International Journal of Quantum Information
Vol. 10, No. 2 (2012) 1250018 (22 pages)

DOI: 10.1142/S0219749912500189

World Scientific
www.worldscientific.com

SECURE QUANTUM CARRIERS FOR QUANTUM STATE SHARING

VAHID KARIMIPOUR*

Department of Physics, Sharif University of Technology, Tehran, Iran
vahid@sharif.edu

MILAD MARVIAN

Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran
milad.marvian@ee.sharif.edu

Received 16 October 2010
Published 26 March 2012

We develop the concept of quantum carrier and show that messages can be uploaded and downloaded from this carrier and while in transit, these messages are hidden from external agents. We explain in detail the working of the quantum carrier for different communication tasks, including quantum key distribution, classical secret and quantum state sharing among a set of n players according to general threshold schemes. The security of the protocol is discussed and it is shown that only the legitimate subsets can retrieve the secret messages, the collaboration of all the parties is needed for the continuous running of the protocol and maintaining the carrier.

Keywords: Quantum carrier; entanglement; secret sharing; threshold schemes.

1. Introduction

Entanglement has been used in many different protocols of quantum information theory, from teleportation and key distribution to secret sharing.[1–13] In all these protocols, entanglement is a resource which is completely consumed by measurements of the parties involved and should be generated anew for next rounds of protocol. It is true that generating and maintaining entanglement between several particles is very difficult. Yet with the developments in realizing quantum repeaters,[14–16] creating and maintaining long distance entanglement between stationary quantum systems becomes more feasible in the (possibly distant) future. It is thus rewarding to imagine if this entanglement can be used in a different way, that is as a carrier of information, which modulates and transmits quantum

* Corresponding author.

information, in the same way as carrier waves in classical communication systems carry modulated messages. In this new application, we can imagine that arbitrary quantum states are uploaded (entangled) to the carrier by the sender and downloaded (disentangled) from the carrier by the receiver(s), in such a way that at the end of the protocol, the carrier remains intact and ready for use in next rounds. The role of the quantum carrier and its entanglement with the messages will be to hide messages from adversaries, hence the term secure quantum carrier.

This new way for using entanglement was first reported in Ref. 17 for quantum key distribution and then was developed for a simple secret sharing scheme in Refs. 9–11. In this paper we want to develop it further and provide quantum carriers for secret sharing schemes for general threshold schemes.[18,19] Needless to say, our aim is not to develop new quantum secret sharing schemes, but to develop a quantum carrier for distributing in a secure way the already known quantum secrets among the parties. Our emphasis is thus on the very concept of secure quantum carrier and the way it can be used in quantum communication protocols. In the particular context of quantum secret sharing, as we will see it allows us to generate broader threshold schemes than those of Refs. 20 and 21.

In particular we have to stress the difference with the works in Refs. 20 and 21 where it was shown that graph state formalism[22] can act as a framework for unifying some of the secret sharing protocols, albeit not for general threshold structures. The idea of Refs. 20 and 21 was to encode the secret in some local actions of the dealer on a vertex of a suitably chosen weighted graph state. Local measurements of the players on different vertices of this graph, could then reveal the secret to authorized subsets of players. In this way, it was shown that threshold schemes of the type $(n, n), (2, 3)$ and $(3, 5)$ can be implemented in a unified way for various forms of channels interconnecting the dealer and the players. Therefore the works of Refs. 20 and 21 belong to the same class as in Ref. 1, in which entanglement is fully consumed due to measurements of the players.

It is to be noted that while the idea of a fixed quantum carrier has an appeal for communication, a price should be paid for its implementation: It requires a larger number of particles to be entangled at the beginning and end of the protocol, but at the end of each round a fixed amount of entanglement remains in the form of a carrier. Nevertheless, it is worth to develop such a concept from theoretical side and hope that it will someday become close to reality.

We remark that although we present our analysis for secure communication of basis states or classical information, the idea also works for sending arbitrary quantum states. In the simplest protocol discussed in the beginning of the paper we explicitly show this, although we will not repeat it for other general schemes.

The structure of this paper is as follows. In Sec. 2 we put forward the basic requirements that a quantum carrier should satisfy, in Sec. 3 we explain the basic method in the simplest possible setting, that is quantum key distribution between two parties. Then in Sec. 4 we briefly explain the use of quantum carrier for the simplest secret sharing scheme, where one dealer wants to share a secret between

two different players who have equal right for retrieving the message collaboratively. For this reason, this is called a $(2, 2)$ secret sharing scheme. This is then generalized to the (n, n) scheme where a secret is to be shared between n players and all the n players can retrieve the message collaboratively. Finally in Sec. 6 we define the carrier for the (k, n) threshold scheme where any of the k players can retrieve the secret, although collaboration of all of the players is needed for the continuous running and security of the protocol. We end the paper with conclusion and outlook.

2. General Considerations on the Quantum Carrier

Suppose that a quantum carrier has been set up for a specific communication task, i.e. for a quantum key distribution between Alice and Bob or a secret sharing scheme, between Alice as the dealer and Bob and Charlie as the players. This quantum carrier should have the following properties:

(i) There should be simple and local uploading and downloading operators, so that the legitimate parties can upload and download messages to or from this carrier.
(ii) While in transit, the messages should be hidden from third parties so that no intercept-resend strategy can reveal the identity of the message.
(iii) Eve should not be able to entangle herself to the quantum carrier without being detected by the legitimate parties. This property is to prevent Eve from conducting more complex attacks.

Once such criteria are met, we say that a secure quantum carrier has been set up for this communication task. In the rest of this paper we present quantum carriers for various communication tasks. We should stress again that these requirements are purely from the theoretical point of view, the main difficulty will obviously be to maintain the carrier for a long enough time so that it can be used for passing many quantum states before the entanglement decays and becomes useless.

3. Quantum Carrier for Key Distribution

The first task that we discuss is the simple communication between two parties, where Alice wants to send a sequence of bits 0 and 1, a classical message, to Bob.[17] Alice encodes the classical bits 0 and 1 into states $|0\rangle$ and $|1\rangle$ (the eigenbases of the Z operator). The quantum carrier is

$$|\phi\rangle_{a,b} := \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle)_{a,b}, \tag{1}$$

where a and b refer to the Hilbert spaces of Alice and Bob, respectively. The Hilbert space of the message is denoted by a number 1 (since one qubit is being transmitted). The uploading operator, used by Alice, is a CNOT operator which we denote by $C_{a,1}$,

$$C_{a,1}|i,j\rangle_{a,1} = |i, i+j\rangle_{a,1}. \tag{2}$$

The downloading operator is $C_{b,1}$, i.e. with control port by Bob and target port the message.

Consider now a classical bit s which is encoded to the quantum state $|s\rangle$ and is to be transferred from Alice to Bob. Alice performs the local operation $C_{a,1}$ on the state $|\phi\rangle_{a,b}|s\rangle_1$, turning this state into

$$|\phi_s\rangle_{a,b,1} = \frac{1}{\sqrt{2}}(|0,0,s\rangle + |1,1,s'\rangle)_{a,b,1}, \tag{3}$$

where $s' := s + 1 \bmod 2$. While in transit the message is in the state

$$\rho_1^s = \frac{1}{2}(|s\rangle\langle s| + |s'\rangle\langle s'|) = \frac{1}{2}I, \tag{4}$$

and hence inaccessible to Eve. At the destination, Bob can download the message from the carrier by his local operation $C_{b,1}$, which disentangles the message and leaves the carrier in its original form, ready for use in the next round. The fact that Bob downloads exactly the same state which has been uploaded by Alice is due to the perfect correlation of the states of Alice and Bob in the carrier. Alice can also use this carrier for sending quantum states to Bob. Linearity of the uploading and downloading operations allows Alice and Bob to entangle and disentangle a quantum state $|\phi\rangle = a|0\rangle + b|1\rangle$ to and from the carrier.

