Sequential quantum secret sharing in noisy environments

Parvaneh Khakbiz · Marzieh Asoudeh

Received: 17 May 2018 / Accepted: 9 November 2018 / Published online: 22 November 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract
Sequential quantum secret sharing (QSS) schemes do not use entangled states for secret sharing, rather they rely on sequential operations of the players on a single state which is circulated between the players. In order to check the viability of these schemes under imperfect operations and noise in the channels, we consider one such scheme in detail and show that under moderate conditions it is still possible to extract viable secure shared keys in this scheme. Although we specifically consider only one type of sequential scheme and three different noise models, our method is fairly general to be applied to other QSS schemes and noise models as well.

Keywords Quantum secret sharing · Noise · Sequential

1 Introduction
Quantum key distribution (QKD) [1,2] and quantum secret sharing (QSS) [3–17] are among the most promising areas in the rapidly developing field of quantum technology. With the growth of demand for secure communication, it is imaginable that in the near future these two protocols will soon be integrated parts of modern communication systems. Both these schemes try to share random sequences of bits between two or more parties in a secure way so that they can use these sequences as a key for encryption and decryption of messages in their further communications. In this sense, QKD is a special case of QSS. In general, if there are N players involved in a QSS scheme, the final result is that each player $R_i$, ($i = 1, \ldots, N$) acquires a random strings of $n$-bits, denoted by $K_i$ so that

$$K_1 + K_2 + \cdots + K_N = 0$$ (1)
where the summation is bitwise and modulo 2. Therefore, when a dealer say $R_1$ wants to send a message $M$ to the other players $R_2, \ldots, R_N$, so that they can only retrieve the message by their full collaboration, he encrypts the message as

$$M \rightarrow M + K_1$$  \hspace{1cm} (2)$$

and sends it to the players who will add their own $K_i$ to make it non-retrievable for any subset of players and retrievable only to the last (authorized player $R_N$) who finds the message in the form

$$M + K_1 + K_2 + \cdots + K_N = M.$$  \hspace{1cm} (3)$$

The main ingredient of almost all the QSS protocols is a multipartite entangled state, like a Greenberger–Horne–Zeilinger (GHZ) state which acts as splitter of information. In view of the extreme fragility of these states and the difficulty for their preparation, there has been a series of attempts to devise QSS protocols which do not need any entanglement [18–22].

While there have been some studies on the performance of entanglement-based QSS schemes [23,24], it seems that there have been almost no studies of the more promising and more practical sequential QSS schemes. There is a report on the effect of noise on a sort of QSS scheme [25]; however, it is not really related to the protocol that we discuss here, since the dealers manipulate entangled states. A related report is that of [26] who studies a protocol with three parties. We should stress that in the protocol [18] that we study here, only a single qubit is circulated between the parties with no entanglement at any stage of the protocol. It is important to note that in view of the highly fragile character of GHZ and other entangled states [27,28], it seems that if QSS schemes become practical in the future, they will be of the sequential rather than the entanglement-based type. Therefore, it is highly desirable to see how in a noisy environment, errors accumulate and how the final error depends on the number of players.

Here we study noise effects in QSS scheme of [18] for arbitrary number of players. We consider two classes of noise. The first class concerns imperfections in the unitary actions of the players, and the second class concerns the noise in the channels between consecutive players. In this later class, we study the effect of a number of well-known and physically motivated channels, namely de-phasing, depolarizing, phase-flip and bit-flip channels. We find that in both classes of imperfections and channel noises, the required precision for establishing a reliable secret scales inversely with the number of players.

The structure of the paper is as follows: In Sect. 2, we briefly describe the general idea of sequential QSS [18,21,22] with emphasis on the special case of the scheme of [18], which will be our model of choice for studying noise effects. To study the sequence of actions of players followed by the effect of noise, we resort to the vectorized formalism for describing states and operations in Sect. 3. Then in Sect. 4, we briefly study the effect of imperfections of unitary actions of players, and then in Sect. 5 we use this formalism to study the effect of de-phasing, depolarizing and bit-flip channels, respectively. We end the paper with a conclusion.
Sequential quantum secret sharing

Sequential quantum secret sharing (QSS) scheme tries to avoid the use of multipartite entangled states and instead tries to develop a scheme which is in the same spirit of the BB84 protocol [1] for quantum key distribution. That is, it is based on circulating and manipulating specific states among the players which if measured in the right basis by the last player will establish a shared random secret key between the players. More concretely, in such schemes there are \( N \) players which we denote by \( R_1, R_2, \ldots, R_N \). The first player prepares a reference state \( |\phi_1\rangle \) (a specific state in a basis \( \{ |e_0\rangle, |e_1\rangle, \ldots, |e_{d-1}\rangle \} \)) in a \( d \)-dimensional space and acts on it by a unitary operator \( U(s_1, p_1) \), where \( s \) and \( p \) stand for a number of secret (private) and public parameters. He then passes the state \( U(s_1, p_1)|e_0\rangle \) to player \( R_2 \) who acts similarly until after a full circle the state comes back to the first player in the form

\[
|\psi_f(\{s, p\})\rangle = U(s_N, p_N) \ldots U(s_2, p_2)U(s_1, p_1)|e_0\rangle
\]  

(4)

The players then announce the public parameters \( p_1 \) to \( p_N \). In a certain fraction of rounds (depending on the scheme, \( \frac{1}{2} \) for [18,21], and \( \frac{1}{d} \) for [22]), which we call valid rounds, the public parameters are such that the state \( |\psi_f(\{s, p\})\rangle \) is one of the states in the basis \( B \), say \( |e_m\rangle \). Since the first players always measure his state in this basis, in such rounds there will be a precise relation between the secret parameters \( s_i \) and the final measured parameter \( m \), in the form

\[
F(m, s_1, s_2, \ldots s_N) = 0. \tag{5}
\]

This relation establishes a shared key between the secret parameters of all the players, in which the parameter \( m \) is also included.

