-4} when the quantum channel depolarising probability is as high as $P_e^q = 0.327$, if a QTC having an interleaver length of 6000 qubits is invoked for the transmission of the pre-shared qubits, while a classical TC is invoked to protect the classical transmission of the measurement results, as shown in Table 2.

7 References

[1] Bennett, C., Brassard, G., Crépeau, C., *et al.*: 'Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels', *Phys. Rev. Lett.*, 1993, **70**, pp. 1895–1899

[2] Pirandola, S., Eisert, J., Weedbrook, C., *et al.*: 'Advances in quantum teleportation', *Nat. Photonics*, 2015, **9**, (10), pp. 641–652

[3] Hosseinidehaj, N., Babar, Z., Malaney, R., *et al.*: 'Satellite-based continuous-variable quantum communications: state-of-the-art and a predictive outlook', *IEEE Commun. Surv. Tutorials*, 2019, **21**, (1), pp. 881–919

[4] Gyongyosi, L., Imre, S., Nguyen, H.V.: 'A survey on quantum channel capacities', *IEEE Commun. Surv. Tutorials*, 2018, **20**, (2), pp. 1149–1205

[5] Cavaliere, F., Prati, E., Poti, L., *et al.*: 'Secure quantum communication technologies and systems: from labs to markets', *Quantum Rep.*, 2020, **2**, (1), pp. 80–106

[6] Ghalaii, M., Ottaviani, C., Kumar, R., *et al.*: 'Long-distance continuous-variable quantum key distribution with quantum scissors', *IEEE J. Sel. Top. Quantum Electron.*, 2020, **26**, (3), pp. 1–12

[7] Zhou, Z., Sheng, Y., Niu, P., *et al.*: 'Measurement-device-independent quantum secure direct communication', *Sci. China Phys. Mech. Astron.*, 2020, **63**, (3), p. 230362

[8] Berrou, C., Glavieux, A., Thitimajshima, P.: 'Near Shannon limit error-correcting coding and decoding: turbo-codes. 1'. IEEE Int. Conf. on Communications, Geneva, May 1993, vol. 2, pp. 1064–1070

[9] Poulin, D., Tillich, J., Ollivier, H.: 'Quantum serial turbo codes', *IEEE Trans. Inf. Theory*, 2009, **55**, (6), pp. 2776–2798

[10] Deng, F.-G., Long, G.L., Liu, X.-S.: 'Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block', *Phys. Rev. A*, 2003, **68**, p. 042317

[11] Nielsen, M.A., Chuang, I.: '*Quantum computation and quantum information*' (Cambridge University Press, UK, 2010)

[12] Einstein, A., Podolsky, B., Rosen, N.: 'Can quantum-mechanical description of physical reality be considered complete?', *Phys. Rev.*, 1935, **47**, pp. 777–780

[13] Pisenti, N., Gaebler, C.P.E., Lynn, T.W.: 'Distinguishability of hyperentangled bell states by linear evolution and local projective measurement', *Phys. Rev. A*, 2011, **84**, p. 022340

[14] Sklar, B.: '*Fundamentals of turbo codes*' (Prentice Hall, USA, 2002)

[15] Knill, E.: 'Quantum computing with realistically noisy devices', *Nature*, 2005, **434**, (7029), pp. 39–44

[16] Gisin, N., Ribordy, G., Tittel, W., *et al.*: 'Quantum cryptography', *Rev. Mod. Phys.*, 2002, **74**, pp. 145–195

[17] Li, X., Wan, N., Zhang, D.: 'Quantum determined key distribution scheme using quantum teleportation'. 2009 WRI World Congress on Software Engineering, Xiamen, China, 2009, vol. 1, pp. 431–434

[18] Naik, D.S., Peterson, C.G., White, A.G., *et al.*: 'Entangled state quantum cryptography: eavesdropping on the Ekert protocol', *Phys. Rev. Lett.*, 2000, **84**, pp. 4733–4736

[19] Schauer, S., Suda, M.: 'Security of entanglement swapping QKD protocols against collective attacks'. The Sixth Int. Conf. on Quantum, Nano and Micro Technologies (ICQNM), Rome, Italy, 2012

[20] Babar, Z., Botsinis, P., Alanis, D., *et al.*: 'The road from classical to quantum codes: a hashing bound approaching design procedure', *IEEE Access*, 2015, **3**, pp. 146–176

[21] Babar, Z., Ng, S.X., Hanzo, L.: 'Exit-chart-aided near-capacity quantum turbo code design', *IEEE Trans. Veh. Technol.*, 2015, **64**, (3), pp. 866–875