To conduct a somewhat complex attacks on the communication, Eve can entangle herself to the carrier and try to intercept-resend the message. To do this the only possibility for her entanglement is

$$|\phi'\rangle_{a,b,e} = |0,0\rangle|\xi_0\rangle + |1,1\rangle|\xi_1\rangle, \tag{5}$$

where $|\xi_0\rangle$ and $|\xi_1\rangle$ are two un-normalized states of Eve's ancilla. Any other form of entanglement, i.e. one in which a term like $|0,1\rangle|\eta\rangle$ is also present in the above expansion, will destroy the perfect correlation between the sequence of bits transmitted between Alice and Bob. In case that the two parties are using the carrier for sending classical bits, Alice and Bob can publicly compare a subsequence of bits to detect the presence of Eve's entanglement. In case that they are using the carrier for sending quantum states, Alice can insert a random subsequence of basis states into the main stream of states and ask Bob to publicly announce his results of measurements of these specific states. This strategy also works in other more complicated schemes presented later, namely the (n, n) and the (k, n) schemes.

In order to prevent this type of entanglement, we now use a property of the carrier (1) which turns out to be important in all the other forms of quantum carriers that we will introduce later on. This is the invariance property of the carrier (1) under Hadamard operations, that is

$$(H \otimes H)|\phi\rangle = |\phi\rangle. \tag{6}$$

At the end of each round, when the message is downloaded and the carrier is clean, both Alice and Bob act on their share of the carrier by Hadamard operations.

In the absence of Eve, the carrier will remain the same, however in presence of Eve, (who supposedly acts on her ancilla by a unitary U) the *contaminated* (entangled with the ancialla of Eve) carrier (1) will turn out to be

$$\begin{aligned}(H\otimes H\otimes U)|\phi'\rangle_{a,b,e} &= |+,+\rangle|\eta_0\rangle + |-,-\rangle|\eta_1\rangle \\ &= \frac{1}{2}(|0,0\rangle + |1,1\rangle)(|\eta_0\rangle + |\eta_1\rangle) \\ &\quad + \frac{1}{2}(|0,1\rangle + |1,0\rangle)(|\eta_0\rangle - |\eta_1\rangle),\end{aligned} \tag{7}$$

where $|\eta_0\rangle = U|\xi_0\rangle$ and $|\eta_1\rangle = U|\xi_1\rangle$. The second term in the carrier will certainly introduce anti-correlations into the basis states communicated between Alice and Bob, unless $|\eta_0\rangle = |\eta_1\rangle$ and hence $|\xi_0\rangle = |\xi_1\rangle$ which means that Eve cannot entangle herself to the carrier.

4. Quantum Carrier for (2,2) Secret Sharing

In this scheme, Alice wants to share a secret with Bob and Charlie so that they can retrieve the message only by their collaboration. The first quantum protocol for this scheme was designed in Ref. 1 where it was shown that measurements of a GHZ state in random bases by the three parties can enable them to share a random secret key. The secure carrier for this protocol was first developed in Refs. 9–11. Its characteristic feature is that two types of carriers, should be used which are turned into each other by the Hadamard operations. The two carriers are

$$|\phi_{\text{odd}}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \tag{8}$$

used in the odd rounds $1, 3, 5, \ldots$ and

$$|\phi_{\text{even}}\rangle := \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle), \tag{9}$$

used in the even rounds, $2, 4, 6, \ldots$. The two types of carriers are turned into each other by the local Hadamard action of the players at the end of each round,

$$H^{\otimes 3}|\phi_{\text{odd}}\rangle = |\phi_{\text{even}}\rangle, \quad H^{\otimes 3}|\phi_{\text{even}}\rangle = |\phi_{\text{odd}}\rangle. \tag{10}$$

This property is crucial in checking the security of the protocol and detection of Eve who may entangle herself with the carrier and intercept the secret bits.

In the odd and even rounds, the secret bit s is encoded differently as

$$\begin{aligned}|\bar{s}_{\text{odd}}\rangle &:= |s,s\rangle, \\ |_{\text{even}}\rangle &= \frac{1}{\sqrt{2}}(|s,0\rangle + |s',1\rangle) = \frac{1}{\sqrt{2}}(|+,+\rangle + (-1)^s|-,-\rangle),\end{aligned} \tag{11}$$

where $s' = s + 1 \bmod 2$. While in the odd rounds, the receivers each receive a copy of the sent bit, in the even rounds they need each other's collaboration for its

retrieval. Therefore Alice can use the odd rounds to put random stray bits and put the message bits in the even rounds.

In our opinion this property of the protocol, that is, a rate of one-half in sending message bits is analogous to discarding one-half of the measured bits in measurement-based protocols. However the bonus here is that Alice can send pre-determined non-random messages.

Note that in both even and odd rounds the carrier can be written as

$$|\phi\rangle_{a,b,c} := \frac{1}{\sqrt{2}} \sum_{q=0} |q\rangle_a |\overline{q}\rangle_{b,c}, \tag{12}$$

where we have dropped the subscripts even and odd to stress the uniformity. The running of the protocol, i.e. the uploading and downloading operations, are based on the following readily verifiable identities which we state for odd and even rounds separately without writing the subscripts "odd" and "even" explicitly:

For odd rounds:

$$\begin{aligned} C_{a,1}C_{a,2}|q\rangle_a|\overline{s}\rangle_{1,2} &= |q\rangle_a|\overline{q+s}\rangle_{1,2}, \\ C_{b,1}C_{c,2}|\overline{q}\rangle_{b,c}|\overline{s}\rangle_{1,2} &= |\overline{q}\rangle_{b,c}|\overline{q+s}\rangle_{1,2}. \end{aligned} \tag{13}$$

For even rounds:

$$\begin{aligned} C_{a,1}|q\rangle_a|\overline{s}\rangle_{1,2} &= |q\rangle_a|\overline{q+s}\rangle_{1,2}, \\ C_{b,1}C_{c,2}|\overline{q}\rangle_{b,c}|\overline{s}\rangle_{1,2} &= |\overline{q}\rangle_{b,c}|\overline{q+s}\rangle_{1,2}. \end{aligned} \tag{14}$$

Equations (12)−(14) show how the encoded secret can be downloaded by Alice and downloaded by Bob and Charlie in different rounds. In the odd rounds, the uploading operator is simply $C_{a,1}C_{a,2}$, and in the even rounds it is $C_{a,1}$. In both types of rounds the downloading operator is $C_{b,1}C_{c,2}$. These string of operators, that is, uploading, carrying and downloading is depicted as follows:

$$|\phi\rangle_{a,b,c}|\overline{s}\rangle_{1,2} \rightarrow \text{upload} \rightarrow \frac{1}{\sqrt{2}} \sum_{q=0}^{1} |q, \overline{q}, \overline{q+s}\rangle_{a,b,c,1,2} \rightarrow \text{download} \rightarrow |\phi\rangle_{a,b,c}|\overline{s}_{1,2}\rangle. \tag{15}$$

The above equation shows that any state $|\chi\rangle = \sum_s \alpha_s |s\rangle$ can be encoded as $|\overline{\chi}\rangle = \sum_s \alpha_s |\overline{s}\rangle$ and transferred by the same operations. So this protocol can also be used for quantum state sharing in a secure way. The problems of security of the carriers and the impossibility of Eve's entanglement with them, has been analyzed in detail in Refs. 9−11. The main points are that (i) the secret state is transferred from Alice to Bob and Charlie in a mixed state and hence carries no information to outsiders and (ii) the carriers in even and odd rounds are turned into each other by local Hadamard actions of Alice, Bob and Charlie, a property which is possible only in the absence of any entanglement with Eve. Any entanglement will have a detectable trace on a substring of transferred states, which will be used to detect the presence of Eve.[9−11]

5. Quantum Carrier for (n,n) Secret and State Sharing

The previous protocol can be generalized to the (n, n) scheme, where all the n players should retrieve the secret collaboratively. In this case the encoding of a bit s to quantum states for odd and even rounds is

$$\begin{aligned} |\overline{s}_{\text{odd}}\rangle &= |s\rangle^{\otimes n} = |s, s, \ldots, s\rangle, \\ |\overline{s}_{\text{even}}\rangle &= \frac{1}{\sqrt{2}}(|+,+,\cdots+\rangle + (-1)^s|-,-,\cdots-\rangle). \end{aligned} \tag{16}$$

Therefore $|\overline{0}_{\text{even}}\rangle$ is an even parity state, and $|\overline{1}_{\text{even}}\rangle$ is an odd parity state.