The first QSS scheme of this kind was introduced in [18], where the players use qubits and their unitary action is a phase gate of the form \( U(\phi)|m\rangle = e^{im\phi}|m\rangle \), where \( \phi \in \{0, \frac{\pi}{2}, \frac{3\pi}{2} \} \), as shown in Fig. 1. This set of phase gates can be divided into two classes, Class 0 = \( \{0, \pi\} \) and Class 1 = \( \{\frac{\pi}{2}, \frac{3\pi}{2}\} \). The 1-bit information as to which class has been chosen by a particular player \( R_n \) is a public parameter which is denoted by \( p_n = 0, 1 \), and the information as to which particular phase has been chosen by the player \( R_n \) within a class is a secret parameter kept only with \( R_n \) to be used at the end of the protocol. Starting from \( |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \), the final state will be

\[
|\psi_f\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\phi_1+\phi_2+\ldots+\phi_N}|1\rangle \right). \tag{6}
\]

At the end of the protocol, all the players announce their class values, \( p_i \). The player \( R_1 \) or the dealer measures the final state (6) in the \( X \) basis. When \( \sum_i p_i = 1 \) (mod 2), the final state (6) is an eigenstate of the \( Y \) operator, leading to a probabilistic result (with no correlation) and the round should be discarded as an invalid round. However, when \( \sum_i p_i = 0 \) (mod 2), the final state is an eigenstate of the \( X \) operator and a perfect correlation exists between the secure parameters and the measurement of the final state. That is
Fig. 1 The idea case of the sequential QSS scheme of [18], where states are acted by perfect gates by the players and are transmitted through noiseless channels

\[
\phi_1 + \phi_2 + \cdots + \phi_N = m, \quad (7)
\]

where \( m \) is the result of measurement of the player \( R_1 \) in the X basis. Let us denote the final result of measurement by \( m \) (\( m = 0 \), for + and \( m = 1 \) for −). Then Eq. (7) shows that the shared secret, defined as

\[
K_1 = \frac{\phi_1}{\pi} + m,
K_i = \frac{\phi_i}{\pi}, \quad i = 2, \ldots, N, \quad (8)
\]

will have perfect correlation as follows:

\[
K_1 + K_2 + \cdots K_N = 0. \quad (9)
\]

This will then allow the players to share a secure key among the players. Since the work of [18], many other schemes have also been proposed for sequential QSS [19,21,22], where the use of entanglement is bypassed.

All this has been described under ideal situation, when the gates act perfectly and the channels are noiseless. In a realistic situations, both assumptions need to be replaced with modest assumptions. Here we assume that the classical channels used for public announcements of public parameters are noiseless, but the gates used by players have some imperfections and also the quantum channels used for transmitting the states are
noisy. We want to see how these two kinds of imperfections affect the reliability of this QSS scheme.

3 Vectorization of states and operations

In a sequential QSS scheme, $N$ players are acting on a reference signal one after the other and in each transmission between any two consecutive players, the signal is also affected by noise in the channel. To determine the admissible level of noise in these channels (which at first are assumed to be identical), we have to find the cumulative effect of both the noise and the actions of different players on the initial state. The basic question we are faced with is to determine in an analytic form the cumulative effect of noise and the actions of all individual players. As we will see, the best approach for doing this is to use the vectorized form of quantum channels which for simplicity is described here for qubit states and channels.

Let $\rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a general one-qubit state. To this corresponds a vector

$$|\rho\rangle = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}. \tag{10}$$

A state like $\rho_0 = |+\rangle\langle+|$ where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is depicted as

$$|\rho_0\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}. \tag{11}$$

More generally, a state $\rho = \sum_{i,j} \rho_{i,j} |i\rangle\langle j|$ can be cast into the vector form $|\rho\rangle = \sum_{i,j} \rho_{i,j} |i, j\rangle$. The inner product of two matrices $A$ and $B$ is the same as the inner product of their vectorized forms, that is

$$tr(A^\dagger B) = \langle A|B\rangle. \tag{12}$$

A quantum channel acts on the state $\rho$ as follows

$$\rho \rightarrow \rho' = E(\rho) = \sum_k A_k \rho A_k^\dagger, \tag{13}$$

where

$$\sum_k A_k^\dagger A_k = I. \tag{14}$$
This operation can be depicted as linear map $\mathcal{E}$ on the vector $|\rho\rangle$. In fact

$$|\rho\rangle \longrightarrow |\rho'\rangle = \mathcal{E}|\rho\rangle, \quad \mathcal{E} = \sum_k A_k \otimes A_k^*. \quad (15)$$

The unitary action $U(s_m, p_m) : |\phi\rangle \longrightarrow |\phi'\rangle$ by the $m$-th player can also be written, first as a quantum channel $\rho \longrightarrow U_m(s, p)\rho U_m^\dagger$ and then vectorized in the form

$$|\rho\rangle \longrightarrow U(s_m, p_m)|\rho\rangle = U(s_m, p_m) \otimes U(s_m, p_m)^*|\rho\rangle. \quad (16)$$

Combining all these actions, we find

$$|\rho_f\rangle = \prod_{m=1}^{N} (\mathcal{E}U(s_m, p_m))|\rho_0\rangle \quad (17)$$

where $|\rho_0\rangle$ is the vectorization of the first pure state started by the first player $R_1$ and $|\rho_f\rangle$ is the vectorized form of the final state received by $R_1$. One can then return the final state from the vectorized form $|\rho_f\rangle$ to the standard matrix form $\rho_f$ and analyze its various properties, although this is not really necessary since all the measurement results and probabilities can also be expressed in vector form as in (12).