Then the protocol runs as in the $(2, 2)$ case with the obvious generalization of the carrier and the uploading and downloading operators. In fact in both types of rounds the carrier can be written as

$$|\phi\rangle = \frac{1}{\sqrt{2}} \sum_{q\in Z_2} |q, \overline{q}\rangle, \tag{17}$$

where $|\overline{q}\rangle$ stands for the encoding in (16) and we have suppressed the subscripts "even" and "odd" for simplicity. The uploading operator will be $\mathcal{C}_A := C_{a,1}\ C_{a,2}\cdots C_{a,n}$ for the odd rounds and $\mathcal{C}_A := C_{a,1}$ for the even rounds. The downloading operator will be the same for both rounds and will be $\mathcal{C}_B := C_{b_1,1}C_{b_2,2}\cdots C_{b_n,n}$.

To show that the protocol runs in exactly the same way as in the (2, 2) scheme, we need to prove the basic properties of the encoded states and the carrier. To this end, we first note from (16) that the following relations hold,

$$H^{\otimes n}|\overline{s}_{\text{odd}}\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{1} (-1)^{sx}|\overline{x}_{\text{even}}\rangle, \quad H^{\otimes n}|\overline{s}_{\text{even}}\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{1} (-1)^{sx}|\overline{x}_{\text{odd}}\rangle. \tag{18}$$

From these two relations one easily shows that the carriers in the even and odd rounds are turned into each other by the local Hadamard actions of players. Second we need the generalization of the properties (13) and (14) to the (n, n) case. To this end we start from the simple properties

$$C_{a,1}|q\rangle_a|+\rangle_1 = |q\rangle_a|+\rangle_1, \quad C_{a,1}|q\rangle_a|-\rangle_1 = (-1)^q|q\rangle_a|-\rangle_1, \tag{19}$$

to obtain

$$\begin{aligned} C_{a,1}|q\rangle_a|\overline{s}_{\text{even}}\rangle_{1,\ldots,n} &= \frac{1}{\sqrt{2}}(C_{a,1}|q\rangle_a(|+,+,\cdots+\rangle + (-1)^s|-,-,\cdots-\rangle)_{1,\ldots,n}) \\ &= \frac{1}{\sqrt{2}}(|q\rangle_a(|+,+,\cdots+\rangle + (-1)^{s+q}|-,-,\cdots-\rangle)_{1,\ldots,n}) \\ &= |q\rangle_a|\overline{(q+s)}_{\text{even}}\rangle_{1,\ldots,n}. \end{aligned} \tag{20}$$

The only other non-trivial relation which we should prove is the following relation for the even rounds which is necessary for the downloading operation, (for the odd

rounds, the involved states are product states and the relation is obvious):

$$C_{b_1,1}C_{b_2,2}\cdots C_{b_n,n}|\bar{q}\rangle|\bar{s}\rangle. \tag{21}$$

To show the validity of this relation we first use the following simple property of CNOT operation, where the first bit is the control and the second bit is the target qubits:

$$\begin{aligned} C|+,+\rangle &= |+,+\rangle, \quad C|+,-\rangle = |-,-\rangle, \\ C|-,+\rangle &= |-,+\rangle, \quad C|-,-\rangle = |+,-\rangle. \end{aligned} \tag{22}$$

Second we use these properties and (16) and the abbreviation $\mathcal{C}_B := C_{b_1,1}C_{b_2,2}\cdots C_{b_n,n}$ to obtain

$$\begin{aligned} \mathcal{C}_B|\bar{q}\rangle|\bar{s}\rangle &= \frac{1}{2}\mathcal{C}_B(|+\rangle^{\otimes n} + (-1)^q|-\rangle^{\otimes n})(|+\rangle^{\otimes n} + (-1)^s|-\rangle^{\otimes n}) \\ &= \frac{1}{2}(|+\rangle^{\otimes n}|+\rangle^{\otimes n} + (-1)^q|-\rangle^{\otimes n}|+\rangle^{\otimes n} \\ &\quad +(-1)^s|-\rangle^{\otimes n}|-\rangle^{\otimes n} + (-1)^{q+s}|+\rangle^{\otimes n}|-\rangle^{\otimes n}) \\ &= \frac{1}{2}(|+\rangle^{\otimes n} + (-1)^q|-\rangle^{\otimes n})(|+\rangle^{\otimes n} + (-1)^{q+s}|-\rangle^{\otimes n}) = |\bar{q}\rangle|\overline{q+s}. \end{aligned} \tag{23}$$

This completes the description and validity of the uploading and downloading procedures for the (n,n) scheme.

In passing we note that the form of the carrier (17) for this (n,n) secret sharing scheme is the same as in the simplest cryptographic protocol, (1). We will see in the next section that the appropriate carrier for the threshold scheme (k,n) where n is an odd prime, is of the same form. We will explain the reason for this general structure in the last section, however before that, we explain in detail the carrier for the (k,n) secret sharing scheme.

6. Quantum Carrier for (k,n) Threshold Secret Sharing

There are situations where there are n players and any subset of k or more members can retrieve the secret, while subsets of smaller size cannot. This is called a (k,n) threshold structure[23,24] in which all the players have equal weight. One can also imagine situations where different players have different weights. This leads to a general access structure, according to which the players form a set $\mathcal{R}$ of say n members and an access structure is a collection $\mathcal{A}$ of subsets of $\mathcal{R}$. The subsets in $\mathcal{A}$ (and their unions) are called authorized subsets and the members of each authorized subset should be able to retrieve the key by their collaboration, while the subsets which are not in $\mathcal{A}$, called adversaries, cannot retrieve the secret. It is known that once a threshold scheme is solved, then other more general access structures will be possible.[25,26] For example if $\mathcal{R} = \{a,b,c\}$ and $\mathcal{A} = \{\{a,b\},\{a,c\}\}$, then we can run a $(3,4)$ threshold scheme giving 2 shares to a and one share to b and c each.

The (k, n) threshold scheme was first generalized to the quantum domain in Ref. 18, where quantum states could also be shared between n parties so that any k of the players could retrieve the quantum state collaboratively. To be in conformity with the no-cloning theorem, n had to be smaller than $2k$. We will deal in detail with the case where $n = 2k - 1$ is a prime number. Other cases where $n < 2k - 1$ are obtained by a simple modification of the $(k, 2k - 1)$ scheme. For example a scheme like $(k, 2k - m)$ is implemented by running the scheme $(k, 2k - 1)$ as usual, but with Alice playing the role of the other $m - 1$ receivers in addition to her usual role. The idea of Ref. 18 was to adapt the polynomial code, first developed in Ref. 27, to the quantum domain. Note that in Ref. 18, quantum mechanics was exploited only for message splitting and not for message distribution. Later it was shown in Refs. 20 and 21 that graph states can be used for combining the two parts of the problem in one scheme, for some threshold schemes, namely for $(2, 3)$, $(3, 5)$ and (n, n) schemes. Here we show that the idea of quantum carrier can be used to provide a method of secure distribution for all secrets of the (k, n) types provided in Ref. 18. Let us first see what a polynomial code is.

6.1. *The polynomial code*

Consider a symbol s. Classically if we want to share this symbol as a secret between n parties, called B_1, $B_2, \ldots, B_n$, so that any k members of the parties can retrieve this symbol and fewer than k members cannot, we can define a real polynomial of degree $k - 1$ in the form

$$P_{\mathbf{c},s}(x) := c_0 + c_1\, x + c_2\, x^2 + \cdots + c_{k-2}x^{k-2} + s\, x^{k-1} \tag{24}$$

and evaluate this polynomial on n distinct points $x_0, \ldots, x_{n-2}$, and x_{n-1}. We can then give the member B_i of the set, the value $P_{\mathbf{c},s}(x_i)$. It is a simple fact that a polynomial of degree $k - 1$ is completely determined by its values on k distinct points. So any k members can compare their values and determine the full functional form of the polynomial and hence the real number s. To make the process simple and less prone to errors, we can substitute the real number field with the field $Z_n := \{0, 1, 2, \ldots, n - 1\}$ (where n is prime). For the n points in Z_n we can take simply $x_i = i$. Hence we can encode the symbol s into a product state $|s\rangle := |P_{\mathbf{c},s}(0)\rangle_{B_1} \otimes |P_{\mathbf{c},s}(1)\rangle_{B_2} \cdots \otimes |P_{\mathbf{c},s}(n-1)\rangle_{B_n}$. Let us now sum such a product state over all possible $\mathbf{c} \in Z_n^{k-1}$, and obtain the code

$$\begin{aligned} s \to |\bar{s}\rangle &:= \frac{1}{\sqrt{n^{k-1}}} \sum_{\mathbf{c}\in Z_n^{k-1}} |P_{\mathbf{c},s}(0)\rangle_{B_1} \otimes |P_{\mathbf{c},s}(1)\rangle_{B_2} \cdots \otimes |P_{\mathbf{c},s}(n-1)\rangle_{B_n} \\ &\equiv \frac{1}{\sqrt{n^{k-1}}} \sum_{\mathbf{c}\in Z_n^{k-1}} |P_{\mathbf{c},s}(0), P_{\mathbf{c},s}(1), \ldots, P_{\mathbf{c},s}(n-1)\rangle. \end{aligned} \tag{25}$$

In order to see how to find a suitable carrier for this code, and indeed in order to show that the carrier for this code falls within the same class of carriers considered so

far, we have to prove further algebraic properties of this code. To do this, we cast it in the form of a Calderbank–Shor–Steane (CSS) code.[28,29]

6.2. *The CSS structure of the polynomial code*

Let n be a prime number. With addition and multiplication modulo n, the set $Z_n := \{0, 1, 2, \ldots, n-1\}$ will be a field. For any n, Z_n^n is a vector space over Z_n, i.e. Z_n^n is the set of all n-tuples $(v_1, v_2, \ldots, v_n)$ where $v_i \in Z_n$. Let C be a linear code, i.e. a subspace of Z_n^n, spanned by linearly independent vectors $\{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{k-2}\}$. Thus C is isomorphic to Z_n^{k-1}. Consider the case where the dual code of C, i.e. the code space spanned by all the vectors which are perpendicular to C, contains C and has one more dimension. Let $C^\perp$ be spanned by the vectors $\{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{k-2}\} \cup \{\mathbf{e}_{k-1}\}$. Thus we have

$$\begin{aligned} C &= \text{Span}\{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{k-2}\}, \\ C^\perp &= \text{Span}\{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{k-2}, \mathbf{e}_{k-1}\}. \end{aligned} \tag{26}$$

In the codes that we will introduce, the special vector $\mathbf{e} := \mathbf{e}_{k-1}$ is normalized so that $\mathbf{e} \cdot \mathbf{e} = -1$. We therefore have

$$\begin{aligned} \mathbf{e}_i \cdot \mathbf{e}_j &= 0, \qquad 1 \le i, \quad j \le k-2, \\ \mathbf{e} \cdot \mathbf{e}_j &= 0, \qquad 0 \le j \le k-2, \\ \mathbf{e} \cdot \mathbf{e} &= -1. \end{aligned} \tag{27}$$

We will now define the following special Chalderbank–Steane–Shor (CSS) code, [19,28–31] whose codewords correspond to the classes of the quotient space $C^\perp/C$:

$$|\bar{s}\rangle := \frac{1}{\sqrt{n^{k-1}}} \sum_{\mathbf{c} \in C} |\mathbf{c} + s\mathbf{e}\rangle. \tag{28}$$

Thus one dit s is coded into the n-qudit state $|\bar{s}\rangle$ which is to be distributed between the n receivers, each component of the vector being given to one participant.

In the appendix, we will show the vectors e_l with components

$$(\mathbf{e}_l)_j = j^l, \quad j = 0, 1, \ldots, n-1, \;\; l = 0, 1, \ldots, k-1 \tag{29}$$

satisfy all the properties listed in (27). Explicitly we have

$$\begin{aligned} \mathbf{e}_0 &= (1, 1, 1, \ldots, 1), \\ \mathbf{e}_{l \ge 1} &= (0, 1, 2^l, \ldots, (n-1)^l). \end{aligned} \tag{30}$$

It is now very simple to see that the CSS code thus constructed is nothing but the polynomial code in (25). To see this we note that the vector $\mathbf{c} \in C$ has the following expansion

$$\mathbf{c} = \sum_{l=0}^{k-2} c_l e_l \tag{31}$$

and hence the components will be

$$(\mathbf{c}+s\mathbf{e})_j=\left(\sum_{l=0}^{k-2}c_l(\mathbf{e}_l)_j\right)+s(\mathbf{e}_{k-1})_j=\left(\sum_{l=0}^{k-2}c_l j^l\right)+sj^{k-1}=P_{\mathbf{c},s}(j). \tag{32}$$

Therefore giving each component to one player, the code will be

$$|\overline{s}\rangle_{b_1,b_2,\ldots,b_n}:=\frac{1}{\sqrt{n^{k-1}}}\sum_{\mathbf{c}\in Z_n^{k-1}}|P_{\mathbf{c},s}(0),P_{\mathbf{c},s}(1),\ldots,P_{\mathbf{c},s}(n-1)\rangle, \tag{33}$$

which is exactly the polynomial code (24). Now that the CSS structure of the polynomial code is revealed, many of its properties can be proved in a simple way. In particular we need the following property which plays an important role in the security of the carrier.

Lemma. *The set of all* (k,n) *codes* (33)*, is invariant under the joint multi-local Hadamard operation, i.e.*

$$H^{\otimes n}|\overline{s}\rangle=\frac{1}{\sqrt{n}}\sum_{x=0}^{n-1}\omega^{-sx}|\overline{x}\rangle, \tag{34}$$

where ω *is a root of unity,* $\omega^n=1$.

Proof. We use a well-known property of the CSS codes according to which,

$$H^{\otimes n}|\overline{\mathbf{w}}\rangle=\frac{1}{|C_1/C_2|}\sum_{\overline{\mathbf{v}}}\omega^{\mathbf{w}\cdot\mathbf{v}}|\overline{\mathbf{v}}\rangle, \tag{35}$$

where $|C_1/C_2|$ is the number of cosets C_1/C_2. To adapt this general relation to our case, we note that in our case $|C^1|=|C^\perp|=n^k$, $|C^2|=|C|=n^{k-1}$, and hence $|C^1/C^2|=n$. Moreover we make the following substitutions,

$$|\mathbf{w}\rangle\rightarrow|\mathbf{c}+s\mathbf{e}\rangle=|\overline{s}\rangle,\quad|\mathbf{v}\rangle\rightarrow|\mathbf{c}+x\mathbf{e}\rangle=|\overline{x}\rangle, \tag{36}$$

and note that

$$(\mathbf{w})\cdot(\mathbf{v})=(\mathbf{c}+s\mathbf{e})\cdot(\mathbf{c}+x\mathbf{e})=-sx. \tag{37}$$

Putting all this together proves the lemma. □

6.3. *The carrier and the uploading and downloading operators*

The quantum carrier is constructed as follows:

$$|\phi\rangle_{a,b_1,\ldots,b_n}=\frac{1}{\sqrt{n}}\sum_{q\in Z_n}|q\rangle_a|\overline{q}\rangle_{b_1,\ldots,b_n}. \tag{38}$$

The important property of this carrier is that it is invariant under the joint action of Hadamard operators, performed by Alice and all the other players. Using (34)

proves this assertion:

$$H^{\otimes n+1}|\phi\rangle = \frac{1}{n}\sum_{x,y,s}\omega^{sx-sy}|x,\overline{y}\rangle = \frac{1}{\sqrt{n}}\sum_{x}|x,\overline{x}\rangle = |\phi\rangle. \tag{39}$$

In order to see how Alice uploads secrets onto the carrier and how the players download the secret from the carrier we need some algebraic properties of the code.