### 4 Gate imperfections

Let us assume that the phases applied by the players are not exactly in the form $\{0, \frac{\pi}{2}, \frac{3\pi}{2}, \pi\}$, but have error with a fixed average. For example, suppose that each player $R_i$, instead of the phase $\phi_i$, applies a phase $\phi_i + \epsilon_i$, where $\epsilon_i$ is a random phase with average $\bar{\epsilon}$. In this case, the final state will be

$$|\psi_f\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + e^{i(\sum_i (\phi_i + \epsilon_i))} |1\rangle \right). \quad (18)$$

We assume that the errors $\epsilon_i$ are not large enough to change the class of the phases and they only randomly shift the phase within a class. Therefore, we only have to consider valid rounds where $\sum_i \phi_i$ is supposed to be 0 or $\pi \mod 2\pi$. The error is committed when $\sum_i \phi_i = 0$ and the measured state is $|\rangle$ or when $\sum_i \phi_i = \pi$ and the measured state is $|+\rangle$. Assuming that in half of the cases $\sum_i \phi_i = 0$ and in the other half $\sum_i \phi_i = \pi$, we find for a specific set of $\epsilon_i$’s

$$P_{\text{error}} = \frac{1}{2} P \left(-| \sum_i \phi_i = 0 \right) + \frac{1}{2} P \left(| \sum_i \phi_i = \pi \right)$$

$$= \frac{1}{2} \left| \langle - | \psi_f \left( \sum_i \phi_i = 0 \right) \rangle \right|^2 + \frac{1}{2} \left| \langle + | \psi_f \left( \sum_i \phi_i = \pi \right) \rangle \right|^2$$
\[ \frac{1}{2} \left( 1 - \cos \sum_i \epsilon_i \right). \]  

The average rate of error will be given by

\[ P_{\text{error}} = \frac{1}{2} (1 - \cos N\epsilon). \]  

As long as \( P_{\text{error}} \ll \frac{1}{2} \), one can use a privacy amplification algorithm to extract a shorter error-free key from a long key. In this paper, we do not consider these algorithms and only note that amount of the shortening of the key depends on the error probability. Let us demand that \( P_{\text{error}} < \frac{\delta}{2} \), where \( \delta \) is a parameter less than one. Then this means that the phase error is bounded as

\[ \epsilon < \arccos \left( 1 - \frac{\delta}{N} \right) \approx \frac{\sqrt{2\delta}}{N}. \]  

5 Effect of noise in the channels

We now turn to the noise in channels. For simplicity at first we assume that the noise parameters are identical, but later this assumption will be relaxed. We consider four different physically motivated noise channels.

5.1 Phase damping channel

The first channel that we study is the phase damping channel

\[ E_1(\rho) = (1 - p)\rho + pA_0\rho A_0^\dagger + pA_1\rho A_1^\dagger, \]  

with \( A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \) and \( A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \). Such a channel which decreases the phase coherence of the state is perhaps the most relevant type of noise both in the present context and in view of practical considerations. It acts on any single-qubit density matrix as follows

\[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \begin{pmatrix} a & (1 - p)b \\ (1 - p)c & d \end{pmatrix}. \]  

\[ E_1 = \begin{pmatrix} 1 & 1 - p \\ 1 - p & 1 \end{pmatrix}. \]
The action of phase gate can also be depicted by a diagonal matrix $R(\phi_i)$

$$U(\phi_i) = \begin{pmatrix} 1 & e^{i\phi_i} \\ e^{-i\phi_i} & 1 \end{pmatrix}. \quad (25)$$

In view of the vectorized form of the initial state (11), we find

$$|\rho_f\rangle = EU(\phi_N) \ldots EU(\phi_2)EU(\phi_1)|\subset_0\rangle = \frac{1}{2} \begin{pmatrix} 1 & \frac{1}{(1-p)^N e^{\sum_i i\phi_i}} \\ (1-p)^N e^{\sum_i i\phi_i} & 1 \end{pmatrix}. \quad (26)$$

In matrix form, the final state will be given by

$$\rho_f = \begin{pmatrix} 1 & (1-p)^N e^{\sum_i i\phi_i} \\ (1-p)^N e^{\sum_i i\phi_i} & 1 \end{pmatrix}. \quad (27)$$

This shows that when, after a full round, the first player measures the state in the $X$-basis, there is no perfect correlation anymore. In fact, the first player obtains both $|+\rangle$ and $|-\rangle$ with the following conditional probabilities:

$$P(+|\sum_i \phi_i) = \langle +|\rho_f|+\rangle = \frac{1}{2} \left( 1 + (1-p)^N \cos \left( \sum_{i=1}^{N} \phi_i \right) \right)$$

$$P(-|\sum_i \phi_i) = \langle -|\rho_f|-\rangle = \frac{1}{2} \left( 1 - (1-p)^N \cos \left( \sum_{i=1}^{N} \phi_i \right) \right). \quad (28)$$

It can be seen that in the absence of noise (when $p = 0$), there is a perfect correlation between the result of the last measurement and the sum of phases. For example, we have $P(+|\sum_i \phi_i = 0) = 1$, and $P(-|\sum_i \phi_i = 0) = 0$.

The presence of noise decreases this correlation and leads to errors. Assuming that all the phases are chosen randomly by the players, we have $P(\sum_i \phi_i) = \frac{1}{2}$, and hence, the probability of error is given by

$$P_{\text{error}} = \frac{1}{2} P \left( -|\sum_i \phi_i = 0 \right) + \frac{1}{2} P \left( +|\sum_i \phi_i = \pi \right) = \frac{1}{2} \left( 1 - (1-p)^N \right). \quad (29)$$

Again if we demand that $P_{\text{error}} < \frac{\delta}{2}$, this leads to the following bound for the noise parameter $p$,

$$p < 1 - (1-\delta)^{\frac{1}{N}} \approx \frac{\delta}{N}. \quad (30)$$
showing that the level of admissible noise decreases inversely with the number of players.