Definition. For any vector $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in Z_n^n$ define the following string of CNOT operators performed by Alice:

$$\mathcal{C}_A(\mathbf{v}) := C_{a,1}^{v_1} C_{a,2}^{v_2} \cdots C_{a,n}^{v_n}. \tag{40}$$

Also define the following multi-local operator for Bob's:

$$\mathcal{C}_B := C_{b_1,1} C_{b_2,2} \cdots C_{b_n,n}. \tag{41}$$

Theorem. *The operator* $\mathcal{C}_A := \mathcal{C}_A(\mathbf{e})$, *for* $\mathbf{e}$ *as in* (30), *uploads the message into the carrier by Alice and the operator* $\mathcal{C}_B^{-1}$ *downloads the message from the carrier by Bob's, leaving the carrier in its original form.*

Proof. We fist show that for any state $|q\rangle_a$ and any message $|\overline{s}\rangle_{1,2,\ldots,n}$

$$\mathcal{C}_A|q\rangle|\overline{s}\rangle = |q\rangle|\overline{s+q}\rangle. \tag{42}$$

This is seen by expansion of $|\overline{s}\rangle$ in components and noting that

$$\begin{aligned}
\mathcal{C}_A|q\rangle|\overline{s}\rangle &= \frac{1}{\sqrt{n^{k-1}}}\mathcal{C}_A|q\rangle \sum_{\mathbf{c}\in\mathbf{Z_n^{k-1}}} |(\mathbf{c}+s\mathbf{e})_1, (\mathbf{c}+s\mathbf{e})_2, \ldots, (\mathbf{c}+s\mathbf{e})_n\rangle \\
&= \frac{1}{\sqrt{n^{k-1}}}|q\rangle \sum_{\mathbf{c}\in\mathbf{Z_n^{k-1}}} |(\mathbf{c}+(s+q)\mathbf{e})_1, (\mathbf{c}+(s+q)\mathbf{e})_2, \ldots, (\mathbf{c}+(s+q)\mathbf{e})_n\rangle \\
&= |q\rangle|\overline{s+q}\rangle.
\end{aligned} \tag{43}$$

From (43), we see that

$$\mathcal{C}_A|\phi\rangle|\overline{s}\rangle = \frac{1}{\sqrt{n}}\sum_{q\in Z_n}\mathcal{C}_A|q,\overline{q}\rangle|\overline{s}\rangle = \frac{1}{\sqrt{n}}\sum_{q}|q,\overline{q}\rangle|\overline{q+s}\rangle. \tag{44}$$

Therefore Alice uploads (entangles) the message $|\overline{s}\rangle$ to the carrier by the local operation $\mathcal{C}_A$. For the other part, we need the following

$$\mathcal{C}_B|\overline{q}\rangle|\overline{s}\rangle = |\overline{q}\rangle|\overline{s+q}\rangle. \tag{45}$$

To show this we note that

$$\begin{aligned}
\mathcal{C}_B|\overline{q}\rangle|\overline{s}\rangle &= \mathcal{C}_B\sum_{\mathbf{c},\mathbf{c}'}|\mathbf{c}+q\mathbf{e}\rangle|\mathbf{c}'+s\mathbf{e}\rangle \\
&= \sum_{\mathbf{c},\mathbf{c}'}|\mathbf{c}+q\mathbf{e}\rangle|\mathbf{c}'+\mathbf{c}+(s+q)\mathbf{e}\rangle = |\overline{q}\rangle|\overline{s+q}\rangle.
\end{aligned} \tag{46}$$

From this last equation we find that

$$\mathcal{C}_B^{-1} \sum_q |q, \bar{q}\rangle |\overline{s+q}\rangle = \sum_q |q, \bar{q}\rangle |\bar{s}\rangle, \tag{47}$$

which means that the players, can download the message from the carrier and put the carrier back to its original form. □

The basic steps of the quantum secret sharing are now clear. A carrier in the form of the state $|\phi\rangle$ is shared between Alice and all the receivers, $B_1, B_2, \ldots, B_n$. Alice operates by his $\mathcal{C}_A$ operator on her part of the carrier and the code state $|\bar{s}\rangle$ and thus entangles the code state to the carrier $|\phi\rangle$. At the destination the players act on the carrier and the code space by $\mathcal{C}_B^{-1}$ and download the state $|\bar{s}\rangle$. From this code state, no less than k players can retrieve the secret symbol s. The carrier is now ready for transferring the next code state.

7. The Security of the Quantum Carrier

In this section we discuss the security of state transmission via the carrier and analyze two types of attacks performed by Eve. The security of the retrieval procedure of the symbol s from the encoded state $|\bar{s}\rangle$ need not concern us and has been discussed elsewhere.[18] Obviously the analysis of security depends on the resources available to Eve. We consider two types of attacks in the following two subsections. This type of analysis applies to all the schemes mentioned up to now.

7.1. *Simple intercept of message by Eve, without her entanglement to the carrier*

In this type of attack we assume that Eve is not entangled with the carrier, but she has access to all the message qudits sent from Alice to the players. After uploading the message, the full state is given by

$$|\phi_s\rangle = \frac{1}{\sqrt{n}} \sum_{q \in Z_n} |q, \bar{q}, \overline{q+s}\rangle_{A,\mathbf{B},1\ldots,n}. \tag{48}$$

While in transit the data qudits are in the state

$$\rho_D = \frac{1}{n} \sum_{s \in Z_n} |\bar{s}\rangle\langle\bar{s}|, \tag{49}$$

which is an equal mixture of all the encoded states. Therefore even if Eve has access to all the data in transit and intercepts all the qudits sent to all the players, she cannot acquire the secret s or the secret state, since she only finds and equal mixture of all the encoded states.

At the destination, the receivers, act by the inverse local operator $\mathcal{C}_B$ and according to (47), disentangle the code from the carrier. They can then retrieve the classical secret s by collaboration of each other according to the access structure.

Once retrieved, we resort to the arguments of Ref. 18 to show that this encoded state is secure against cheating of groups of unauthorized players.

Therefore in the simplest intercept attack, Eve does not acquire any information about the secret symbol s. We now consider more general attacks.