If the noise parameters are not equal which is quite expected in view of different distances between the players, then a simple look at the previous analysis leads to generalization of (29) with the following

$$P_{\text{error}} = \frac{1}{2} \left( 1 - \prod_{i=1}^{N} (1 - p_i) \right). \quad (31)$$

This shows that if one of the channels has a large noise, i.e., $p_i \approx 1$, then $P_{\text{error}} \approx \frac{1}{2}$, rendering the whole scheme useless. To understand this effect, note that assume that the $i$-th channel has $p_i = 1$. Then any previous state which is necessarily in the form $\frac{1}{2} \begin{pmatrix} 1 & c \\ c^* & 1 \end{pmatrix}$, when passing through this channel, becomes equal to $\frac{1}{2} I$, and this completely mixed state is never affected by the actions of the subsequent players, leading to no correlation at the end of the protocol.

5.2 Depolarizing channel

The second channel that we consider is the depolarizing channel defined as

$$E_2(\rho) = (1 - p)\rho + \frac{p}{2} \text{tr}(\rho)I. \quad (32)$$

To vectorize this channel, we note that for a qubit $\text{tr}(\rho) = a + d$ and rewrite this as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \begin{pmatrix} (1 - \frac{p}{2})a + \frac{p}{2}d \\ (1 - p)c \\ (1 - \frac{p}{2})d + \frac{p}{2}a \end{pmatrix}. \quad (33)$$

which shows that the vectorized form of the channel is given by

$$E_2 = \begin{pmatrix} 1 - \frac{p}{2} & 1 - p & \frac{p}{2} \\ 1 - \frac{p}{2} & 1 - p & \frac{p}{2} \\ \frac{p}{2} & \frac{p}{2} & 1 - \frac{p}{2} \end{pmatrix}. \quad (34)$$

The combination of this channel with the unitary action of each player is given by

$$E_2 U(\phi_m) = \begin{pmatrix} 1 - \frac{p}{2} & \frac{p}{2} \\ (1 - p)e^{i\phi_m} & (1 - p)e^{-i\phi_m} \\ \frac{p}{2} & 1 - \frac{p}{2} \end{pmatrix}. \quad (35)$$
The product of all these matrices is then given by

$$\prod_{m=1}^{N} \mathcal{E}_2 R(\phi_m) = \begin{pmatrix} \frac{1+\eta N}{2} & (1-p)^N e^{i \sum_m \phi_m} & \frac{1-\eta N}{2} \\ \frac{1-p N}{2} & (1-p)^N e^{-i \sum_m \phi_m} & \frac{1+p N}{2} \end{pmatrix}$$

(36)

where $\eta = (1-p)$. The final density matrix $|\rho_f\rangle$ is obtained by acting this linear operator on the vectorized form of the state $|+\rangle\langle+|$. This state which will be measured by the player $R_1$ is given by

$$|\rho_f\rangle = \frac{1}{2} \begin{pmatrix} (1-p)^N e^{i \sum_m \phi_m} \\ (1-p)^N e^{-i \sum_m \phi_m} \\ 1 \end{pmatrix}.$$  

(37)

Although the channels act differently on general input states, it is seen that the final state is the same as the one in the previous subsection. Therefore, the same analysis and the same bound are also valid here.

### 5.3 Bit-flip channel

The last channel that we study is the bit-flip channel which requires a more detailed analysis. It is defined by

$$E_3(\rho) = (1-p)\rho + pX\rho X.$$  

(38)

which transforms the state in the following way

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow \begin{pmatrix} (1-p)a + pd & (1-p)b + pc \\ (1-p)c + pb & (1-p)d + pa \end{pmatrix}.$$  

(39)

From this, we can extract the matrix form of the CPT map $E_2$:

$$E_3 = \begin{pmatrix} 1-p & 1-p & p \\ 1-p & p & 1-p \\ p & 1-p & 1-p \end{pmatrix}.$$  

(40)

The concatenation of the action of the $m$-th player and the action of the channel $E_2$ is given by

$$E_3 R(\phi_m) = \begin{pmatrix} 1-p & (1-p)e^{i \phi_m} & p e^{-i \phi_m} \\ (1-p)e^{i \phi_m} & p e^{-i \phi_m} & 1-p \end{pmatrix}.$$  

(41)
The above matrix has a block form, written as

\[ E_3 U(\phi_m) = A_m \oplus B_m, \]  

(42)

where

\[ A_m = \begin{pmatrix} 1 - p & p \\ p & 1 - p \end{pmatrix} \]  

(43)

is the outer block matrix and

\[ B_m = \begin{pmatrix} (1 - p) e^{i\phi_m} & p e^{-i\phi_m} \\ p e^{i\phi_m} & (1 - p) e^{-i\phi_m} \end{pmatrix} \]  

(44)

is the inner block matrix. This form easily allows us to multiply a sequence of such matrices in a straightforward way. We readily find

\[ \prod A_m = \frac{1}{2} \left( 1 + \gamma^N 1 - \gamma^N \right). \]  

(45)

where

\[ \gamma = (1 - 2p). \]  

(46)

The calculation of \( \prod B_m \) is a little tricky. First, we note that

\[ B_m = ((1 - p)I + pX) e^{i\phi_mZ}. \]  

(47)

In general (i.e., for arbitrary values of \( \phi_m \)), it is difficult to simplify a product of such matrices, since the passing of \( e^{i\phi_mZ} \) creates complicated terms when cumulated after many passings. However, we note that \( \phi_m \) takes only specific values from the set

\[ \left\{ 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2} \right\} \equiv \{ I, iZ, -I, -iZ \}. \]  

(48)

This can be written compactly as

\[ e^{i\phi_mZ} = (-1)^{s_m} (iZ)^{p_m}, \]

where \( s_m \in \{0, 1\} \) and \( p_m \in \{0, 1\} \) are, respectively, the secret and public parameters of the player \( R_m \). In fact, the parameter \( p \) shows the class and \( s \) shows the phase within the class. \( p \) is made public and \( s \) is kept secret. In order to calculate \( \prod B_m \), we rewrite \( B_m \) as follows:

\[ B_m = ((1 - p)I + pX) (-1)^{s_m} (iZ)^{p_m}. \]  

(49)
It is now easy to pass $ZP_m$ through different terms in the product. For example, we find

$$B_1 B_2 = (-1)^{s_1+s_2} ((1 - p)I + pX) (iZ)^{P_1} ((1 - p)I + pX) (iZ)^{P_2}$$

$$= (-1)^{s_1+s_2} ((1 - p)I + pX) ((1 - p)I + p(-1)^{P_1} X) (iZ)^{P_1+P_2} \quad (50)$$

Continuing in this way, we find:

$$\prod_{m} B_m = (-1)^{s_1+s_2+\cdots+s_N} \prod_{m=1}^{N} [(1 - p)I + p\xi_{m-1}X] (iZ)^{\sum_{m=1}^{N} p_m} \quad (51)$$

where

$$\xi_m = (-1)^{\sum_{i=1}^{m} p_i} \quad (52)$$

Hereafter we consider only the case of valid rounds where $\sum_{m=1}^{N} p_m = 0$ which considerably simplifies subsequent calculations. Using the fact that $HXH = Z$, where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard matrix, we find

$$\prod_{m} B_m = H \begin{pmatrix} a_N \\ b_N \end{pmatrix} H \quad (53)$$

where

$$a_N = \eta_N \prod_{m=1}^{N} (1 - p + p\xi_{m-1}), \quad b_N = \eta_N \prod_{m=1}^{N} (1 - p - p\xi_{m-1}) \quad (54)$$

in which we have used $\sqrt{\xi_N}$ as a short way of writing $(i)^{\sum_{m=1}^{N} p_m}$ and $\eta_N$ is determined by the sum of secret parameters:

$$\eta_N := (-1)^{\sum_{m=1}^{N} s_m} \quad (55)$$

Multiplying the Hadamard matrices, the product of inner matrix blocks is found:

$$\prod_{m} B_m = \frac{1}{2} \begin{pmatrix} a_N + b_N & a_N - b_N \\ a_N - b_N & a_N + b_N \end{pmatrix} \quad (56)$$

The final density matrix in the vectorized form is now given by

$$|\rho_f\rangle = \frac{1}{2} \begin{pmatrix} 1 + \gamma^N & 1 - \gamma^N \\ a_N + b_N (a_N - b_N) & a_N - b_N (a_N + b_N) \\ (1 - \gamma^N) \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad (57)$$
or

\[ |\rho_f\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ a_N \\ a_N \\ 1 \end{pmatrix} \] (58)

In matrix form, this density matrix is given by:

\[ \rho_f = \frac{1}{2} \begin{pmatrix} 1 & a_N \\ a_N & 1 \end{pmatrix}. \] (59)

We can now calculate the error probability. To this end, we note that contrary to the previous cases, the probability of results of measurement in the \( X \) basis depends not on the sum of parameters but on each of them. This is due to relation (54). So we find

\[
P(+|\{s_i\}) = \frac{1}{2} (1 + a_N) = \frac{1}{2} \left( 1 + (-1)^{\sum_{m=1}^{N} s_m} \prod_{m=1}^{N} (1 - p + p\xi_{m-1}) \right)
\]

\[
P(-|\{s_i\}) = \frac{1}{2} (1 - a_N) = \frac{1}{2} \left( 1 - (-1)^{\sum_{m=1}^{N} s_m} \prod_{m=1}^{N} (1 - p + p\xi_{m-1}) \right).\] (60)

As a test we note that when \( p = 0 \), we find that

\[
P(+|\{s_i\}) = \frac{1}{2} (1 + (-1)^{\sum_{m=1}^{N} s_m}) = \delta \left( \sum_{m=1}^{N} s_m, 0 \right),
\]

\[
P(-|\{s_i\}) = \frac{1}{2} (1 - (-1)^{\sum_{m=1}^{N} s_m}) = \delta \left( \sum_{m=1}^{N} s_m, 1 \right),\] (61)

which shows that when \( \sum_{m=1}^{N} s_m = 0 \), the measurement result is definitely + and when \( \sum_{m=1}^{N} s_m = 1 \), then the measurement result is definitely -. This is the perfect correlation which is expected in the absence of noise.