7.2. *Entanglement of Eve to the carrier and intercept-resend attack*

We now assume that in addition to access to the message channel, Eve can entangle herself to the carrier. Let us see if she can do appropriate action for intercepting the encoded state $|\overline{s}\rangle$ and not an equal mixture. Consider the first round where the symbol s_1 is encoded to $|\overline{s}_1\rangle$ and sent by Alice. The state of the carrier and the message after Alice uploading operation will be

$$|\phi^{(1)}(s_1)\rangle_{a,B,M} = \frac{1}{\sqrt{n}} \sum_q |q, \overline{q}\rangle_{a,B} |\overline{q+s_1}\rangle_M, \tag{50}$$

where a stands for Alice, B for all the players $B_1, \ldots, B_n$ and M for the n message qudits, $m_1, m_2, \ldots, m_n$. Eve can now set her n ancilla qudits $E := (e_1, e_2, \ldots, e_n)$ to $|\overline{0}\rangle_E$, and then do the following operations: acts by $\mathcal{C}_{M,E} := C_{m_1,e_1} C_{m_2,e_2} \cdots C_{m_n,e_n}$ which transforms the state $|\phi^{(1)}(s_1)\rangle_{a,B,M} |\overline{0}\rangle_E$ to

$$|\phi^{(2)}(s_1)\rangle_{a,B,M,E} = \frac{1}{\sqrt{n}} \sum_q |q, \overline{q}\rangle_{a,B} |\overline{q+s_1}\rangle_M |\overline{q+s_1}\rangle_E. \tag{51}$$

When Alice and the players execute the first round of the protocol to the end and the players extract the state $|\overline{s_1}\rangle$, Eve acquires nothing from the symbol s_1, however she has achieved in entangling herself with the carrier in the form

$$|\phi'\rangle_{a,B,E} = \frac{1}{\sqrt{n}} \sum_q |q, \overline{q}\rangle_{a,B} |\overline{q+s_1}\rangle_E. \tag{52}$$

In the second round, when the symbol s_2 is being sent and the full state is of the form

$$|\phi'(s_2)\rangle_{a,B,E,M} = \frac{1}{\sqrt{n}} \sum_q |q, \overline{q}\rangle_{a,B} |\overline{q+s_2}\rangle_M |\overline{q+s_1}\rangle_E, \tag{53}$$

Eve performs the following sequence of operations: (i) acts by $C^{-1}_{M,E}$ to produce the state

$$|\phi'^{(1)}(s_2)\rangle_{a,B,E,M} = \frac{1}{\sqrt{n}} \sum_q |q, \overline{q}\rangle_{a,B} |\overline{q+s_2}\rangle_M |\overline{s_1-s_2}\rangle_E, \tag{54}$$

(ii) measures the ancillas to acquire $s_1 - s_2$, and (iii) acts by $\mathcal{C}_{M,E}$ to put back the full state in the form (53). When Alice and the players finish the second round, they acquire the symbol s_2, but Eve also acquires the symbol $s_1 - s_2$, while she is still entangled with the carrier in the form (52) and is ready to do the same attack for the next round. In this way she is able to retrieve the sequence of symbols

$$s_1 - s_2, \quad s_1 - s_3, \quad s_1 - s_4, \ldots. \tag{55}$$

This sequence enables her to find the whole message by checking n different choices for the original symbol s_1. This shows that if there is a possibility for Eve's entanglement with the carrier, she is able to successfully intercept all the data.

In order to prevent this, Alice and the players act on their respective qudits of the carrier, by Hadamard operations. As we have seen above, this operation leaves the pure form of the carrier invariant. Let us see if this operation is able to detect an entanglement of Eve, i.e. a contamination of the carrier. It is clear that if the carrier contains terms which are not of the form $|q, \overline{q}\rangle_{a,B}$, then there will be mismatches between what Alice uploads and what the players download. This mismatch can easily be detected by public announcements of some stray bits which are deliberately inserted into the stream of the symbols. In order to escape this detection, the only admissible form of Eve's entanglement with the carrier is

$$|\phi'\rangle = \sum_q |q, \overline{q}\rangle \otimes |\xi_q\rangle, \tag{56}$$

where ξ_q are a collection of un-normalized states of Eve. The method of detection in this case is the same as in the simple $(2, 2)$ case, discussed after Eq. (7). Also in view of the discussion in Sec. 7.3, only the legitimate parties or even a subset of them are required to publicly announce the results of their measurements.

In order to prevent this type of apparently undetectable entanglement, we note that the pure carrier is invariant under the action of Hadamard operators, while this contaminated carrier is not. In order to retain the correlations, Eve may operate on her ancilla by a suitable operator U to change the above state into

$$(H \otimes H^{\otimes n} \otimes U)|\phi'\rangle = \frac{1}{n} \sum_{q,x,y} \omega^{q(x-y)} |x, \overline{y}\rangle \otimes U|\xi_q\rangle. \tag{57}$$

In order to retain the original form of correlations between Alice and the players in the carrier, the operator U must satisfy the following property

$$U \sum_q \omega^{q(x-y)} |\xi_q\rangle = n|\eta_x\rangle \delta_{x,y} \quad \forall\, q, \tag{58}$$

for some states $|\eta_x\rangle$. Putting $x = y$ one finds that $|\eta_x\rangle$ is independent of x and hence a rearrangement shows that

$$\sum_q \omega^{q(x-y)} (U|\xi_q\rangle - |\eta\rangle) = 0. \tag{59}$$

Acting on the left hand side by the inverse Hadamard operation, one finds that $U(|\xi_q\rangle - |\eta\rangle) = 0$, which means that all the states ξ_q are equal to each other and hence the state $|\phi'\rangle$ cannot be an entangled state. Therefore Eve cannot entangle herself to the carrier without being detected.

Note that we have assumed that Eve is an external agent and all the players have run the protocol as they should, i.e. have performed their Hadamard operation on

the carrier at the end of each round. In principle one can assume that a subgroup of players collaborate with Eve, i.e. perform other operations than Hadamard in order to ease undetectable entanglement of Eve with the carrier. For example consider a $(2, 3)$ scheme with players B_1, B_2 and B_3. The question is whether one of the players, say B_1 is capable to collaborate with Eve to retrieve the secret symbol s? To be honest, we have not been able to either devise a successful attack of this type or a method for its prevention.

7.3. *The role of players collaborations*

It is part of the protocol that all the players should perform their CNOT's on the state $|\phi_s\rangle$ in order to download the state $|\overline{s}\rangle$, but once this state is downloaded, then no less than k players can collaborate to retrieve the symbol s as proved in Ref. 18. One may then argue that this is not a genuine (k, n) threshold scheme, since for downloading the state $|\overline{s}\rangle$ from the carrier, all the players should collaborate.

The important point is that the CNOT operation of all the players are needed only for cleaning of the carrier from remnants of messages, and in fact any k players can retrieve the symbol s from the state that they download from the carrier, but the running of the protocol for other rounds needs collaboration of all the players.

This assertion can be proved as follows: Let K be any set of k members who want to retrieve the message. Denote by $\mathcal{C}_K$ the joint CNOT operations of the k players belonging to the set K, i.e.

$$\mathcal{C}_{\mathbf{K}} := \bigotimes_{j\in K} \mathcal{C}_{B_j,j.} \tag{60}$$

Denote also by $\mathcal{C}_{\mathbf{N-K}}$ the joint CNOT operations of the rest of $N - k$ players. Also denote by $\mathcal{M}_{\mathbf{K}}$, the local operation and classical communications that the k players perform among themselves to recover the symbol s from $|\overline{s}\rangle$. We have shown that the sequence of operations $\mathcal{M}_{\mathbf{K}}\mathcal{C}_{\mathbf{K}}\mathcal{C}_{\mathbf{N-K}}$ when acting on the state $|\phi_s\rangle$ in (48) produces the symbol s unambiguously and leaves the carrier clean of the remnants of the message, i.e. disentangle the state $|\overline{s}\rangle$ from the carrier. It is important to note that due to their local nature the two operations $\mathcal{M}_{\mathbf{K}}$ and $\mathcal{C}_{\mathbf{N-K}}$ commute, so that we have the identity

$$\mathcal{M}_{\mathbf{K}}\mathcal{C}_{\mathbf{K}}\mathcal{C}_{\mathbf{N-K}} = \mathcal{C}_{\mathbf{N-K}}\mathcal{M}_{\mathbf{K}}\mathcal{C}_{\mathbf{K}} = \mathcal{C}_{\mathbf{N-K}}(\mathcal{M}_{\mathbf{K}}\mathcal{C}_{\mathbf{K}}). \tag{61}$$

However if the operation on the left hand side of this relation leaves the k players in the set K with an unambiguous symbol s, we can conclude that the operations $(\mathcal{M}_{\mathbf{K}}\mathcal{C}_{\mathbf{K}})$ does the same thing, because the remaining operation $\mathcal{C}_{\mathbf{N-K}}$, by its local nature, has no effect on the qudits retrieved by the set K. The sole effect of $\mathcal{C}_{\mathbf{N-K}}$ is to disentangle completely the carrier from the message state and make it ready for the next round. Such collaboration is of course necessary for the continuous running of the protocol like any other communication task. Let us now study a simple example, in which we will also see in explicit terms the above argument.