Let us denote by \( \{s_i\}_0 \), the set of all parameters \( \{s_1, s_2, \ldots s_N\} \) such that their sum equals zero, i.e., \( \{s_i\}_0 = \{s_1, s_2, \ldots s_N \mid s_1 + s_2 + \cdots + s_N = 0\} \) with a similar definition for \( \{s_i\}_1 \). Then, the conditional probabilities that we need are the following:

\[
P(+|\{s_i\}_1) = \frac{1}{2} \left( 1 - \prod_{m=1}^{N} (1 - p + p\xi_{m-1}) \right)
\]

\[
P(-|\{s_i\}_0) = \frac{1}{2} \left( 1 - \prod_{m=1}^{N} (1 - p + p\xi_{m-1}) \right).\] (62)
The equality of these two terms makes the calculation of the final error probability feasible, since, using \( \sum_{\{s_i\}_0} + \sum_{\{s_i\}_1} = \sum_{s_1,s_2,\ldots,s_N} \), we can write

\[
P_{\text{error}} = \sum_{\{s_i\}_0} P(s_1, s_2, \ldots, s_N) P(-|\{s_i\}_0) + \sum_{\{s_i\}_1} P(s_1, s_2, \ldots, s_N) P(+|\{s_i\}_1)
\]

\[
= \frac{1}{2} \sum_{s_1,s_2,\ldots,s_N} P(s_1, s_2, \ldots, s_N) \left( 1 - \prod_{m=1}^{N} (1 - p + p\xi_{m-1}) \right)
\]

(63)

Naturally, due to independence of the actions of players, we have the uniform distribution \( P(s_1, s_2, \ldots, s_N) = \frac{1}{2^N} \). We also note that all the parameters \( \xi_m \) are also independent, taking the values 1 and \(-1\) with equal probabilities. Therefore (in view of \( \xi_0 = 1 \)) we find

\[
\sum_s (1 - p + p\xi_0) = \sum_s (1 - p + p) = 2 \sum_s (1 - p + p\xi_m)
\]

\[
= \sum_s (1 - p + p\xi_m) = 2 - 2p.
\]

(64)

Putting everything together, the final error probability will be

\[
P_{\text{error}} = \frac{1}{2} \left( 1 - (1 - p)^{N-1} \right).
\]

(65)

This leads to the same bound as in (30) with \( N \) replaced with \( N - 1 \).

In view of the lengthy calculations of this case, let us study the simplest case in a concrete way, where \( N = 2 \), and follow the operations from the beginning. The player \( R_1 \) prepares the state \( |\psi_0\rangle = |+\rangle \) and acts on it by his phase gate to produce \( |\psi_1\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i\phi_1}|1\rangle) \). This state undergoes the bit-flip noise and becomes

\[
\rho_1 = \frac{1}{2} \begin{pmatrix}
(1 - p)e^{i\phi_1} & 1 \\
1 & (1 - p)e^{-i\phi_1} + pe^{i\phi_1}
\end{pmatrix}.
\]

(66)

When reached to \( R_2 \), it is acted by a second phase gate \( R(\phi_2) \) and becomes

\[
\rho_1 = \frac{1}{2} \begin{pmatrix}
(1 - p)e^{i\phi_1+i\phi_2} & 1 \\
1 & (1 - p)e^{-i\phi_1-i\phi_2} + pe^{i\phi_1+i\phi_2}
\end{pmatrix}
\]

\[
= \frac{1}{2} \begin{pmatrix}
1 & a \\
\bar{a} & 1
\end{pmatrix}
\]

(67)

where the last equality defines the parameter \( a \). Before deriving the final matrix, when noise acts on this matrix, let us find the density matrix at this stage for various values of \( \phi_1 \) and \( \phi_2 \) in the valid rounds. These values are shown in Table 1 together with the form of the matrix \( \rho_1 \). It is now clearly seen that all of these later states are invariant under bit-flip noise and so the final density matrix \( \rho_f \) is the same as \( \rho_1 \) shown in
Table 1 Different final states of the sequential QSS protocol (Fig. 1) in the presence of bit-flip noise and the corresponding probabilities for obtaining them

| $\phi_1$ | $\phi_2$ | $a$ | $\rho_1$                     | $P(\phi)$ | $P(\psi)$ | $P_{\text{error}}$ |
|---------|---------|-----|-----------------------------|-----------|-----------|---------------------|
| 0       | 0       | 1   | $|+\rangle\langle+|$         | 1*        | 0         | 0                   |
| 0       | $\pi$   | -1  | $|-\rangle\langle-|$         | 0         | 1*        | 0                   |
| $\pi$   | 0       | -1  | $|-\rangle\langle-|$         | 0         | 1*        | 0                   |
| $\frac{\pi}{2}$ | $\frac{\pi}{2}$ | 2$p$ - 1 | $\frac{1}{2} \begin{pmatrix} 1 & 2p - 1 \\ 2p - 1 & 1 \end{pmatrix}$ | $p$ | $(1 - p)^*$ | $p$ |
| $\frac{\pi}{2}$ | $\frac{3\pi}{2}$ | 1 - 2$p$ | $\frac{1}{2} \begin{pmatrix} 1 & 1 - 2p \\ 1 - 2p & 1 \end{pmatrix}$ | $(1 - p)^*$ | $p$ | $p$ |
| $\frac{3\pi}{2}$ | $\frac{\pi}{2}$ | 1 - 2$p$ | $\frac{1}{2} \begin{pmatrix} 1 & 1 - 2p \\ 1 - 2p & 1 \end{pmatrix}$ | $p$ | $(1 - p)^*$ | $p$ |
| $\frac{3\pi}{2}$ | $\frac{3\pi}{2}$ | 2$p$ - 1 | $\frac{1}{2} \begin{pmatrix} 1 & 2p - 1 \\ 2p - 1 & 1 \end{pmatrix}$ | $(1 - p)^*$ | $p$ | $p$ |

Table 1. The last three columns show probabilities of obtaining $+$ and $-$ in the final measurement of $X$ by the first player $R_1$ and the probability of error. Note that in each row, the superscript $*$ denotes which result is expected (in view of the parameter $\phi_1 + \phi_2$). This easily determines the error probability in each case:

From the table, we see that in 4 out of 8 cases the probability of error is $p$, making the total probability of error equal to $\frac{p}{2}$, in accord with Eq. (65).

6 Amplitude damping channel

As the last example, we consider the amplitude damping (AD) channel which is a non-unital channel and express the probability of photon loss in transmissions between the players. The computations of this case are very similar to the previous ones. We will be briefed and only quote the results. The channel is given by

$$E_4(\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger,$$

with $A_0 = \begin{pmatrix} 1 & 0 \\ 0 & \cos \theta \end{pmatrix}$ and $A_1 = \begin{pmatrix} 0 & \sin \theta \\ 0 & 1 \end{pmatrix}$. Under this channel, the vectorized form of the density matrix transforms as $|\rho\rangle \rightarrow E_4|\rho\rangle$ where

$$E_4 = \begin{pmatrix} 1 & \sin^2 \theta \\ \cos \theta & \cos \theta \\ 0 & \cos^2 \theta \end{pmatrix}.$$  

The final state will be $|\rho_f\rangle = \left[\prod_{m=1}^{N} E_4 R(\phi_m)\right] |\rho_0\rangle$ where $|\rho_0\rangle$, as in the previous cases, is the vectorized form of the initial density matrix $\rho_0 = |+\rangle\langle+|$. The matrix form of the final state will be given by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & \sin \theta \\ 0 & -\sin \theta & \cos \theta \end{pmatrix}.$$
\[ \rho_f = \frac{1}{2} \left( \frac{2 - \cos^2 N \theta}{\cos^N \theta e^{i \sum_m \phi_m}} \cos^N \theta e^{-i \sum_m \phi_m} \cos^2 N \theta \right). \] (70)

The probability of measuring + or − by the first player on this final state is easily found to be

\[ \langle + | \rho_f | + \rangle = \frac{1}{2} \left( 1 + \cos^N \theta \cos \left( \sum_{i=1}^N \phi_i \right) \right), \]

\[ \langle - | \rho_f | - \rangle = \frac{1}{2} \left( 1 - \cos^N \theta \cos \left( \sum_{i=1}^N \phi_i \right) \right). \] (71)

According to the protocol, there will be errors when \( \sum_i \phi_i = 0 \) and the first player obtains − or when \( \sum_i \phi_i = \pi \) and the first player obtains +. Thus, the error rate is given by

\[ P_{\text{error}} = \frac{1}{2} (1 - \cos^N \theta). \] (72)

Again if we demand the final error rate is less than \( \frac{\delta}{2} \), this means that the level of admissible noise in the amplitude damping channel should be limited to:

\[ \cos \theta \geq 1 - \frac{\delta}{N}. \] (73)

This means that the level of admissible noise decreases inversely proportional to the number of players which is indeed very promising.

### 7 Impact on security

Although quantum key distribution protocols like the BB84 have been rigorously proved to be absolutely secure, to the best of our knowledge very little has been done to prove the absolute security of quantum secret sharing schemes. In fact the only work which has started to address this problem for the original three player scheme of Buzek et al. [3] is reference [24]. This is of course expected in view of the complex nature of QSS protocols and the different means which cheating can occur, i.e., collaboration of Eve with a subset of the players, entangling herself in various ways with the states of the players, intercept and resend by dishonest parties in different stages, malicious action by some players in the public announcements of the bases, etc. In fact, many of the QSS schemes introduced in the literature including the multiparty schemes [29,30] have later been proved to be insecure against certain types of attacks, and ways for their improvement against these types of attacks have also been proposed. The attacks include intercept–resent [20] and Trojan horse [31,32] among other types. This is also true for the sequential scheme studied in this paper [18] where it was shown in [20] to be insecure against a specific kind of intercept and resent attack. The protocol was
later improved in [33] which again turned out not to be secure against another attack [34]. In the same paper [34], a modified scheme using some error-correcting code was proposed to remove the vulnerability of the scheme.

In this paper, we are not introducing a new kind of secret sharing scheme, rather we are mainly with the effect of noise on the transmission of states between the parties, and therefore, all the considerations for the insecurity of the original protocol [18] or its improvement [33] against the attacks discussed are also valid here. The usefulness of our consideration and our bounds on the final error rates helps the players to distinguish between different sources of errors, namely those which are caused by the malicious actions of adversaries or cheating players and those which are caused by the noise in the channels used for transmission of states between the players. The very fact that the later error rate scales in a specific way with the number of players which is very different from the case where intercept recent or Trojan horse attack occurs is quite useful in this discrimination.

8 Conclusion

We have used the vectorized form of quantum channels and quantum operations to study the effect of different gate imperfections and different kinds of noise on sequential quantum secret sharing schemes. The noise model considered is de-phasing, depolarizing and bit-flip channels. Quite similar analysis and results can also be obtained for phase-flip channel and the amplitude damping channels, although for the sake of brevity the corresponding analysis has not been reported. We have considered only one type of scheme [18] based on sequential manipulations of qubits and have found that the accumulated error probability cannot render the protocol ineffective. In all the noise models, we have found that in order to extract an error-free shared secret key, the tolerable noise parameter in the channels and the tolerable error in gates scale linearly with the error and inversely with the number of players in the scheme. Although we have studied only one type of QSS scheme, the method is fairly general to apply it for other schemes and for other noise models. This means essentially that the QSS scheme of [18] and hence the other sequential models [21,22] are effective even in the presence of noise. An open problem even in the absence of noise is how to perform QSS with \((k, n)\) access structures in a sequential way and without entanglement. These are the schemes in which any subset of \(k\) players out of \(n\) players can retrieve the key and subsets of lower size cannot [35–38].