8. Example: The (2, 3) Threshold Scheme

The simplest threshold scheme is the scheme $(2, 3)$ for which

$$P_{c,s}(x) = c_0 + sx \tag{62}$$

and hence

$$\begin{aligned} s \to & \frac{1}{\sqrt{3}} \sum_{c_0} |c_0, c_0 + s, c_0 + 2s, \rangle \\ & = (I \otimes X \otimes X^2)^s \frac{1}{\sqrt{3}} \sum_{c_0} |c_0, c_0, c_0\rangle \end{aligned} \tag{63}$$

or more explicitly as

$$\begin{aligned} 0 \to |\bar{0}\rangle &= \frac{1}{\sqrt{3}}(|000\rangle + |111\rangle + |222\rangle), \\ 1 \to |\bar{1}\rangle &= \frac{1}{\sqrt{3}}(|012\rangle + |120\rangle + |201\rangle), \\ 2 \to |\bar{2}\rangle &= \frac{1}{\sqrt{3}}(|021\rangle + |102\rangle + |210\rangle). \end{aligned} \tag{64}$$

Note that for qudits, the operators X and Z (to be used later) are defined as $X|i\rangle = |i + 1, \mod d\rangle$ and $Z|i\rangle = \omega^i|i\rangle$, where $\omega^d = 1$. Equation (63) shows what kind of encoding circuit Alice has to use to encode a state $\sum_s a_s|s\rangle$ to $\sum_s a_s|\bar{s}\rangle$. The encoding circuit is shown in Fig. 1. Moreover it is easily seen from (64) that the operator $\overline{Z}$ defined as

$$\overline{Z} := (I \otimes Z \otimes Z^2) \tag{65}$$

acts as follows on the code states

$$\overline{Z}|\bar{s}\rangle = \omega^{-s}|\bar{s}\rangle. \tag{66}$$

These encoded states have the nice properties that

$$\begin{aligned} Z_1^{-1} \otimes Z_2|\rangle &= \omega^s|\rangle, \\ Z_2^{-1} \otimes Z_3|\rangle &= \omega^s|\rangle, \\ Z_3^{-1} \otimes Z_1|\rangle &= \omega^s|\rangle, \end{aligned} \tag{67}$$

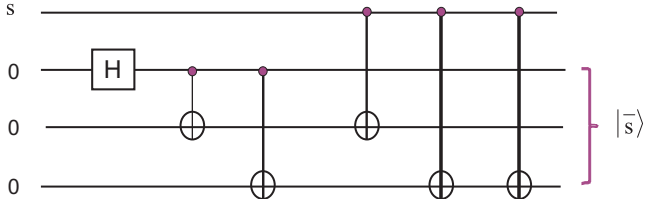

Fig. 1. (Color online.) The encoding circuit used by Alice, for generating the (2, 3) code $|\bar{s}\rangle$ from s.

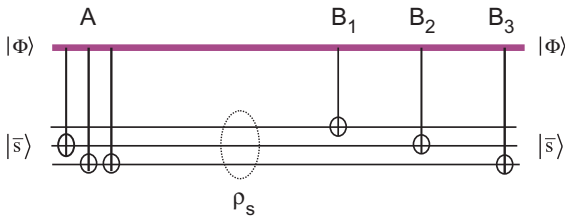

Fig. 2. (Color online.) The schematic form of the carrier (thick line) and the uploading (by A) and downloading (by B_1, B_2 and B_3) for a simple $(2,3)$ threshold scheme.

which shows clearly that any two of the receivers can retrieve the classical secret s by local measurements of the encoded state. The uploading and downloading operators for this scheme are shown in Fig. 2.

Let us now see explicitly in this example, an instance of the general discussion after Eq. (59). In other words, we want to show that although the CNOT action of all three receivers is necessary for disentangling the state $|s\rangle$ from the carrier, it does not mean that full collaboration of the participants is necessary for recovering the message s. That is let us show that even without the collaboration of B_3, B_1 and B_2 can indeed disentangle and retrieve the message from the carrier. The collaboration of B_3 is only needed to clean the carrier from the message.

Assume that only two of the participants, say B_1 and B_2 enact their CNOT's on the state $|\phi_s\rangle$. The resulting state will be

$$\mathcal{C}_{B_1}^{-1}\mathcal{C}_{B_2}^{-1}|\phi_s\rangle = \frac{1}{\sqrt{3}}\sum_{j,k}|i\rangle_A|j, j+i, j+2i\rangle_{B_1B_2B_3}|k, k+s, k+j+2(i+s)\rangle_{123}.$$

Thus measurements of qudits 1 and 2 by these two participants reveals the secret s, without any need for collaboration of B_3.

On the other hand suppose that the player B_3 wants to retrieve the message symbols on his own. To this end he adds to the quantum carrier $|\phi\rangle_{A,B_1,B_2,B_3}$ an extra qudit, in the state $|\xi_0\rangle_{B'_3}$ and at the end of each round, when all the parties are supposed to act on the carrier by Hadamard operators, B_3 acts by a suitable bi-local operator on his two qudits, so that in conjunction with the Hadamard operators of A, B_1 and B_2, the quantum carrier transforms to

$$|\phi'\rangle = \sum_{i,j}|i, j+i, j+2i, j\rangle_{A,B_1,B_2,B_3}|\eta_j\rangle_{B'_3}. \tag{68}$$

This is the only operation he can do in order not to destroy the correlations between stray qudits which is checked randomly by Alice and the participants.

Now when the other participants proceed as usual for entangling a code state $|\bar{s}\rangle$ to and from the quantum carrier, B_3 wants to proceed in a different way to reveal the symbol s on his own. The state of the quantum carrier and the code state $|\bar{s}\rangle$, which at the beginning of a round is $|\phi'\rangle|\bar{s}\rangle$, after Alice CNOT operations will

develop as follows:

$$|\phi'_s\rangle = \sum_{i,j} |i\rangle_A |j+i, j+2i, j, \eta_j\rangle_{B_1,B_2,B_3,B'_3} |\overline{i+s}\rangle_{1,2,3} \tag{69}$$

where we use the subscripts $1, 2, 3$ to denote the qudits which are respectively sent to B_1, B_2 and B_3.

It is now easily verified that the density matrix of the qudits $B_3, B'_3, 1, 2$ and 3 is given by

$$\rho_{B_3,B'_3,1,2,3} = \sum_j |j\rangle\langle j|_{B_3} \otimes |\eta_j\rangle\langle\eta_j|_{B'_3} \otimes \sum_i |\overline{i+s}\rangle\langle\overline{i+s}|, \tag{70}$$

which is independent of s. Therefore even when one of the participants entangles a qudit to the quantum carrier, refrains from cooperation with others in applying Hadamard gates and/or inverse CNOT operations, he cannot obtain any information about the secret symbol s.

The collaboration of all the participants, is only necessary for disentangling completely the data from the carrier and making it ready for next use. This is certainly a feature that any communication protocol should have.

9. Discussion

We have developed the concept of quantum carrier[9−11,17] to encompass more complex classical secret and quantum sharing schemes. We have described the procedure of uploading and downloading messages to and from the carrier in increasingly complex situations, i.e. for quantum key distributions, for $(2, 2)$, (n, n) and (k, n) threshold schemes. As described in the text, for each task a different quantum carrier is required, although it seems that they all have similar forms (38). We have also shown that simple intercept-resend attacks can destroy the pattern of entanglement in the carrier which can be detected by legitimate parties. In the general (k, n) secret sharing scheme, although collaboration of all parties is required for the continuous running of the protocol (i.e. cleaning of the carrier from the remnants of the transmitted messages), any set of k players can download and retrieve the message.