Acknowledgements This work was financially supported by the Grant no. 96011347 from Iran National Science Foundation (INSF). M. A. would like to thank Abdus Salam International Center for Theoretical Physics (ICTP), where part of this research was carried out. She also thanked V. Karimipour for many discussions and Fabio Benatti for his valuable comments.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEEInternational Conference on Computers, Systems and Signal Processing, vol. 175, pp. 8. New York (1984)
2. Ekert, A.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 67, 661–663 (1991)
3. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A 59, 1829 (1999)
4. De Sen, A., Sen, U., Zukowski, M.: Multiqubit W states lead to stronger nonclassicality than Greenberger–Horne–Zeilinger states. Phys. Rev. A 68, 032309 (2003)
5. Xiao, L., Long, G.L., Deng, F.-G., Pan, J.-W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A 59, 1829 (1999)
6. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A 59, 162 (1999)
7. Xiao, L., Lu Long, G., Deng, F.-G., Pan, J.-W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A 69, 052307 (2004)
8. Zhang, Z-j, Man, Z-x: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A 72, 022303 (2005)
9. Deng, F.-G., Long, G.L., Zhou, H.-Y.: Probabilistic teleportation of an arbitrary GHZ-class state with a pure entangled two-particle quantum channel and its application in quantum state sharing. Phys. Lett. A 340, 43 (2005)
10. Bagherinezhad, S., Karimipour, V.: Quantum secret sharing based on reusable Greenberger–Horne–Zeilinger states as secure carriers. Phys. Rev. A 67, 044302 (2003)
11. Chen, Y.-A., et al.: Experimental quantum secret sharing and third-man quantum cryptography. Phys. Rev. Lett. 95, 200502 (2005)
12. Gaertner, S., Kurtsiefer, C., Bourennane, M., Weinfurter, H.: Experimental demonstration of four-party quantum secret sharing. Phys. Rev. Lett. 98, 020503 (2007)
13. Tyc, T., Sanders, B.C.: How to share a continuous-variable quantum secret by optical interferometry. Phys. Rev. A 65, 042310 (2002)
14. Lance, A.M., Symul, T., Bowen, W.P., Tyc, T., Sanders, B.C., Lam, P.K.: Continuous variable (2,3) threshold quantum secret sharing schemes. New J. Phys. 5, 4 (2003)
15. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Tripartite quantum state sharing. Phys. Rev. Lett. 92, 177903 (2004)
16. Grosshans, F., Van Assche, G., Wenger, J., Brouni, R., Cerf, N.J., Grangiera, P.: Quantum key distribution using Gaussian-modulated coherent states. Nature 421, 238–241 (2003)
17. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 88, 057902 (2002)
18. Schmid, C., Trojek, P., Bourennane, M., Kurtsiefer, C., Zukowski, M., Weinfurter, H.: Single qubit quantum secret sharing. Phys. Rev. Lett. 95, 230505 (2005)
19. Yan, F.-L., Gao, T.: Quantum secret sharing between multiparty and multiparty without entanglement. Phys. Rev. A 72, 012304 (2005)
20. He, G.-P.: Secret sharing without monitoring signal disturbance. Phys. Rev. Lett. 98, 028901 (2007)
21. Karimipour, V., Asoudeh, M.: Quantum secret sharing and random hopping; using single states instead of entanglement. Phys. Rev. A 92, 030301 (2015). (Rapid Communications)
22. Tavakoli, A., Herbauts, I., Zukowski, M., Bourennane, M.: Sequential quantum secret sharing in noisy environments (preprint). arXiv:1501.05582
23. Chen, K., Lo, H.-K.: Multi-partite quantum cryptographic protocols with noisy GHZ states. Quantum Inf. Comput. 7, 689 (2007)
24. Kogias, I., Xiang, Y., He, Q., Adesso, G.: Unconditional security of entanglement-based continuous-variable quantum secret sharing. Phys. Rev. A 95, 012315 (2017)
25. Ray, M., Chatterjee, S., Chakrabarty, I.: Sequential quantum secret sharing in a noisy environment aided with weak measurements. Phys. J. D 70, 114 (2016)
26. Adhikari, S., Chakrabarty, I., Agrawal, P.: Probabilistic secret sharing through noisy quantum channels. Quantum Inf. Comput. 12, 0253 (2012)
27. Bohmann, M., Sperling, J., Vogel, W.: Entanglement and phase properties of noisy NOON states. Phys. Rev. A 91, 042332 (2015)
28. Bohnmann, M., Sperling, J., Vogel, W.: Entanglement verification of noisy NOON states. Phys. Rev. A 96, 012321 (2017)
29. Zhang, Z-j, Li, Y., Man, Z-x: Multiparty quantum secret sharing. Phys. Rev. A 71, 044301 (2005)
30. Zhu, X., Fan, Z.: Secure direct communication based on secret transmitting order of particles. Phys. Rev. A 73, 022338 (2006)
31. Deng, F.-G., Li, X.-H., Zhou, H.-Y., Zhang, Z-j: Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys. Rev. A 72, 044302 (2005)
32. Li, X.-H., Deng, F.-G., Zhou, H.-Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A 74, 054302 (2006)

33. Schmid, C., et al.: Reply to comment on experimental single qubit quantum secret sharing. Phys. Rev. Lett. 98, 028902 (2007)

34. He, G.P., Wang, Z.D.: Single qubit quantum secret sharing with improved security. Quantum Inf. Comput. 10, 28 (2010)

35. Lance, A.M., Symul, T., Bowen, W.P., Tyc, T., Sanders, B.C., Lam, P.K.: Continuous variable (2, 3) threshold quantum secret sharing schemes. New J. Phys. 5, 4 (2003)

36. Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. Phys. Rev. A 78, 042309 (2008)

37. Lau, H.-K., Weedbrook, C.: Quantum secret sharing with continuous-variable cluster states. Phys. Rev. A 88, 042313 (2013)

38. Wu, Y., Cai, R., He, G., Zhang, J.: Quantum secret sharing with continuous variable graph state. Quantum Inf. Proc. 13, 1085 (2014)