We hope that together with the previous results, the concept of quantum carrier can attract the attention of other researchers who will develop it into more complex forms. An important question is whether there can be universal carriers between a set of players, which can be used for various cryptographic tasks on demand of the players, i.e. quantum key distribution between the sender and a particular receiver, or secret sharing between the sender and a particular set of players. Another interesting general question is whether there exist general carriers which can be used to simultaneously send many messages to different receivers via a single quantum carrier, in the same way that frequency modulation is used for such a goal in classical communication. Finally the question of general proof of security of these types of carrier-based protocols remain to be investigated.

Acknowledgment

We would like to express our deep gratitude to the two referees of this paper, especially referee B, whose careful reading of the manuscript and many constructive suggestions were essential in improving the presentation of our results. We also thank R. Annabestani, S. Alipour, S. Baghbanzadeh, K. Gharavi, R. Haghshenas and A. Mani for very valuable comments. M. M. is deeply indebted to M. R. Koochakie for very stimulating discussions. Finally V. K. would like to specially thank Farid Karimipour, for his kind hospitality in Villa Paradiso, north of Iran, where the major parts of this manuscript was written.

Appendix

In this appendix we want to prove that the vectors in (30) satisfy the properties (33). That is if we define

$$(\mathbf{e}_l)_j = j^l, \quad j = 0, 1, \ldots, n-1, \quad l = 0, 1, \ldots, k-1, \tag{A.1}$$

then

$$\begin{aligned} &\mathbf{e}_i \cdot \mathbf{e}_j = 0, \quad 1 \leq i, \quad j \leq k-2, \\ &\mathbf{e} \cdot \mathbf{e}_j = 0, \quad 0 \leq j \leq k-2, \\ &\mathbf{e} \cdot \mathbf{e} = -1. \end{aligned} \tag{A.2}$$

Let p be an odd prime and define

$$S_k(p) := \sum_{j=1}^{p-1} j^k. \tag{A.3}$$

First we prove that,

$$S_k(p) = -\delta_{k,p-1}, \quad \text{mod } p. \tag{A.4}$$

Consider the following identity:

$$\sum_{j=1}^{p-1} [(j+1)^m - j^m] = p^m - 1 \equiv -1. \tag{A.5}$$

Expand the first term by using the binomial theorem to find

$$\sum_{j=1}^{p-1} \left[1 + \sum_{r=1}^{m-1} \binom{m}{r} j^r \right] = -1. \tag{A.6}$$

Interchange the order of the two summations and use the definition (A.3) to obtain

$$\sum_{r=1}^{m-2} \binom{m}{r} S_r(p) + m S_{m-1}(p) = 0. \tag{A.7}$$

This gives us a recursion relation in the form

$$S_{m-1}(p) = \frac{-1}{m} \sum_{r=1}^{m-2} \binom{m}{r} S_r(p). \tag{A.8}$$

The recursion relation is valid for $2 < m < p$. The lower bound is obvious from the upper limit on the summation. The upper bound is due to the fact that for $m = p$, the denominator itself vanishes modulo p. Equation (A.8) leads for example to

$$\begin{aligned} S_2(p) &= -\frac{1}{3}\left[\binom{3}{1} S_1(p)\right], \\ S_3(p) &= -\frac{1}{4}\left[\binom{4}{1} S_1(p) + \binom{4}{2} S_2(p)\right], \\ S_4(p) &= -\frac{1}{5}\left[\binom{5}{1} S_1(p) + \binom{5}{2} S_2(p) + \binom{5}{3} S_3(p)\right], \\ &\vdots \end{aligned} \tag{A.9}$$

Direct calculation gives $S_1(p) = 1 + 2 + 3 + \cdots (p-1) = \frac{p(p-1)}{2}$ which is zero mod p, since $p - 1$ is even. The recursion relations above then imply that $S_m(p) = 0$ for all $1 \leq m < p$. The case $m = p$ should be calculated directly, using the Euler theorem which states that for every prime number p, $j^{p-1} = 1 \bmod p$. The result is immediate, namely $S_{p-1}(p) = -1$.

Now using the relation (A.4) it is easy to verify that the vectors $\mathbf{e}_i$ in (A.1) satisfy the desired properties in (A.2).

References

1. M. Hillery *et al.*, *Phys. Rev. A* **59** (1999) 1829.
2. A. Karlsson *et al.*, *Phys. Rev. A* **59** (1999) 162.
3. A. M. Lance *et al.*, *Phys. Rev. Lett.* **92** (2004) 177903.
4. T. Tyc and B. C. Sanders, *Phys. Rev. A* **65** (2002) 042310.
5. A. M. Lance *et al.*, *Phys. Rev. A* **71** (2005) 033814.
6. A. M. Lance *et al.*, *New. J. of Phys.* **5** (2003).
7. Y.-A. Chen *et al.*, *Phys. Rev. Lett.* **95** (2005) 200502.
8. S. Gaertner *et al.*, *Phys. Rev. Lett.* **98** (2007) 020503.
9. S. Bagherinezhad and V. Karimipour, *Phys. Rev. A* **67** (2003) 044302.
10. V. Karimipour, *Phys. Rev. A* **72** (2005) 056301.
11. V. Karimipour, *Phys. Rev. A* **74** (2006) 016302.
12. Zj. Zhang and Zx. Man, *Phys. Rev. A* **72** (2005) 022303.
13. Zj. Zhang, Y. Li and Zx. Man, *Phys. Rev. A* **71** (2005) 044301.
14. H. Briegel *et al.*, *Phys. Rev. Lett.* **81** (1991) 5932.
15. Z. S. Yuan *et al.*, *Nature* **454** (2008) 1098.
16. K. F. Reim *et al.*, *Phys. Rev. Lett.* **107** (2011) 053603.
17. Y. S. Zhang *et al.*, *Phys. Rev. A* **64** (2001) 024302.
18. R. Cleve *et al.*, *Phys. Rev. Lett.* **83** (1999) 648.
19. P. K. Sarvepalli and A. Klappenecker, *Phys. Rev. A* **80** (2009) 022321.

20. D. Markham and B. C. Sanders, *Phys. Rev. A* **78** (2008) 042309.
21. A. Keet *et al.*, *Phys. Rev. A* **82** (2010) 062315.
22. M. Hein *et al.*, in Quantum Computers, Algorithms and Chaos, *Proc. of the International School of Physics Enrico Fermi*, Varenna, Italy, July, 2005.
23. G. Blakely, *Proc. AFIPS* **48** (1979) 313.
24. A. Shamir, *Commun. ACM* **22** (1979) 612.
25. S. Goldwasser, *Proc. CRYPTO 88*, Santa Barbara, CA, 21−25 August, 1990, Lect. Notes Comput. Sci., Vol. 403.
26. D. Gottesman, *Phys. Rev. A* **61** (2000) 042311.
27. D. Aharonov and M. Ben-Or, Fault-tolerant quantum computation with constant error rate in, *Proc. 29th Ann. ACM Symp. on Theory of Computing* (ACM, New York, 1998), pp. 176−188.
28. A. R. Calderbank and P. W. Shor, *Phys. Rev. A* **54** (1996) 1098.
29. A. Steane, *Proc. Roy. Soc. Lond. A* **452** (1996) 2551.
30. M. Grassl and T. Beth, *Proceedings X. Int. Symposium Theoretical Electrical Engineering*, Magdeburg, 1999, pp. 207−212.
31. M. Grassl *et al.*, *Int. J. Found. Comput. Sci.* (*IJFCS*) **14**(5) (2003) 757.